GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at http://www.giac.org/registration/gcfa

FORENSICS PLAN GUIDE

by

Gerald L. King

June 12, 2006

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

FORENSICS PLAN GUIDE
TABLE OF CONTENTS

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

FORENSICS PLAN GUIDE

Foreword

This document does not discuss First Response roles and responsibilities. The document starts from the point where an incident has been verified and the determination has been made that a forensic investigation is needed.

A Forensic Plan is a combination of dynamic checklist and template for recording computer investigation processing steps and information. The dynamic checklist aspect of the Forensic Plan originates from the precept that each investigation is unique. As such, each investigation has numerous contributing factors that have not been discovered nor anticipated during the planning phase of the investigation. Every investigation has components that are always required and present. These components create the basic framework of the checklist. The common phases of a forensic investigation are the identification phase, preservation phase, data collection phase, examination phase and reporting phase. As the investigation proceeds and more information is uncovered pertaining to other possible crimes, the checklist can be expanded to insure that the new information is properly documented and handled.

Since investigations have dynamic qualities, it would be inefficient to restructure current documentation each time new information was discovered. The establishment of a standard or template for recording investigative information facilitates accurate and timely recording of events, actions and information.

This document defines a single concept for illustrating the basic elements of a Forensic Plan from the first initial contact through submission of the final Forensic Report. As the investigation proceeds through the forensic processes, checklist items will be accomplished and the results of those actions will be recorded in the Forensic Plan.

Often critical decisions are made during the initial contact and Preliminary Investigation Discussion (PID). This is where the scope and type of investigation are often decided. If an investigator is unprepared to discuss the requirements for a particular type of investigation, an inaccurate resource estimate will result. This often will lead to an unsuccessful investigation. The investigator must be prepared to discuss with management and properly estimate the resources required to complete the forensic investigation. Decisions made during the Preliminary Investigation Discussion will provide the framework for the forensic investigation. A framework is needed to insure that the agreed upon goals are accomplished.

During the forensic investigation, other information may be discovered that highlights other activities that need to be reported and possibly researched. The investigator must decide what items are essential to this particular investigation and restrict efforts accordingly.

© SANS Institute 2006, Author retains full rights.

1. Incident and Investigation Review.

1.1. Determine the intent and scope of the investigation. Every investigation starts with the initial contact. This is when the investigator is first contacted concerning a possible investigation. Well-organized clients will have a computer Incident Response Plan (IRP) and Team. The investigator should utilize any information provided by an Incident Response (IR) team. Usually, this will be an Incident Point of Contact (POC) list, Incident Assessment and a Incident Investigation Report. These reports may provide a great deal of the information the investigator needs to conduct the investigation. Regardless of any IR information, the investigator must always be prepared to conduct an information gathering discussion to obtain sufficient information to be able to direct a Preliminary Investigation Discussion meeting. This PID will be where the client or management presents any perceived ideas concerning the investigation, discusses their desired goals of the investigation, and identifies the computers to be investigated. This list might expand as additional information is revealed. The investigator must be prepared to provide an initial estimate of the amount of resources (time, equipment, personnel and cost) to complete the investigation. During the PID the type of legal investigation is decided upon (non-liturgical, liturgical or criminal) and type of activity to investigate. Depending upon the estimated cost and type of legal investigation, management may decide to not pursue the investigation. The investigator should be prepared to suggest alternatives.

1.2. Determine legal restrictions. During the initial contact the investigator should inform the client of the need to contact their appropriate legal counsel concerning the event and inform counsel of the desire to conduct a forensic investigation. The investigator should recommend that the client's Human Relations department be contacted and request a representative be present at the PID to discuss employee privacy issues, employee use of company assets, employee conduct at work, and company policies concerning the event or incident as appropriate. The company legal counsel should present any concerns and recommendations during the PID. (See paragraph 7 for further discussion of legal topics.)

1.3. Determine the limits of the investigator's authority. The investigator should insure that the client has a clear understanding of the type of investigation and the activity to be investigated. The investigator should insure that he clearly understands the limits of his authority. The investigator may be authorized to analyze any workstations in one particular area of the client's facility but may require client permission to analyze workstations in another area, servers may need to be analyzed online, and management workstations may only be analyzed in the presence of legal counsel. Any restrictions or constraints imposed by the client must be fully understood, identified and documented during the PID.

© SANS Institute 2006, Author retains full rights.

1.4. Determine what the client wants from the investigation. The investigator must be prepared to discuss with client the possible outcomes from the investigation. Any expectations of the client must be discussed and any misconceptions must be corrected before the start of the investigation. Often clients do not fully understand the information and invasion of employee's privacy that results from a forensic investigation. Clients also have misconceptions of what information can accurately be determined. The investigator must insure that the client's expectations are realistic within the established resource framework and timeframe. The investigator needs to discuss with the client the contents of the final report. Some clients may want a summary report suitable for dissemination to the public and a confidential report for corporate management provided by the investigator.

1.5. Determine resource availability. The investigator should estimate the amount of resources (time, equipment and manpower) that will be required to complete the investigation. Resource limitations are always a consideration in any investigation. The investigator needs to discuss with the client what resources will be required and in what quantity. The discussion needs to address the impact of any resource shortages or limitations. The investigator needs to have a clear understanding of the resources he is allowed to request and in what quantity. The investigator needs to discuss with the client how additional resources are requested and what the acceptable timeframe is for fulfilling the request. The client and investigator need to have a clear understanding of the cost of the investigation and clearly identify any cost restraints or budget ceilings. The investigator must constantly manage his time to accomplish the established goal.

1.6. Determine the escalation procedures. The investigator needs to discuss with the client how to escalate or notify the client of operational problems involving the investigation. Also, how additional or specific resources, equipment or personnel cooperation are to be obtained from the client's representatives.

1.7. Determine liaison and reporting requirements. The investigator should insure that the client provides a liaison for coordination of status reports and other investigative actions. The liaison should be capable of coordinating with the client's legal counsel and law enforcement authorities as required. The investigator should discuss when status reports are to be made, in what format and to whom. Status reports are very beneficial to the client and investigator. However, frequent detailed status reports become very work intensive and unproductive for the investigator. An agreed upon format and frequency is essential. An end of day activity summary should be sufficient for most clients.

1.8. Document known facts and initial incident time-line. A lot of this information may be provided by an IR Team. The creation of the incident POC and contact information list should be one of the first things the investigator requests during the initial contact meeting. This list should be prepared and available at the PID meeting. The client should be instructed to create a summary of known incident

© SANS Institute 2006, Author retains full rights.

facts and information, along with a basic timeline of incident events. The client should provide a list of personnel with knowledge of the event and a description of what information they possess. The investigator should ask if the client has performed a damage assessment and what the results of that assessment revealed. This information should be available at the PID meeting.

1.9. Determine facts of the incident. The PID will be where the majority of the known information of an incident will be presented to the investigator. This information may be presented as results from a formal IR Team or informal IR group tasked by the client to research the incident. The investigator should be prepared to conduct interviews of personnel in attendance at the PID. The information obtained from the interviews will establish the basic reference points of the investigation. The investigator should validate all essential information provided at the PID with other sources. Witnesses interpret situations differently according to their own impressions, values and fears. In other words, witnesses do not always get the whole situation correct; sequence of events may be out of order or timeframes can be compressed or expanded. Regardless of the source of the incident information, the investigator should re-validate important substantive facts that will be part of the final report.

2. Investigative Approach Formulation.

2.1. Review of Preliminary Investigation Discussion information. Upon completion of the PID meeting the investigator should have sufficient information to start planning the investigation. The investigator must review notes and information presented to determine the optimum approach. There may not be enough solid information to accurately determine an initial approach. Personnel interviews may need to be conducted in order to determine if sufficient information exists to proceed. [Wild Goose chases tend to be rather expensive and unsatisfying from the client and investigator's perspective!] The investigator will need to classify the client request and current known information according to the type(s) of activities to investigate. The client request and the type of activities to investigate may not correspond; the client may want an employee investigated for fraud but known information indicates only inappropriate computer use activity. The investigator should classify the investigation according to the Computer Activity and Crime Chart. This will assist in determining possible evidence sources. Identify and document reported dates, times and report events for basic timeline. A review of the initial time-line reference for determining the beginning focal point of the investigation should be conducted.

2.2. Risk assessment. The investigator needs to perform a risk assessment for the investigation. This will analyze the available case information for areas that warrant special concerns, such as evidence corruption or destruction, password protected files or data encryption schemes. The suspect's knowledge and capabilities must be considered. Is the suspect technically capable of hiding or obscuring the evidence? Are there any time constraints or restrictions concerning

© SANS Institute 2006, Author retains full rights.

evidence collection and processing? Basically, the investigator needs to evaluate the location of potential evidence, evidence life expectancy, suspect knowledge, and equipment and processing requirements that can affect the evidence. These conditions or requirement must be considered and minimized by the investigator. This should be documented in the Forensic Plan.

2.3. Procedural investigative questions. There are key procedural aspects to every investigation that needs to be identified and resolved or determined. The investigator needs to insure that witnesses are willing and able to testify. This issue may or may not be important to the case. Sufficient evidence may be obtained without the need to present witness testimony in court. The importance of an eyewitness should never be overlooked. The investigator should re-validate any witness testimony to insure accuracy and quality of the provided information. Witness statements should be documented including specific dates and times – no future or past date references (for example, tomorrow, two days ago, yesterday, last week or Monday afternoon.) The investigator must resolve these references to exact dates as much as possible. A formal request should be made for all external evidence items, such as Internet Service Provider (ISP) records, digital security camera recordings, witness testimony and other external relevant sources. All computers and equipment to be reviewed by the investigator must be formally documented (recommend Evidence Form, Evidence Collection Log and Case Log.) Review the Federal Rules of Evidence procedures for any situations that might create legal problems concerning any potential evidence. (This is especially necessary for inexperienced investigators.) Insure all data items are identified for data collection. Insure that any Search Warrant restrictions or limitations are understood and that only defined evidence is processed.

2.4. Initial investigation specific questions. The investigator needs to analyze the known case information and develop specific tasks to be accomplished. Can computers be seized or must images be collected on-site? Are there any data sources that require off-site processing? The different types of evidence to be collected and processed will need to be determined, such as magnetic tape, multimedia cards, printed documents and photographs to identify a few. Each media type has unique processing requirements. Based upon the investigation and different types of data, the various data need to be collected in different manners. A database would require a different collection mechanism than several photographs. The investigator must answer the above questions before an estimate can be made concerning needed equipment and media to complete data collection. The investigator will need to determine the type of systems that will be involved in the data collection process (Linux, Unix, Windows, servers, desktops, workstations) in order to determine approach, techniques and tools, refer to the Crime Category DOJ (Department of Justice) First Responders Guide, page 37, for data collection approach, techniques and tools. Determine whether forensic disk images will be required or plain file copies will be sufficient. This information must be recorded in the Forensic Plan.

© SANS Institute 2006, Author retains full rights.

2.5. Create checklist for data collection requirements. The investigator needs to create a checklist that identifies all evidence items to process at local and remote storage locations. The location of incident sites should have been determined during the PID and initial case information review.

2.6. Time-line Review. Update the initial time-line and establish a beginning focal point for the investigation. Revalidate all reported dates, times and events from the initial timeline. Insure the Time Line is recorded in the Forensic Plan.

2.7. Technical Skill Review. Review the defined procedures for comparison with current resources and technical skill levels. Insure support personnel are capable of handling the appropriate type of hardware, software and operating systems involved in the data collection effort. Identify any technical skill shortcomings and the alternative solutions in the Forensic Plan.

2.8. Create initial Forensic Plan. The last step in formulating a forensic approach is to create the Forensic Plan. The Forensic Plan Template can be used to record the information obtained through the initial contact and the Preliminary Investigation Discussion. These basics facts will guide the investigator's actions. The template narrative is designed to refresh the memory and form a checklist of actions to be performed. The basic investigation information can be documented on the provided blank numbered pages. The basic format easily allows for the summary format to be recorded and tracked. An area has been designated for actions, task and comments. This will allow the template to assist in tracking key information and actions to be performed throughout the entire investigation. The contents of the template should be reviewed for appropriateness to the current proposed approach. The template is a tool to be used and modified by the investigator for their purpose.

2.8.1. Forensic Plan Template. Each section of the template is presented to assist in each phase of the forensic process. Initially, open the Template and modify the document header and footer fields to record the organizational affiliation. Insure that the middle section is modified to properly identify the case number.

2.8.2. Utilize Forensic Plan Template to build Forensic Plan. Specific answers to questions can be recorded in the answer section of the document. The "Action, Task, Description and Comment" field can be used to record actions, tasks or comments. The section heading "Forensic Plan" is provided to record specific information that is needed or should be recorded in the plan. This will include things such as, client imposed limitations or search warrant restrictions.

The template is not designed to document all the data associated with a forensic investigation. However, if the template is used in conjunction with the provided forms, information and evidence can easily be managed. It is strongly suggested that evidence should be recorded in the Case Log and identified on the Evidence Collection Log. Investigative leads or tasks should be documented

© SANS Institute 2006, Author retains full rights.

on the Forensic Lead and Task Assignment Sheet. When evidence is collected, an Evidence Form or Evidence Tag is completed and the Evidence Form number and item number are recorded in the Forensic Plan Template**Error! Bookmark not defined.Error! Bookmark not defined.**. As leads are worked, their results are recorded on the Evidence Fact Sheet. This form number should be documented on the Forensic Lead and Task Assignment Sheet. All forms and documents should be assigned case numbers and document numbers that are unique to each case. This information must be recorded in the Case Log.

3. Identification and Preservation.

3.1. Incident scene security. An important part of any forensic investigation is identifying the computers to be analyzed. Securing the computer is important to prevent tampering, but the area around the computer is important as well. The investigator should immediately survey the incident scene identifying all ingress and egress points. If possible, the incident areas should be identified with crime scene tape or some means of notifying personnel that a particular area is off-limits to non-authorized personnel. Some investigations may require guards to control access to the incident area and only allow authorized investigators access. Often the computer user will write down userid's and passwords, notes concerning visited web sites or locations of additional information. Actual printed copies of evidence may exist. The incident area must be controlled in order to insure accurate and timely evidence identification and preservation. The type of investigation can mandate very stringent procedures to control and protect incident or crime scenes. As the incident scene is being secured the investigator should be creating a sketch of the incident scene.

3.2. Evidence identification. The initial incident scene survey will reveal evidence locations. The investigator should identify each potential source of evidence with a numbered photo tent. As the investigator places the numbered photo tent, a corresponding entry should be made in the Case Log and incident scene diagram describing the evidence denoted by the photo tent. Multi-colored photo tents are beneficial for this process. If multi-colored photo tents are not available, one inch colored dots can be attached to the photo tent to obtain the same affect. (Note: This becomes very beneficial when dealing with non-crime scene technicians.) Each color of photo tent should indicate evidence processing category: white for single item, blue for a collection of numerous items such as a stack of papers, red for sensitive items, yellow for items that require special processing. This type of categorization assists the data collection team. As photo tents are placed, a photographic record should be made to preserve the incident scene because the incident scene will be altered during the data collection process. After all physical evidence has been identified the investigator should create a rough incident scene diagram in the Case Log and document the general orientation of the area and approximate locations of all the evidence photo tents. Identify all equipment that must be seized for further forensic review

© SANS Institute 2006, Author retains full rights.

or evidence retention. Department of Justice First Responders Guide (page 27) provides general instructions.

3.3. Photograph the incident scene. When processing the incident scene, insure that all equipment, computer screens, peripherals and network cabling is identified and photographed. Insure all loose items, trash cans, paper recycle containers, sticky tabs, papers and notes, desk drawers, cabinets are identified as potential evidence areas. If the computer is connected to a network, officially request a network diagram defining the network layout and architecture, components, security controls, and network equipment locations.

3.4. Search Warrant processing. If the search is in support of a Search Warrant, insure that only equipment specified in the Search Warrant is identified. The use of a network may require the Search Warrant be amended to include other networked computers not originally defined in the Search Warrant. Equipment and computers in this situation will need to be identified and secured until approval can be obtained for their search. Equipment and computers in this category should be identified with a black numbered photo tent.

4. Data Collection.

4.1. Process incident scene and collect physical evidence. The evidence collection phase of an incident investigation may be very complex with many different types of physical evidence requiring collection. Collect all physical and non-technical evidence related to the incident scene (papers, reports, media, etc.) All volatile evidence should be processed as quickly and efficient as possible. Insure that an Evidence Form is completed for each piece of evidence identified for collection and each item is photographed in a manner that reveals the most information. If additional evidence is discovered during the collection phase, this evidence must be processed the same as other evidence (described in Case Log, numbered and photographed). In the event the investigation is being performed by a team of individuals, one member should be assigned the primary duty as Evidence Custodian. Team members should defer evidence collection questions to this person. The Evidence Custodian should be familiar with the DOJ standards for collecting physical evidence. After all physical evidence has been collected (bagged, tagged and stored), evidence that cannot be seized should be processed. This may require detailed digital photographs or digital recordings of the evidence.

4.2. Process incident scene and seize physical computer evidence. Insure unformatted floppy is stored in each floppy drive. This will prevent the system from being accidentally booted in most of the cases. Label and photograph all external cables and power cords. Label and photograph the internal cabling of the system. A better precaution would be to disconnect the power and controller cables from all disks and external devices. If disconnecting the internal cabling is not an option, then place evidence tape over all drive bays. The power cord

© SANS Institute 2006, Author retains full rights.

should be removed and evidence tape placed over the power plug. All evidence tape secured to the equipment must be dated and signed by the investigator processing the equipment. The investigator should officially request the latest sets of backups performed on the computers. All digital evidence collected must be stored in anti-static bags to prevent damage. Do not use plastic evidence bags for digital media due to potential for static electricity and condensation. Paper evidence bags are acceptable in the absence of anti-static bags.

4.3. Process incident scene for digital evidence. In the event computers or other forms of digital evidence cannot be seized, this type of evidence must be imaged on site. When computers are involved, it is best to image a system that is not operational. Imaging an operational system may be all that can be obtained. This should be done as only the very last resort. However, it is not always necessary to image an entire system. Imaging an entire system may be impractical due to size, terabyte or larger online disk storage.

4.4. Collect data from live system. Insure all media used to receive evidence have been properly sanitized and prepared for use. If it is necessary to use client's servers as temporary data collection point, review server security controls and network security. Determine possible risk to collected evidence prior to collection as evidence. [Risk must be documented in Forensic Plan.] Use First Responder's Evidence Disk (FRED) for file information. Collect volatile digital evidence first (memory dump, process listing, network connections, etc.). Use utilities appropriate for the Operating System (OS) being used, Windows Forensic Toolkit or Helix. Use dcfldd for memory dump. Use dcfldd for swap space. Use psinfo on Windows or appropriate OS utility. Use fport or netstat –a. Image all drives on suspect's computer with dcfldd and collect all log information on suspect. RAID devices will require logical drive imaging.

4.5. Collect special content data. The investigator must not overlook special content data, such as e-mail, graphic pictures, or other documents. In the event the investigation's search and seizure is limited to specific a type of information, special care must be taken in order not to violate these restrictions. The investigator must be careful not to overlook alternate or covert storage methods – naming files with incorrect names or file extensions, hiding data content in archives, appending or hiding data inside other files, storing data in file slack space and storing data in unallocated drive space. Numerous techniques can be used to hide or prevent the intentional disclosure of the intended information. When the investigator is restricted with a special content search, the investigator should discuss proposed search methods with legal counsel prior to initiating the search.

4.5.1. E-mail content. Determine the availability of an e-mail server or whether e-mail is provided by an external service. If a local server is providing the e-mail service determine the availability of backups, historical e-mail archives and e-mail transaction logs documenting receipt and transmission of e-mail traffic. Establish

© SANS Institute 2006, Author retains full rights.

the need for this information and arrange for subpoena or Search Warrant for external content and logs. E-mail content can be stored in numerous mail program formats and binary data structures. These formats can vary from ASCII text files to encrypted binary files. The various file types can also be included in any of the various archive file types. E-mail data stores can be located on removable media or any network storage location available to the user. E-mail can be stored on the e-mail server or any combination of the above-mentioned items.

4.5.2. Graphics or photographic images. Determine the need for this type of information. Special handling is required for Child Pornography to protect the victims. Insure appropriate safeguards are implemented. There are roughly 161 different computer graphic programs that can be used to store images. Attachment D contains a spreadsheet that provides general information about computer graphic file types and locations for additional information. This information was extracted from the Frequently Asked Questions (FAQ) on graphics located at the following location: "http://www.faqs.org/faqs/graphics/fileformats-faq/part1/".

4.5.3. Documents. Determine the type of documents and content required. Documents are subject to numerous forms of transmission techniques. Documents are subject to data hiding and transposition ciphers and various other forms of deception methods to prevent document contents from being revealed or disclosed. Document formats are presented in Attachment E.

4.6. Review Forensic Workstation and Procedures. The forensic workstation should be prepared and ready for use. Sanitized and formatted forensic media and hard drive should be available for use in the imaging process. The investigator should have a full understanding of how new devices are handled by their forensic system. Failure to understand how the forensic workstation will handle new devices can cause evidence corruption. For example, Windows operating systems will open, read and update newly discovered NTFS and FAT partitions – this will alter file times on numerous files. Linux kernels using "hotplugs" can discover and mount as read-write an assortment of file systems and partitions. Fedora Core 4 can recognize many USB storage devices and mount those devices as read-write. This would alter the date timestamps on the drive. It is strongly advised to utilize a write blocking technology when imaging any disk drives. This will prevent inadvertent disk drive contamination by the investigator or the forensic workstation.

4.7. Collect data/hard drives from powered-down system. Each investigation has unique circumstances and evidence collection requirements. The recommended approach would be to confiscate the entire computer and return the computer to a controlled environment for processing. The least recommended approach is to image a live system. Data collection efforts are normally somewhere between these two extremes. A thorough understanding of data collection principles and

© SANS Institute 2006, Author retains full rights.

procedures will enable the investigator to confidently handling a vast majority of the cases. The investigator must insure that hardware write blocking technology is installed prior to attaching the evidence hard drive to the workstation. If the investigator is unsure of the proper procedure or data collection technique, the investigator must stop and seek qualified advice before irreparable evidence damage occurs. Insure all drives on suspect's computer are properly documented and processed. The investigator should be familiar with the DOJ NIJ Forensic Examination of Digital Evidence: A Guide for Law Enforcement.

4.8. Review forensic documentation. The investigator should periodically review the Case Log and Evidence Collection Log to insure all the evidence is being collected. All documented evidence in the Case Log should have been recorded on the Evidence Collection Log. The Evidence Collection Log will be provided to the Evidence Custodian to insure all evidence has been processed and properly received into custody. The Evidence Collection Log can also serve as an assignment sheet for team members working the incident scene. The Lead Investigator should assume responsibility for the maintenance of this log until turned over to the Evidence Custodian. After the Evidence Collection Log is turned over to the Evidence Custodian any new evidence discoveries will be recorded on the Forensic Lead and Task Assignment Sheet (FLTAS). When all the evidence recorded on the Evidence Collection Log has been collected and turned over to the Evidence Custodian, any evidence documented on the FLTAS can be transferred to the Evidence Collection Log. This process is repeated until all known evidence has been collected and processed by the Evidence Custodian.

4.9. Review collected evidence for anomalies. The process of reviewing collected evidence will produce both potential leads and new data collection task assignments. It should begin with a review of the Case Log and Evidence Collection Log. Only on TV sitcoms are investigators afforded the luxury of indefinite time frames and completion isolation. Police and other legal authorities are provided a great deal more latitude in this arena. However, corporate investigators are rarely granted such liberties. Incident scenes can be very chaotic. The investigator must insure that all the evidence identified in the Case Log was properly recorded on the Evidence Collection Log. Any discrepancies concerning items of evidence should be noted and resolved, explained or identified as evidence tampering, inadvertent contamination or theft. The best approach is to document any anomalies for presentation in the Forensic Report.

4.10. Review collected evidence for prospective leads. Leads can come from references in documents, notes on sticky pads or desk blotters, printed emails, desk calendars, photographs, book marks, business cards or any other item of physical evidence. Leads should be identified and recorded on the FLTAS; the entry should document the specific lead and the reference and case relationship. Direct references to items not documented on the Evidence Collection Log should be recorded as a task for evidence collection on the FLTAS sheet. This

© SANS Institute 2006, Author retains full rights.

prevents confusion about what evidence is being collected and what evidence still needs to be collected. This does not mean that all the evidence has been identified and collected. Evidence discovery will continue throughout the investigation. This provides a mechanism by which an incident scene can be processed, documented and collected in a timely and efficient manner by several team members. When all the evidence recorded on the Evidence Collection Log has been collected, the investigator can then update the Evidence Collection Log with the new evidence collection requests. All recorded evidence collection requests should be researched, completed, or noted as unsuccessful and why. This must be done prior to releasing the incident scene.

5. Examination.

5.1. Use certified forensic work media and hard drives. It is imperative that all work media and hard drives used in the examination process must be sanitized and certified or verified as clean. This eliminates the possibility of data corruption due to residual information from previous investigations be processed.

5.2. Process forensic image working copy only. Analysis, research or any investigative work must never be performed on the actual digital evidence or forensic image. When forensic images of digital evidence are made, insist that a working copy be created and verified at the same time. Since disk drives come in varying sizes, it may be difficult to find a disk drive to match the original evidence drive. It is recommended that an image file be created on certified hard drives. This approach insures that cryptographic hashes will match the original evidence drive. The image can be mounted under LINUX with /dev/loopback device and be processed as a normal file system.

5.3. Create digital evidence processing file structure on work media. A predefined work structure should be created upon the working case drive. This structure should provide directories for each category of evidence file and process state (raw, processed and final). The following structure is fairly detailed and phase orientated. This structure is not completely compatible with Autopsy. Autopsy categorizes by Case and Host. The majority of Autopsy's files will reside under a directory named after the Host.

```
Case drive root directory->
 /Case_3Mar06_Jones_01
        /images                 image of files of case evidence
        /raw                    Contains raw disk or media files
                /unallocated    unallocated data remnants and files
                /recovered      deleted files recovered
                /slack          data recovered from slack space
                /swap           system swap space data remnants
                /text           Text or ASCII files: logs, txt, bat, script files
```


© SANS Institute 2006, Author retains full rights.

/graphics	Graphic files: files requiring special viewers
/data	Data file: binary files (not exe, com or archives)
/documents	Documents: word (doc, rtf), pdf,
/applications	Application programs: word, excel, PPT, Adobe
/archives	Archive file: zip, arc, tar, z, tgz, cab
/encrypted	Any files that are encrypted
/os	Operating System files: files OS locations
/processed	
/unallocated	unallocated data remnants and files of no value
/recovered	deleted files recovered of no value
/slack	data recovered from slack space
/swap	system swap space data remnants
/text	Text files searched for key words (no hits)
/graphics	Graphic files not “known” or not containing any case related info
/data	data files not containing any case information
/documents	documents files not containing any case info
/applications	application programs “known”
/archives	processed archives not containing case info
/decrypted	decrypted file not containing case info
/os	operating system files “known”
/final	Files with case relevance or importance
/unallocated	unallocated data remnants and files
/recovered	deleted files recovered
/slack	data recovered from slack space
/swap	system swap space data remnants
/text	text files with case information
/graphics	graphic files with case information
/data	data files containing case information
/documents	document files containing case information
/applications	application files with case relevance
/archives	archives files with case relevance
/decrypted	decrypted file with case relevance
/os	OS files with case relevance
/reports	Case Reports
/unknown	Files or content that could not be identified
/unallocated	unallocated data remnants and files
/recovered	deleted files recovered
/slack	data recovered from slack space
/swap	system swap space data remnants
/data	data files with unknown content
/applications	application programs unknown purpose
/encrypted	files that could not be decrypted
/known_files	
/data	known binary file signatures [client based]
/applications	known application file signatures client based

© SANS Institute 2006, Author retains full rights.

/text known text files client based

5.4. Process raw digital evidence. Processing the raw digital evidence is one of the tasks that can be mostly automated. The type of forensic image created (image of a physical drive or image of a logical drive) will dictate additional processing. There is a natural order to the processing of these data components. The following steps are presented to organize the processing to maximize the automated processing capabilities. All of the below data components, except allocated data, should be processed with Foremost and strings. Foremost will potentially identify any files and strings, which may provide any type of clues (email addresses, phone numbers, file names, passwords, URL addresses, IP addresses, etc.) (See Cookbook Search Raw Data for Leads.)

5.4.1. Physical data extraction and logical file separation. A physical hard drive image will have to be manually inspected and analyzed (allocated partitions and unallocated hard disk space). This process may be simple in a single drive, single partition, or a completely allocated disk drive. The process may be complex with multi-volume RAID configurations (Images of RAID arrays should be done at the logical drive or volume level.) The determination to subdivide the image into functional images such as Drive 1 “C Drive”, Drive 1 “D Drive” and Drive 1 unallocated partition space depends upon the investigator’s personal preference, local policies, and forensic tools capabilities. Some forensic tools such as Encase can process the entire image by building internal structures and pointers to the various hard disk structures. This process may also involve the need to processing backup tapes and images files for data and files.

5.4.2. Extract allocated data. All the allocated data from a partition or disk should be extracted for processing. The contents of allocated data will generate all the files that comprise the files on that disk. These files will be analyzed and processed further by other tools.

5.4.3. Extract unallocated data. During normal operation computer files are allocated and deleted. File systems are not usually very efficient at reusing previously deleted space (disk fragmentation). Normally, file systems are never completely utilized. The unused or unallocated file space can contain a wealth of information for the forensic investigator.

5.4.4. Extract swap space (Unix). Swap space is an area allocated on the disk to which the system periodically copies memory contents. Swap space is used frequently when a user uses programs that use more memory than is available on the computer. The system copies some of the programs to swap space in order to free up memory for the program currently needing more memory. Swap space can contain documents, pictures, passwords, and programs that a user previous used on the computer.

© SANS Institute 2006, Author retains full rights.

5.4.5. Windows unique processing.

5.4.5.1. Extract file slack space. Files are allocated in Windows by blocks, 1K or 4K or greater, depending upon the Operating Systems and size of the hard drive. The actual size and contents of almost every file are not an exact multiple of the file systems' block factor. That means that as files are deleted and overwritten, remnants of previous files using the same physical area on the disk may exist. This data can be extracted and analyzed, possibly providing leads or crucial evidence.

5.4.5.2. Extract pagefile.sys. The pagefile.sys is the Windows' swap file. This file can contain previous or current programs being executed and the data those programs are using, this could be complete graphics files or word documents. The data is this file is unstructured as compared to a file system. Anything that a program uses or has used may be contained in the pagefile.sys. This file should be processed with Foremost and strings for potential fragments of information.

5.4.5.3. Extract hiberfil.sys. The hiberfile.sys file is use when a computer is put into hibernation mode. The content of memory and additional process information is written to this file. When the computer is restarted the contents of the file is read back into memory and program executions resume from the point at which they were stopped. As with the pagefile.sys this file can contain almost anything. This file also should be processed with Foremost and strings for potential fragments of information.

5.4.6. Process memory dumps or images. System memory, if saved during collection on a live system, can contain passwords, userids, web site address, document, graphic images and program contents running on the computer at the time the image was taken. This is extremely valuable when working network intrusion and cases involving hacking.

5.5. Refine digital evidence.

5.5.1. Identify and process composite files. Often composite files are used to hide documents, passwords, pictures and other illegal content. A composite file is a file that contains other files, normally considered an archive file. Sometimes these archives are event password protected. All archives files on the system must be un-archived or decompressed so the contents can be inspected. The normal approach would be to create a directory with the name of the archive and un-archive the contents into that directory for inspection.

5.5.2. Identify and process encrypted and password protected files. This is probably one of the hardest and most time-consuming tasks in digital evidence examination, especially when the suspect does not want to cooperate. In cases of this nature, the investigator must rely upon some nontraditional means of

© SANS Institute 2006, Author retains full rights.

gaining access to encrypted files. Some of these methods involve the use of password cracking programs and brute force techniques; seldom are these efforts successful. The investigator must attempt to locate or determine the password or encryption key by other means. The FBI has been known to install hardware "key logging" programs to capture user passwords in order to gain access to password-protected archives. Wiretaps are illegal for non Law Enforcement personnel. Suspects and most computer users often hide or transcribe their passwords or phrases in obscure places. The investigator's job is to discover these locations if possible or build the case without this data.

5.5.3. Identify and process e-mail repository and attachments. Electronic Mail files often contain direct and indirect leads to evidence. E-mail files can contain actual evidence of criminal or inappropriate behavior. The investigator must thoroughly investigate e-mail containers on local and remote computers when possible. Extreme care should be taken when dealing with remote e-mail accounts. These accounts may be personal in nature and fall outside the control of corporate ownership. Although business provided e-mail services are considered business resources and can be searched by corporate investigators, tort issues may arise. If the business has not established policies concerning the use of business e-mail and the business owner rights, legal issues could arise. Corporate investigators should consult corporate legal counsel before accessing remote e-mail accounts. The investigator must be familiar with the many different methods of e-mail use: web-based email (Hotmail, Yahoo Mail, or Google Mail), remote e-mail services (pop3 accounts) and local e-mail mailboxes (Outlook and Outlook Express, Eudora, MS Exchange, Linux/Unix mail).

5.5.4. Data reduction. This is the process in which the amount of data or quantity of files to be analyzed and processed are reduced. This reduction process is usually reiterative. The investigator would first remove or eliminate files that are "known good". Known good files is the term used to refer to files that are provided by the operating system, application software or some other resource and the file's contents have been verified and considered good and the cryptographic signature of the file is computed and stored in a "trusted repository". If the investigator were to compare the cryptographic signature of a file on the suspect system with the same name as a file in the repository and those signatures matched, the investigator could be assured that the file being researched is "known good." There are several available repositories. US DOJ National Drug Intelligence Center (NDIC) HashKeeper repository is used by several commercial forensic software vendors, National Institute of Standards and Technology (NIST) maintains the National Software Reference Library (NSRL) database which contains several large repositories of publicly available software cryptographic signatures. However, the NSRL database is known to contain Hacker Tools signatures also. A big disadvantage in using the NSRL database is that there is no way to distinguish between safe files and bad files, which defeat the purpose of using them in a forensic investigation as currently provided by NSRL. Removing "known good" files from the amount of data the

© SANS Institute 2006, Author retains full rights.

investigator must research can save valuable time. The investigator may choose to remove certain file types, such as windows executables, or chose only to research ASCII text files. The investigator could be restricted by company policy or legal constraints to look at only certain type files or files owned by a particular person. The investigator will probably want to remove duplicate files but careful consideration must be given to what is a duplicate file. Two files can exist on the system with the same name, the same size and contain the same information but different time stamps. Which is the duplicate and why? Are they really duplicates? The only way to verify is to compare their cryptographic signatures. Regardless of the reason, this process must be completely thought out and fully understood before being completed. Evidence could be easily deleted and removed, if the investigator is not careful. (See Cookbook Section Build Known Good File (KGF) Repository.)

5.5.5. Generate file lists and hash values. The process of generating file lists and hash values and gathering other information about the files can be greatly simplified with automated scripts. Computer systems can contain enormous quantities of files. For an investigator to properly analyze a file, the file's characteristics must be determined. What are the contents of the file? Is it an executable program (exe, com, sys, dll, msi, etc.), application data file (jpg, gif, pdf, doc, vbs, etc,), archive file (zip, arc, cab, tar, tgz, etc,)? Are the file contents correct for the file extension? What is the file size? Who is the owner of the file? When was the file created? When was the file last modified? When was the file last accessed? A cryptographic signature or hash value of a file is a quick way to make a comparison of two files. The open source program sorter available in the SleuthKit can perform these functions and more. This generating of file lists (include dates and times) and hash values will allow the investigator to identify potential files for further analysis.

5.6. Process Refined Digital Evidence.

5.6.1. Categorize files. When all the remaining system data has been refined, the data can be categorized based upon file content. By grouping familiar files together those files can be processed quicker as a group. This process is easily automated or performed by most commercial forensic tools. The "Sorter" program provided in the SleuthKit software package performs this task quite well. Additionally, Sorter can be customized to suit the investigator preferences. (See Cookbook Section Sorter Customization and Use).

5.6.2. Construct mismatch file list. This process often leads to key investigative leads. People often attempt to try and hide the true contents of a document by changing the extension of the file. This often will fool an untrained investigator or system administrator. There are utilities that will reveal or display what the true contents of a file are. The most common tool is the Linux/Unix file command. The SleuthKit incorporates the file command with the "Sorter" utility to assist in the categorization of files. The Sorter utility will identify categorized files based

© SANS Institute 2006, Author retains full rights.

upon the file's contents and then identify files that are erroneously assigned the incorrect file extension and document this information in a mismatched audit file.

5.6.3. Collect and document hidden data. This part of the forensic investigation is probably the most technically challenging. Data hiding for an expert has grown to almost an art form. The novice computer hacker may successfully hide their information from the average investigator. The more experienced investigator will most assuredly discover the hidden information. Common techniques involve hiding data in Windows' file slack, unallocated file space, unallocated disk space and use of the Host Protected Area (HPA) of disks. Steganographic tools are beginning to gain popularity. Information can be hidden in normal picture images such as jpeg files, bitmap file or gif files. Steganographic methods are being directed toward MP3 music files as well. The investigator must not overlook the possibility of these techniques being used by innovative computer users. There are numerous methods for hiding data. The investigator must insure his/her forensic software tools box contains tools to identify these efforts.

5.6.4. Create and document investigative leads. All efforts of the investigation to this point have been an endeavor to identify all the pieces and parts of data for the investigators. Obviously, hidden data, decrypted data or password-protected data may provide positive proof, direct evidence or indirect investigative leads. Most cases are built and proved by normal file attributes and email contents. Sure headlines are great, but do not overlook readily available information for investigative leads.

5.6.4.1. Indexing file information and data contents. When dealing with any large number of items the best approach is to organize the data for quick access and rapid data retrieval. This does not necessarily mean this information must be recorded in a database. There are several commercial tools available to assist in this effort. Most of the forensic software vendors incorporate file-indexing technology into their products. If you do not have access to this technology, all is not lost – Microsoft Excel or OpenOffice offers spreadsheet technologies can assist in this area to some degree. The DTSEARCH program is a commercial program that extremely speeds searching for strings and ASCII data, such as data searched in keyword or dirty word searches.

5.6.4.2. Parse all data for text strings (perform keyword/dirty word search). Probably at the center of every investigation is the success of this step. This process reveals the most investigative leads However, all the work done so far has been leading up to this process. This is when the investigator searches the accumulated data for keywords, keyword phrases, text strings, names or other specific information in an effort to identify files that contain the search references. A poorly crafted search will result in thousands or hundreds of thousands of hits or maybe none. The more specific information

© SANS Institute 2006, Author retains full rights.

the investigator has available, the more likely a search will produce valuable investigative leads. (See Cookbook Section Search Raw Data for Leads.)

5.6.4.3. Review file content. A successfully crafted search should produce a sufficient quantity of investigative leads. Each of these leads will possibly have to be researched by the investigator. This may mean viewing hundreds of photographs or parsing hundreds of emails. All this research may provide no direct evidence, only indirect leads such as email comments or references to other activities or time periods of activity. The investigator may have to build his/her case upon file and program access dates and times from one computer and file content on another computer. The investigator must not get funnel vision and look for one specific piece of evidence. File contents are only part of the picture, file ownership, file access date and times, file creation date and times, and file modification date and times must be part of the picture as well. Obtaining all this information is part of the refining process.

6. Analysis.

6.1. Temporal analysis. This is the process of correlating known events with digital objects date and time stamps. The result of this correlation is a timeline reflecting computer activity. Computer object's date and time stamps are constantly being updated by routine Operating System activity. As the timeframe between the computer incident being investigated and the beginning of the forensic investigation grows, the ability to create a comprehensive activity record diminishes. Depending upon the crime or incident being investigated, the detail of the timeline may be of less importance. Another important aspect of temporal analysis is the proper synchronization of different time sources. Electronic components usually require human intervention during the initial setup and configuration. This manual initiation of the starting time is extremely inaccurate at reflecting the exact time. In order to accurately synchronize all pieces of digital evidence, the investigator must determine the difference in time between the digital evidence and the timeframe of the base timeline. This difference is referred to as skewing or time skew. Another consideration often overlooked is the difference in time associated for time zones. When analyzing digital objects, all times must be normalized to central timeframe for reference, all times should be normalized to Greenwich Mean Time (GMT). However, the analyst or investigator should follow current department standards.

6.2. Relational analysis. This is the process of determining how digital objects are connected to the various components of the investigation. The cohesion or strength of the connectivity between objects is determined by the number of connections between the objects. The simple process of associating value to common characteristics should illustrate that objects with high values share more common characteristics. These high value objects represent higher degrees of connectivity between the objects. This should illustrate the relationship between the different objects or evidence. There are several methods for documenting

© SANS Institute 2006, Author retains full rights.

relational analysis; such as a matrix illustrating object class attributes or a more graphical presentation such as a bubble diagram.

6.3. Functional analysis. This process documents how objects function and how illustrating or diagramming those functions reveals similarities and context connections between each object. For example, a phone modem has a particular function; establish a telephone connection to another telephone modem via an analog signal. A phone modem must use a phone line and telephone switch in order to complete the connection. If a suspect accesses a web site, numerous functions are executed; internet connectivity is established, access to a computer, knowledge of computer, knowledge of a computer program to access the web site, knowledge of the web site. In this particular example, there are five distinct functions. No one function can accomplish the task; but all five are needed. This example could be broken down into additional functions such as, connecting to the internet, logging in or on the computer and performing information searches. All of the activities perform a particular function. These functions are related to each other in some form or manner. All functions will affect change upon the system, some at a very minuscule level while others provide a wealth of information. Functional analysis presents the shared or common dependency of functions and objects. The stronger the bond or greater the dependency between objects, the more objects are connected. For example, a phone modem requires a phone line, telephone switch and another distant modem to function. If a phone line does not exist, then there is no relationship between the modem on the computer and the distant modem.

6.4. Evidence analysis. An investigator may use all three of these analysis techniques to prove a position. The investigator must be completely objective in this analysis. Exculpatory evidence must be given equal weight as incriminating evidence. All evidence must be validated and crosschecked. The evidence must be tied to the suspect and not possess any ambiguities. For example, just because a pornographic picture was found on the computer does not necessarily mean the owner of the computer was the person responsible for putting the image on the computer. Maybe the owner of the computer was away on a business trip when the image appeared on his computer. As the investigator, you would have to prove that the owner was able to access the computer and place the image on the computer. Or you would have to present a provable scenario by which the computer image could have gotten on the computer.

6.4.1. Evidence analyses define ownership of evidence. An important part of evidence is establishing the connection between the evidence and the suspect. The investigator should always attempt to prove ownership of the evidence. The following questions should assist in that effort.

- Was the suspect using the computer when the object was accessed, created or modified?
- Was the object located in an area created by the suspect?

© SANS Institute 2006, Author retains full rights.

- Is the suspect the owner of the object?
- Is the suspect solely responsible for the equipment containing the object?
- Is the access to the equipment controlled by the suspect (password-protected or physically secured)?

6.4.2. Evidence analyses define use of evidence. Another important fact is the use of evidence by the suspect. The following questions should assist in that effort.

- Has the suspect accessed, created or modified the object?
- Has the suspect been in direct contact with the object?
- Has the suspect had in-direct contact with the object?

6.4.3. Evidence analyses define access of evidence. Almost as important as use is proving access to the evidence. The following questions should assist in that effort.

- Does the suspect have the knowledge to be able access, create, or modify the object?
- Does the suspect have the capabilities (tools) to be able to access, create, or modify the object?
- Has the suspect actually accessed the object and how?

6.4.4. Evidence analyses define knowledge of evidence. Sometimes when ownership, use or access cannot be proved, the investigator may be able to demonstrate the suspect had knowledge of the evidence. The following questions should assist in determining knowledge of the evidence.

- Does the object possess any internal attributes that directly involve the suspect?
- Is the object protected, obscured or hidden my any means?
- Is the object named similar to other object names the suspect has used?
- Does the object contain words, terms or phases used by the suspect?
- Does the object contain parts of images or things similar to the suspect?
- Was the file password protected by a password known by the suspect?

7. Legal Aspects. The legal aspects of a forensic investigation must be considered at the very beginning of every investigation. For example, the reasonable expectation of privacy has different standards of evaluation between the corporate workplace and the federal workplace. The latitude investigators have in the corporate environment is almost non-existent in the government workplace. In the corporate workplace because the computers and network services are provided by the employer, the owner or manager can authorized the review or inspection of an employee's email account without a lot of difficulty or consequences. However in the government workplace, the rules are different. The government employee has the expectation of privacy and to conduct a search of an employee's mailbox without a Search Warrant can completely void

© SANS Institute 2006, Author retains full rights.

all evidence obtained from the search. In the corporate or business environment the courts allow the owners and managers more leeway in these matters. However, without corporate policy and employee policies addressing these issues, the owner and managers may be liable for civil TORT damages. This especially becomes a factor when the employee is found to be innocent of the suspected illegal on inappropriate conduct.

7.1 Computer Fraud and Abuse Act. There are several criminal laws that involve the use of computers. One of the most frequently referred to of these laws is the Computer Fraud and Abuse Act. This law is commonly referred to as the "Hacker Act". The purpose of this law is to establish the conditions under which a person can be prosecuted for causing damage to computers, computer information or violating a person's privacy. Damages must exceed $5,000 in one year. However, there is a very liberal interpretation as to how the costs of damages are interpreted: cost of the damage and cost to repair the damage. Plus multiple incidents can be combined to meet the $5,000 threshold. The law applies to any "protected" computer; any government computer, any computer involved in interstate or foreign commerce or any computer used by the banking industry. The definition for damage is very liberal also: damage or alteration of medical records, any thing affecting our national defense or security, any thing that causes physical injury to anyone, or causes a threat to the public health and safety. The penalties range from 1 year in prison to 10 years in prison and a fine for the first offense. The punishment is determined by the hacker's "state of mind" or his intentions. In other words, was the damage caused by the hacker's reckless behavior, or did the hacker intentionally cause the damage, or did damage occur inadvertently by his actions?

7.2 Federal Wiretap Act. The Federal Wiretap Act primarily involves communications. Since the vast majority of computers are networked and communications is the main objective behind networking computers, the law becomes involved. The purpose of this law is to protect voice and electronic communications from illegal interception. Simply put network sniffing is illegal unless one of the numerous exceptions applies. There are three key exceptions. The first exception allows for the protection of the owner's property or systems under attack. The next exception is the consent exception, if you have the consent of the user to monitor the communications. This is usually accomplished by the use of banners stating, "Using the computer constitutes your permission to be monitored." In most of the cases where this exception is used, the system owner must prove that the user received the banner notification before monitoring began. The third exception is the computer trespasser exception. This allows the system owner to monitor the attacker while the system is being attacked. Of course, it is legal to monitor in support of a court order or law enforcement. These exceptions do not authorize the system owner or operator to perform unlimited monitoring.

© SANS Institute 2006, Author retains full rights.

7.3 Electronic Communication and Privacy Act. The Electronic Communications and Privacy Act protects the right of the customers or subscribers of Service Provider services. This statute restricts the rights of the Service Provider to provide information concerning a customer's communications, or revealing the content of a customer's communications or information concerning a customer's network activity. Normally, this law is involved with undelivered e-mail and network activity by customers. Again, there are several exceptions to this law. The first exception states that the recipient of the communications can authorize the disclosure of the communications. The second exception states that a court order or Search Warrant can authorize the disclosure of this communications information. The third exception involves the Service Provider inadvertently obtaining the content of communications that involves criminal activity. This information can be provided to Law Enforcement. The fourth exception is the Service Provider's right to protect his property or service. The fifth exception states the Service Provider can provide the contents of communications to government agencies when the Service Provider inadvertently obtained the contents of a communication and the Service Provider believes that an emergency situation exists and a person may be serious injured.

7.4 Traditional crimes. There are numerous other traditional laws that can be applied to computers. One of the most frequently investigated crimes is Child Pornography. Computers are often involved in the acquisition, transfer and distribution of Child Pornography. Other criminal activities are Internet Gambling, Intellectual Property theft, and the Digital Millennium Copyright Act.

7.5 Title 42 Section 2000aa. Another aspect that can affect a forensic investigation is Title 42 Section 2000aa. This statute makes it illegal to prevent the publication of information to the public, such as, newspaper articles, magazines, books or via other media. This can be interpreted as violation of a person's First Amendment Rights. This is not saying that publishing illegal content is authorized. The investigator must insure that when seizing equipment or evidence that the commingling of valid First Amendment content is not prevented by the investigator's actions, see Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993),

8. Finalize Forensic Plan. Each of the previous sections in the Guide was designed to identify restrictions, limitations, locations, possible forms, collection, examination, analysis and management processes that affect and govern the information to be obtained and documented by the Forensic Plan. The proper execution of the Forensic Plan transforms the mass of available digital data into evidence. Note the operative word is proper; a Forensic Plan ill conceived or poorly executed will result in an enormous waste of resources and evidence.

The current trend of "flying by the seat of your pants" is only good for limited mileage. Forensic Plans developed and documented on the back of "Café Expresso" napkins do not provide the professional with any means to evaluate his process and techniques for effectiveness. There is a calculated risk

© SANS Institute 2006, Author retains full rights.

that a professional's work will be criticized by fellow practitioners. The professional can learn and improve by this process. A tremendous misconception exists concerning Forensic Plans. Forensic Plans should be formulated and documented to facilitate change. A Forensic Plan should be a living document that improves as the investigation progresses. This does not mean that the contents of the plan should be discarded at the first indication of difficulty. The plan should document successes and failures. Failures may not be caused by the plan but due to unique properties of the evidence or investigation.

9. Presentation.

9.1. Organize forensic documentation. An investigation has not been concluded until the paperwork is done. Analysis of all the evidence must be collected; all the evidence logs should be reviewed for the disposition of the evidence. Evidence could have been sent out for analysis or data recovery service. Investigator notes, expert witness testimony, witness statements should be audited and reviewed. Digital evidence working files, comments, research and processing steps should be permanently archived. All digital evidence analysis and reports must be prepared for court presentation. All the evidence must be reviewed and audited to insure all evidence is present.

9.2. Develop Forensic Presentation. When the investigator has the analysis of all the digital and physical evidence available, the presentation can be developed. The investigator will have to organize the presentation into a logical sequence of events (actions and results). Each event should be composed of three parts; what action was performed, why that action was performed and what the results of that action were. This progression should lead the reader to the final conclusion or purpose of the report. (See Cookbook for Forensic Report.)

9.3. Create Forensic Report. This document must communicate the results of the investigator's efforts. This communication must be technically accurate and easy to understand. Each step in the logical sequence of events must be reviewed to insure accurate results are being presented. The investigator must not jump to conclusions without proof. If the evidence has ambiguous meanings be sure you state that fact, do not fall to the temptation to overstate your position. Develop diagrams that illustrate complex or difficult concepts. Provide appendixes and references to support technical assertions.

9.4. Perform literary edit. This process involves reviewing the document for language content, grammar, spelling, punctuation, abbreviations and special terms. The document should be reviewed once for each of the categories previously mentioned.

© SANS Institute 2006, Author retains full rights.

9.5. Prepare final Forensic Report. Insure the final Forensic Report is permanently archived with all appendixes and supporting data.

9.6. Perform technical validation of Forensic Report. The process should involve other team members. Each step in the Forensic Report should be reviewed and validated with evidence analysis review. Reviews should be conducted by a person other than the person that performed the initial analysis. This allows for impartial reviews.

10. Archiving the case. When the final Forensic Report has been generated and delivered to the client, the case must be archived. All evidence must be secured and the "Chain of Custody" must be maintained. All reports, notes, working papers and digital evidence must be archived and secured with the original digital evidence. In cases where clients experienced hacker activities or malicious conduct by an employee, the client may choose to take no immediate action. However, if the situation reoccurs, the client may choose to seek legal recourse. For evidence and case to be viable, the "Chain of Custody" must be maintained on all evidence. The client may not wish to accept the burden of this responsibility and rely upon the forensic consultant to provide these services. (See Cookbook for further information on archiving case documents and digital evidence.) Recommend the forensic consultant discuss the disposition of case evidence and case archives as part of their standard contract. The client may be better suited to support this need and have more of a vested interest in maintaining the case archive than the consultant. However, if the latter is not the case, the consultant should insist upon appropriate financial compensation for providing this reoccurring service.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

11. Definitions.

Archive - is storage of data, usually longterm.

ASCII - American Standard Code for Information Interchange is a code representing text in computers and communications equipment.

Autopsy - is software used to perform the examination phase of a computer forensic investigation.

Baseline - is an established set of data the contents of which are known and are used for comparison.

Binary - is the numbering system based upon only two characters.

BMP - bitmap, is an image file format.

Cache – is an area where frequently accessed data can be stored for rapid access.

Case Log - is the document in which is written each stage of the process and analysis of a crime scene.

Chain of Custody - refers to the handling of evidence and its integrity. It usually documents the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence.

Crime Scene and Evidence Documentation Kit - can be the portion of a Jump Kit used to process evidence at a crime scene.

Crime Scene Processing Kit - can be the portion of a Jump Kit used to process evidence at a crime scene.

Cryptographic Signature - pertains to a calculated value (file integrity hashes) of the contents of a file that is used to verify identical files.

Cryptography - is the art of obscuring the content of a message that is not disguised.

Digital Evidence Kit - can be the portion of a Jump Kit used to process digital evidence at a crime scene.

DLT - Digital Linear Tape is a standard for magnetic tape technology.

DoD - Department of Defense.

DOJ - Department of Justice.

© SANS Institute 2006, Author retains full rights.

Evidence Custodian - is the team member responsible for maintaining the documentation and integrity of collected evidence.

Evidence Locker - is a location in memory created by the software Autopsy to be used during a computer forensic investigation.

Evidence Tag - is the document attached to evidence and containing identifiying information for forensic use.

Evidence Transportation Kit - can be the portion of a Jump Kit that is used to prepare evidence from a crime scene for transport and storage.

FAT - File Allocation Table is a file system for the Microsoft Operating System, MS-DOS.

First Responder - is the person is responsible for determining if an incident occurred and gathering the information needed by the Incident Response Team .

Floppy - is a data storage device encased in flexible medium, as in floppy disk.

FLTAS - Forensic Lead and Task Assignment Sheet.

Foremost - is software that searches files

Forensic - pertains to courts of law.

FRED - First Responder's Evidence Disk is software which may be used for the acquisition of computer based evidence.

GIF - Graphics Interchange Format is a bitmap image format to compressing files of pictures/diagrams.

GREP - is software that searches for a match to a string of data and prints the matches.

HashKeeper - is a database maintained by the Department of Justice containing known files used as baselines.

Hash Values - are digital fingerprints of data files that are used in comparisons.

Helix - is software that is used to create copies of data from computer systems.

Hibernation Space - is a portion of memory that holds information so that it is available after a power down and upon restart of the computer system.

IDE - Integrated Drive Electronics is an interface for connecting storage devices.

© SANS Institute 2006, Author retains full rights.

Inode - is a data structure on Unix style file system that provides information about the file.

IR - Incident Response.

ISP - Internet Service Provider

JPEG - is a format for compression of photographic images.

Jump Kit - is the equipment and supplies required to process a crime scene containing computer and digital evidence. It may consist of multiple kits for specific uses, such as Crime Scene Processing Kit, Digital Evidence Kit, Evidence Transportation Kit, and Crime Scene and Evidence Documentation Kit.

Keyword Search - is a function of software to locate a given string of characters.

KBF – Known Bad File – is a file that is known to be bad (malware, virus, trojan, worm) or contain content that is considered illegal.

KGF – Known Good File – is a file that is known to be good (original software installation media).

Lead Investigator - is the person on a forensic team who is responsible for managing the personnel and documentation of a criminal incident scene.

Loopback Device - allows the investigator to restrict the function of certain programs during an investigation.

MACTIME – Modification Access Changed Time represents the three categories of file times: modification time, access time, and creation time.

Malware - is software designed to infiltrate or damage a computer system.

MD5sum - is a computer program which calculates and verifies MD5 hashes to verify the integrity of files.

MFT - Master File Table is a component of the NTFS file system that is standard for managing file transfers.

Mission Brief - is the meeting conducted by the Team Leader before deployment to a crime scene. At this meeting, the basic objectives, duties, and timeline should be discussed. Information from this meeting should be documented in the Case Log.

NDIC - National Drug Intelligence Center is the center for strategic domestic counterdrug intelligence under the U.S. Department of Justice.

© SANS Institute 2006, Author retains full rights.

NIJ – National Institute for Justice.

NIST - National Institute of Standards and Technology promotes measurement science, standards, and technology under the U.S. Department of Commerce. It was previously known as the National Bureau of Standards.

NSRL - National Software Reference Library collects software and maintains a reference library of information, called the Reference Data Set, under the Department of Justice's National Institute of Justice.

NTFS - New Technology File System is the standard file system for Windows NT, Windows 2000, Windows XP, and Windows Server 2003.

Open Source - Software that is freely available for use.

OS – Operating System.

Parse - is the process whereby data is broken down into its constituent parts.

Partition - pertains to memory in a computer being divided into separate portions for function or storage.

Password - is a secret series of characters used to block access to certain data.

PNG - Portable Network Graphics is a compressed bitmap image format.

Quality Assurance Assistant – is the member of a forensic team whose duty is to review the evidence documentation for omissions or errors.

RAID - Redundant Array of Inexpensive Disks or Redundant Array of Independent Disks is a system, which uses multiple hard drives to share data in order to increase capacity, reliability, or speed.

RAR - is a file format for data compression and archiving.

RDS - Reference Data Sets are baseline files from a reference library of information maintained for comparison use.

Sanitize - refers to the method used to wipe all previously meaningful data from a storage device. The US Department of Defense standard for these methods are found in document 5220.22-M.

SANS – Sesame, Audit, Networking and Security Institute provides computer security training and certification.

© SANS Institute 2006, Author retains full rights.

SCSI - Small Computer System Interface is the standard interface and command set for transferring data between devices.

Slack Space - holds data between the end of file and end of file system cluster or sector.

SleuthKit - is software that is used to perform the examination phase of a computer forensic investigation.

SOP - Standard Operating Procedure.

Sorter - is software that categorizes files by their named extension.

Steganography - pertains to the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. An example of this is code hidden within the code of a picture. Steganalysis is the art of discovering and rendering useless such covert messages.

String - is a series of characters that have a special meaning when grouped together.

Swap Space - is a location in memory where data pertaining to a process can be stored until needed for processing in virtual memory.

TIFF - Tagged Image File Format is used for storing images.

URL - Uniform Resource Locator is a web address consisting of a character string in a standardized format, which refers to a resource on the Internet.

USB - Universal Serial Bus is the standard bus designed to connect computer devices.

Userid - User identifier pertains to a series of characters that identify a specific user.

Username - identifies a specific account in a domain.

Verification - is the process whereby a fact is confirmed.

Vulnerability - refers to being open to attack.

WFT - Windows Forensic Tool chest provides automated incident response on a Windows system by collecting security-relevant information from the system.

Windows Domain - consists of a group of computers running Windows Operating Systems that share a central directory database, which contains user accounts and security information.

© SANS Institute 2006, Author retains full rights.

Working Image - is a copy made of evidence for the purpose of testing without damaging evidence.

Write Protect - refers to a device that blocks data from being written to digital or magnetic media.

ZIP - is a file format for data compression and archive.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

Index

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

This is working document skeleton designed to assist in the basic data gathering and preparation aspects of computer forensics cases.	
QUESTIONS | TASKS	**ANSWERS**
1. Incident and Investigation Review.	
1.1. Initial contact.	
Determine the intent and scope of the investigation.	
What typeof incident or event prompted the call from the client?	
Does the client have any specific knowledge of the incident or event?	
Does the client have an Incident Response (IR) Plan?	
Is the IR Plan current?	
How outdated is the IR Plan?	
Is the IR Plan Point of Contact (POC) list valid?	
Does the client have an Incident Response Team?	
Has the IR Team been notified and are they working the incident?	
If so, what results have been discovered?	
Is the Team composed of personnel trained and knowledgeable in handling IR incidents?	
Schedule Preliminary Investigation Discussion meeting.	
Inform client to have technical and management POC at meeting.	
Inform client to have legal counsel present at meeting present.	
Inform client to have Human Resources (HR) manager present at meeting.	
Preliminary Investigation Meeting.	
1.2 Determine legal restrictions.	
Does the company have current employee policies?	
If so, how current?	
Do policies address the problem or incident?	
Will this incident be prosecuted (criminal or civil)?	
Obtain HR manager's opinion or viewpoint.	
Obtain legal counsel's opinion or viewpoint.	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

	ACTION | TASK | DESCRIPTION | COMMENTS	**FORENICS PLAN TASK**
1		
1.1		
1.2		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

1.3. Determine the limits of the investigator's authority.	
What authority does the investigator have?	
Can workstations be collected for off-site processing?	
Can production servers be taken down, as required?	
How much notice Is required?	
What type of access to personnel is allowed?	
1.4. Determine what the client wants from the investigation.	
Does the client want to identify criminal activity and prosecute?	
Does the client want to identify company policy abuses or ethical business problems?	
Does the client want to identify intrusions and determine root cause and document fix?	
What does the client hope to achieve?	
Does the client realize the amount of work and cost versus potential outcome?	
What type of report is the client expecting?	
Investigator must manage client expectations!	
Client may want a summary report for general release and detailed corporate report.	
1.5. Determine resource availability.	
Will client be providing Information Technology (IT) support?	
What are the budget constraints?	
Outside third party performing work - average $100-200 per hour.	
How are additional resources requested?	
How long between presenting resource request and granting request?	
What is the time-frame for the investigation?	
Quicker results will require more personnel.	
Investigator needs to estimate amount of time and effort required to accomplish the contracted investigation.	
1.6. Determine escalation procedures.	
The investigator must have a means to escalate important incidents to management's attention.	
The investigator needs to discuss how to report problems to management.	
1.7. Determine liaison and reporting requirements.	
Who is the investigator's primary POC.	
What type of status reports are required?	
How often are status reports required and by whom?	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

1.3		
1.4		
1.5		
1.6		
1.7		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

1.8. Document known facts and initial incident time-line.	
Document or obtain incident POC and contact information list	
Obtain facts and initial incident time-line from IR Team, if available?	
Create summary of incident or event.	
Document known facts.	
Create investigator's basic incident time-line.	
Create list of personnel with knowledge of the event.	
Document their knowledge.	
Client should perform a damage assessment and document the results.	
1.9. Determine facts of the incident.	
The investigator should be prepared to conduct interviews.	
The information obtained from the interviews will establish the basic reference points of the investigation	
Witnesses interpret situations differently according to their own impressions, values and fears. Witnesses do not always interpret or identify their experiences correctly. Questions should be asked twice at different times and phrased slightly differently each time.	
The investigator should validate and cross check all essential information provided.	
2. Investigative approach formulation.	
2.1. Review of Preliminary Investigation Discussion information.	
Document key facts and information.	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

1.8		
1.9		
2		
2.1		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

2.2. Risk assessment.	
What are the risks to the investigation by the suspect?	
Can evidence be destroyed or damaged by the suspect?	
Are remote storage facilities involved?	
Are remote IT facilities involved?	
Who has knowledge that an investigation is in progress?	
What is the likelihood files will be encrypted or password protected?	
How technically adept is the suspect?	
What is the possibility that the suspect is acting as part of a group?	
What is the possbility the suspect has insider help?	
Does the client have in place any security protocols and audit procedures?	
When was the last audit performed?	
Does the client or suspect have access to the security controls?	
Are there any critical timeframes concerning the incident and the collection of evidence?	
Is there any special hardware needed to collect the evidence?	
Are there any external sources of evidence that require (legal processing)?	
2.3 Procedural investigative questions.	
Initial Investigation Specific questions.	
Can computers be seized or must images be collected on-site?	
If on-site, how long can the servers be off-line?	
Are there any off-site data sources that require processing?	
What type of OS's are involved? Linux, UNIX, Windows	
What are the hardware platforms? Sun, HP, SGI, Intel	
What type of equipment is being used? servers, desktops, workstations	
How many machines must be imaged?	
Are hard drives SCSI, IDE, SCA, SATA?	
Are the hard drives in a RAID Configuration?	
What level of RAID?	
How many hard drives per machine?	
What are the sizes of the hard drives?	
What are the different types of evidence to be collected and processed? magnetic tape, multimedia cards, database files	
Does the investigator have equipment and media capable of processing the incident scene? scsi, mca	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

2.2		
2.3		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

Are laptop computers or portable processing equipment involved?	
2.4. Initial investigation specific questions.	
Will off-site evidence collection be required?	
ISP Logs, Remote Server Logs, ISP mailboxes?	
2703 Letter?	
Search Warrant or Subponea?	
What are the different types of evidence to be collected?	
Documents, manual, papers, photos, printer material.	
Are there any special collection requirements -- after hours, covert operations!	
Network monitoring? Keylogging? Camera -visual recording?	
Have legal requirements been identifed and resolved with LE and legal counsel?	
2.5. Create checklist for data collection requirements.	
Document local storage areas that need to be processed.	
Document alternate employee work areas for processing.	
Document evidence items that must acquired (suspect Laptop).	
Define and document special items that should be checked during identification!	
2.6 Time line review.	
Review Time Line for omissions.	
2.7 Technical skill review.	
Establish list of required skills for evidence processing.	
Review team member qualifications and insure matched assignments.	
Establish alternatives for technical shortcommings.	
2.8 Create initial Forensic Plan.	
Start Forensic Plan Template.	
3. Identification and preservation.	
All Items in this section should be recorded in Case Log	
3.1. Incident scene security.	
Create Incident scene diagram.	
How many locations are involved with the incident?	
Can the incident scene(s) be properly secured?	
How many entrances and exits?	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

2.4		
2.5		
2.6		
2.7		
2.8		
3		
3.1		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

Are there any security access controls (swipe cards, camera, etc, ..)?	
3.2. Evidence identification.	
What constitutes physical evidence in this case?	
Is there a clear understanding of the evidence to be identified?	
Can the evidence be clearly identified?	
What is the evidence identification method?	
Review Search Warrant for compliance to restrictions or conditions.	
3.3. Photograph the incident scene.	
Can the incident scene be photographed?	
Who has the authority to clear evidence photographs? Determine if the photographs contain proprietary, classified, or sensitive information.	
When can photographing the incident scene begin?	
3.4. Search warrant processing.	
Are there any restrictions imposed by the search warrant?	
Is the evidence clearly defined in the search warrant?	
Does the legal description accurately describe the search location?	
4. Data collection.	
All Items in this section should be recorded in Case Log	
4.1. Process incident scene and collect physical evidence.	
How many items have been logged in the Case Log?	
How many items have been logged on the Evidence Collection Log?	
Does the Case Log and Evidence Collection Log agree?	
Has the evidence been clearly identified and do the team members understand their assignments?	
4.2. Process incident scene and seize physical computer evidence.	
How many computers have been identified for collection?	
Has the location been photographed for network cabling?	
Have the computers and cabling been labeled?	
Has the computer work area been photographed?	
Are the computers on?	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

3.2		
3.3		
3.4		
4		
4.1		
4.2		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

Have the computer screens been photographed?	
Has all physical evidence been properly documented and logged?	
4.3. Process incident scene for digital evidence.	
What type of digital evidence is suspected to be present?	
Magnetic Tape Media?	
USB Key drives?	
Other -	
4.4. Collect data from live system.	
Review Forensic Laptop Setup and Imaging and Procedures.	
Are Laptop and peripherals functioning properly?	
Is adequate disk space available?	
Are adequate media supplies available?	
Are there any special requirements?	
Does Forensic Laptop have capacity to support live data?	
Is there a server available to receive live data?	
Who will have access to the live captured data?	
Can the live data be protected until removed for evidence?	
Alternative solution?	
4.5. Collect special content only, e-mail, graphic pictures, documents, etc.	
How will evidence be identified?	
Graphics?	
Documents?	
Other?	
4.5.1 E-mail content.	
Is e-mail private, corporate or government?	
Private/Government need Search Warrant or suspect approval.	
Who approved e-mail search under what authority?	
Corporate requires management approval! Who approved?	
How many e-mail accounts are involved and what types?	
How will evidence be identified?	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

4.3		
4.4		
4.5		
4.5.1		

© SANS Institute 2006, Author retains full rights.

4.5.2. Graphics or photographic images.	
Is evidence image content fully understood?	
How will victim confidentially be protected?	
4.5.3. Documents. .	
Document formats are Appendix E	
4.6. Review Forensic Workstation.	
4.7. Collect data/hard drives from powered-down system.	
4.8. Review case evidence.	
Case Log	
Evidence Collection Log	
Forensic Lead and Task Assignment Sheet.	
4.9. Review collected evidence for anomalies.	
Have anomalies been resolved?	
Has evidence been re-collected without problems?	
4.10. Review collected physical evidence for prospective leads.	
Prospective leads?	
Are there any evidence collection tasks unaccomplished?	
5. Examination. (Crime Category Forensic Report {FR}, page 37).	
All Items in this section should be recorded in Case Log	
5.1. Insure only certified forensic work media and hard drives are used in the examination process. The investigator should only be using a certified forensic working copy of the original evidence.	
5.2. Process forensic image work copy.	
5.3. Create digital evidence processing file structure on work media.	
5.4. Process raw digital evidence.	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

4.5.2		
4.5.3		
4.6		
4.7		
4.8		
4.9		
4.10		
5		
5.1		
5.2		
5.3		
5.4		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

5.4.1 Perform physical data extraction and logical file separation.	
5.4.2 Extract allocated data.	
5.4.3 Extract unallocated space.	
5.4.4 Extract swap space.	
5.4.5 Windows unique processing.	
5.4.5.1. Extract file slack space.	
5.4.5.2. Extract pagefile.sys	
5.4.5.3. Extract hiberfil.sys	
5.4.6. Process memory dumps or images.	
5.5. Refine digital evidence.	
5.5.1. Identify and process composite files.	
5.5.2. Identify and process encryted and password protected files.	
5.5.3. Identify and process e-mail respository and attachments.	
5.5.4 Data reduction.	
File types to ignore?	
Ignore Known Good Files.	
NSRL RDS 2.11	
KGF Hashsets	
Windows ---	
Unix ---	
Identify high potential suspect file (Investigation dependent)	
KBF Hashsets	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

5.4.1		
5.4.2		
5.4.3		
5.4.4		
5.4.5		
5.4.5.1		
5.4.5.2		
5.4.5.3		
5.4.6		
5.5		
5.5.1		
5.5.2		
5.5.3		
5.5.4		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

Rootkits.	
Special	
Pornography (HashKeeper)	
Other	
5.5.5. Generate file lists and hash values.	
5.6. Process refined digital evidence.	
5.6.1. Categorize files.	
5.6.2. Construct mismatch file list.	
Suspect files	
Unknow exec/libs/etc's	
5.6.3. Collect and document hidden data.	
5.6.4. Create and document investigative leads.	
Strings generation!	
Unallocated space	
Swap space	
Windows	
pagefile.sys	
hiberfil.sys	
File carving (Foremost or Scalpel)	
Swap space	
Windows	
pagefile.sys	
hiberfil.sys	
5.6.4.1. Indexing file information and data contents.	
5.6.4.2. Parse all data for text strings.	
Perform Keyword/Dirty word searchs.	
Document potential leads.	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

5.5.5		
5.6		
5.6.1		
5.6.2		
5.6.3		
5.6.4		
5.6.4.1		
5.6.4.2		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

5.6.4.3. Review file content.	
Note items of interest in Case Log.	
6. Analysis.	
6.1. Temporal analysis.	
Generate Digital Evidence Time line.	
Incorporate Witness statements.	
Incorporate External events time stamps.	
6.2. Relational analysis.	
Determine relationships between evidence.	
Develop relationships between information fragments.	
6.3. Functional analysis.	
Determine objects to examine.	
Define objects' characteristics.	
Determine objects' common connections.	
Characteristics.	
Time.	
By-products.	
6.4. Establish evidence revelance.	
6.4.1 Define evidence ownership.	
How/What defines evidence ownership?	
Sole ownership or control?	
Implied or explicit control?	
Define connections/relationships.	
Computer use and evidence MACTIMES?	
Was evidence in user file space?	
Other evidence attributes.	
Data hiding or obscurity.	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

5.6.4.3		
6		
6.1		
6.2		
6.3		
6.4		
6.4.1		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

Security protections -- password controls, facility or location.	
6.4.2 Define access capabilities.	
Suspect knowledge -- create, modify or access.	
Suspect capabilities - create, modify or access.	
Suspect opportunity - create, modify or access.	
Define direct contact.	
Define indirect contact.	
7. Legal aspects.	
7.1 Computer Fraud and Abuse Act.	
7.2. Federal Wiretap Act.	
7.3. Electronic Communications Privacy Act.	
7.4. Traditional crimes.	
7.5 Title 42 Section 2000aa.	
8. Finalize Forensic Plan.	
9. Presentation.	
9.1 Organize forensic documentation.	
Compile examination notes.	
Reconstruct incident, event or crime (Story board).	
9.2 Develop Forensic Presentation.	
Develop best presentation model.	
Define missing data or evidence connectors (if any).	
9.3 Create Forensic Report.	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

6.4.2		
7		
7.1		
7.2		
7.3		
7.4		
7.5		
8		
9		
9.1		
9.2		
9.3		

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

9.4	**Perform technical validation of Forensic Report.**	
	Validate evidence examination and interpetation with team.	
9.5 Perform literary edit and review.		
	Review content for spelling.	
	Review report for style consistency.	
9.6. Prepare final Forensic Report.		
	Generate final report.	
	Review report for all appendixes and attachments.	
	Insure sufficent copies are generated and signed.	
	Provide Forensic Report to customer.	
	Verify customer has Forensic Report.	
10. Case archiving.		
	Insure all documents, research, notes and case papers are archived.	
	Duplicate and verify archive.	
	Update case file with locations of archives and media.	
	Create CD-R/DVD-R of report for distribution as required.	
	Duplicate and verify CD-R/DVD-R.	

© SANS Institute 2006, Author retains full rights.

CASE ddMMMyy_LastName_##

9.4		
9.5		
9.6		
10		

© SANS Institute 2006, Author retains full rights.

FORENSIC COOKBOOK

by

Gerald L. King

June 12, 2006

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

TABLE OF CONTENTS

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

1. Introduction.

The purpose of this cookbook is not to replace the technical references created by the respective authors or expert authorities. This document augments those references by illustrating the use of the select products and procedures, providing additional insight and configuration advice.

The information presented in this document is the result of years of work in the computer security field and the application of current software and techniques. Technical manuals abound with discussions on the various commercial forensic software products. This manual only discusses Open Source software products for several simple reasons, availability, adaptability and cost.

In an effort to insure a minimum of hardware and software conflicts, a very conservative generic hardware platform was used. The main forensic workstation used in this cookbook was a Dual Pentium III A-Bit Vp6 motherboard equipped with two 866mhz Pentium III processors and two gigabyte of PC133 memory. Two additional systems were used to test hardware and software compatibility; 1ghz Pentium III processor on and Intel 815 motherboard with 512meg of PC133 memory and an 800mhz Intel Celeron Processor on an Intel 815 motherboard with 512meg of PC100 memory was also used. Tests were initiated on an SOYO motherboard with 700mhz AMD Thunderbird Athlon processor but this motherboard shorted, killing both it and the processor, thus ending the AMD test.

2. Preparation for Forensics Investigations.

Computer forensic investigations are complex projects requiring a combination of managerial and technical abilities. Investigators are required to perform a broad range of tasks, from running a preliminary investigation meeting to analyzing the contents of a hard drive. Each and every task performed by a forensic investigator is subject to strict review and criticism. An unproductive preliminary investigation meeting can result in a client being provided incorrect or inappropriate advice that causes an unmerited investigation, which does not fulfill the client's request or needs. As with any effort, failure to prepare is preparing to fail. This is not saying that you will be prepared for every possible situation you may encounter, but you can be prepared for most situations. When the unexpected happens, you will be better prepared and more able to complete your investigation and prevent damage to evidence and your investigation.

2.1. Administrative and Personnel Responsibilities.

2.1.1. Professional Training.

Technical professionals competing in the Information Technology workplace must constantly keep abreast of new technologies and improved techniques. Professionals involved in the realm of computer security and computer forensics have several additional requirements. Not only must these professionals fully understand the new technology, they must be able to analyze and develop procedures and techniques to dissect the innermost components of the new technology. Along with new technology comes new software and new security threats, the computer forensic professional must understand these security threats and develop recognition techniques. Computer Forensic Science is being drawn into

© SANS Institute 2006, Author retains full rights.

the world of professional governance. As such, practitioners of computer forensic science will one day require some type of board certification and continual training requirements – similar for most professionals in the legal and medical fields.

2.1.2. Computer Forensic Training.

The SANS GCFA Course should be taken as an initial training requirement with the mandatory Silver certification test. There are other courses and certifications available in the marketplace.

2.1.3. Systems Training.

Systems administration training in at least two of the various supported Operating Systems should be required as well, such as Windows XP and Linux/Unix. There may be the need for additional training requirements for specialized platforms; Solaris, HP-UX, AIX, and MAC-OS. These platforms all have some unique disk and software management applications.

2.1.4. Elementary Criminal Justice Training.

Criminal justice courses will not increase the technical ability to perform an operating system dissection but will expand the understanding of the legal aspects and requirement

2.1.5. Hands-on Technical Practice.

After completing any training, that training should be applied to practical situations. This will reinforce presented techniques, skills and thought processes outside of a classroom or academic environment. Workstations should be available for practicing new approaches and techniques. For personnel working in a team environment, I suggest “train the trainer” concept. Allow one person to attend some type of new training and then have that person develop lesson plans and train other personnel. As part of the training, the group should develop potential SOP’s for using the new technology demonstrated by the training.

2.1.6. Hands-on Incident Scene Practice.

Training on procedures for processing incident scenes and for proper evidence documentation and collection should be part of every computer forensic investigators’ training regimen. Forensic Investigators should never be deployed without first undergoing several training sessions. Each session should be critiqued by appropriate personnel and corrective instruction provided as needed.

2.1.7. Case Management.

There are very few administrative tasks that can cause a computer forensic investigator more headaches that this aspect of computer forensics. These aspects are not taught or even addressed in many training courses. When this task is not done or not done properly, the results of the computer forensic investigator’s efforts may be totally worthless.

Depending upon the computer forensic investigators’ organizational or work structure, this task may be performed by Law Enforcement or a company attorney responsible for complying with a Discovery Subpoena. The computer forensic person (investigator, technician or analyst) must have a thorough understanding of how to handle evidence, document evidence, document work processes and results,

© SANS Institute 2006, Author retains full rights.

and insure the appropriate documentation is complete and accurate. If organizational or departmental policies and procedures exist, then they should be followed. If no procedures exist, develop, document and use your own procedures.

2.1.8. Evidence Custodian

This function should be the responsibility of one person. This person will insure that evidence is properly documented, packaged and secured until delivery to the evidence locker. This person should ideally be assigned this responsibility prior to deployment, as the evidence custodian would be responsible for providing the appropriate evidence processing supplies and equipment. An evidence processing kit with appropriate supplies should be constantly stocked and available for deployment to incident areas. An evidence processing handbook with instructions and procedures should be included as part of the deployment kit.

2.1.9. Lead Investigator.

This function should be the responsibility of one person. This person will have overall responsibility of the incident scene. When working with various Law Enforcement agencies, field agents or detectives assume this responsibility. A forensic investigator may be placed in a situation where he is the sole authority figure – he must insure the investigation is handled properly. This person usually makes team work assignments while on site. This person should be responsible for the Case Log and evidence identification and collection. Duties and responsibilities of this position should be completely defined and documented with all supporting policies and procedures.

2.1.10. Quality Assurance Assistant.

This is probably the most demanding and unappreciated position on the team. This individual must insure that all case documents are completed properly and contain correct references and information. In addition, this person must assist the team with evidence collection and processing. The vast majority of the duties performed by this person will be distributed between the Lead Investigator and Evidence Custodian when there are staffing and budget considerations.

2.1.11. Team Members.

All team member assignments should be documented in the Case Log. Every team member should know the responsibilities of each member of the team. Team member positions, duties and responsibilities should be documented as part of Standard Operating Procedures.

2.2. Software Toolkit Review.

This section will document the software that is part of the computer forensic investigators' toolkit. This software should be installed and tested prior to deployment. Standard Operating Procedures concerning the use of the software toolkit should be provided as part of the toolkit. This toolkit's purpose is to work with image files and the data extracted from those image files. The exception to this rule is Windows Forensic Toolkit (WFT). WFT is really an Incident Response Toolkit item.

2.2.1. Windows (Windows Forensic Toolkit).

© SANS Institute 2006, Author retains full rights.

Do not perform computer forensics upon Windows OS platforms unless write-blocking hardware is installed on evidence disks, or disks containing image files. There are commercially available Windows-based computer forensic software products that operate under Windows OS's. However, these products use their own proprietary format when imaging evidence disks. These proprietary image files are then processed by the forensic software. A popular expensive product is Encase. The vast majority of the free Windows' forensic utilities are for Incident Response.

One freely available tool is the Windows Forensic Toolkit (WFT). This collection of software utilities allows first responders to gather important system information in an orderly and documented procedure. The WFT approach minimizes the footprint of files modified during incident identification and verification process.

2.2.2. Linux Fedora Core 4.

The Linux Fedora Core 4 Operating System is based upon the now commercial software Linux Red Hat. Fedora is the Open Source version of Linux Red Hat. Linux has many inherent capabilities that provide an ideal forensic software platform. One of the most important capabilities is the "loopback device". This allows the system administrator or forensic investigator to mount file system images or hard drives in a controlled and restricted environment. These are the options the forensic investigator should use when using a "loopback device" for maximum protection: Readonly, nosuid, nodev, nosuid, noatime.

Installation of Fedora Core 4 can be achieved by following the Fedora Core 4 Installation Guide at http://fedora.redhat.com/docs/fedora-install-guide-en/fc4/. This guide is fairly comprehensive and very easy to understand. However, consider these recommendations. First, insure that all the hard drives you planned to permanently use with the system are sanitized and connected to the system.

Next, use a system configured with two permanently attached hard drives, the first drive will contain the base operating system software and utilities and will be the "/" or root drive. The second hard drive will be the case file and working drive. This will allow one connection for a combination DVD and CD read-write drive and one extra IDE connector for a removable hard-drive carriage. As for sizes of these hard disks, it is recommended that you use nothing smaller than 40gig for the "/" or root drive and as large as you can get for your case file and working drive. The case file and working drive will contain your working forensic image and all the extracted data files. This needs to be at least 2.5 times a big as the largest image you plan on processing. If you need larger, you can use a 300gig hard drive as your "/" or root drive. However, you would have to partition the drive into three or more partitions, "/boot","/" and then a working area partition. Partition configurations like that are problematic because you have no way of sanitizing the working areas without risking destroying your operating system and application partitions. If you really need the extra storage, then purchase an add-on IDE controller interface card. These cards can provide up to four additional IDE hard drive interfaces. Before purchasing your expanded IDE interface card, do a little online research. Check out the Linux Forums at http://www.fedoraforum.org/forum/index.php? and get the recommendations from people that have actually installed and used these cards. Not all advertising claims are 100% accurate. Cards that might work well with Windows XP or Windows 2000 may not work with Linux kernels 2.4 or 2.6.

© SANS Institute 2006, Author retains full rights.

The next recommendation is going to sound silly and non-professional. The forensic investigator should practice installing and setting up his workstation several times. One of the biggest dangers is for the forensic investigator to be afraid to rebuild his workstation. The forensic workstation can become corrupted or infected with malware. The forensic investigator must have 100% confidence in his tools and techniques.

2.2.2.1. SleuthKit & Autopsy.

These two software packages comprise the majority of the software that is needed to perform the examination phase of an investigation. The forensic investigator must become extremely familiar with the tools and products used during the investigation. These products are not as robust as commercially available products, but the zero dollar price is a great equalizer. When that is coupled with the numerous Linux utilities that are available and the power of various scripting languages, the capabilities for expanding and adapting are endless.

2.2.2.1.1. Building SleuthKit & Autopsy.

SleuthKit and Autopsy programs have some very specific requirements on organization. You can build these applications anyplace on your system that has sufficient hard drive space. Autopsy has some very special output requirements that need to be considered during installation. Autopsy imports “dd created image files” of hard disk drives or disk partitions into a location referred to as the “Evidence Locker”. This location is specified during the installation process. This location will contain the images to be used by Autopsy. All operations performed during the analysis and data examination processes will store data in the Evidence Locker location. This location will need a lot of disk space. It is recommended that you designate a directory in the root directory of the working disk; name this directory something that is meaningful and easy to type, “elocker” or “locker”. Following is a recommended structure for files and data:

/forensics	This is the forensics mount point which will be the root directory for all forensic executables, reference files and source files.
/forensics/bin	This is where all the forensic utilities are stored.
/forensics/src	This location contains all the forensics application source files.
/forensics/KBF	This location contains all “Known Bad Files” depositories.
/forensics/KGF	This location contains all “Known Good Files” depositories.
/forensics/KGF/NSRL	This location contains NSRL file indexes.
/forensics/documentation	This location contains forensic documentation (utilities references and procedures).

/forensics/documentation/references

/forensics/documentation/procedures

© SANS Institute 2006, Author retains full rights.

"/forensics/wrk" is a mount point under the mount point "/forensics". The /forensics file system must be mounted before the /forensics/wrk file system can be mounted.

/forensics/wrk	This is a mount point for forensic working case data (images and files.)
/forensics/wrk/locker	This is Autopsy's Evidence locker

Current sources for the SleuthKit and Autopsy are maintained on Sourceforge. Brian Carrier's Web Site contains history, full descriptions, examples and download links at <http://www.sleuthkit.org/>. You can obtain the sources via http access. After successfully obtaining the above two sources, copy the sources into the /forensics/src directory. These files are stored in tar archives that have been compressed with gzip – denoted by the "gz" file extension. The files must first be decompressed, this is done with the "gzip –d" command.

Command: gzip –d autopsy-2.06.tar.gz This creates the autopsy-2.06.tar archive.

Command: gzip –d sleuthkit-2.03.tar.gz This creates the sleuthkit-2.03.tar archive.

The files must be extracted from the tar archive.

Command: tar –xvf sleuthkit-2.03.tar

Command: tar –xvf autopsy-2.06.tar

Command: ln –s sleuthkit-2.03 sleuthkit This creates a symbolic soft link between the directory sleuthkit-2.03 and sleuthkit. With the sleuthkit symbolic link, we do not have to remember the entire directory name only the symbolic link name (sleuthkit).

Command: cd sleuthkit

Command: make This compiles the SleuthKit programs according to parameter and values created by the program creator.

Command: make install This installs the programs into the appropriate location for executable programs. This location is "/forensics/src/sleuthkit/bin".

Command: cd ../forensics/src

Command: ln –s autopsy-2.06 autopsy

Command: cd autopsy

Command: sh configure This runs a shell script that asks several questions and creates a configuration file for the building of the Autopsy program. Following are the step-by-step instructions:

Question: Where is SleuthKit located?

Answer: "/forensics/src/sleuthkit"

Question: Where is the NSRL database files located?

Answer: "/forensics/KGF/NSRL"

Question: Where is the evidence locker?

Answer: "/forensics/wrk/locker"

Command: make

© SANS Institute 2006, Author retains full rights.

Command: make install

Command: mv autopsy /forensics/bin

Command: cd ../sleuthkit/bin

Command: mv * /forensics/bin

There are two things wrong with this approach. When the SleuthKit executables were built, the program Sorter updated files in the directory src/share/sorter. These files are configuration files that tell Sorter how to categorize files by extensions. In a clean installation this directory should have been moved or created in the /forensics/bin directory. It makes for easier maintenance to leave these files in their original location. The second problem occurs when "make install" built the "file" command. The "file" command configuration files were created in the src/share/file directory. Additionally, the "file" executable was copied to the "/usr/local/bin" directory and the configuration files were copied to the "/usr/local/share/file" directory. The system file "file" resides in /usr/bin with configuration files in /usr/share/file. The new SleuthKit "file" executable resides in both /usr/local/bin with configuration files in /usr/local/share/file and /forensics/src/sleuthkit/file with configuration files in /forensics/src/sleuthkit/share/file. Delete the versions located in the /usr/local/ directory. This way you are executing either a system level version of the "file" command or a forensic level version, determined by the contents of the PATH variable.

2.2.2.1.2. Sorter Adaptation and Use.

The Sorter utility will probably be the most used utility in the SleuthKit Toolkit. Adaptations to "Sorter" will allow the forensic investigator to create definition files that categorizes files in an approach that is comfortable to the investigator's work style. Sorter will read an image file and extract the various file types based upon file contents and file extensions. The files will be placed into a directory based upon their respective categories; images will be placed in an image directory, text files in a directory called text, so forth and so on. The investigator can control this behavior by specifying more detailed categories and associating only specific file extensions to that category. For example, the investigator can create a category call "jpg" and place in that directory only files that have the jpg extension. Because of the way the category matches occur, you are limited somewhat. The "windows.sort" file identifies and categories a majority of the Windows OS files.

The key to customizing Sorter configuration files is to determine the output of the file command. Grep the ~/sleuthkit/share/file/magic for a descriptive value such as "image." This will produce numerous descriptions containing the word "image"; some references will be to file system images. The project impact of modifications to the category descriptions can be estimated and fine-tuned. Any modifications should be fully tested prior to live casework.

The following entries can be used to automatically extract, identify and categorize the following images types: JPEG, GIF, TIFF, PNG, BMP. The original version of the images.sort file identified all these image types and placed all these files in the images category. Since Steganographic capabilities have begun to emerge as a viable data hiding mechanism, each file type may require additional processing to discover hidden data. The decision to force each file type into a separate category

© SANS Institute 2006, Author retains full rights.

seems like a logical decision. The following sample images.sort file will handle the five major graphic image types. There are numerous types recognized by the file command.

```
#Category Images Cut Line
#Save this snippet as images.sort in your sleuthkit/share/sorter directory
# category  cat_name       keywords
# ext       ext1,ext2,ext3 keywords

# Category Images
category    images         image data
category    images         graphic image

category    JPG            JPEG image data
ext         jpg,jpeg,jpe   JPEG image data

category    GIF            GIF image data
ext         gif            GIF image data

category    TIF            TIFF image data
ext         tif            TIFF image data

category    PCX            PCX(.*?)image data
ext         pcx            PCX(.*?)image date

category    PNG            PNG image data
ext         png            PNG image data

category    BMP            bitmap data
ext         bmp            PC bitmap data
#Category Images Cut Line
```

The Sorter process is quite simple and breaks down into essentially three functional tasks. The following order is presented for illustration purposes. First, Sorter reads the configuration files in ~/sleuthkit/src/share/sorter and determines the categories. The default.sort file is read first and then the default file system type configuration file is read. This is based upon the "-f fstype" parameter: bsdi, ext2/3, fat[12/16/32], freebsd, ntfs, openbsd, solaris, swap, and ufs1/2. If a default configuration file exists, that file is read, such as freebsd.sort, linux.sort. openbsd.sort solaris.sort or windows.sort. Duplicate category rules are eliminated; the last read rule has precedence.

Second, the file command (SleuthKit's file command) inspects the file and determines the type of file by using a ruleset defined in sleuthkit/src/share/file/magic.

Third, the category string is matched with the output of file. If the string is matched by the category string, the ext rule is matched. If a match is made and the ext matches, the file is identified by that category and extension. Depending upon the options selected, a log entry or the file is copied to the appropriate directory. If the extension does not match the extension rule, an extension mismatch log entry is made in the category audit file and the extension mismatch log file.

The string rules are regular expressions, which provide a wide range of text parsing possibilities. Mostly the matches will be straightforward literal strings, as in

© SANS Institute 2006, Author retains full rights.

the archives.sort file configuration file. The general rule for the archive category is that any file that contains the word “archive” in the output from the file command is considered an archive file. You may have multiple category rules for a category. The archives.sort configuration rule has 13 category definitions for “archives.” Anytime the output from the file command matches one of those rules, the file is considered as belonging to the archives category and any extension rule matches are performed for that particular category match. The extension mismatches are determined by the extension rule or by turning off extension checking with command line arguments.

#Category Archives Cut Line
#Save this snippet as archives.sort in your sleuthkit/share/sorter directory

```
#category     archives
category      archives    Zip archive data
ext           zip,jar     Zip archive data
ext           wmz         Zip archive data

category      archives    tar archive
ext           tar         tar archive

category      archives    Microsoft Cabinet
ext           cab         Microsoft Cabinet File

category      archives    compress data
ext           gz,tgz      gzip compressed data
ext           Z           compress'd data
ext           bz2         bzip2 compressed data
ext           bz          bzip  compressed data

category      archives    RPM
ext           rpm         RPM

category      archives    cpio archive

category      archives    ARC archive data
ext           arc         ARC archive data

category      archives    LHa archive data
ext           lha         LHa archive data
ext           lzh         LHa archive data

category      archives    shell archive text
ext           shar        shell archive text

category      archives    uuencoded or xxencoded text
ext           uue         uuencoded or xxencoded text
ext           uu          uuencoded or xxencoded text
ext           bhx         uuencoded or xxencoded text
ext           xxe         uuencoded or xxencoded text
ext           xx          uuencoded or xxencoded text
```


© SANS Institute 2006, Author retains full rights.

```
category        archives    BinHex binary text
ext             hqx         BinHex binary text

category        archives    StuffIT Archive
ext             sit         StuffIT Archive

category        archives    RAR Archive data
ext             rar         RAR Archive data

category        archives    ARJ Archive data
ext             arj         ARJ Archive data

# The below types to be implemented when source files are available for testing
#B64,LZW,LBR,MSX,PAK,PIT,TAZ,_Q_,ZOO
#Category Archives Cut Line
```

The previously described concept is best represented by the composite.sort configuration file. Any file type that contains other files is defined as belonging to the composite category. This works great for identifying composite files.

```
#Category Composite Cut Line
category composite archive
category composite compress
category composite cabinet
category composite rpm
category composite filesystem
#need for file to recognize MS Backup files bkf
#Category Composite Cut Line
```

These files can be used with Sorter to extract all archive files or all image files from a disk image file.

Command: sorter –f ntfs –d /forensics/evidence/case_jones_030106/data/sorter –C archives.sort –h –s /forensics/images/jones_hda1.dd

Command: sorter –f ntfs –d /forensics/evidence/case_jones_030106/data/sorter –C images.sort –h –s /forensics//images/jones_hda1.dd

This command only generates an audit report identifying composite files.

Command: sorter –f ntfs –d /forensics/evidence/case_jones_030106/data/sorter –C composite.sort –h /forensics//images/jones_hda1.dd

2.2.2.1.3. Building Known Good File (KGF) Repository.

2.2.2.1.3.1. Creating KGF Repository for Windows XP SP1.

This process does not need to be very complex. Create several versions of your KGF repository, md5 values of the installation media, md5 values of all the files contained in any composite files (MS Cabinet files, Zip files, etc.), and md5 values of all the files after a successful installation. When performing a KGF check, the exact

© SANS Institute 2006, Author retains full rights.

location of the file on the media or system when the md5 value was obtained is not important because md5 values are being compared. However, when attempting to identify suspect files the exact location of files is important. By careful planning and preparation, the KGF repository can be used for several purposes, md5 value comparison for eliminating KGF's and suspect file identification (date, size, location and type.)

Step 1: Mount the vendor media on your forensic workstation onto the /media mount point.

Command: mount –t iso9660 /dev/cdrom /media/cdrom

Output: # (Command prompt will be displayed upon success, otherwise an error message will be output.)

Step 2: Use the find command to identify all the files stored on the vendor's installation media and generate a md5 cryptographic value for each file.

Command: cd /media/cdrom

Output: #

Command: find . –exec /forensics/bin/md5 {} \; > forensics/NSRL/xpsp1base.md5

Step 3: Use the find command to identify all the files stored on the vendor's installation media and generate a comma separated list suitable for importing into a database or spreadsheet. The below command will identify all regular file types and output the file's change date and time, modification date and time, access date and time, size, octal permissions value, and the file path and name with each field separated by a ",".

Command: find . –type f –fprint "%CD %CT,%TD %TT,%AD %AT, %s, %#m, %p\n" /forensics/KGF/NSRL/xpsp1_base.csv

Output: #

.md5 hash value for each file identified by the previous find command.

Step 4: Identify all composite files (various archive file types). Use the appropriate utility to explode or extract the contents of the composite files. When all the contents of the composite file have been exploded, a md5 hash value can be generated for each file contained within the composite file. These md5 hash values can be appended to the file containing the md5 hash values of the installation media. Microsoft installation media contains normal files and archive files called cabinet files. The open source Linux utility cabextract located at the following online address "http://freshmeat.net/redir/cabextract/993/url_rpm/cabextract-1.1-1.i386.rpm" can be used to extract Microsoft Cabinet file contents. The following bash script can be used to locate Microsoft Cabinet files on installation media and create an md5 cryptographic hash value for each file contained inside the Microsoft Cabinet file.

```
#! /bin/bash
# mount the installation media at the appropriate location (cdrom or cdrecorder)
mount –t iso9660 /dev/cdrom /media/cdrom
# make temporary directory to contain expanded cabinet files
# insure you have enough space, 100meg should do
mkdir /tmp/work
# change to temporary working directory
```


© SANS Institute 2006, Author retains full rights.

```
cd /tmp/work
# locate cabinet files on installation media.  Microsoft uses two methods to identify
# cabinet files. One method is to use the “cab” extension to designated cabinet
# files and the second method involves changing the last character of the filename
# extension to an underline “_” to represent a cabinet file.
find /media/cdrom –type f –name “*.cab” –fprint /tmp/files1
find /media/cdrom –type f –name “*_”    –fprint  /tmp/files2
cat /tmp/files1 /tmp/files2 > /tmp/files_to_expand
rm –f /tmp/files1 /tmp/files2
# loop thru /tmp/files_to_expand reading each filename and extracting the files
# into the /tmp/work directory
for i in `cat /tmp/files_to_expand`
do
# Need the basename
filename=`basename $i`
cp $i /tmp/work/$filename
/forensics/bin/cabextract –q /tmp/work/$filename
rm –f /tmp/work/$filename
filename=`ls -1`
/forensics/bin/md5 /tmp/work/$filename
rm –f /tmp/work/$filename
done > /forensics/KGF/NSRL/xpsp1basecabs.md5
rm –f /tmp/work
```

Perform installation of software on a clean system. Once the software is configured and the computer is functioning, an md5 baseline of the system should be generated. If the baseline is created while the resident OS is running, the date and time stamp of every file on the system will be modified. An alternative solution would be to mount the disk on a Linux forensic workstation in read only mode and generate the md5 baseline. This would prevent the modification of any file attributes in the baseline of the system. Another approach would be to use a Forensic Live CD to boot the system and generate the md5 baseline. This procedure is best performed by utilizing a Forensic Live CD Operating system CD, such as Helix 1.6. Several of the Microsoft Cabinet files are quite large and the Helix 1.6 ramdisk is too small to contain the Cabinet File and the extracted contents. In order to overcome this shortcoming, mount a network share and use the network share as a temporary working directory with Samba on Linux or a Windows shared drive.

Step 5: Shutdown the system on which software was just installed and boot the Helix 1.6 GUI with a Helix 1.6 Forensic Live CD.

Step 6: Configure the network card.

Click the Xfce menu icon (first icon on the left side of the task bar).

Move the pointer to the Helix Tools menu item. The Helix Tools menu pops up on the right.

Move the pointer to the Network menu item. The Network menu pops up on the right.

Move the pointer to the “Network card configuration” item and select this option. If you have several network cards, the “netcardconfig Xdialog” will appear and request you select a network card to configure. Otherwise you will receive the

© SANS Institute 2006, Author retains full rights.

“netcardconfig Xdialog” box asking to use “DHCP broadcast”. If you do not have a DHCP server on your network, you will have to configure your network card by providing answers to all the netcardconfig Xdialog questions.

Step 7: Mount a network share for temporary file space. First, open a root shell by clicking on the second icon on the left side of the task bar. Next, mount your network share by using the smbmount command.

Command: smbmount “network share name” “mount point” “username=[username of account with access to network share]” “password=[password for username]”

This is an example for mounting the forensics directory on the server GLK2 as /mnt on the Helix 1.6 system. If you do not provide the username and password the system will present a dialog box requesting this information.

Command: smbmount //GLK2/forensics /mnt username=king password=passwd

The following script will generate an md5 cryptographic hash file containing the md5 values from all the Microsoft cabinet files located in the system baseline. Additionally, an option has been provided to generate a file information file. Edit the script variables to change mount points and temporary working directory names.

```
#! /bin/bash
PATH=$PATH:/usr/local/sleuthkit-1.73/bin:
export PATH
# fileinfo variable used for decision of creating data for fileinfo repository
# fileinfo=0 # No fineinfo information created
 fileinfo=1 # fileinfo information will be created
# set mntptsys to directory where the system will be mounted information gathering
 mntptsys=/mnt1
# set tempdir to location for temporary directory this should be working area on
# a smbmount point.  Probably 300 to 500meg will be required
 tempdir=/mnt/temp
# mount the installation media at the appropriate location (cdrom or cdrecorder)
mount -t ntfs /dev/hda1 $mntptsys -o "ro,noatime"
# make temporary directory to contain expanded cabinet files
# insure you have enough space, 100meg should do
find $mntptsys -type f -exec md5 {} \; >  $tempdir/xpsp1sys.md5

if [ $fileinfo -eq 1  ]
  then
     find $mntptsys -type f -fprintf $tempdir/xpsp1sys.fls "%CD %CT,%TD
%TT,%AD %AT, %s, %#m,%p\n"
fi
mkdir $tempdir/work
# change to temporary working directory
cd $tempdir/work
# locate cabinet files on installation media.  Microsoft uses two methods to identify
# cabinet files. One method is to use the “cab” extension to designate cabinet
# files and the second method involves changing the last character of the filename
# extension to an underline “_” to represent a cabinet file.
find $mntptsys -type f -name "*.cab" -fprint $tempdir/files1
find $mntptsys -type f -name "*_" -fprint  $tempdir/files2
cat $tempdir/files1 $tempdir/files2 > $tempdir/files_to_expand
rm -f $tempdir/files1 $tempdir/files2
# loop thru /tmp/files_to_expand reading each filename and extracting the files
```


© SANS Institute 2006, Author retains full rights.

```
# into the /tmp/work directory
IFS=$'\012'
for i in `cat $tempdir/files_to_expand`
do
# Need the basename
prefilename=`echo $i | sed -e 's/ //g'`
filename=`basename $prefilename`
cp "$i" $tempdir/work/$filename
$tempdir/cabextract -q $tempdir/work/$filename
if [ $fileinfo -eq 1  ]
  then
     find . -type f -fprintf $tempdir/tmp.fls "%CD %CT,%TD %TT,%AD %AT, %s,
%#m,%p\n"
     cat $tempdir/tmp.fls >> $tempdir/xpsp1syscabs.fls
     rm -f $tempdir/tmp.fls
fi
chmod 755 $tempdir/work/$filename
rm -f $tempdir/work/$filename
filename=`ls -1`
md5 $tempdir/work/$filename
chmod 755 $tempdir/work/$filename
rm -f $tempdir/work/$filename
done > $tempdir/xpsp1syscabs.md5
cd $tempdir
rmdir $tempdir/work
umount $mntptsys
```

Step 8: After the script has run, move the md5 and file information files to your KGF repository directory. You may choose to combine them with the other xpsp1 md5 files or keep them separate. There is an advantage to keeping each NGF repository platform and version independent. Identification of specific files and their origin can be accomplished quicker. However, processing with Sorter can become more difficult.

```
cp $tempdir/*.md5 /forensics/KGF
cp $tempdir/*.fls /forensics/KGF
```

Step 9: Autopsy utilizes the SleuthKit utility hfind to quickly locate md5 cryptographic hash values in specially generated index files. The hfind is also used to create the index files from md5 cryptographic hash files.

```
hfind –i md5sum xpsp1syscabs.md5
hfind –i md5sum xpsp1sys.md5
hfind –i md5sum xpsp1basecabs.md5
hfind –i md5sum xpsp1base.md5
```

Step 10: Combine all the xpsp1 md5 files into one file for general use with Autopsy.

```
cat xpsp1sys.md5 xpsp1syscabs.md5 xpsp1base.md5 xpsp1basecabs.md5 >
xpsp1.md5
hfind –i md5sum xpsp1.md5
```

The md5 hash index files can be used outside of Autopsy with the hfind command to locate md5 hash values for files.

© SANS Institute 2006, Author retains full rights.

2.2.2.1.3.2. Creating NSRL Known File Repository.

Download the NSRL RDS (Reference Data Sets) and expand each zip archive file. This will create 4 directories: RDS_A, RDS_B, RDS_C and RDS_D. It is recommended that you remove known "Hacker Tools" from the base file and create an alert file with that file. The "Hacker Tools" currently are only in the RDS_D/NSRLFile.txt. The following bash script will accomplish this task. This will take several hours to process the NSRLFile.txt file to remove associated with the "Hacker Tools" category. Then the hfind index file must be created using "hfind-I nsrl-md5".

```
#! /bin/sh
grep "Hacker Tool" NSRLProd.txt | cut -d, -f1 | sort | uniq > hackerprodids
rm -f newNSRLFile.txt newhackertools.txt
IFS=,
 while
  read a b c d e f g h
 do
   droprcd=0
   while
     read prodcode
     do
       if [ "$f" = "$prodcode" ]
          then
            droprcd=1
             echo "$a,$b,$c,$d,$e,$f,$g,$h" >> newhackertools.txt
       fi
     done < hackerprodids
   if [ $droprcd -eq 0 ]
      then
       echo "$a,$b,$c,$d,$e,$f,$g,$h" >> newNSRLFile.txt
   fi
 done <RDS_D/NSRLFile.txt
```

The above script ran for 5 hours on a dual P3 866 forensic workstation while processing the March 2006 release of the NSRL RDS_D/NSRLFile.txt. Autopsy allows only one NSRLFile.txt file for md5sum values. The NSRLFile.txt file from each of the RDS directories must be combined into one file. This file will be almost 2.7gig. The following command will create the combined NSRLFile.txt.

```
cat  RDS_A/NSRLFile.txt RDS_B/NSRLFile.txt RDS_C/NSRLFile.txt
newNSRLFile.txt > NSRLFile.txt
```

After the single NSRLFile.txt has been created, the hfind index must be created for md5sum lookups. The below commands will create the NSRLFile.txt hfind index file, move the newhackertool.txt to Alerts.txt, create the Alerts.txt hfind index file and move the Alerts file to the Know Bad File Directory.

```
hfind –i nsrl-md5 NSRLFile.txt
```


© SANS Institute 2006, Author retains full rights.

```
mv newhackertools.txt Alerts.txt
hfind –I nsrl-md5 Alerts.txt
mv Alerts.txt ../KBF
mv Alerts.txt-md5.idx ../KBF
```

2.2.3. Foremost .

The Foremost utility will be used upon the file swap space, windows (pagefile.sys, hiberfile.sys, and file slack space), unallocated disk space and any files in which the content cannot be easily determined. The Foremost utility depends upon the Foremost.conf file to obtain the information used to determine what file contents denote a file header or trailer. In some case files do not have specific trailer records and these files need a default value to define the amount of data to capture after locating a file header. Foremost data processing will not, repeat will not, provide exact file contents for several reasons. Files are not normally stored on a disk sequentially. So when Foremost sees a file header, it may read the contents of other files before finding a trailer or filling the default output buffer. Foremost may find many partial file fragments and these fragments may provide important leads or clues to previous computer activity.

2.2.4. Grave-robber.

The Grave-robber utility can only be used on Unix type systems. This utility collects a myriad of host information. This tool can be used on a "live" system, or the disk image of a file system. This utility can review a running process and copy the memory associated with the running process.

2.2.5. Lazarus.

Lazarus provides a view of the unstructured data of a disk and the ability to manipulate the presented data. The file abstraction layer of the file system is ignored because the data being represented are disk blocks and a representation of their content. Lazarus allows the investigator to view a hard disk image as blocks of data on the disk. The usefulness of Lazarus is not readily apparent to a novice or person without a great deal of IT systems experience. Each investigator must decide if Lazarus deserves a place in their personal toolkit.

2.2.6. Helix 1.6.

This software is based upon a Live-CD distribution. This means that the CD contains a configured live operating system that can be booted and operated from the CD. This is great for Incident Response Teams. Helix 1.6 can be used to create forensic images on local and remote systems. For those persons wanting a consistent environment, Helix 1.6 can be installed on a hard drive and used just like other distributions of Linux.

2.3. Jump Kit.

The purpose of the Jump Kit is to insure that the forensic Investigator has all the

© SANS Institute 2006, Author retains full rights.

required equipment and supplies to process a crime scene containing computer and digital evidence. These may include preparing equipment for transportation or performing on site forensic images. In an effort of efficiency the duplicate items have been removed from the corresponding tables.

Depending upon local policy and preparedness procedures, Jump Kits may be divided into separate kits, such as Crime Scene Processing Kit, Digital Evidence Kit, Evidence Transportation Kit, and Crime Scene and Evidence Documentation Kit. These individual kits are usually designed for a single purpose.

2.3.1. Equipment.

The following equipment recommendations are based upon on-hand supplies. All equipment should be covered by a manufacturer's warranty and in serviceable condition. (Ideally, current technology product offerings should be used when available.)

2.3.1.1. Laptop Computer.

ITEM NO	QTY	DESCRIPTION
1	1	Laptop Computer Pentium III 800mhz
2	1	512mb PC 133 Memory
3	1	DVD-CDR
4	1	3.5, 144mb Floppy Drive
5	1	USB Mouse
6	1	PCMCIA Fast Ethernet Card
7	1	PCMCIA Wireless Ethernet 802.g Card
8	1	PCMCIA SCSI-2 Adapter Card
9	1	USB 2.0 Adapter Card
10	1	USB Desktop Scanner

2.3.1.2. Computer Accessories.

ITEM NO	QTY	DESCRIPTION
1	10	DLT Tape Drive
2	10	DLT Cleaning Tapes
3	2	SCSI2 Cable
4	1	Digital Camera with media card
5	2	Digital Camera batteries packs (new or recharged)

© SANS Institute 2006, Author retains full rights.

2.3.1.3. Tools.

These tools are often required in gaining access to computer evidence or preparing evidence for transportation.

ITEM NO	QTY	DESCRIPTION
1	1	Small PC Tool Kit
2	1	Bolt Cutter
3	1	Pry Bar
4	1	Hacksaw with extra blades
5	1	100ft Extension Cord
6	2	Power Strips
7	2	Bubble wrap 1 package
8	2	Strapping Tape 50ft Rolls
9	1	Large Garbage bags 1-box
10	5	Large cardboard boxes
11	1	Toolbox Assorted wrenches, screwdrivers and pliers
12	2	Box Cutter (holder and blades)
13	*2*	Scissors (Large)

2.3.2. Magnetic Media.

This list identifies blank magnetic media for use in digital evidence collection and documentation. All media should be sanitized and certified acceptable for forensic use prior to being labeled. The following items are only representative of a general environment. Local equipment requirements will dictate appropriate media types.

ITEM NO	QTY	DESCRIPTION
1	30	3.5, 144mb Floppy Disks
2	10	DLT IV Tapes
3	50	CD-R 40X
4	50	DVD-R 8X
5	2	Digital Camera Media 64mb

2.3.3. Evidence Processing Supplies.

This is primarily a list of supplies needed for processing the incident scene for

© SANS Institute 2006, Author retains full rights.

evidence identification, collection and transportation. This does not include tools.

ITEM NO	QTY	Description
1	100	Evidence Security Bags, 9-Inch x 12-Inch
2	2	Tamper-Proof Evidence Tape, 2"W x 55 yards
3	2	NIK Tamper-Guard Evidence Tape, 1-3/8"W x 84'L
4	100	Label Chain of Possession Labels, 4" x 5 ¾" adhesive labels
5	100	Evidence Bags Paper, 8-1/8-Inch x 6-Inch x 15 ¾-Inch
6	1	Photo Tents – 3 ½", Numbers 1-15
7	100	Evidence Labels w/o chain of custody, 3 ½" x 6 ¼"
8	2	Barrier Tape "Crime Scene Do Not Enter", Blk on Yellow, 3"x1000'
9	1	Lightly powdered latex gloves box, Large
10	30	Evidence Collection Worksheets, Computer Evidence Worksheets, Forensic Lead and Task Assignment Sheets
11	1	Combo Tag & Chain of Custody Label, Box 100
12	1	Combo Tag Ties, Box 100
13	2	Documentation Supplies, Notepads (1-pkg), Pens (1-box), Pencils (1-box), Pencil Sharper, Permanent Ink Markers Assorted Colors (Red, Blue, Green, Black, Yellow, Orange)
14	2	Assorted Color 1" Dots(Yellow, Blue, Red, White, Black)
15	25	Anti-static bags, 8 ½" x 11"
16	2	Packages of assorted self adhesive labels (50 each)
17	2	Blue painter's tape Roll, 1" 35 yards

2.3.4. Physical Evidence Equipment.

The following list contains items used in processing physical evidence.

ITEM NO	QTY	DESCRIPTION
1	2	Flash Light with batteries
2	1	Magnifying Glass 3"
3	1	Assorted Brushes (1/8" to 2") Nylon
4	30	Velcro Bands (equipment cords, network cable straps)
5	1	Small Hand Dolly 150lb
6	5	Packing blankets/Equipment Covers

© SANS Institute 2006, Author retains full rights.

7	1	Plastic Sheeting, 10'x60'
8	1	Leather work gloves, Large
9	5	Evidence Boxes, 11 ½" x 23" (paper ream box)
10	10	Envelopes, 11" x 13"
11	1	Color Inkjet Printer with extra ink cartridges
12	2	8 ½" X 11" Paper Reams

2.3.5. Digital Evidence Equipment.

The following list of items will be used in processing digital evidence.

ITEM NO	QTY	DESCRIPTION
1	4	250gb IDE Disk Drives
2	1	IDE Write Blocker Adapter
3	1	SCSI Write Blocker Adapter
4	2	USB-> IDE Adapters
5	2	80pin IDE Cable
6	1	IDE 40pin to 44pin Adapter (2.5" laptop drive to 3.5)

2.3.6. Support Documentation.

Reference manuals for all equipment should be kept up to date with the appropriate vendor updates. Technical manuals for the various supported Operating Systems and Forensic Applications should be kept updated and in good condition.

2.4. Forensic Analysis Workstation.

2.4.1. Equipment.

The Forensic Analysis Workstation should be as high-end as possible. This should be equipped with the fastest processors available and the maximum amount of memory. The fastest available workspace drives should be included.

Due to budget limitations the following two equipment configurations have been used and tested in the preparation of this report.

- A-Bit VP6 Motherboard
- Dual Pentium III 866mhz Processors
- 2 Gig PC133 Memory
- 1 80 gig Western Digital Hard drives
- 1 40 gig Maxtor Hard Drive

© SANS Institute 2006, Author retains full rights.

- 1 200 gig Western Digital Hard Drives
- 1 250 gig Seagate Hard Drive (SMB Network Shared drive)
- 1 300 gig Seagate Hard Drive (SMB Network Shared drive)
- 1 DVD-RW 4X Drive
- 1 CDR 40X
- 1 3.5, 144mb Floppy
- 1 Dell 920 Inkjet Printer/Scanner

- Intel 815EEA Motherboard
- Pentium III 1gz Processor
- 512meg PC 133 Memory
- CDRW 40X
- 2-IDE Hard Drive Removable Carriages and Trays
- 1-5 port USB 2.0 Interface Card

2.4.1.1. Identify USB-IDE Adapter.

Step 1. Insure USB-IDE adapter is powered off.

Step 2. Obtain evidence disk drive from Evidence Custodian, if appropriate.

Step 3. Verify Evidence tag and case description to insure you have the proper evidence.

Step 4. Remove disk drive from anti-static bag.

Step 5. Connect disk drive to the USB-IDE write protect adapter via the 40 pin plug.

Step 6. Connect power plug.

Step 7. Turn on the USB-IDE write protect adapter.

Step 8. View /var/log/messages to determine when device is recognized by the system.

Command: tail –f /var/log/messages

Sample Output:

```
Initializing USB Mass Storage driver...
scsi0 : SCSI emulation for USB Mass Storage devices
usbcore: registered new driver usb-storage
USB Mass Storage support registered.
usb-storage: device found at 2
usb-storage: waiting for device to settle before scanning
Vendor: WDC AC26  Model: 400B            Rev: 32.0
  Type:   Direct-Access                    ANSI SCSI revision: 00
  Vendor: BIBIBIBI  Model: BIBIBIBIBIBIBIBI  Rev: BIBI
  Type:   Direct-Access                    ANSI SCSI revision: 00
```


© SANS Institute 2006, Author retains full rights.

usb-storage: device scan complete
SCSI device sda: 12594960 512-byte hdwr sectors (6449 MB)
sda: Write Protect is off
sda: Mode Sense: 00 14 00 00
sda: assuming drive cache: write through
SCSI device sda: 12594960 512-byte hdwr sectors (6449 MB)
sda: Write Protect is off
sda: Mode Sense: 00 14 00 00
sda: assuming drive cache: write through
sda: sda1
sd 0:0:0:0: Attached scsi disk sda
SCSI device sdb: 1701602668 512-byte hdwr sectors (871221 MB)
sdb: Write Protect is off
sdb: Mode Sense: 00 14 00 00
sdb: assuming drive cache: write through
SCSI device sdb: 1701602668 512-byte hdwr sectors (871221 MB)
sdb: Write Protect is off
sdb: Mode Sense: 00 14 00 00
sdb: assuming drive cache: write through
sdb:<6>usb 1-5: reset high speed USB device using ehci_hcd and address 2
usb 1-5: reset high speed USB device using ehci_hcd and address 2
usb 1-5: reset high speed USB device using ehci_hcd and address 2
NTFS driver 2.1.26 [Flags: R/W MODULE].

After the device is recognized by the forensic workstation, the investigator needs to determine how to properly address the disk drive. The above first highlighted block of text illustrates the system recognizing the recently attached disk drive as "USB Mass Storage devices." This system will use SCSI emulation to access the device "scsi0 : SCSI emulation for USB Mass Storage devices." The disk drive was identified as "WDC AC26 Model: 400B." There are three additional pieces of information that are very important. The first is "SCSI device sda: 12594960 512-byte hdwr sectors (6449 MB) "; this identifies the disk drive being connected to SCSI controller "sda." The "sda" address will be used to access the drive. The second piece of information is that the disk drive is not write protected "sda: Write Protect is off." This is why it is important to have a hardware write protection device. The third piece of information is "sda: sda1." This states that the disk drive has one valid partition "sda1." In order to access that partition the address "sda1" will be used.

2.4.1.2. Printers.

The availability and portability of printers and supplies must be considered. Laser

© SANS Institute 2006, Author retains full rights.

printers are usually more bulky and prone to damage. A relatively cheap all-in-one Inkjet printer and scanner should fulfill the majority of needs of the team at remote locations. Insure that software drivers are included as part of Jump Kit.

- 1- USB Color Inkjet printer
- 1- USB Laser printer.
- 1 – Box of Printer Paper
- 1 – Extra Toner Cartridge
- 1 – Extra Inkjet Cartridge

2.4.2. Media.

2.4.2.1. Preparing Work Media.

Preparing digital evidence work media is essential to any forensic investigation. The investigator must insure that only digital evidence from the current investigation is being accessed or referenced. Contamination from previous casework can cause irreparable case damage for client, investigator and legal authorities. All media to include hard drives must be completely overwritten with binary ones, binary zero's and again a fixed known pattern for easy recognition. Department of Defense (DoD) hard disk wiping standards recommends 7 write passes before the drive is considered clean of previous data. The following is a list of randomly picked utilities advertised as compliant with US DoD 5220.22-M standards for drive wiping: Paragon Software Disk Wiper 7.0, Jetico Inc. BCWipe 3.0, Active@ Kill Disk - Hard Drive Eraser, Acronis Drive Cleanser 6.0, ZDelete.NET Disk Wiper, AEVITA Wipe and Delete. The aforementioned list is not comprehensive and should not be considered as such. After the drive has been wiped to the investigator's satisfaction, the drive or media can be formatted or used to receive a forensic image.

2.4.2.2. Sanitizing Removable Media.

All removable media should be sanitized and formatted before use. The media should be sanitized in accordance with DoD 5220.22-M standards. After the media has been sanitized, the media must be formatted for use. Only zero free defects media should be used in forensic processing. The media should have a new label affixed to exterior surface. The new label should reflect the date and signature of the person responsible for certifying the media. If DoD 5220.22-M approved software is not available for the sanitization process, the following procedure can be substituted as an interim solution. This procedure follows DoD guidelines in writing data to all the sectors on the disk 7 times. We are alternating writing 0's and random numbers to every sector on the disk for a total of 7 writes.

Step 1: Use the dd command to nullify the media on the forensic workstation.

Command: dd if=/dev/zero of=/dev/fd0 bs=512

Command Explanation: "dd" Invoke the dd command

"if=/dev/zero" this instructs dd to get input from file /dev/zero. This is a system

© SANS Institute 2006, Author retains full rights.

device driver that will return binary zero's as data for every input read request.

"of=/dev/fd0" this instructs "dd" to direct output to the system device file of /dev/fd0 which is normally configured as the system's "A Drive" 3.5 Floppy Drive.

"bs=512" states that all IO operations will be in data blocks of 512 bytes, which is the sector size on floppy disks.

(The forensic workstation user needs to be familiar with all devices attached to the workstation and their physical IO requirements. Additionally, all device addressing or referencing terminology should be fully documented and explained.)

Step 2: Use the dd- command to write random numbers to the removable media.

Command: dd if=/dev/urandom of=/dev/fd0 bs=512

Command Explanation: "dd" Invoke the dd command

"if=/dev/urandom" this instructs dd to get input from the file /dev/urandom. This is a system device driver that will return a continuous string of random numbers.

"of=/dev/fd0" this instructs "dd" to direct output to the system device file of /dev/fd0 which is normally configured as the system's "A Drive" 3.5 Floppy Drive.

"bs=512" states that all IO operations will be in data blocks of 512 bytes, which is the sector size on floppy disks.

Step 3: Repeat Step 1.

Step 4: Repeat Step 2.

Step 5: Repeat Step 1.

Step 6: Repeat Step 2.

Step 7: Repeat Step 1.

Step 8: Format the media for appropriate use (MSDOS/Windows or Linux/Unix).

MSDOS Command: format C: /FS:NTFS /V:FOR_LAB_1 /X

Linux Command: mk.ext2fs –c /dev/hdd1

Step 9: Fill out the media label and affix label to the exterior of the media.

2.4.2.3. Certification Process of New Hard Drives for Forensic Use.

Although the manufacturing process has improved greatly over the past two decades, hard drives still have manufacturing defects or bad sectors. Hard drives are low level formatted at the factory as part of the manufacturing quality control process. Only hard drives with a very low percentage of bad sectors passed the quality control process. This percentage is less than .01 percent. The low-level formatting process identifies the bad sectors at the hardware level. Hard drives should be certified prior to use. This certification process does not guarantee that the hard drive will remain error free. This process is an audit and control process that assists the forensic investigator. When a forensic image is made on a disk, the investigator has a higher degree of assurance that the image will remain true.

This process will involve sanitizing the hard drive and then creating a pseudo

© SANS Institute 2006, Author retains full rights.

forensic image on the hard drive completely filling all available sectors. The pseudo forensic image will then be used in the creation of a forensic image file on another hard drive of greater size. Cryptographic signatures will be generated on both images and both signatures should match. If the signatures do not match, reattempt to image the hard drive to be certified into another pre-certified hard drive of greater size. Generate the cryptographic signature of the forensic image file created on the new hard drive. This should match the value of cryptographic signature of the hard drive being certified. If these values do not match, the hard drive being certified should be low-level formatted and the imaging process repeated. If the drive does not pass this process, the hard drive should not be used to store forensic images because the integrity of the image cannot be verified. Only use hard drives that pass this process.

2.4.2.4. Procedure for Sanitizing Hard Drives.

All hard drives should be sanitized and formatted before each use on new cases. The hard drive should be sanitized in accordance with DoD 5220.22-M standards prior to being formatted for use. If DoD 5220.22-M approved software is not available for the sanitization process the following procedure can be substituted as an interim solution. This procedure follows DoD guidelines in writing data to all the sectors on the disk 7 times. We are basically alternating the writing of 0's and random numbers to every sector on the disk for a total of 7 writes.

Step 1: Use the dd command to nullify the hard drive on the Forensic Workstation.

Command: dd if=/dev/zero of=/dev/hd[b-d] bs=1024

Command Explanation: "dd" Invoke the dd command

"if=/dev/zero" this instructs dd to get input from file /dev/zero. This is a system device driver that will return binary zero's as data for every input read request.

"of=/dev/hd[b-d]" this instructs "dd" to direct output to the system device file of /dev/hd[b-d]". The operator performing this operation should be familiar with the forensic workstation and know the identity of new disk drives. Normally, the primary IDE hard drive is called "/dev/hda", the second IDE hard drive is called "/dev/hdb", the DVD/CD-R is called "/dev/hdc", and the third IDE drive is called "/dev/hdd". However, systems can be configured differently and the operator should have definitive knowledge of the workstation before attempting this procedure. If you do not know what you are doing – STOP and seek assistance.

"bs=1024" states that all IO operations will be in data blocks of 1024 bytes, which is the standard block size for most Linux and NTFS systems.

(The Forensic Workstation user needs to be familiar with all devices attached to the workstation and their physical IO requirements before attempting this procedure.)

Step 2: Use the dd- command to write random numbers to the removable media.

Command: dd if=/dev/urandom of=/dev/hd[b-d] bs=1024

Command Explanation: "dd" Invoke the dd command

"if=/dev/urandom" this instructs dd to get input from the file /dev/urandom. This is a system device driver that will return a continuous string of random numbers.

© SANS Institute 2006, Author retains full rights.

"of=/dev/hd[b-d]" this instructs "dd" to direct output to the system device file of /dev/hd[b-d] which should be your new hard drive.

"bs=512" states that all IO operations will be in data blocks of 512 bytes, which is the sector size on floppy disks.

Step 3: Repeat Step 1.

Step 4: Repeat Step 2.

Step 5: Repeat Step 1.

Step 6: Repeat Step 2.

Step 7: Repeat Step 1.

Step 8: Format the media for appropriate use (MSDOS/Windows or Linux/Unix).

MSDOS Command: format C: /FS:NTFS /V:FOR_LAB_1 /X

Linux Command: mk.ext2fs –c /dev/hdd1

Step 9: Fill out the Hard Drive Equipment Tag and affix label to the exterior of the hard drive.

2.4.2.5. CD-R, DVD-R Media.

CD-R and DVD-R media are considered write once media. There is no reuse capability for this type of media. This media does not require certification or sanitizing. Media of this type must be physically destroyed by being shredded with a CD-R shredder, or sanded with 100 grit sandpaper until only the clear plastic surface is present. This media can be incinerated as an appropriate means of destruction.

2.4.2.6. Magnetic Tape Media.

Magnetic tape certification processes require specialized equipment that is fairly expensive and time consuming to maintain and operate. Magnetic tape media is considered expendable by many organizations. This means that when a tape has exceeded its life, normally determined by the number of times it has been read and written, or a subjective decision by the operator on the number of tape read/write errors, the tape is replaced. Magnetic tape media has a very long storage life when stored in accordance with manufacturers' recommendations. Certifying magnetic tape for forensic image use is purely a subjective decision by the forensic facility. Magnetic tapes are not like hard-drives with an exactly known quantity of areas to hold information. There are rather complex mathematic calculations required to compute the exact size or amount of information that can be recorded on magnetic tapes. For example, information is written to tape based upon tape recording density per inch and data block size. Blocks are considered records; each record has a data component and block checksum value. Between each record is a dead space called an inter-record gap; then there are file headers and trailers and volume headers and trailers. The newer tape drives even provide data compression and data encryption. Long story short answer, it can be performed with surety by normal forensic technicians in a timely manner but with the following recommendation. If any tape errors are reported during the process, recreate the image on another tape until zero

© SANS Institute 2006, Author retains full rights.

errors are reported. Tapes that report errors during any imaging should be discarded. If you experience numerous errors on completely different tapes, call for hardware support on your tape drive. For the die-hard purists, here is a procedure developed for DLT 4000 Tape Drives.

Step 1: Roughly calculate the number of 1K blocks that can be written to your tape. For example: If you are using 20gig tapes, 20 * 1000 equals 20,000 1k blocks; add 5000 to that number yielding 25,000. Use the dd command and use the /dev/zero or /dev/urandom as your input device. Select your tape drive device name, usually /dev/st0.

Command: dd if=/dev/zero of=/dev/st0 bs=1024 count=250000

This will instruct dd to write 25,000 zero filled 1024 byte blocks of data to your tape drive. The tape drive should report a write error when the tape has been filled and dd will exit reporting the number of blocks read and written. The written number is the max blocks that can be written to your tape.

Step 2: Create forensic image on your hard drive.

Command: dd if=/dev/urandom of=tape_image bs=1024 count=(number from step 2).

Step 3: Create cryptographic signature of tape_image

Command: md5sum tape_image

Step 4: Write tape_image file to magnetic tape.

Command: dd if=tape_image of=/dev/st0 bs=1024

Step 5: Read forensic_image from tape creating cryptographic signature

Command: dd if=/dev/st0 | md5sum

Step 6: Compare the two cryptographic signatures, they should equal.

2.5. Deployment Procedures.

These procedures should be incorporated into a standard SOP to insure consistent team preparedness and deployment. The Deployment Checklist should be reviewed by the Team Leader before personnel deploy.

2.5.1. Deployment Checklist Verification.

ITEM NO	STATUS	Description
1		Jump Kit Inventory Laptop Computer
2		Jump Kit Inventory Computer Accessories
3		Jump Kit Inventory Tools
4		Jump Kit Inventory Digital Media
5		Jump Kit Inventory Evidence Processing Supplies

© SANS Institute 2006, Author retains full rights.

6		Jump Kit Inventory Physical Evidence Tools
7		Jump Kit Inventory Digital Evidence Equipment
8		Jump Kit Inventory Documentation
9		Personnel Duty Assignments
10		Directions to remote sites locations
11		Mission Description.

2.5.2. Mission Brief and Personnel Assignments.

Prior to departing to the remote site, a Mission Brief should be conducted by the Team Leader. The Mission Brief will discuss the basic objectives of the deployment and estimated time-line. The Team Leader will appoint the Lead Investigator and Evidence Custodian. Other personnel assignments may be implemented at this time or left to the Lead Investigator to make once on-site.

Personnel assignments and duties should be discussed prior to deployment. Each team member should have an absolute understanding of his responsibilities. Organizations responsible for numerous teams should have personnel staffing guides. Small organizations should have team assignment descriptions with required skills and duties.

The Mission objective and team personnel assignments should be recorded in the Case Log.

2.5.3. Evidence Collection Review.

Each type of evidence collection procedure should be documented and practiced on laboratory equipment. The evidence collection review will discuss the possible types of evidence to be discovered at the on-site location and possible techniques for collecting that evidence. Potential risks to the evidence and possible mitigation procedures should be discussed.

2.5.4. Dry-run Procedural Walk-thru.

Each team member should present and discuss in brief detail their proposed duty assignment and how they will proceed once on site. The Team Leader should critique the Walk-thru, correcting any omissions, errors, or team assignment changes.

3. First Responder Overview.

The main goal of the First Responder is to determine if a security incident occurred. If an incident did occur, the responder must collect as much information as possible in a forensically sound manner. The First Responder will notify the Incident Response Team and provide collected information to the Incident Response team in order for them to prepare a Response Strategy. The Response Strategy must consider the organization's business objective, legal obligations, any public disclosure requirements and even political concerns while addressing the cause of the incident. A possible solution to the incident or event should be provided by the Incident Response report, which is provided to senior management.

© SANS Institute 2006, Author retains full rights.

First Responders should be trained in forensic methods and tools for capturing critical evidence. Forensic examination and data collection techniques must be documented and practiced by personnel assigned First Responder duties.

4. Evidence Collection.

The purpose of this section is not to instruct on how to process, document or photograph an incident scene. *This type of instruction is taught by certified Crime Scene Investigators. Incident scene photography presented in this section is used for auditing purposes and critiques.* Once the incident scene has been identified and secured, the Lead Investigator can begin the initial survey for evidence. An incident scene sketch will be made in the Case Log, with egress and ingress points clearly identified. A photo should capture the overall orientation (North, South, primary ingress) of the incident scene. The initial survey will identify sources of evidence to be processed or excluded from evidence collection. Each source of evidence will be marked with a number photo tent for a photographic record. The number marker will be recorded in the Case Log accompanied by a brief narrative description. Several photos should be taken to identify all evidence markers. Photograph records should be made of all potential evidence sources in sufficient detail to identify the source of evidence.

When support is being provided to Law Enforcement, the forensic investigator should not touch any computer equipment or accessories until cleared by the Lead Investigator (use of a key board or mouse may destroy fingerprints). Insure you have the Lead Law Enforcement's permission before proceeding. It is better to be safe than sorry.

4.1. Physical.

When processing an incident scene for physical evidence, the forensic investigator is looking for clues, leads, passwords, file locations, and data identification attributes that will assist in processing the digital evidence. All identified or contributory evidence must be properly processed to be of value. The written password may be the only connector between the suspect and the digital evidence. All identified evidence must be recorded in the Case Log or FLTAS (Forensic Lead and Task Assignment Sheet) for evidence collection.

4.1.1. Documents.

When processing documents, such as binders, pamphlets and books, check for pieces of paper between the pages. (Note the page numbers where the paper was found.) Additionally, pay particular attention to any highlighted text and notes written in the margins or on the pages (note the page numbers). If passwords or non-sensible phrases are found, these could be encoded passwords. Check other books or similar documents for the identical page numbers. A technique for hiding information is to hide the information in the same place in other references. As with any evidence, insure any discovered information is recorded in the Case Log or on the FLTAS.

4.1.2. Photographs.

Digital photography of an incident scene serves two purposes. The first purpose is to provide a detailed record of the location of all evidence sources. Sometimes

© SANS Institute 2006, Author retains full rights.

during evidence collection and data collection efforts, items are accidentally or otherwise relocated. The second purpose is to provide an audit trail of all the identified evidence that should be collected and processed.

Photographs of evidence should show sufficient detail to identify the evidence. Use visual pointers to highlight the important information. (Use a pen to point to a password recorded on a piece of paper, for example). Photographs should not be considered suitable substitutes for the actual evidence.

All computer equipment should be photographed in detail. All cables should be identified, clearly labeled and visible in photographs. When equipment is being imaged on-site, each phase of the process should be photographed; this is to insure that the equipment can be returned to an operational state after imaging.

4.2. Digital Evidence.

This section identifies several tools and illustrates their use in performing imaging of digital evidence and their associated processes.

4.2.1. Identify Partition Information – mmls Tool.

The disk drive is connected to the system and recognized by the operating system. Identify the contents of the disk. First determine the contents of the disk drives' partition table with the command mmls. This is a utility provided in "The Coroners Toolkit". The fdisk command could also be used.

Command: mmls /dev/sda

Command Output.

```
[root@unix-for forensics]# mmls /dev/sda
DOS Partition Table
Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0012578894   0012578832   NTFS (0x07)
```

This identifies three partition table entries. The first is defined as the "Primary Table" and contains 1 sector of information – this should be the system's boot record. The second entry is for unallocated space of 62 sectors. This should be noted in the Case Log for investigation of hidden information. The third partition entry is a NTFS file system that is 12,578,832 sectors in length. The disk drive contains 12,594,960 sectors because the disk drive reported this information when discovered by the system, "SCSI device sda: 12594960 512-byte hdwr sectors (6449 MB)." This means 16,066 sectors are not allocated. This fact should be noted in the Case Log for later investigation.

4.2.2. Create Forensic Image Using the dd Command.

© SANS Institute 2006, Author retains full rights.

Create forensic images of disk drive. There are numerous forensic imaging techniques available. All the commercial products provide their own proprietary imaging mechanism, ENCASE, PRODISCOVER, X-WAYS, The Forensic Toolkit and numerous others. The following instructions pertain to the Open Source and free Linux utilities, Open Source utility "dcfldd" and Linux command "dd." For brevity and demonstration purposes, simple names have been used, such as "winxp_sda." During real casework, proper case media content descriptor names should be used at all times.

Step 1: Create forensic image "winxp_sda of disk drive /dev/sda with Linux "dd."

Command: dd if=/dev/sda of=winxp_sda bs=1024

Command explanation: "dd" command invocation sequence

"if=/dev/sda" designates the use of an input file of "/dev/sda"

"of=winxp_sda" designates the use of an output file "winxp_sda"

"bs=1024" designates blocksize of 1024 bytes. This is the standard block size of NTFS partitions.

We are going to copy data from /dev/sda (raw or physical device) to the file "winxp_sda" in blocks of 1024 bytes. The file will be located in the current directory.

Command: dd if=/dev/sda of=winxp_sda bs=1024

Command Output:

root@unix-for images]# dd if=/dev/sda of=winxp_sda bs=1024

6297480+0 records in

6297480+0 records out

This command read 6,297,480 1024 bytes records from the input device and wrote 6,297,480 1024 bytes records to the output file. This means the file "winxp_sda" contains 12,594,960 512 byte records. This confirms information reported previously about the number of sectors on the disk drive. This should be noted in the Case Log as this verifies the size of the disk drive.

Step 2: Create cryptographic signature of disk drive and image file "winxp_sda" as verification that the forensic image is exactly identical to the physical evidence.

Command: md5sum /dev/sda

Command Output:

[root@unix-for images]# md5sum /dev/sda

3b00b3342288f72b91a73427b190268b /dev/sda

Command: md5sum winxp_sda

Command Output:

[root@unix-for images]# md5sum winxp_sda

3b00b3342288f72b91a73427b190268b winxp_sda

© SANS Institute 2006, Author retains full rights.

4.2.3. Create Working Forensic Images of Forensic Image.

This process accomplishes two important tasks for the investigator. First, this will provide the investigator with a working copy of the evidence to use in the investigatory process and additional verification that the forensic image is a duplicate of the evidence.

Step 1: Create working copy of the forensic image with the dd command.

Command: dd if=winxp_sda of=wrk_winxp_sda bs=1024

Command Output:

```
[root@unix-for images]# dd if=winxp_sda of=wrk_winxp_sda bs=1024
6297480+0 records in
6297480+0 records out
```

Step 2: Verify the cryptographic signature of the forensic image working copy. This signature must match exactly the signatures created in paragraph 4.2.2, step 2.

Command: md5sum wrk_winxp_sda

Command Output:

```
[root@unix-for images]# md5sum wrk_winxp_sda
3b00b3342288f72b91a73427b190268b  wrk_winxp_sda

Cryptographic signatures from paragraph 3.2.2 step 2.
3b00b3342288f72b91a73427b190268b  winxp_sda
3b00b3342288f72b91a73427b190268b  /dev/sda
```

The cryptographic signatures of all three files match. The winxp_sda and wrk_winxp_sda files are exact duplicates of the evidence disk. The wrk_winxp_sda can be used by the investigator during the examination and analysis phase of the investigation.

4.2.4. Complete Hard Drive Forensic Image Process.

Once the forensic image and working copy are made and verified, the evidence disk can be returned to the Evidence Custodian. The Evidence Sheet, Case Log and Forensic Lead and Task Assignment Sheet can be updated.

Step 1: Power off the USB-IDE adapter.

Step 2: Disconnect the disk drive from the USB-IDE adapter.

Step 3: Allow the disk drive to cool before returning drive to the anti-static bag.

Step 4: Verify Evidence Tag and Case Description to insure you are storing the disk drive in the proper evidence container.

© SANS Institute 2006, Author retains full rights.

Step 5: Complete a new Evidence Sheet and Evidence Tag for the created forensic images. Insure the Evidence Sheet contains a detailed record of the image creation process. The cryptographic signature and the cryptographic command used must be identified. Additionally, in larger facilities it has proven beneficial to identify the forensic workstation and any special equipment used in the process, the date and time the image was created, and the name of the technician or investigator who created the images. Identify where the working copy of the forensic image is stored on the forensic workstation. *[The investigator should follow all established facility operating procedures, if they exist.]*

Step 6: Update the Case Log documenting the previously completed actions.

Step 7: Update the Evidence Sheet for the evidence disk drive and return both items of evidence to the Evidence Custodian.

Step 8: Update the Equipment Tag for the hard drive with the case data reflecting hard drive contents, date and time contents were created and the name and signature of the investigator responsible for accomplishing those actions.

4.2.5. Create Forensic Images of Various Removable Media.

4.2.5.1. CD-R and DVD-R.

This function is easiest performed on a Windows workstation with one the commercially available products such as: ROXIO Easy Media Creator 8, Nero 7 Ultra Edition CD/DVD Burning Suite, GEAR PRO 7.0 Professional or Mastering Edition, NewSoft Presto DVD Powersuite 1.1, Sonic MyDVD Studio Deluxe 5, Ulead DVD MovieFactory 3 Disc Creator, Pinnacle Instant CD/DVD 8. The previous mentioned list is a random sampling of software that is available. As with any software the Investigator should become familiar with its use concerning forensic imaging tasks.

4.2.5.2. Floppies, Jazz and ZIP Media.

Media should be duplicated with the Linux/Unix dd or dcfldd command, as Windows shell commands do not copy the entire media contents. A better solution should be to create a dd image of each floppy with md5 hash value and burn all the media images on CD-R media.

4.2.5.3 Magnetic Tape Media.

Magnetic tape media should be duplicated with the Linux/Unix dd or dcfldd command. The forensic investigator should be aware that an exact media image will not be guaranteed with magnetic tape media due to the physical mechanics and properties of magnetic tape. An exact copy of the data stored on the tape should be possible to capture. Recommend the Linux/Unix dd or dcfldd command be used to create an image of the tape on a hard drive due to processing time required to read and write tapes. It would be much faster to process the image on disk and verify the md5 hash values. After a forensic image has been obtained, the image can be transferred to tape or other media at the investigator's convenience for storage.

© SANS Institute 2006, Author retains full rights.

5. Digital Evidence Examination.

The examination phase of the forensic process is where all the disk images are examined and the contents inventoried and categorized. The Department of Justice (DOJ) National Institute of Justice (NIJ) published the Forensic Examination of Digital Evidence: A Guide for Law Enforcement April 2004. This guide recommends that technical procedures be developed, documented and tested for reproducible results. The guide provides recommendations for processing digital evidence at the various stages in the forensic process. The establishment of standard techniques will insure that the data is processed identically. These processes should identify all archive files and backup files so their contents can be extracted. Any files requiring special processing such as encrypted files or password protected files must be identified. Most of the work in this process can be automated. The SleuthKit utility Sorter performs a large part of functions in this process. Sorter is unable to inspect composite file structures. These files must be processed manually via some type of external processing other than Sorter. Sorter can be used to identify these composite files.

5.1. Data Compilation.

This is the process in which all the raw hard drive or file system images are searched for composite file structures. All composite files must be identified and all the individual components must be extracted. All encrypted or password protected files must be identified and opened or cracked to expose their contents. The unallocated space in the disk images must be examined for potential file fragments or deleted files. File slack space must be examined on Windows architecture systems for file fragments and potential content.

5.1.1. Identify and Process Composite Files.

This task is easily accomplished with the SleuthKit utility Sorter. Sorter can read a disk image, analyze all directory structures and classify every file found. Sorter uses the "file" command on every file and compares the file extension against the internal attributes of the file. Sorter will create a log entry in the appropriate category log file based on internal file attributes. Files with inappropriate or incorrect file extensions can be identified and logged. A most useful capability of Sorter is the ability to extract files from the disk image and place the files in directories based upon the file's classification. For instance, all archive files (zip, arc, cab, tar, Z, gz) can be stored in one directory for processing. There is one draw back, in order to be selective you must create or modify Sorter configuration files. This is not an overly complicated process but this process must be thoroughly tested before use in a formal investigation by the investigator. The file created in paragraph 2.2.2.1.2 Sorter Adaptations archives.sort will identify most archive files. The file composite.sort incorporates Microsoft backup files, and any other composite files that the Linux file command can identify. This makes the decision a matter of personal preference. For the task of identifying composite files for further processing, the file composite.sort best fulfills this requirement.

Command: sorter –f ntfs –d /forensics/evidence/case_jones_030106/data/sorter –C composite.sort –h -i raw –o 63 /forensics/images/jones_hda.dd

© SANS Institute 2006, Author retains full rights.

The composite file could be extracted and stored in the category composite with the following command.

Command: sorter –f ntfs –d /forensics/evidence/case_jones_030106/data/sorter –C composite.sort –h -s -i raw –o 63 /forensics/images/jones_hda.dd

5.1.2. Process Unallocated Disk Space.

Unallocated disk space can be processed several ways. The investigator can use Autopsy to process unallocated disk space. Autopsy File Analysis Keyword Search will generate strings from the entire disk image or unallocated space in the image. After the unallocated strings file has been generated by Autopsy, the user can enter a keyword search of both string files or load the unallocated file and just search that file. There are 5 predefined searches to assist the user. The screen even offers the option of viewing a Regular Expression cheat sheet.

Sorter can identify deleted files that have intact inode directory entries along with other files when processing an image. Sorter is only able to extract files in unallocated space that have directory entries. If the part of the files inodes have been reallocated, the file contents may not be completely accurate.

The investigator can manually process the unallocated space with the SleuthKit dls utility. This would be required as preparation for performing “keyword searches”.

Command:

```
dls –e –f ntfs –o 63 –i raw /forensics/images/jones_hda1.dd > /temp/jones_hda1.unalloc
```

Command:

```
strings -8 –radix /temp/jones_hda1.unalloc > /temp/jones_hda1.unalloc.str
```

Command:

```
foremost –v –c /forensics/foremost.conf –o /temp/unalloc_foremost  /temp/jones_hda1.dd
```

5.1.3. Process File Slack Space.

This process really only works on FAT and NTFS file systems. The SleuthKit utility dls has a “copy only slack space” option “-s”. This can be used to create a file that contains only file slack space for keyword searches, strings generation and file recovery with Foremost.

Command:

```
dls –s –f ntfs –o 63 –i raw /forensics/images/jones_hda1.dd /temp/slackspace
```

Command:

```
strings -8 –radix /temp/slackspace > /temp/slackspace.str
```

Command:

```
foremost –v –c /forensics/foremost.conf –o /temp/slack_foremost  /temp/slackspace
```

5.1.4. Process Swap Space.

Swap space processing on Windows systems requires the swap space to be extracted from a disk image as a file before examination. The process on Unix

© SANS Institute 2006, Author retains full rights.

systems is not as complex. Regardless of the amount of effort involved, swap space should always be processed. The only exception to the always rule is where sufficient evidence is readily available.

Processing swap space should be based upon strings generation, keyword searches, and Foremost processing. Strings generation may reveal user ids, passwords, file or image names, addresses (internet, mail, or physical location), phone numbers, and numerous other potential investigative leads. Sometimes partial or complete documents, images, or emails can be found.

5.1.5. Unix Swap Space.

Swap space on a Unix system is usually allocated to a separate and complete file system called swap. The SleuthKit utility mmls will display a disk drive's partition entries. However, other utilities may present the partition information in a more understandable format (sfdisk). The swap partition can be extracted with dd when working with a disk drive image or created as a separate disk image when connected to a Linux forensic workstation. First the swap partition must be identified. That can be done by using the mmls command.

```
[root@unix-for media]# mmls -t dos /dev/sda
DOS Partition Table
Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  -----   0000000000   0000000000   0000000001   Primary Table (#0)
01:  -----   0000000001   0000000062   0000000062   Unallocated
02:  00:00   0000000063   0000530144   0000530082   Linux (0x83)
03:  00:01   0000530145   0122190389   0121660245   Linux (0x83)
04:  00:02   0122190390   0138576689   0016386300   Linux (0x83)
05:  00:03   0138576690   0160071659   0021494970   DOS Extended (0x05)
06:  -----   0138576690   0138576690   0000000001   Extended Table (#1)
07:  -----   0138576691   0138576752   0000000062   Unallocated
08:  01:00   0138576753   0148810094   0010233342   Linux (0x83)
09:  01:01   0148810095   0152906669   0004096575   DOS Extended (0x05)
10:  -----   0148810095   0148810095   0000000001   Extended Table (#2)
11:  -----   0148810096   0148810157   0000000062   Unallocated
12:  02:00   0148810158   0152906669   0004096512   Linux Swap / Solaris
x86 (0x82)
13:  02:01   0152906670   0154946924   0002040255   DOS Extended (0x05)
14:  -----   0152906670   0152906670   0000000001   Extended Table (#3)
15:  -----   0152906671   0152906732   0000000062   Unallocated
16:  03:00   0152906733   0154946924   0002040192   Linux (0x83)
17:  03:01   0154946925   0156987179   0002040255   DOS Extended (0x05)
18:  -----   0154946925   0154946925   0000000001   Extended Table (#4)
19:  -----   0154946926   0154946987   0000000062   Unallocated
20:  04:00   0154946988   0156987179   0002040192   Linux (0x83)
21:  04:01   0156987180   0158015339   0001028160   DOS Extended (0x05)
22:  -----   0156987180   0156987180   0000000001   Extended Table (#5)
23:  -----   0156987181   0156987242   0000000062   Unallocated
24:  05:00   0156987243   0158015339   0001028097   Linux (0x83)
25:  05:01   0158015340   0159043499   0001028160   DOS Extended (0x05)
26:  -----   0158015340   0158015340   0000000001   Extended Table (#6)
27:  -----   0158015341   0158015402   0000000062   Unallocated
28:  06:00   0158015403   0159043499   0001028097   Linux (0x83)
29:  06:01   0159043500   0160071659   0001028160   DOS Extended (0x05)
30:  -----   0159043500   0159043500   0000000001   Extended Table (#7)
31:  -----   0159043501   0159043562   0000000062   Unallocated
```


© SANS Institute 2006, Author retains full rights.

```
32:  07:00   0159043563   0160071659   0001028097   Linux (0x83)
[root@unix-for media]#
```

In this particular case mmls's output is rather bizarre. The sfdisk linux utility provides more usable information in the needed format.

```
[root@unix-for images]# /sbin/sfdisk -f -l -s /dev/sda
80043264

Disk /dev/sda: 9964 cylinders, 255 heads, 63 sectors/track
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

   Device Boot Start     End   #cyls    #blocks   Id  System
/dev/sda1   *      0+     32      33-    265041   83  Linux
/dev/sda2         33    7605    7573   60830122+  83  Linux
/dev/sda3       7606    8625    1020    8193150   83  Linux
/dev/sda4       8626    9963    1338   10747485    5  Extended
/dev/sda5       8626+   9262     637-   5116671   83  Linux
/dev/sda6       9263+   9517     255-   2048256   82  Linux swap / Solaris
/dev/sda7       9518+   9644     127-   1020096   83  Linux
/dev/sda8       9645+   9771     127-   1020096   83  Linux
/dev/sda9       9772+   9835      64-    514048+  83  Linux
/dev/sda10      9836+   9899      64-    514048+  83  Linux
/dev/sda11      9900+   9963      64-    514048+  83  Linux
[root@unix-for images]#
```

This provides the exact information we need; sda6 is the swap partition. The dd command can extract our swap partition from the disk drive.

Command:

dd if=/dev/sda6 of=/forensics/images/jones_sda6.dd bs=1024 count=2048256

Obtaining the swap partition from a whole disk image is better done by using the mmls output. Use the starting location on the slice identified as "Linux swap" as the skip count in dd.

Command:

dd if=/forensics/images/jones_sda.dd of=/temp/jones_sda6_swap bs=512 skip= 0148810158 count=4096512

If this partition image was added into Autopsy, the file analysis options will be limited because it is a swap partition. The only options available will be Keyword Search and Data Unit examination. A Unix swap partition can be processed using the strings and Foremost utilities.

Command:

strings -8 –radix /forensics/images/jones_sda6_swap > /temp/jones_sda6_swap.str

Command:

foremost –c /forensics/bin/foremost.conf –o /temp/jones_foremost /forensics/images/jones_sda6_swap

5.1.6. Windows Swap Space.

Swap space on a Windows system is contained in a file that is allocated to a particular size, usually 1 ½ times the amount of memory on the machine. On

© SANS Institute 2006, Author retains full rights.

Windows 3.1 and some later versions, the swap file is called 386SPART.PAR. Windows 95 and 98 called the swap file WIN386.SWP. In Windows NT/2000/XP, the Windows swap file is named PAGEFILE.SYS. One special feature about the swap file is that the file is not fragmented. This means that whatever the size, the file will be allocated as one contiguous section of the disk.

There are several ways to extract the pagefile.sys from the disk image. You can manually extract the files with the SleuthKit utility fls and icat. Or you can use Autopsy's functionality to your advantage. Use Autopy's file analysis capability to identify the inode information for pagefile.sys. Select file analysis from the Host Manager screen. This will present the file analysis screen. The main panel will display the Current Directory. Upon startup the root directory for the image being analyzed will be presented. All the files in the root directory will be shown, the filenames and meta data will be highlighted as links. You can select either a file or meta data. (Do not right click any filenames unless it is an ASCII file and small, because Autopsy will display the file's contents in the bottom panel. This can take a long time to read the file and build a display containing meaningless unprintable characters.) Right clicking the meta data link will generate a screen displaying the inode data (results of an istat command). You are offered the selections: Report, View Contents or Export Contents. Select Export Contents. The browser will present the Save As dialog box, depending upon your browser's configuration. Note: Insure the destination you select has sufficient storage space to hold a copy of the file. The size depends upon how the system being investigated was configured. On a 512meg test system the pagefile.sys was over 800meg. You can also record the meta data inode number in the MFT Entry Number box on the far left side of the panel and manually use icat to extract the pagefile.sys file.

Command:

```
icat –s –f ntfs –i raw –o 63 /forensics/images/win-for.img 27-128-1 > /temp/pagefile.sys
```

After the files are stored in the temporary working directory, be sure to change their filemode to 555 or "r_x,r_x,r_x." This write protects the file from being accidentally modified.

The next step is to extract ASCII strings from the files for easy viewing of any potential leads such as, passwords, userids, filenames, web addresses, phone numbers or any piece of information that might assist your investigation.

Command:

```
strings -8 --radix /temp/pagefil.sys > /temp/win-for_pagefile.str
```

Command:

```
strings -8 –radix /temp/hiberfil.sys > /temp/win-for_hiberfil.str
```

Command:

```
foremost –c /forensics/bin/foremost.conf –o /temp/pagefile_foremost /temp/pagefile.sys
```

Command:

```
foremost –c /forensics/bin/foremost.conf –o /temp/hiberfil_foremost /temp/hiberfil.sys
```

By setting the string length to 8, only strings 8 characters or greater are generated. You may need to set a smaller value but the volume of information to sift and discard

© SANS Institute 2006, Author retains full rights.

grows rather rapidly.

Next you can run Foremost against both files and discover if any known file formats are discovered. The files Foremost recovers probably will not match any sizes or md5sums of files in your KGF repository. Foremost tries to determine the true end of file but often misses that mark and resorts to a flat file size limit stated in the configuration file or will terminate one file when the file header of another is located. The potential files discovered by Foremost can be viewed with a hex editor or researched with strings and established procedures for investigating rogue or hostile programs..

The exact same process can be applied to memory dump images. Some of the earlier versions of dd were not completely accurate in gathering all of memory.

Another approach if you do not want to bother with Autopsy is to generate a file listing with SleuthKit fls and ils commands.

Command:

```
fls –r -m “mount point” –f ntfs –i raw –o 63 –s “time correction in seconds”  > /temp/file-list.txt
```

Command:

```
ils –f ntfs –i raw –o  63-m /temp/file-list.txt
```

Command:

```
grep pagefile.sys /temp/file-list.txt
```

Command:

```
icat –s –f ntfs –i raw –o 63 /forensics/images/win-for.img 27-128-1 > /temp/pagefile.sys
```

Command:

```
foremost –c /forensics/bin/foremost.conf –o /temp/pagefile_foremost /temp/pagefile.sys
```

5.1.7. Windows Hibernation Space.

Windows 2000 and XP have the ability to copy memory and other key information into a file called hiberfil.sys for power down and restarts. The hiberfil.sys file can contain a wealth of information. The hiberfil.sys file is processed the same as swap space. Perform the same steps as for pagefile.sys in Autopsy and the manual processing steps.

Command:

```
fls –r -m “mount point” –f ntfs –i raw –o 63 –s “time correction in seconds”  > /temp/file-list.txt
```

Command:

```
ils –f ntfs –i raw –o  63-m /temp/file-list.txt
```

Command:

```
icat –s –f ntfs –i raw –o 63 /forensics/images/win-for.img 12421-128-1 > /temp/hiberfil.sys
```

Command:

```
grep hiberfil.sys /temp/file-list.txt
```

Command:

© SANS Institute 2006, Author retains full rights.

icat –s –f ntfs –i raw –o 63 /forensics/images/win-for.img 12421-128-1 > /temp/hiberfil.sys

Command:

foremost –c /forensics/bin/foremost.conf –o /temp/hiberfil_foremost /temp/hiberfil.sys

5.1.8. Process System Memory (If Available).

Processing the memory from a system will be similar to processing swap space. Keyword searches and strings generation may reveal user ids, passwords, partial documents or files. When researching intrusions or suspicious system activity, complete programs may be contained in the memory snapshot. However, extracting a complete operating program from a memory snapshot for forensic evidence should be done by a forensic professional with systems experience. *(That topic is beyond the scope of this paper.)* The results of strings generation and keyword searches should not be overlooked or disregarded. Foremost should be used to process a memory snapshot for discovery of potential files or graphic images.

Command:

foremost –c /forensics/bin/foremost.conf –o /temp/memory_foremost forensics/images/jones_mem.dd

Another technique is to generate a strings file based upon memory contents. This is performed like most other strings extractions.

Command:

strings –8 –radix /forensics/images/jones_mem.dd > /temp/jones_mem.str

The radix value identified with each string can be used when viewing the memory dump with a hexadecimal editor, the radix is an offset.

5.2. Data Reduction.

This is the process in which the data compiled during the data compilation step is reduced. This process is reiterative in nature. The first step is the elimination of all known good files. Each files' md5sum value is compared to the md5sum value in a known good md5sum repository. After all the known good files are removed from the data, other data reduction steps may be processed. Files in the data may be eliminated based upon whether their creation and modification date is less than a particular specified time period. Files could be removed based upon file content, as when only picture or image files are needed. Data reduction searches can be positive or negative. Positive searches identify files meeting a particular criterion. Negative searches identify files not meeting a particular criterion.

Use the SleuthKit utility Sorter to process the Known Good File (KGF) repository to identify and remove files from the data that will yield no positive results or potential leads.

Command:

sorter –f ntfs –d /forensics/locker/case_03Jan06_jones_01/data/sorter –C windows.sort –h –s –a /forensic/evidence/KBF/alert_images –x /forensics/evidence/KGF/xpsp1 –n /forensics/evidence/KBF/NSRLFile.txt /forensics/images/jones_hda1.dd

© SANS Institute 2006, Author retains full rights.

The above command will process the NTFS image located in /forensics/evidence/case_jones_030106/images/hda1.dd. All known good files matched with the KGF xpsp1 dataset will be ignored. All known files matched with the new NSRLFile.txt dataset will be ignored. (Hacker Tools were removed from the dataset.) The remaining files will be extracted and categorized according to the windows.sort configuration file. Additionally, any files found matching files identified in the KBF alert_images dataset will be saved in the alert directory.

```
#! /bin/bash
# mount the installation media at the appropriate location (cdrom or cdrecorder)
mount –t iso9660 /dev/cdrom /media/cdrom
# make temporary directory to contain expanded cabinet files
# insure you have enough space, 100meg should do
mkdir /tmp/work
# change to temporary working directory
cd /tmp/work
# locate cabinet files on installation media. Microsoft uses two methods to identify
# cabinet files. One method is to use the “cab” extension to designated cabinet
# files and the second method involves changing the last character of the filename
# files and the second method involves changing the last character of the filename
# extension to an underline “_” to represent a cabinet file.
# extension to an underline “_” to represent a cabinet file.
find /media/cdrom –type f –name “*.cab” –fprint /tmp/files1
find /media/cdrom –type f –name “*_”    –fprint  /tmp/files2
cat /tmp/files1 /tmp/files2 > /tmp/files_to_expand
rm –f /tmp/files1 /tmp/files2
# loop thru /tmp/files_to_expand reading each filename and extracting the files
# into the /tmp/work directory
for i in `cat /tmp/files_to_expand`
do
# Need the basename
filename=`basename $i`
cp $i /tmp/work/$filename
/forensics/bin/cabextract –q /tmp/work/$filename
rm –f /tmp/work/$filename
filename=`ls -1`
/forensics/bin/md5 /tmp/work/$filename
rm –f /tmp/work/$filename
done > /forensics/NSRL/xpsp1basecabs.md5
rm –f /tmp/work
```

5.2.1. DOJ HashKeeper Database.

HashKeeper is a database maintained by the Department of Justice. This database contains entries submitted by various groups (mostly law enforcement). The HashKeeper data repository contains information similar to the NSRL Known File repository with the exception of known bad files (identified child pornography images). Most of the commercial forensic applications incorporate HashKeeper data into their datasets, according to their advertised literature. The following is an example of one of the datasets that comprise the HashKeeper database. The

© SANS Institute 2006, Author retains full rights.

HashKeeper database could be exported into a format compatible with Autopsy and Sorter. This particular extract came from an early specialty submission of a set of child pornography pictures, provided by:

```
 SA Brad Kropp
AFOSI, Det 307
(609) 754-3354
Case # 00307D7-S934831",3/15/2001 13:35:14


"file_id","hashset_id","file_name","directory",
     "hash","file_size",
       "date_modified","time_modified","time_zone","comments",
                "date_accessed","time_accessed"
83136,12,"DSC00013.JPG","E:\MUCHACHITAS\03-31-2000 842P",
     "04AAC6B860736F11518668D29B4C80CC",168972,
          2/20/1998 0:00:00,12/30/1899 7:38:00,"w",,,
83106,12,"DSC00001.JPG","E:\MUCHACHITAS\02-04-2000 741P",
     "BB90EC73DA6D04AEC271F28D83F50D96",177164,
          2/4/2000 0:00:00,12/30/1899 18:44:00,"w",,,
83128,12,"DSC00004.JPG","E:\MUCHACHITAS\03-31-2000 842P",
     "174A3D69D935E1F5682A41AB437F678D",176140,
          2/20/1998 0:00:00,12/30/1899 7:31:00,"w",,,
83129,12,"DSC00005.JPG","E:\MUCHACHITAS\03-31-2000 842P",
     "3DD6C6A334B21C9CDBBBE5A74A5ABE68",168972,
          2/20/1998 0:00:00,12/30/1899 7:32:00,"w",,,
83130,12,"DSC00006.JPG","E:\MUCHACHITAS\03-31-2000 842P",
     "68A2CFA346D014F74B8875C7F74BBEA6",181260,
          2/20/1998 0:00:00,12/30/1899 7:33:00,"w",,,
83131,12,"DSC00007.JPG","E:\MUCHACHITAS\03-31-2000 842P",
     "44ED0D71DE6260C3F3EA90B3339843D1",176140,
          2/20/1998 0:00:00,12/30/1899 7:35:00,"w",,,
83132,12,"DSC00008.JPG","E:\MUCHACHITAS\03-31-2000 842P",
     "52395DB8EC05F445E2DD4710611D4D14",175116,
          2/20/1998 0:00:00,12/30/1899 7:35:00,"w",,,
```

5.2.2. Using Alert, KGF and NSRL Known File Repository.

These repository files will primarily be used with Autopsy and the Sorter utilities. These files can be used individually with the hfind utility to verify a file as a known good file or as a known bad file. In order to use the NSRL Repository you will have to modify the Autopsy Perl modules. The code is fairly well commented in the latest version 2.0.3 and above. This is only needed if you plan on using Autopsy as your interface. A simple work-around would be to convert the NSRLFile.txt into a straight md5sum format and build your own KGF cryptographic signature set, which shall be referred to as a hash set. The NSRLFile.txt could easily be converted over a weekend. The script provided in paragraph 2.2.2.1.3.2 processed the NSRLFile.txt file in a little over 24 hours.

Once you have your KGF or KBF hash sets, the hash sets can be searched with the hfind command manually or use the Hash database lookup screens within Autopsy. When using Autopsy in this manner, it is a simple cut and paste operation.

Processing numerous lookups via cut and paste is very time consuming. Hfind has the option to allow a lookup file. This is a file containing the md5sum value of files to be searched in a particular KGF hash set. Simply create a file with one md5sum per line (the md5sum can be the only thing on the line), include as many

© SANS Institute 2006, Author retains full rights.

hash values that need to be verified.

```
[root@unix-for king]# cat hashset

3e2324ad0260c1bbf3fbb88052868d3b
1da3187f6cafdbe34ca88e41972c93b8
88cf0ff92a4a9fa7bd9b7513b2e9e22b
[root@unix-for king]#

hfind -f hashset /forensics/KGF/KGF/winxpsp_md5.txt

3e2324ad0260c1bbf3fbb88052868d3b  .\Documents and
  Settings\admin\Application  Data\Microsoft\CryptnetUrlCache
  \Content\B82262A5D5DA4DDACE9EDA7F787D0DEB
1da3187f6cafdbe34ca88e41972c93b8 .\Documents and
  Settings\admin\Application Data\Microsoft\CryptnetUrlCache
  \Content\7C8A03C4580C6B04FDF34357F3474EDC
88cf0ff92a4a9fa7bd9b7513b2e9e22b .\Documents and Settings\
  Default User\Application Data\desktop.ini
88cf0ff92a4a9fa7bd9b7513b2e9e22b .\Documents and Settings\All
  Users\Application Data\desktop.ini
88cf0ff92a4a9fa7bd9b7513b2e9e22b .\Documents and
  Settings\admin\Application Data\desktop.ini
88cf0ff92a4a9fa7bd9b7513b2e9e22b .\Documents and
  Settings\Gerry\Application Data\desktop.ini
88cf0ff92a4a9fa7bd9b7513b2e9e22b .\WINDOWS\system32\config\
  systemprofile\Application Data\desktop.ini
```

5.3. Data Categorization.

This process serves two purposes. The first purpose is to verify each file's content and insure that the assigned extension is valid, if appropriate. Each file is then categorized based upon the determined file content. The second purpose is to identify files that failed the verification process. Files failing verification are potential candidates for inspection concerning data hiding by changing a file's extension. This is a very basic technique for attempting to hide the contents of files.

The SleuthKit Sorter utility can be used to perform this process. The windows.sort configuration file provided in Appendix 13 Customized Configuration Files can be used with Sorter to categorize the files of a windows system.

> Command: sorter –f ntfs –d /forensics/evidence/case_jones_030106/data/sorter –C windows.sort –h –s /forensics/images/jones_hda1.dd

5.4. Search Raw Data for Leads.

This process is usually referred to as the "dirty word" or "keyword" search. This search process is performed on all the files on the system, unallocated space, file slack space, swap space, save memory and unallocated partition space. The investigator can use the grep utility to manually process files looking for various dirty or keywords in the files contained on the system being investigated. An investigator could possible locate key evidence in a short period of time.

Grep works best on ASCII text files. Files containing binary information or data must be first processed with the strings command. Strings will search a requested file looking for four ASCII characters and a null character. A four-byte string is the minimum default string length. Strings will generate output for any length string greater than 3 ASCII characters. Using grep to find information or leads in the ASCII

© SANS Institute 2006, Author retains full rights.

string file on the system is a simple matter.

Even locating potential leads in slack space, swap space or memory can prove quite problematic. This is because you do not have a known entity to examine. Instead you may be dealing with only a few bytes of file slack or 1gig of memory. By using strings to generate a file of ASCII strings and then using the grep to search the file, you look for information quickly. Strings can assist by telling you where the match occurred in the current file and by telling you the offset from the beginning of the file; this is the purpose of the "—radix" option. This process does not provide any type of context for reference. The investigator is now left to his own knowledge and experience.

However, another step can be utilized in this process. You can modify the Foremost utility to sift through the raw data looking for file headers and trailers and printing out their offset from the beginning of the file or data remnant. Process the file with strings and grep and then marry up these two reports by offset values. This identifies matches that are sometimes close to file headers or trailers. Sometimes this information is helpful when you only have a file header and a little extra data. This could contain key information by providing another piece to the puzzle.

5.5. Using Foremost to Search Files for Hidden Content.

This is not a complex process. The investigator needs to obtain a good reference listing of file headers and trailers. (Gary Kessler at Champlain College has compiled a rather large list.) The following deviates somewhat from Gary Kessler's list and the reference provided in the Foremost configuration file. Most of the file selection options are turned off in the default foremost.conf file. The default header and trailer lines can be uncommented by removing the "#" at the being of the line. The file can be easily modified with a text editor. (Do not edit the foremost.conf on a windows workstation and then save the file on a Unix workstation. Text lines in a Windows text file contain a carriage return and line-feed character.) Additional cautionary note is warranted: Foremost can generate rather large files; do run Foremost against a hard disk image or partition image unless you have a lot of disk space and extra time to sort through the output.

Command: foremost –c /forensics/src/foremost.conf –o /temp/special_foremost anyfile

Foremost is a free data carving utility. This utility will provide you with a basic capability. There are ample commercial tools on the market. Foremost is a great learning tool for investigatory work (research and training). The other commercial products provide a greater header and trailer recognition dataset. This will increase the investigator's productivity but at a financial cost.

6. Digital Evidence Analysis.

The analysis of digital evidence is not an exact science. Most successful investigators employ an "ad hoc" reiterative combination of the five basic forms of analysis (chronological, relational, functional, baseline and vulnerability).

Depending upon the type of investigation, the investigator decides upon the best productive approach. For example, when looking for child pornography, the investigator may start out-processing evidence with functional analysis, by attempting to locate all images of child pornography. This approach may give way to relational

© SANS Institute 2006, Author retains full rights.

analysis when the investigator must connect the images to the suspect. The investigator may then turn to chronological analysis by creating a time-line to prove the suspect was using the computer when the images were stored and viewed on the computer. There may be many stops and restarts using each of these analysis techniques as leads are investigated and eliminated or added to validate the investigator's case.

The baseline form of analysis is used to sift through a large quantity of data in the hope of identifying potential leads. This technique is commonly used in computer intrusions or investigations where very little information is known. The investigator removes all known good files and then researches files that have changed from the initial baseline. The problem with this technique is that the investigator must have an initial baseline or must create a baseline from vendor media. This process can be fast or slow depending upon the availability of valid baselines. This analysis technique will only serve to initially identify potential leads. The investigator will have to utilize other techniques to redefine and validate the clues. Chronological or functional analysis techniques could be used to identify other system components modified or accessed at a particular time. Functional analysis could be used to evaluate the purpose of the discovered lead and how that component functions with other system components.

The vulnerability analysis technique would be used to analyze a complex network of computers and system for possible intrusions. All the vulnerabilities would be identified and researched on the various systems. Potential leads would yield to chronological analysis for verification across the network or other systems. There is no one technique that is best for all situations. The investigator must be practiced in all these forms of analysis. National Institute for Justice has published some very general guidelines for performing analysis on digital evidence. These guidelines do not explain how to conduct an analysis but present the different types of crimes and the associated forms of digital evidence found and the possible analysis techniques.

6.1. Chronological Analysis.

Regardless of the type of crime or activity being investigated a chronological timeline often provides clarity to a complex investigation. Often the timeline will reveal periods of time for which evidence is required. These time periods may establish exculpatory evidence or present inconclusive results due to the lack of any evidence. The investigator should include and document all known facts in the timeline. Witness statements and times of printed documents may often present another perspective when included in a computer event timeline.

Autopsy provides a mechanism for generating a timeline based upon computer file Modification Access Changed Times (MACTIMES). The process is can be accomplished by selecting the File Activity Time Lines from the Host Manager screen and then selecting the option to generate a data file. After the data file is generated, the time line can be generated by selecting Create Time line. The user is presented a menu to complete for a starting and ending time, if desired. Otherwise, the time line is generated based on the earliest and latest date and time stamps.

Autopsy provides a nice monthly selectable view of the time line events. As important information is discovered, the investigator can make annotations inside Autopsy. The investigator should insure that a computer date and time event can be

© SANS Institute 2006, Author retains full rights.

validated with other sources, such as internet web pages, ISP records, and remote internet site logs. Many users find the browser view of the time line difficult and slow. Therefore the recommendation is to view the time line with a text editor of choice, preferably one with a good search capability.

6.2. Functional Analysis.

The use of functional analysis in computer investigations provides information on how computer software, hardware, or data operates or is manipulated by the system or an individual component. This information may identify actions that occurred or were required to occur. By using webbing or tables, entire processes can be diagrammed. Often the investigator has to build a process diagram with bits and pieces of residual computer information.

For example, the evidence of child pornography on a computer must be linked to an event image written to the disk. This will result in several pieces of data, such as a date and time stamp of when the image was written to the disk and information on image size and file ownership. Next, the investigator must determine how or what process transferred the image to the disk. What devices are available or capable of performing this action? What software is available that can create or manipulate the image?

The diagram for one piece of evidence/component may merge with other diagrams. The investigator must decide whether this is important or inconsequential, having no relevance to the investigation. Normally a complex junction or overlay of several trees usually represents a hub of activity worthy of investigation.

Probably the biggest problem with diagramming is the mechanics of their construction. The best approach is to start with known facts and work to completely define the functional source of that fact. As components or functional elements are added to the diagram, each element is assigned a probability value from a scale of 1 to 10 with 1 being not likely to 10 being extremely possible.

In example 1, the pornographic image was 3.5 meg bytes. A floppy can hold 1.44 meg. This would mean the image would have to be compressed by greater than 60% to be stored on a floppy. The probability of that occurring is low, therefore assign a value less than 5, such as a 3 or 4. The image can readily be transferred from a CD-R or USB device; they are assigned values of 10. The input devices, such as keyboard and audio microphone and auxiliary line in, are assigned low numbers due to complexity required to create an image with the keyboard or converting audio output to digital, value 2. The serial port can provide the image via a cable connected to a camera or via modem connection to a remote system, bulletin board or ISP; those are assigned a value 10. As each functional capability is added, the probability of that element supporting the action is evaluated. There may be no telecommunications software installed and no log entries indicating modem use, so the value of that item would be 4. Because IE has never been configured, value the ISP element as 4. All local ISP's can be contacted concerning possible accounts for the suspect. Telephone records can be requested to determine possible phone calls made to the ISP's. By functionally researching items and assigning probability values, the investigator can narrow the elements to search. So far 3 items are fully capable of transferring the image: the CD-R, USB or serial port and camera. These options might be further narrowed by determining USB device

© SANS Institute 2006, Author retains full rights.

access and camera software installation. Another functional analysis path would be analysis of the times and when the items were created, modified or accessed. In particular, virus detection software can periodically scan computer files changing their access times.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

6.3. Relational Analysis

This form of analysis presents how individual evidence artifacts or computer information are connected to the various components of the investigation: suspect, websites, email, or file MACTIMES. The relationships between evidentiary items can be diagrammed with a bubble chart. Each bubble represents an item of interest and arrow lines connect the bubbles. The direction of the arrow indicates which item initiated the relationship. Attributes can be assigned to each bubble to highlight important facts. Cohesion values can be assigned to each connection to indicate frequent or strong connections, usually on a scale of 1 to 10, where 1 represents weak cohesion and where a value of 10 represents a very strong bond between items.

Relational analysis provides a mechanism for establishing connectivity between the suspect, suspect's actions, and evidence. For example, relational analysis can be used to connect an image to a pornographic website, and you can connect that same image to a person. This can be done by defining a series of relationships between information available on the computer and through external data sources, such as the ISP's and remote websites. ISP records will have to be subpoenaed in order to obtain network activity logs. In most cases, sufficient information resides on the computer to allow the investigator to continue researching and collecting evidence to either prove or disprove the suspect's involvement in the event.

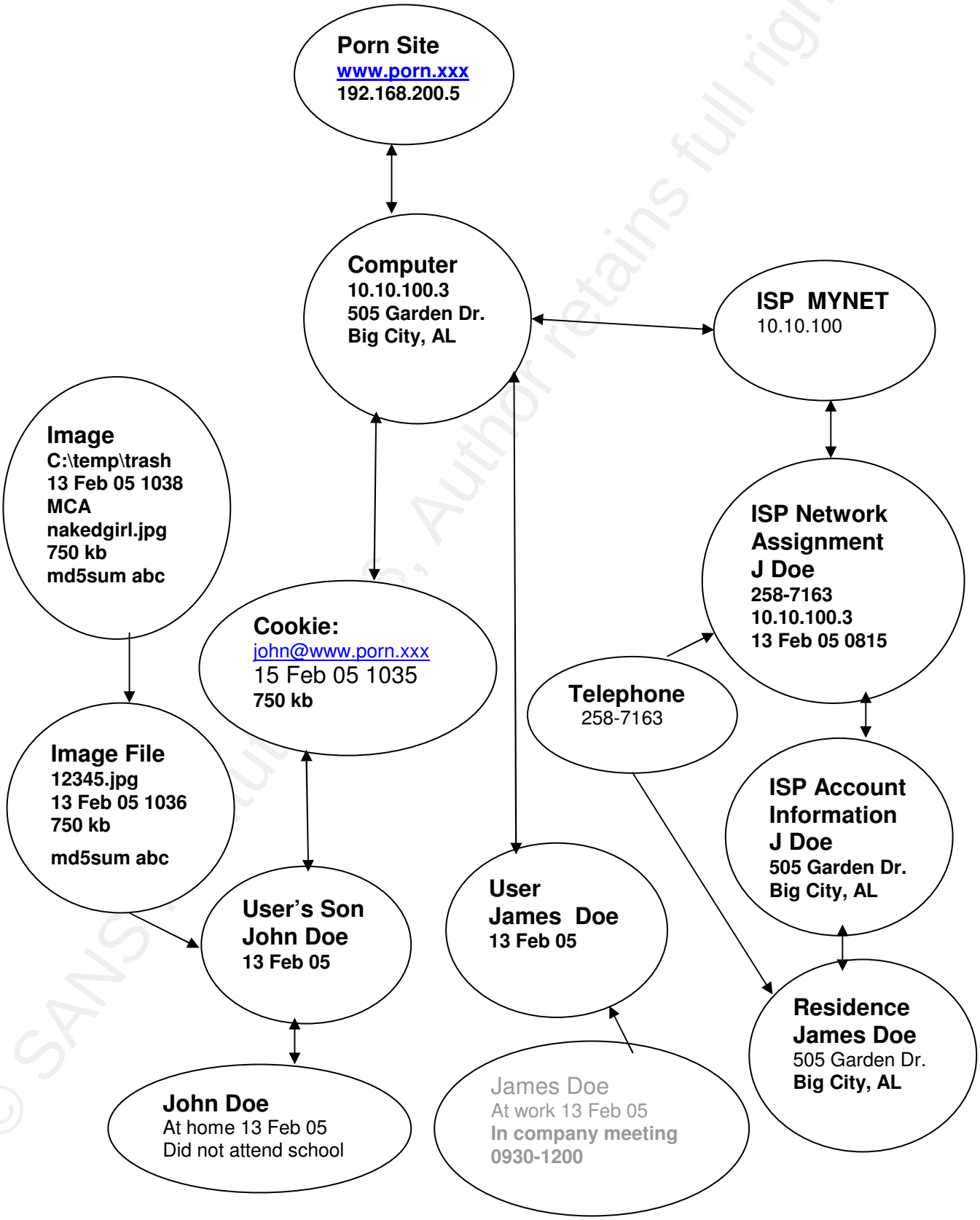
The computer can be connected to a network address. The network address can connect the computer to a website through website logs and ISP records. The computer user can be connected to the website by cookies, URL cache records, and IE history records. The pornographic image can be connected to the user by MACTIMES, temporary internet files, recently accessed files, and computer user storage area. Connecting the computer user to a person may be accomplished through the use of a user id and password. Witness statements can provide collaborating evidence such as: John was home sick on 16 Feb 05, or Joe was at work attending a meeting from 0930 to 1200. The image was written to the system at 1036; John was home and Joe was at work.

This relationship can easily be diagrammed with a bubble chart. Items with numerous connections are potential investigative leads for research and verification.

Items with high values indicate strong cohesion and relationships. A technique for managing the information on each item or node is to assign a number to each node and record specific details and scoring rationale on a numbered index card. As items are researched, information may change the cohesion values.

© SANS Institute 2006, Author retains full rights.

Relational Analysis Bubble Chart



© SANS Institute 2006, Author retains full rights.

6.4. Baseline Analysis.

Baseline Analysis is used primarily for computer intrusion investigations and computer auditing. This analytical approach requires that an initial or approved baseline be available for comparative analysis. A baseline of the system under investigation is created and is compared against the approved baseline. This approach becomes ineffective when the baseline is outdated due to software upgrades not recorded in the baseline or on the computer being investigated. A contributing factor to the success or failure of a baseline investigation is the establishment and enforcement of IT policies concerning software installations and user file storage.

Baselines can constitute KGF data sets. The SleuthKit utility Sorter can easily generate an audit report to identify rogue files. Additionally, Sorter could be used to collect all the rogue files for examination. By the proper application of IT policies the auditing of computer workstations could be minimized. When investigating computer intrusions, the rogue files provide a starting location to search for potentially compromised executables and root kits. When Sorter is used with an alert file, known virus files, root kits, and Trojans can easily be located. The alert file could be used to identify versions of programs that possess vulnerabilities. Rarely is baseline analysis alone used to investigate computer crime. However, baseline analysis can be extremely effective when investigating numerous computers for intrusion. Baseline analysis is expensive from an IT processing point of view due to the time required to image, store and process each IT resource. However, minimal manpower is required for the comparative analysis aspect of this approach when performed with Sorter.

6.5. Vulnerability Analysis.

The application of Vulnerability Analysis is predominately used in the investigation of computer intrusions. This analysis technique facilitates investigating large networks comprised of numerous computers. The computers are evaluated for known vulnerabilities. Computers reporting the presence of vulnerabilities are researched for potential evidence of the exploited vulnerability. Analysis of this type requires in depth knowledge of vulnerabilities, application of exploitation, and concealment techniques. When evidence of exploitation has been discovered, the investigation of that computer shifts to one of the more traditional analysis methods, chronological or temporal analysis, or functional analysis to further research the intruder actions and methods. Often the relational analysis approach will be used to establish connections between other network computers, users, compromised software and data. Baseline analysis may even be used to discover the full extent of a computer system's compromise.

Vulnerability analysis of a network is usually conducted by a person that has been trained and certified to perform network vulnerability scans. Warning: An improperly conducted network vulnerability scan can cause extreme havoc upon an operation network. Improperly configured scanners can lock every account on a Windows Domain controller, crash systems, routers and firewalls, and generate enormous amounts of firewall and syslog entries. Vulnerability scans can easily cause denial of service attacks against computer systems resulting in criminal and civil law suits.

Upon completion of the vulnerability scan, the results are presented to investigators to research and analyze each system. Investigators in this case are usually members of an Incident Response Team. When evidence is found and confirmed, the system is imaged or a live analysis and data capture is performed in the case of operationally critical servers.

© SANS Institute 2006, Author retains full rights.

The results of the live data capture are then usually provided to forensic investigators for further analysis.

6.6. Event Reconstruction.

In this process, each item of evidence or contributing fact is formally documented and connected to other items of evidence forming a complete documentation trail for an event. Each item of evidence is reviewed for ambiguity and the need for supporting evidence or information. All information concerning a piece of evidence must be documented and evaluated for strengths and weaknesses. When evidence cannot be absolutely connected, the investigator must either state this fact or present why this fact must stand alone. The investigator must be careful not to present speculations as facts.

When documenting evidence, the investigator should have a consistent approach in recording pertinent information. (The best method for insuring consistency is the establishment of Standard Operating Procedures.) All items of computer evidence have attributes, such as modification and creation date and time, size, paths, owner ID, and file name. When documenting similar items of evidence all items should be documented identically. For example, when documenting evidence from an NTFS system, the following attributes should be documented via istat command:

$STANDARD-INFORMATION TIMES:
Created: Tue May 8 08:00:00 2001
File Modified: Tue May 8 08:00:00 2001
MFT Modified: Sun Feb 9 16:56:47 2003
Accessed: Sun Feb 9 16:56:47 2003
Name: dciman
Size: 8464
UID: 0

And the output of mac.exe or macdaddy.pl

Tue May 08 2001 08:00:00 8464 m..-/-rwxrwx 0 0
402-128-4C:/WINNT/SYSTEM32/DCIMAN32.D11
Sun Feb 09 2003 16:56:47 8464 .AC-/-rwxrwxrwx 0 0
902-128-4 C:/WINNT/SYSTEM32/dciman32.d11

A document for evidence should include the following information for consistency: Case Number, Evidence Sheet Number, FLTAS Item Number, Full Path Name, istat datat or MACTIMES from mactime or macdaddy, brief description of evidence, evidence bindings or links to other information or evidence, ownership description, case value and relevance. The use of a common format as presented in the Evidence Fact Sheet is suggested.

© SANS Institute 2006, Author retains full rights.

It is recommended that each item be documented for the Case Log. This prevents having to backtrack to obtain information concerning an item of evidence when creating the Forensic Report. This form of documentation reduces the ambiguity or uncertainty of the evidence to the case.

6.7. Verification of Evidence

The verification process of evidence is essential to accurately document a crime or event. Ideally, this should be performed by a team member other than the person that collected or documented the evidence. This insures that no assumptions are being made concerning the relevance of the evidence to the event or case. Each item on the Evidence Worksheet must be checked for accuracy. All data sources should be reviewed, and any procedures used to collect the data need to be reviewed. The recompilation of MD5 values for evidence items and the collection of file attribute information should be mandatory. A review of the steps used during research should be examined and performed to insure the same results are obtained. Errors or discrepancies should be documented in the verification section of the worksheet. Note: This part of an investigation must not be tainted by relationship issues between team members. Honest and accurate critiques are essential to the investigatory process.

The verification process should insure that no subjective comments or speculations are documented concerning the evidence. When serious errors are revealed that affect the viability of evidence, the lead investigator must decide on how to handle this item of evidence: recollect the evidence, discard the evidence, or re-evaluate the importance of the evidence to the case.

When all the evidence has been verified, the investigator will use the evidence to document the findings. These findings could establish the suspect's innocence or guilt. The possibility exists that the evidence may present inconclusive results. The investigator must always consider the possibility of insufficient evidence or the ambiguity of evidence. Upon completion of the verification process, the decision must be made to conclude the investigation and build the forensic report.

7. Forensic Report.

The part of the forensic investigative process that is the hardest for most people is writing of the Forensic Report. All the many hours of research and meticulous work are summarized and condensed into a few pages of manuscript. The transformation of technical concepts and jargon into plain English is almost an art. The aim should be common, easy to understand language in lieu of a lot of techno-babble.

There are no standards for computer forensic reports. However, there are two formats emerging as the potential standards. There is a format presented in the book, "Incident Response & Computer Forensics" by Kevin Mandia, Chris Prosise and Matt Pepe, published by McGraw-Hill/Osborne, 2003. The other format is presented in the book "Guide to Computer Forensics and Investigations" by Bill Nelson, Amelia Phillips, Frank Enfinger and Christopher Steuart, published by Thomson Course Technology, 2006.

7.1. Report Contents.

A forensic report should contain the following sections and contents:

© SANS Institute 2006, Author retains full rights.

Executive Summary

Objective

Computer Evidence Analyzed

Relevant Findings

Support Details

Investigative Leads

Additional Subsections:

Attacker Methodology

User Applications

Internet Activity

Recommendations

The Executive Summary should contain:

- Who authorized the forensic investigation.
- Why the forensic investigation was necessary.
- List the summarized, significant finding.
- Provide signature block for investigator.

The Objectives should define the goals of the investigation and tasks to be performed in the investigation.

The Computer Evidence Analyzed provides specific details and descriptions of evidence analyzed.

The Relevant Finding provides a summary of the findings of relevant items found during the investigation.

Support Details provides an in-depth look and analysis of the relevant finding. This section outlines all the tasks undertaken to meet the objectives.

Investigative Leads provides a description of outstanding actions that could be performed if the investigator had more time and resources.

Additional Report Subsections provide the reader with additional information to assist in understanding the importance of actions taken by the suspect or investigator.

7.2. Creation of Basic Report.

Even though a standard template may be used for presenting forensic evidence, the investigator must organize the forensic details in a way that effectively communicates the objective of the report. The preparation of an outline is essential to documentation and writing process. The investigator must evaluate the type of approach to be used: the chronological presentation of events, or present the main conclusion first and then follow by supporting evidence, or present the supporting events as the groundwork for the main conclusion. The outline will enable the writer to see any shortcomings or missing elements

© SANS Institute 2006, Author retains full rights.

before a lot of effort is expended. If the investigator had used an Evidence Worksheet, rearranging content would be fairly simple.

Regardless of the writing approach taken, the same approach should be used for each section. Research and conclusion can initially be taken directly from the evidence worksheets to create the initial draft.

The Objectives should be taken from the Preliminary Investigation Meeting (PIM.) The Computer Evidence Analyzed should be taken from the Hard Drive Evidence Worksheet, Computer Evidence Worksheet and Equipment Evidence Tags. The Relevant Finding will come from the Evidence Worksheets binding section and research sections.

The Support Details section should be comprised of the research sections of the Evidence Worksheets. The investigative leads will come from the Evidence Collection Log and Forensic Lead and Task Assignment Sheet.

7.3. Evidence Review and Validation.

This is a review of the information taken from all the various forms and worksheets that are incorporated into the Forensic Report. A good practice to follow when reviewing the basic report is to annotate the report with the form tracking number from the form that contained the original information. This approach forces the investigator to review the evidence form to obtain the proper tracking number. This will not guarantee that short cuts will not be taken but this reduces the possibility of clerical errors and the discovery of missing or lost evidence after report publication. This process should be conducted by the team member assigned quality assurance duties.

8. Archiving the Case for History.

Archiving case documentation is an essential part of the investigatory process. As cases work their way through the legal system, it may be months or years between when the investigation was concluded and when a court appearance or deposition may be required. This does not normally present difficulty for law enforcement agencies, but contractors may not be prepared for long-term storage and protection of artifacts entrusted to them.

All printed documents and reports should be affixed with a document number and page number (1 of #). The document number should be comprised of the case number and a unique sequential number reflecting the number of documents in the case. All documents should be recorded in an electronic format capable of being printed to near original quality. All documents will be defined and recorded in a master document index. All evidence available in electronic format will be assigned a new document tracking number and stored with the new document number. An entry in the master document index will record the new document number, the storage location, and the previously assigned name. The original computer file will be stored in a repository with all the other computer file evidence.

When all documents and files have been assigned a new document tracking number and stored as original copies, the master document index and document tracking files will be recorded onto CD-R or DVD-R. If the amount of data makes this impractical, the data may be recorded to magnetic tape. If magnetic tape is used, the first file on the tape must be a plain ASCII file that describes the contents of the data, the type of equipment used, model and serial number, and the commands and software used to transfer the data to the tape. Additionally, the name and telephone number of the person responsible for creating the tape must be included.

© SANS Institute 2006, Author retains full rights.

_____ASCII File Header Record on magnetic tape ----------

Case 01May06_Doe_01

Description: This case involves Mr. John Doe, 123 Main Street, Big City, AL 12345,

Mr. Doe was suspected of using a work computer provided by his employer “Gas Works”, 456 Backwater Road, Big City, AL 12345, per Manager Jane Goody.

Case file include hard drive image, witness statements, forensic evidence, forms, correspondence and final report. Case conclude on 12 June 06.

Equipment: Compaq DLT III Tape Drive, Model No. THD-2345, SN: 12348s89j

Archive tape created at Business Office by Gerry King, 123-444-8909 on 13 June 06.

Command: tar –cvf /dev/st0 /forensics/case_01May06_Doe_01

Verified by: Gerry King 14 June 06

_____ASCII File Header Record on magnetic tape ----------

9. Definitions.

Alert - is notification of event or special condition.

Archive - is storage of data, usually longterm.

ASCII - American Standard Code for Information Interchange is a code representing text in computers and communications equipment.

Autopsy - is software used to perform the examination phase of a computer forensic investigation.

Baseline - is an established set of data the contents of which are known and are used for comparison.

Binary - is the numbering system based upon only two characters.

BMP - bitmap, is an image file format.

Cache – is an area where frequently accessed data can be stored for rapid access.

Case Log - is the document in which is written each stage of the process and analysis of a crime scene.

CD-R - Compact Disk Recordable is a storage disk, write once media.

Cookie - is a packet of data sent by the server to a browser and returned unchanged. It is used for authenticating, tracking, and maintaining data about users.

Crime Scene and Evidence Documentation Kit - can be the portion of a Jump Kit used to process evidence at a crime scene.

© SANS Institute 2006, Author retains full rights.

Crime Scene Processing Kit - can be the portion of a Jump Kit used to process evidence at a crime scene.

Cryptographic Signature - pertains to a calculated value (file integrity hashes) of the contents of a file that is used to verify identical files.

Cryptography - is the art of obscuring the content of a message that is not disguised.

Digital Evidence Kit - can be the portion of a Jump Kit used to process digital evidence at a crime scene.

Discovery Subpoena - is a legal order submitted by the opposing attorney requesting that information concerning a case be provided.

DLT - Digital Linear Tape is a standard for magnetic tape technology.

DoD - Department of Defense.

DOJ - Department of Justice.

DVD-R - Data Video Disk Recordable is a storage disk, write once media.

Evidence Custodian - is the team member responsible for maintaining the documentation and integrity of collected evidence.

Evidence Locker - is a location in memory created by the software Autopsy to be used during a computer forensic investigation.

Evidence Tag - is the document attached to evidence and containing identifiying information for forensic use.

Evidence Transportation Kit - can be the portion of a Jump Kit that is used to prepare evidence from a crime scene for transport and storage.

FAT - File Allocation Table is a file system for the Microsoft Operating System, MS-DOS.

First Responder - is the person is responsible for determining if an incident occurred and gathering the information needed by the Incident Response Team.

Floppy - is a data storage device encased in flexible medium, as in floppy disk.

FLTAS - Forensic Lead and Task Assignment Sheet.

Foremost - is software that searches files

Forensic - pertains to courts of law.

FRED - First Responder's Evidence Disk is software which may be used for the acquisition of computer based evidence.

GIF - Graphics Interchange Format is a bitmap image format to compress files of pictures/diagrams.

© SANS Institute 2006, Author retains full rights.

GREP - is software that searches for a match to a string of data and prints the matches.

HashKeeper - is a database maintained by the Department of Justice containing known files used as baselines.

Hash Values - are digital fingerprints of data files that are used in comparisons.

Helix - is software that is used to create copies of data from computer systems.

Hibernation Space - is a portion of memory that holds information so that it is available after a power down and upon restart of the computer system.

IDE - Integrated Drive Electronics is an interface for connecting storage devices.

Inode - is a data structure on Unix style file system that provides information about the file.

IR - Incident Response.

ISP - Internet Service Provider

Jaz - is a disk storage system.

JPEG - is a format for compression of photographic images.

Jump Kit - is the equipment and supplies required to process a crime scene containing computer and digital evidence. It may consist of multiple kits for specific uses, such as Crime Scene Processing Kit, Digital Evidence Kit, Evidence Transportation Kit, and Crime Scene and Evidence Documentation Kit.

Keyword Search - is a function of software to locate a given string of characters.

KBF – Known Bad File – is a file that is known to be bad (malware, virus, trojan, worm) or contain content that is considered illegal.

KGF – Known Good File – is a file that is known to be good (original software installation media).

Lead Investigator - is the person on a forensic team who is responsible for managing the personnel and documentation of a criminal incident scene.

Loopback Device - allows the investigator to restrict the function of certain programs during an investigation.

MACTIME – Modification Access Changed Time represents the three categories of file times: modification time, access time, and creation time.

Malware - is software designed to infiltrate or damage a computer system.

MD5sum - is a computer program which calculates and verifies MD5 hashes to verify the integrity of files.

© SANS Institute 2006, Author retains full rights.

MFT - Master File Table is a component of the NTFS file system that is standard for managing file transfers.

Mission Brief - is the meeting conducted by the Team Leader before deployment to a crime scene. At this meeting, the basic objectives, duties, and timeline should be discussed. Information from this meeting should be documented in the Case Log.

NDIC - National Drug Intelligence Center is the center for strategic domestic counterdrug intelligence under the U.S. Department of Justice.

NIJ – National Institute for Justice.

NIST - National Institute of Standards and Technology promotes measurement science, standards, and technology under the U.S. Department of Commerce. It was previously known as the National Bureau of Standards.

NSRL - National Software Reference Library collects software and maintains a reference library of information, called the Reference Data Set, under the Department of Justice's National Institute of Justice..

NTFS - New Technology File System is the standard file system for Windows NT, Windows 2000, Windows XP, and Windows Server 2003.

Open Source - Software that is freely available for use.

OS – Operating System.

Parse - is the process whereby data is broken down into its constituent parts.

Partition - pertains to memory in a computer being divided into separate portions for function or storage.

Password - is a secret series of characters used to block access to certain data.

PNG - Portable Network Graphics is a compressed bitmap image format.

Quality Assurance Assistant – is the member of a forensic team whose duty is to review the evidence documentation for omissions or errors.

Radix - is a stable sorting algorithm.

RAID - Redundant Array of Inexpensive Disks or Redundant Array of Independent Disks is a system which uses multiple hard drives to share data in order to increase capacity, reliability, or speed.

RAR - is a file format for data compression and archiving.

RDS - Reference Data Sets are baseline files from a reference library of information maintained for comparison use.

© SANS Institute 2006, Author retains full rights.

Sanitize - refers to the method used to wipe all previously meaningful data from a storage device. The US Department of Defense standard for these methods are found in document 5220.22-M.

SANS – SysAdmin, Audit, Networking and Security Institute provides computer security training and certification.

SCSI - Small Computer System Interface is the standard interface and command set for transferring data between devices.

Slack Space - holds data between the end of file and end of file system cluster or sector.

SleuthKit - is software that is used to perform the examination phase of a computer forensic investigation.

SMB - Server Message Block is the system management bus.

SOP - Standard Operating Procedure.

Sorter - is software that categorizes files by their named extension.

Steganography - pertains to the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. An example of this is code hidden within the code of a picture. Steganalysis is the art of discovering and rendering useless such covert messages.

String - is a series of characters that have a special meaning when grouped together.

Swap Space - is a location in memory where data pertaining to a process can be stored until needed for processing in virtual memory.

TIFF - Tagged Image File Format is used for storing images.

URL - Uniform Resource Locator is a web address consisting of a character string in a standardized format which refers to a resource on the Internet.

USB - Universal Serial Bus is the standard bus designed to connect computer devices.

Userid - User identifier pertains to a series of characters that identify a specific user.

Username - identifies a specific account in a domain.

Verification - is the process whereby a fact is confirmed.

Vulnerability - refers to being open to attack.

WFT - Windows Forensic Toolkit provides automated incident response on a Windows system by collecting security-relevant information from the system.

Windows Domain - consists of a group of computers running Windows Operating Systems that share a central directory database which contains user accounts and security information.

© SANS Institute 2006, Author retains full rights.

Working Image - is a copy made of evidence for the purpose of testing without damaging evidence.

Write Protect - refers to a device that blocks data from being written to digital or magnetic media.

ZIP - is a file format for data compression and archive.

10. References.

ACPO (1999) Good Practice for Computer Based Evidence, Association of Chief Police Officers.

Carrier, Brian. *Autopsy*. May 2006. http://www.sleuthkit.org/autopsy/index.php

Carrier, Brian. *File System Forensic Analysis*. Upper Saddle River, NJ; Addison-Wesley, 2004.

Carrier, Brian. *The Sleuth Kit*. May 2006. http://www.sleuthkit.org/sleuthkit/index.php

Carvey, Harlan. *Windows Forensics and Incident Recovery*. Addison-Wesley, 2004.

Casey, Eoghan. *Digital Evidence and Computer Crime*. 2nd ed. London: Academic Press, 2004.

Casey, Eoghan. *Handbook of Computer Crime Investigation, Forensic Tools and Technology.* Academic Press, 2002.

Ellis, Stuart and Paul W. Frields. Fedora Core 4 Installation Guide. Red Hat. 2005.

Fahey, Doug, *Helix Incident Response and Computer Forensics*. May 2006. http://www.e-fense.com/helix/index.php

Kornblum, Jesse. "Preservation of Fragile Digital Evidence by First Responders." Digital Forensics Research Workshop, August 2002.

Kruse II, Warren G. and Jay G. Heiser, *Computer Forensics: Incident Response Essentials.* Pearson Education, 2001.

Mandia, Kevin, Chris Prosise, and Matt Pepe, *Incident Response and Computer Forensics*. 2nd ed. Emeryville: McGraw Hill/Osborne, 2003.

© SANS Institute 2006, Author retains full rights.

Marcella, Albert J., Ph.D. and Robert S. Greenfield editors. *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes.* CRC Press LLC, 2002.

Meyer, Craig W. and Gary M. Morgan. "Investigative Uses of Computers" FBI Law Enforcement Bulletin, Volume 69, Number 8, August 2000, Washington, DC.

Nelson, Bill, Amelia Phillips, Frank Enfinger and Christopher Steuart. Guide to Computer Forensics and Investigations 2nd ed.

US DOJ (2001) "Electronic Crime Scene Investigation: A Guide for First Responders", National Institute of Justice, NCJ 187736, http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

US DOJ (2002) Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation. http://www.cybercrime.gov/s&smanual2002.htm

US DOJ (2004) "Crime Scene Investigation: A Reference Guide for Law Enforcement", National Institute of Justice, NCJ 200160, http://www.ncjrs.gov/pdffiles1/nij/200160.pdf

US DOJ (2004) "Forensic Examination of Digital Evidence: A Guide for Law Enforcement.", National Institute of Justice, NCJ 199408, http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Vacca, John R. Computer Forensics: Computer Crime Scene Investigation. Hingham: Charles River Media, 2002.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

11. Forms.
11.1. Evidence Form.

Investigations Unit **This form is to be used for only one piece of evidence** **Fill out a separate form for each piece of evidence.**			
Case No.:		Unit Number:	
Investigator:			
Nature of Case:			
Location where evidence was obtained:			

Item # ID	Description of evidence:	Vendor Name	Model No./Serial No.

Evidence Recovered By:		Date & Time:	
Evidence Placed in Locker:		Date & Time:	

Evidence Processed By:	Disposition of Evidence	Date/Time
		Page __ of __

© SANS Institute 2006, Author retains full rights.

11.2. Evidence Form.

SECURITY INVESTIGATIONS **This for is to be used for one to ten pieces of evidence**					
Case No.:		Investigating Organization:			
Investigator:					
Nature of Case:					
Location where evidence was obtained:					
Description of evidence:		Vendor Name	Model No./Serial No.		
Item #1					
Item #2					
Item #3					
Item #4					
Item #5					
Item #6					
Item #7					
Item #8					
Item #9					
Item#10					
Evidence Recovered By:			Date & Time:		
Evidence Placed in Locker:			Date & Time:		
Item #	Evidence Processed By:	Disposition of Evidence		Date/Time	
				Page of	

© SANS Institute 2006, Author retains full rights.

11.3. Computer Evidence Worksheet.

Computer Evidence Worksheet

Case Number: _____ **Exhibit Number:** _____

Laboratory Number: _____ **Control Number:** _____

Computer Information

Manufacturer: _____ Model: _____

Serial Number: _____

Examiner Markings: _____

Computer Type: Desktop ☐ Laptop ☐ Other: _____

Computer Condition: Good ☐ Damaged ☐ **(See Remarks)**

Number of Hard Drives: _____ 3.5" Floppy Drive ☐ 5.25" Floppy Drive ☐

Modem ☐ Network Card ☐ Tape Drive ☐ Tape Drive Type: _____

100 MB Zip ☐ 250 MB Zip ☐ CD Reader ☐ CD Read/Write ☐

DVD ☐ Other: _____

CMOS Information Not Available ☐

Password Logon: Yes ☐ No ☐ Password = _____

Current Time: _____ AM ☐ PM ☐ Current Date: ___/___/___

CMOS Time: _____ AM ☐ PM ☐ CMOS Date: ___/___/___

CMOS Hard Drive #1 Settings Auto ☐

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

CMOS Hard Drive #2 Settings Auto ☐

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

© SANS Institute 2006, Author retains full rights.

11.4. Computer Evidence Worksheet continued.

Sub Exhibits Split From This Computer

Sub Number	Type	Where Found

Remarks

© SANS Institute 2006, Author retains full rights.

11.5. Hard Drive Evidence Worksheet.

Hard Drive Evidence Worksheet

Case Number: _____ **Exhibit Number:** _____

Laboratory Number: _____ **Control Number:** _____

Hard Drive #1 Label Information [Not Available ☐] **Hard Drive #2 Label Information** [Not Available ☐]

Manufacturer: _____	Manufacturer: _____
Model: _____	Model: _____
Serial Number: _____	Serial Number: _____
Capacity: _____ Cylinders: _____	Capacity: _____ Cylinders: _____
Heads: _____ Sectors: _____	Heads: _____ Sectors: _____
Controller Rev. _____	Controller Rev. _____
IDE ☐ 50 Pin SCSI ☐	IDE ☐ 50 Pin SCSI ☐
68 Pin SCSI ☐ 80 Pin SCSI ☐ Other ☐	68 Pin SCSI ☐ 80 Pin SCSI ☐ Other ☐
Jumper: Master ☐ Slave ☐ Cable Select ☐ Undetermined ☐	Jumper: Master ☐ Slave ☐ Cable Select ☐ Undetermined ☐

Hard Drive #1 Parameter Information

DOS FDisk ☐ PTable ☐ PartInfo ☐ Linux FDisk ☐ SafeBack ☐ EnCase ☐ Other:

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

LBA Addressable Sectors: _____ Formatted Drive Capacity: _____

Volume Label: _____

Partitions

Name:	Bootable?	Start:	End:	Type:
	☐			
	☐			
	☐			
	☐			

Hard Drive #2 Parameter Information

DOS FDisk ☐ PTable ☐ PartInfo ☐ Linux FDisk ☐ SafeBack ☐ EnCase ☐ Other:

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

LBA Addressable Sectors: _____ Formatted Drive Capacity: _____

Volume Label: _____

Partitions

Name:	Bootable?	Start:	End:	Type:
	☐			
	☐			
	☐			
	☐			

© SANS Institute 2006, Author retains full rights.

11.6. Hard Drive Evidence Worksheet continued.

Image Archive Information

Archive Method: Direct to Tape ☐ NTBackup ☐ Tar ☐ Other :* _____ Compressed? ☐

Attach appropriate worksheet for backup method used.

Tape Type: DAT 24 ☐ Dat 40 ☐ DLT ☐* Other *: Number Used:

**Requires Lab Director Approval*

Analysis Platform Information

Operating Systems Used: DOS ☐ Windows ☐ Mac ☐ *nix ☐ Other: _____

Version: _____

Analysis Software Base: I-Look ☐ EnCase ☐ DOS Utilities ☐ *nix Utilities ☐ Other:*

Version: _____

Restored Work Copy/Image Validated:	Yes ☐ No ☐

List of utilities used other than base

Utility	Version	Purpose

Analysis Milestones

Milestone	Remarks	Initials
Run Anti-Virus Scan		
Full File List with Meta Data		
Identify Users/Logons/ISP Accounts, etc.		
Browse File System		
Keyword/String Search		
Web/E-mail Header Recovery		
Recover & Examine Free/Slack Space		
Examine Swap		
Unerase/Recover Deleted Files		
Execute Programs as Needed		
Examine/Recover Mail/Chat		
Crack Passwords		

© SANS Institute 2006, Author retains full rights.

11.7. Evidence Collection Log.

Evidence Collection Log Date:_____

Case Number:_____

Sheet Number: _____ of _____

[Item Number] Item Description	Collecting Investigator Date/Time	Evidence Custodian Tag Number

© SANS Institute 2006, Author retains full rights.

11.8. Equipment Evidence Tag.

EVIDENCE TAG

Agency _____

Item No._____ Case No._____

Date of Collection _____ Time of Collection _____

Collected By _____

Description of Evidence _____

_____

_____

Location of Collection _____

_____

_____

Type of Offense _____

Victim _____

Suspect _____

CHAIN OF CUSTODY

Received From _____ By _____

Date _____ Time _____

Received From _____ By _____

Date _____ Time _____

Received From _____ By _____

Date _____ Time _____

Received From _____ By _____

Date _____ Time _____

© SANS Institute 2006, Author retains full rights.

11.9. Forensic Lead and Task Assignment Sheet.

Forensic Lead & Task Assignment Sheet Date:_____

Case Number:_____

Task Assignment Sheet Number: _____ of _____

[Lead Number] Lead Description	[Task Number] Assigned to:	Evidence Collection Sheet Item Number

© SANS Institute 2006, Author retains full rights.

11.10. Evidence Fact Sheet

EVIDENCE FACT SHEET

Case Number _____ **Date** _____

Computer Serial Number _____

Evidence Reference Name _____

Evidence Description _____

Bindings _____

Evidence INODE Attributes _____

MAC TIMES _____

MD5SUM _____

Research _____

© SANS Institute 2006, Author retains full rights.

CASE STUDY

1. Introduction. This case study will identify the steps taken during the forensic investigation of John Webb's computer. Due to the sensitive nature of the content of this investigation the client's personal information has been changed to protect his identity. The use of several forensic tools will be discussed in the processing of the digital data associated with this investigation. The tool discussion will concentrate on the use of the tools to extract and identify the various data formats and contents. The discussion will cover the steps and processes that enable a sound forensic methodology to determine the cause of this investigation.

2. Investigation Review. The participants of this case are: John Webb, Mary Beth Webb (wife), Jack Webb (eldest son), Amy Webb (daughter) and Gerry King (Computer Consultant). This case had a peculiar beginning. John Webb was acquainted with me through mutual friends. John was experiencing some periodic abnormal behavior on this computer. John thought that I might be able to recommend some quick fix or someone that could determine what the problem was and provide some recommendations. I currently was between job assignments and took this case as a means to hone my skills.

I informed John that I would be willing to meet John at his residence the next day at 5:30 PM to discuss the specifics of his problem and present my requirements. I scheduled this meeting for two reasons. First, I wanted time to prepare for the case and do some research. Second, I wanted to question John in a familiar environment, where he would feel more comfortable and at ease. I continued a friendly conversation while asking John questions about the computer. I would compare the answers tomorrow with the responses I obtained today.

2.1. Initial Meeting. I asked how many people at home used the computer. John rather quickly volunteered a great deal of information: John was the main user and used the computer to read MSN mail, surf the web and play online chess. John stated his wife hated the computer and would not be caught dead using it. Occasionally, his daughter Amy would download pictures from her camera. She might even chat with friends but he really did not know. Amy had moved out sometime back and had not been around much. Jack, his oldest, did not show any particular interest one way or another. The times that John had tried to show Jack something, he stated he wasn't interested.

I started inquiring about more specific items. I stated that I hated XP in order to see John's reaction. John said he had no problem with XP that he could re-call, except for last year. I tried to install Service Pack 2 and his computer locked up and would not work. John went on to say, he did a several things, many of which he could not remember. He did remember reloading Service Pack 1 over the top of what had already been loaded. I kidded John

© SANS Institute 2006, Author retains full rights.

that he was some sort of Windows SA. He quickly countered, “Hardly. Those were the worst three weeks of the year. I did not know what else to do.”

I continued to ask more questions about John’s online activity and computer game activity. John stated he tried some of those money-making deals by visiting websites and building up points but that had not done much. He just surfed, read mail and played an occasion game of online chess.

I asked John what has caused him to seek help with his computer. John recounted that ever since last year, after the Service Pack 2 incident, the computer seemed to get worst at times. He also stated that when he almost had made his mind up to do something, the computer would straighten up and fly right, so to speak. John also stated that he had put this off long enough and now was as good as anytime to get his computer fixed. We concluded our conversation with my request for John to write down everything that he had done to the computer and when. I instructed him not to leave out the smallest detail. I stated I would need this information tomorrow at our meeting.

2.2. Information Acquired. I quickly decided to summarize the information that I had obtained from John. I would use this to build my questions for tomorrow’s meeting. My initial assessment of the information was as follows:

1. John - no computer training, tries to follow instructions but does not really understand some of the more complex computer instructions.
2. Mary Beth - potential sleeper (tries to seem more ignorant of computers than she is), may not want others to know she uses the computer?
3. Amy – novice computer user, no training, no experience, seldom uses computer.
4. Jack – neophyte, no training, no experience, shows no interest.
5. OS Windows XP SP1, loaded on top of failed SP2 installation.
6. Computer would slowdown and would not allow user to do anything.
7. MSN E-mail account.
8. John – participates in click-for-cash schemes, probably has Spyware.
9. John – plays online games, another opportunity for malware.

2.3. Investigative Questions. Questions for tomorrow’s meeting.

1. Did John create accounts and passwords for his family?
2. Does everyone share the same E-mail account?
3. Who is John’s ISP and what type of connection?
4. Need to know about backups. Probably none.
5. Need to determine AV and Spyware software use.

© SANS Institute 2006, Author retains full rights.

6. Does the slowdown occur at any particular time or is the slowdown associated with any particular action on John's part?

7. How does John shut down the computer?

8. How often does John defrag the hard drive?

9. Has John added any software or made any hardware changes?

2.4. Initial Assessment. The system probably has never been properly maintained. Due to the level of user experience and apparent disregard for safe surfing, there is a good likelihood that some form of Spyware or malware is present. Since no apparent maintenance has been performed, the system could be suffering disk fragmentation problems or periodic hardware malfunctions, depending upon the age of the system.

2.5. Second Meeting. I met John at his residence the next day at 5:30. We proceeded into his home office where the computer was located. The room was neatly organized and the computer desk and computer were uncluttered. There existed a tray of 3-½ inch floppies, all neatly labeled. It did not appear that John was someone who was constantly loading and removing software. John reached to turn the computer on and I stopped him. I stated that would not be necessary. I told John that I had a few questions for him and that I would then take the computer for a couple of hours. I asked John if he had the information I requested from yesterday. John stated that he did not, but he would get it as soon as possible. John looked a little distressed and I inquired as to why. John stated that he had something to do on the computer and that I could take the computer tomorrow for as long as I needed. I agreed and stated that I would be by tomorrow morning to pick up the computer.

2.6. More Information Acquired. I then proceeded to ask the questions on my list. All of John's answers now were short and curt. I maintained a calm methodical approach to the questions. John answered the questions as follows:

1. Did John create accounts and passwords for his family? *No!*

2. Does everyone share the same E-mail account? *Not really.*

3. Whose is John's ISP and what type of connection? *DSL through the Phone Company.*

4. Need to know about backups? *Nope*

5. Need to determine AV and Spyware software use. *Yes, he had virus software. I could check it out.*

© SANS Institute 2006, Author retains full rights.

6. Does the slowdown occur at any particular time or is the slowdown associated with any particular action on John's part? *I don't know.*

7. How does John shut down the computer? *Start menu and shutdown.*

8. How often does John defrag the hard drive? *What is that? Oh! Nope!*

9. Has John added any software or made any hardware changes? *No hardware changes, maybe a game or two.*

2.7. Secondary Assessment. I noticed a discernable change in John's attitude. John was no longer chatty. I believe John was not expecting me to take the computer, and this appeared to have concerned him. I decided not to press the issue. I had the information I needed to begin. (Key point: Unless you have a contractual obligation with the client for information and services, do not expect prompt consideration to your requests. Always have an alternate approach, such as imaging the computer!)

So far, I had obtained about all the specifics I could get from the client. I assessed the computer skills of the users of the computer. There does not appear to be any nefarious activity of concern, such as a hacking teenager, or a chat room and IM addict. Probably, the most dangerous activity was the web surfing. The AV and Spyware software should prevent any harmful actions, provided it was enabled and up-to-date. There were no apparent hardware changes. Software games can be quite problematic coupled with the aborted XPSP2 upgrade and XPSP1 reload.

3. Computer Collection. I picked the computer up the next morning as agreed. I photographed the computer work area and computer cabling. I took the computer back to my shop and removed the case covers. I photographed the inside of the computer. I removed the hard drive and photographed the hard drive and recorded the hard drive model and serial number.

Maxtor Model 2R015H1, SN R148TP2C,

15GB hard drive LBA 29207520 operating at 5400 RPM.

4. Digital Data Collection. I installed a sanitized and formatted disk drive into my forensic workstation. I connected the hard drive to the Forensic Workstation's USB drive adapter and waited for the system to identify the new controller and attached drive. The controller registered as sda with one logical device sda1. I viewed the drive's partition information with mmls. (This command integrates the drive partition table and prints out the contents.) Three slot entries were discovered.

Slot 00 Primary Table (#0) contained 1 Sector

Slot 01 Unallocated Starting sector 1 ending sector 62 with Length of 62

Slot 02 NTFS(0x7) Starting sector 63 ending sector 29286494 length 29286432

© SANS Institute 2006, Author retains full rights.

The partition table information looked fine. I created an image of the unallocated partition with dd on the sanitized hard drive.

dd if=/dev/sda of=jack_sda_part1 skip=1 count=62 bs=512

I then created an image of the whole drive with dd.

dd if=/dev/sda of=jack_sda_dd bs=512

I allowed dd to determine the end of drive and report the number of sectors read and written.

dd reported 29286494 in and out

I then proceeded to load the image into Autopsy and generate an Md5sum value of the image. Next, I selected the file analysis mode and just started browsing the directories on the hard drive. I was attempting to get a feel for how the system was configured and used by John. I was immediately surprised at the number of files that were showing as deleted; an interesting observation was that adjacent entries indicated identical file sizes. This was not for one or two entries per directory but several entries. I noted this characteristic as something I would have to research.

I shifted back to the root directory. I wanted to determine the number of user accounts that been created on the system. The basic user account was in place, but it was duplicated as "John.John." The same duplication occurred for the other accounts, such as administrator and administrator.John. Additionally, there were two local service and network service accounts.

I decided to browse the user directories. I chose to inspect the "Local Settings" as most people overlook this directory. I looked at the "Temporary Internet Files" directory in each user account. Each directory had multiple temporary directories. The temporary directories contained the normal files created when people surf the network. I was really not interested in John's internet habits. However, I did need to know if John visited sites of questionable content, such as hacking sites, pornography or hate sites. I viewed the Internet Cookies and noticed that John visited pornography sites quite frequently. Next, I needed to determine what software was installed on the computer.

Upon going to the Program Files directory, I noticed that John did in fact have a Norton Anti-Virus program and a Webroot Spyware program. From a casual inspection of those files' date and time stamps, the programs were recently updated, within the past couple months. I obtained a list of the software programs and proceeded to research the programs of which I had little knowledge. The list was quite extensive. There were 54 program directories;18 of the programs I did not recognize. I spent a few minutes searching the Web and found sufficient information about the programs to allay any worries.

© SANS Institute 2006, Author retains full rights.

I decided not to be overly concerned with all the files on the computer, as I did not have a baseline with which to compare files. Also, John had stated that he had no backups. I roughly categorized the files as follows:

Graphics	bmp, gif, jpeg, png, pnf, cursors, fonts
Text	text, inf, xml, Unicode, other ASCII files
Multimedia	audio, video
Executables	msdos (com, exe), windows exe, dll files
Unknown	data files
Applications	archives, compressed, tar, MS Applications

5. Data Identification and Reduction. I had already established the basic exclude database and NSRL database. The hacker tools were extracted for the NSRL RDS_D and were used to create an Alert database.

There were 1720 archives or compressed files that needed to be extracted as part of the examination process. I decided to write a script to perform this function while addressing other research items. When Sorter completed the data extraction and categorization function, roughly 71,752 files were extracted. The only problem was that only 12,201 were excluded and the remaining files failed to match any reference in the Exclude database. I had already decided not to be concerned with the 27,000 graphic files and 10,000 text files. The major concern was that I had over 35,000 files to resolve.

These were too many files to reduce to a manageable set. I contacted John and arranged to pick up all his software disks and CD's. I would have to make an extract exclude database from John's media. Hopefully, this would narrow the margin down considerably.

John's media was used to create the newexclude.txt file that contained over 25,000 additional entries. I had to create a script to process the newexclude database. Sorter does not have the ability to re-process for partial sets. After creating the newexclude database, the number of unresolved executables was greatly reduced. The 2431 executable programs were reduced to 120 files and 74 of those referenced dead inodes. The Windows executables went from 805 files to 127 files of which 37 were dead inodes. Of the remaining files, over 100 were Windows shortcut lnk files. The newexclude database greatly reduced the number of file to be considered. I still had 5 tasks to perform, and two were rather large (reviewing the graphics and text files).

6. Examination. Since I already knew John visited pornography sites from viewing the Cookies in Internet Explorer, I decided to view the Internet Cache index.dat files as well. This would reaffirm John's internet usage. Almost

© SANS Institute 2006, Author retains full rights.

every time John used the computer, he visited pornography sites. Since this was done so frequently, I decided to check for Child Pornography. I had obtained about 150 graphics picture md5sum's provided by Law Enforcement agencies to the HashKeeper database. I extracted the md5sum values from those specialty sets and ran a comparison of the values against the Jpegs and gifs md5sum values. This can be done rather easily with a script and the hfind command in SleuthKit. You create a file with just the md5sum values and that is input to hfind and your database.

Hfind will process each entry, print the found entries and identify entries for which a Hash was not found. The only difficult process is to convert the not found hashes back into filenames. That is easily done by creating an IDX file with the md5sum values of your files and running the not found entries against the original table. It seems complicated, but it's really a simple script.

The results of the Child Pornography search was that no hits were found. This was a good thing. If I had found Child Pornography images, I could have turned that information over to Law Enforcement. I would not have broken any laws or violated any privacy laws. When John turned the computer over to me, John gave up any reasonable right to privacy.

7. Analysis. Several issues were still unresolved. One was the rather large number of dead inodes and inodes referencing the same data structure. When I performed the md5sum comparison, a large number of inodes reported the identical md5sum value for numerous files. In some cases, there were 10 identical references to the same data structure. Based upon the total number of available inode entries and the number of allocated entries, John's hard drive was approximately 40% filled with just over 6gig of data.

The system did possess 1 file that is associated with the Trojan Trojan.m00, sometimes referred to as the BloodHound Exploit 13. Although Trojan.m00 was present, there was no indication that the system was infected. This Trojan supposedly occurred in February 2005. This time frame matched the date and times of the m00.exe file in "C:\" directory and the start[1].exe 12 Feb 2005 1402 located in "C:\Documents and Settings\John\Local Settings\Temporary Internet Files\Content.IE\WRKL25WF\start[1].exe". These files have identical m5dsum values. However, the Trojan was not found to be present in memory. Four unique strings (ja0ara8aza, !$DAMdUU, Q aba(a, SQRVWU) were extracted from the m00.exe binary, and the pagefile.sys file was searched for each string yielding no results. Additionally, the registry hives (sam, system, software, security) located in "C:\Windows\System32\Config" were dumped and searched for m00.exe or start[1].exe. Also the registry files in the users directories UsrClass.dat and NTUSER.DAT were dumped and searched also. All the Cookies directories were searched for entries near to 12 Feb 2005 1402. The last site visited before m00.exe was recorded on the system was www.galsteam.com at 12 Feb 2005 1357.

© SANS Institute 2006, Author retains full rights.

The next task was to transfer the image to a hard drive and operate the image in a live SandBox environment. This would allow the system to operate, but I could control the network activity. After configuring the SandBox, I installed John's hard drive into a small system. John's system was running an AMD Thunderbird Athlon processor at 700mhz with 512 meg of ram. Upon configuring a system close to that original set up, I started the system with John's image. The system did some initial reconfiguration because of the motherboard, processor and bus differences. I did not feel these would prove detrimental to the test. The system booted and reconfigured itself as normal, but the hard disk light stayed on for almost 5 minutes after the Windows XP user desktop was presented.

I went to the start menu, chose programs, accessories, system tools, and disk defrag. When disk defrag starts, the first step is to analyze the disk. This took several minutes and reported 40 percent fragmented and the drive at 50% capacity. This undoubtedly would cause some performance issues. I closed the disk defrag utility and watched my firewall for any activity. The only traffic I observed was the periodic Windows broadcast. I allowed the system to run for several hours. I occasionally moved the mouse or typed commands on the keyboard to determine system responsiveness. I did not notice any unresponsive behavior.

7. Review and Report.. There are not definitive results or evidence to explain the sluggish behavior of the system. John's Norton Anti-Virus updates were several months old, 15 Feb 2006. The Webroot Spyware software had not been updated for several months. There are no Norton Anti-Virus entries concerning an infestation, and Webroot entries reflected 15 Feb 2006 only entries. There will be no report due to the client's request and cost overruns.

8. Recommendations. Three possibilities were offered to the client.

8.1. A short-term solution would be to defrag the hard drive and monitor system performance. If the situation does not degrade significantly, then this may work indefinitely.

8.2. A better solution would be to wipe and sanitize the hard drive, reformat the drive, and reinstall the operating system. Then reload the Anti-Virus software and Spyware software. After each of these applications have been updated, then proceed with remaining software installation.

8.3. If John is going to continue to browse sites of questionable content, John must keep his Anti-Virus and Spyware software up-to-date. I recommend that John should stay away from sites offering questionable content (hacker sites, Search and Click schemes, P2P software [Kazaa, eDonkey], and pornography sites.)

9. Final Note. This investigation was initially allotted 16 hours of consultant time. This task consumed over 29 hours of processing time and 24 hours of analysis time. The biggest expenditure of time was processing the hard drive files and having to re-process due to not having a proper

© SANS Institute 2006, Author retains full rights.

the hard drive files and having to re-process due to not having a proper baseline. Due do the over budget concerns, several tasks were left unresolved.

1. I would like to have performed more research on Norton Anti-Virus and Webroot to determine if these products did in fact recognize and report the Trojan.

2. I would have wanted to experiment with the client's computer to determine the actual cause of the slowdown.

I personally suspect that due to the age of the system and components, the problem possibly is a cooling issue. I have experienced similar problems on older equipment.

© SANS Institute 2006, Author

© SANS Institute 2006, Author retains full rights.

13. Appendix.

Customized Configuration Files

```
Archives.sort
#Category Archives Cut Line
#save this snippet as archives.sort in your sleuthkit/share/sorter directory

#category   archives
category    archives  Zip archive data
ext       zip,jar   Zip archive data
ext       wmz    Zip archive data

category    archives  tar archive
ext       tar    tar archive

category    archives  Microsoft Cabinet
ext       cab    Microsoft Cabinet File

category         archives  compress data
ext              gz,tgz    gzip compressed data
ext           Z    compress'd data
ext       bz2    bzip2 compressed data
ext       bz   bzip compressed data

category    archives  RPM
ext       rpm    RPM

category    archives  cpio archive

category    archives  ARC archive data
ext       arc    ARC archive data

category    archives  LHa archive data
ext       lha    LHa archive data
ext       lzh    LHa archive data

category    archives  shell archive text
ext       shar   shell archive text

category    archives  uuencoded or xxencoded text
ext       uue    uuencoded or xxencoded text
ext       uu   uuencoded or xxencoded text
ext       bhx    uuencoded or xxencoded text
ext       xxe    uuencoded or xxencoded text
ext       xx   uuencoded or xxencoded text

category    archives  BinHex binary text
ext       hqx    BinHex binary text

category    archives  StuffIT Archive
ext       sit    StuffIT Archive

category    archives  RAR Archive data
ext       rar    RAR Archive data

category    archives  ARJ Archive data
ext       arj    ARJ Archive data
# The below types to be implemented when source files are available for testing
#B64,LZW,LBR,MSX,PAK,PIT,TAZ,_Q_,ZOO
```


© SANS Institute 2006, Author retains full rights.

```
#Category Archives Cut Line

Composite.sort

##########-----Composite.sort----Cut Line---------------####################
#Category composite
category composite archive
category composite compress
category composite cabinet
category composite rpm
category composite filesystem
#need for file to recognize MS Backup files bkf
##########-----Composite.sort----Cut Line---------------####################

Images.sort
##########-----Images.sort----Cut Line---------------##################
#
#Category Images
category    images      image data
category    images      graphic image

category    JPG         JPEG image data
ext       jpg,jpeg,jpe     JPEG image data

category    GIF         GIF image data
ext       gif         GIF image data

category    TIF         TIFF image data
ext       tif         TIFF image data

category    PCX         PCX(.*?)image data
ext       pcx         PCX(.*?)image date

category    PNG         PNG image data
ext       png         PNG image data

category    BMP         bitmap data
ext       bmp         PC bitmap data
#
##########-----Images.sort----Cut Line---------------##################

Windows.sort

##########-----Windows.sort----Cut Line---------------##################
#########################################################################
# Multimedia
#########################################################################
# Audio
category    audio  Playlist

# Audio
category    audio     Winamp
ext       avs    Winamp plug in
category      audio     WAVE audio
ext       wav    WAVE audio
category      audio     Microsoft ASF
ext       wmv    Microsoft ASF
ext       wma    Microsoft ASF
category      audio     MPEG ADTS
ext       WAV    MPEG ADTS, layer I, v1
ext       wav    MPEG ADTS, layer I, v1
category    audio     AVI
```


© SANS Institute 2006, Author retains full rights.

```
ext       avi          AVI
category    audio     Playlist
ext       wpl    Windows Media Player Playlist

category    midi      MIDI
ext       mid,rmiMIDI

category    MP3     MP3
ext       mp3     MP3

# Images
category    JPEG    JPEG image data
ext       jpg,jpeg,jpe   JPEG image data

category    GIF     GIF image data
ext       gif     GIF image data

category    TIF     TIFF image data
ext       tif     TIFF image data

category    PNG     PNG image data
ext       png     PNG image data

category    BMP     bitmap data
ext       bmp     PC bitmap data

category    Fonts   font
ext       ttf     true type font

# Video
category    video     RealMedia
ext       rm    RealMedia

category    video     Macromedia Flash data
ext       swf     Macromedia Flash data

category    ICM      Microsoft ICM Color Profile
ext       icm      Microsoft ICM Color Profile
##########################################################################
# archive & compression
##########################################################################

category    ZIP    Zip
ext       zip,jarZip archive data
ext       wmz     Zip archive data

category    TAR     tar
ext       tar     tar archive

category    MSCab     Cabinet
ext       cab     Microsoft Cabinet File

category    archivearchive

category       database  DB
ext            db        Berkeley DB

##########################################################################
# compression
##########################################################################
category       compress    compress
ext            gz,tgz      gzip compressed data
```


© SANS Institute 2006, Author retains full rights.

```
ext           Z           compress'd data

###############################################################################
# Executables
###############################################################################
category    msdosexec MS\-DOS executable
ext       exe,dll,com MS\-DOS executable
ext       ocx,sys,tlb MS\-DOS executable
ext       drv,cpl,scr MS\-DOS executable
ext       ax   MS\-DOS executable
ext       386,acm,flt MS\-DOS executable
ext               fon,lrc,vxd MS\-DOS executable
ext       x32    MS\-DOS executable
category    msdosexec executable MS\-DOS
ext       exe    MZ executable MS\-DOS
ext       com    MZ executable MS\-DOS

category    winexecPE executable MS Windows
ext       exe,dll,com PE executable MS Windows
ext       ocx,sys,acm PE executable MS Windows
ext       tlb,drv,scr PE executable MS Windows
ext       cpl,ax,vdx  PE executable MS Windows
ext       fon,rll,tsp PE executable MS Windows
category    exec   NE executable MS Windows
ext       exe,dll,com NE executable MS Windows
ext       ocx,sys,acm NE executable MS Windows
ext       tlb,drv,scr NE executable MS Windows
ext       cpl,ax,vxd  NE executable MS Windows
ext       fon,tsp     NE executable MS Windows

category    exec   relocatable
ext       dll    relocatable
category    exec   batch file
ext       bat    batch file
ext       nt   MS-DOS batch file text
ext       cmd    MS-DOS batch file text
# source code
category    exec   MSVC program database
ext       pdb    MSVC program database
category    exec   \sscript

###############################################################################
# Java

category    exec   class data
ext       class    Java class data


###############################################################################
category    exec   object
ext       o    object

category    exec   python compiled

category    exec   MS Windows shortcut
ext       lnk    shortcut

###############################################################################y
# Images
category    icon   icon resource
ext       ico    ms\-windows icon resource
```


© SANS Institute 2006, Author retains full rights.

```
category    cursor cursor
ext       cur    ms\-cursor
ext            ani         animated cursor

###########################################################################
category    MSmbox Outlook binary email folder
ext       pst    Outlook binary email folder

category    MSdocs Microsoft Office Document
ext       doc,dot   Microsoft Office Document
ext       msc,pcbMicrosoft Office Document
ext       ppt,potMicrosoft Office Document
ext       xls    Microsoft Office Document
ext       msi    Microsoft Office Document
category    MSdocs Microsoft Word Document
ext       doc    Microsoft Word Document
category    MSdocs conversion doc
ext       wpc    conversion doc

category    MSss   Microsoft Excel Worksheet
ext       xls,xlt     Microsoft Excel Worksheet
ext       cvs         Microsoft Excel Worksheet

# MS Access DB
category    MSdb   Microsoft Access Database
ext       mdb    Microsoft Access Database

category    PNF    PNF
ext       pnf    PNF
ext       PNF    PNF
ext       pnf    PNF Windows

category    documents Rich Text Format
ext       rtf    Rich Text Format
category    documents document
ext       ps,eps PostScript document

category    InternetExplorer Microsoft Internet Explorer Cache File
ext       dat    Microsoft Internet Explorer Cache File Version Ver 5.2

# Corel & Word Perfect
category    Coreldocs Corel\/WP
ext       wpg,wpd,shw Corel\/WP

# Lotus
category    Lotus    Lotus 1\-2\-3
ext       wb2    Lotus 1\-2\-3
ext       wk4    Lotus 1\-2\-3

# Adobe
category    AdobePDF  PDF document
ext       pdf    PDF document


###########################################################################
#Unicode
###########################################################################
category    unicodeUniCode
ext       mof    MOF,MLF UniCode File
ext       mfl    MOF,MLF UniCode File
###########################################################################
# HTML
```


© SANS Institute 2006, Author retains full rights.

```
#############################################################################
category    html    HTML document text
ext       hhk     HTML document text
ext       htm,htaHTML document text
ext       html,css  HTML document text
#############################################################################
# Text
#############################################################################
category    text    ASCII(.*?)text
ext       txt     ASCII(.*?)text
ext       log     ASCII(.*?)text
ext       h    ASCII(.*?)text
ext       sh,csh ASCII(.*?)text
ext       conf    ASCII(.*?)text
ext       inc     ASCII(.*?)text
ext       wpl     ASCII(.*?)text
ext       xdr     ASCII(.*?)text
ext       js   ASCII(.*?)text
ext       sam     ASCII(.*?)text
ext       scf     ASCII(.*?)text
ext       scp     ASCII(.*?)text
ext       gpd     ASCII(.*?)text
ext       dun     ASCII(.*?)text
ext       isp     ASCII(.*?)text
ext       XML     ASCII(.*?)text
ext       DTD     ASCII(.*?)text
ext       reg     ASCII(.*?)text
ext       asp     ASCII(.*?)text
ext       vbs     ASCII(.*?)text
ext       xdr     ASCII(.*?)text
ext       xsl     ASCII(.*?)text
ext       c,cpp,h,js  ASCII(.*?)text
ext       mof     ASCII(.*?)text
ext       sql     ASCII(.*?)text
ext       htt     ASCII(.*?)text
ext       hxx     ASCII(.*?)text
ext       cpx     ASCII(.*?)text
ext       obe     ASCII(.*?)text
ext       ini,inf     ASCII(.*?)text
ext       srg,depASCII(.*?)text
ext       htm     ASCII(.*?)text
ext       htm,cssASCII(.*?)text
ext       css     ASCII(.*?)text

category      text        character data
ext           txt         character data

category    text    ISO\-8859(.*?)text
ext           txt         ISO\-8859(.*?)text
ext       ini       ISO\-8859(.*?)text
ext       inf     ISO\-8859(.*?)text

category    text    exported SGML document text
ext       htm     exported SGML document text

category    text    \ssource

#############################################################################
# INF
#############################################################################

category    inf     Lisp
```


© SANS Institute 2006, Author retains full rights.

```
ext       inf    Lisp/Scheme program text

###############################################################################
# XML
###############################################################################
category    XML    XML
ext       xml    XML Template
ext       xml    XML Mapping
ext       xml    XML Document
ext       xdr    XML document text
ext       xsl    XML document text
ext       msc    XML document text
ext       manifest  XML document text
ext       dtd    XML document text
ext       Policy XML document text

###############################################################################
# Other
###############################################################################
# Disk
category    disk   boot sector
category    disk   filesystem data

# Crypto
category    crypto PGP
ext       asc    PGP armored

# Postscript Printer Description
category    system PPD file
ext       ppd    PPD file

# 'file' reports 'data' for all unknown binary files
# do not bother with extensions with this
category    data   ^data$
# category    ignore      raw G3 data, byte\-padded

###############################################################################
# System
category    system Help Data
ext       hlp    Windows Help Data
ext       chm    Windows Help File

category    system Registry file
ext       dat,log,sav Registry file

category    system MS\-Windows shortcut
ext       lnk    MS\-Windows shortcut

category    system Internet shortcut
ext       url    Internet shortcut

category    system hyperterm
ext       ht   hyperterm
#
##########-----Windows.sort----Cut Line----------------###################

Foremost.conf

##############-------Foremost.conf----CUT LINE-------
################################
# date 1 Jun 06
# Foremost configuration file
```


© SANS Institute 2006, Author retains full rights.

```
#-----------------------------------------------------------------------
#
# The configuration file is used to control what types of files foremost
# searches for. A sample configuration file, foremost.conf, is included with
# this distribution. For each file type, the configuration file describes
# the file's extension, whether the header and footer are case sensitive,
# the maximum file size, and the header and footer for the file. The footer
# field is optional, but header, size, case sensitivity, and extension are
# not!
#
# Any line that begins with a '#' is considered a comment and ignored. Thus,
# to skip a file type just put a '#' at the beginning of that line
#

# Headers and footers are decoded before use. To specify a value in
# hexadecimal use \x[0-f][0-f], and for octal use \[0-3][0-7][0-7].  Spaces
# can be represented by \s. Example: "\x4F\123\I\sCCI" decodes to "OSI CCI".
#
# To match any single character (aka a wildcard) use a '?'. If you need to
# search for the '?' character, you will need to change the 'wildcard' line
# *and* every occurrence of the old wildcard character in the configuration
# file. Don't forget those hex and octal values! '?' are equal to 0x3f and
# \063.
#
# If you would like to extract files without an extension enter the value
# "NONE" in the extension column (note: you can change the value of this
# "no suffix" flag by setting the variable FOREMOST_NOEXTENSION_SUFFIX
# in foremost.h and recompiling).
#
# The REVERSE keyword after a footer instructs foremost to search backwards
# starting from [size] bytes in the extraction buffer and working towards the
# beginning. This is useful for files like PDF's that have multiple copies of
# the footer throughout the file.  When using the REVERSE keyword you will
# extract bytes from the header to the LAST occurence of your footer within the
# window determined by the [size] of your extraction.
#
# The NEXT keyword after a footer instructs foremost to search forwards for data
# that starts with the header provided and terminates or is followed by data in
# the footer -- the footer data is not included in the output.  The data in the
# footer, when used with the NEXT keyword effectively allows you to search for
# data that you know for sure should not be in the output file.  This method for
# example, lets you search for two 'starting' headers in a document that doesn't
# have a good ending footer and you can't say exactly what the footer is, but
# you know if you see another header, that should end the search and an output
# file should be written.

# To redefine the wildcard character, change the setting below and all
# occurrences in the formost.conf file.
#
#wildcard  ?

#    case size header      footer
#extension   sensitive
#
#-----------------------------------------------------------------------
# EXAMPLE WITH NO SUFFIX
#-----------------------------------------------------------------------
#
# Here is an example of how to use the no extension option. Any files
# containing the string "FOREMOST" would be extracted to a file without
# an extension (eg: 00000000,00000001)
#      NONE     y      1000     FOREMOST
```


© SANS Institute 2006, Author retains full rights.

```
#
#---------------------------------------------------------------------
# GRAPHICS FILES
#---------------------------------------------------------------------
#
#
# AOL ART files
   art  y  150000  \x4a\x47\x04\x0e \xcf\xc7\xcb
   art  y  150000  \x4a\x47\x03\x0e \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
   gif  y  155000000 \x47\x49\x46\x38\x37\x61   \x00\x3b
   gif  y  155000000 \x47\x49\x46\x38\x39\x61   \x00\x00\x3b
   jpg  y  200000000 \xff\xd8\xff\xe0\x00\x10   \xff\xd9
#
# PNG   (used in web pages)
   png  y  200000  \x50\x4e\x47?  \xff\xfc\xfd\xfe
#
#
# BMP   (used by MSWindows, use only if you have reason to think there are
#       BMP files worth digging for. This often kicks back a lot of false
#  positives
#
   bmp  y  100000  BM??\x00\x00\x00
#
# TIF
   tif  y  200000000 \x49\x49\x2a\x00
#
#---------------------------------------------------------------------
# ANIMATION FILES
#---------------------------------------------------------------------
#
# AVI (Windows animation and DiVX/MPEG-4 movies)
   avi  y  4000000 RIFF????AVI
#
# Apple Quicktime
#    Some users have reported that when using these headers that the
#    headers repeat inside the files. This can generate lots of smaller
#    output files. You may want to consider using the -q (quick mode)
#    flag to avoid this problem.
#
   mov  y  4000000????????\x6d\x6f\x6f\x76
   mov  y  4000000????????\x6d\x64\x61\x74
#
# MPEG Video
   mpg  y  4000000\x00\x00\x01\xba \x00\x00\x01\xb9
   mpg     y   4000000\x00\x00\x01\xb3 \x00\x00\x01\xb7
#
# Macromedia Flash
#fws y  4000000FWS
#
#---------------------------------------------------------------------
# MICROSOFT OFFICE
#---------------------------------------------------------------------
#
# Word documents
#
# look for begin tag and then wait until the next one (NEXT TAG) -- usually word
documents
# and other Ole2 structured storage files are 'near' each other.  Just make the file
# size large enough to catch our maximium size file.  Look in the audit file to see
if any were chopped.
```


© SANS Institute 2006, Author retains full rights.

```
#
   doc  y  12500000  \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00
\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 NEXT
   doc  y  12500000  \xd0\xcf\x11\xe0\xa1\xb1
#
# Outlook files
   pst  y  400000000 \x21\x42\x4e\xa5\x6f\xb5\xa6
   ost  y  400000000 \x21\x42\x44\x4e
#
# Outlook Express
   dbx  y  4000000\xcf\xad\x12\xfe\xc5\xfd\x74\x6f
   idx  y  4000000\x4a\x4d\x46\x39
   mbx  y  4000000\x4a\x4d\x46\x36
#
#------------------------------------------------------------------
# WORDPERFECT
#------------------------------------------------------------------
#
#wpc y  100000 ?WPC
#
#------------------------------------------------------------------
# HTML
#------------------------------------------------------------------
#
   htm  n  50000   <html      </html>
#
#------------------------------------------------------------------
# ADOBE PDF
#------------------------------------------------------------------
#
   pdf  y  5000000%PDF  %EOF\x0d REVERSE
#
#
#------------------------------------------------------------------
# AOL (AMERICA ONLINE)
#------------------------------------------------------------------
#
# AOL Mailbox
   mail y  500000  \x41\x4f\x4c\x56\x4d
#
#
#
#------------------------------------------------------------------
# PGP (PRETTY GOOD PRIVACY)
#------------------------------------------------------------------
#
# PGP Disk Files
#  pgd  y  500000 \x50\x47\x50\x64\x4d\x41\x49\x4e\x60\x01
#
# Public Key Ring
#  pgp  y  100000 \x99\x00
# Security Ring
#  pgp  y  100000 \x95\x01
#  pgp  y  100000 \x95\x00
# Encrypted Data or ASCII armored keys
#  pgp  y  100000 \xa6\x00
# (there should be a trailer for this...)
#txt y  100000 -----BEGIN\040PGP
#
#
#------------------------------------------------------------------
# RPM (Linux package format)
```


© SANS Institute 2006, Author retains full rights.

```
#-----------------------------------------------------------------
rpm  y  1000000\xed\xab
#
#
#-----------------------------------------------------------------
# SOUND FILES
#-----------------------------------------------------------------
#
  wav     y 200000  RIFF????WAVE
#
# Real Audio Files
  ra y  1000000\x2e\x72\x61\xfd
  ra y  1000000.RMF
#
#-----------------------------------------------------------------
# WINDOWS REGISTRY FILES
#-----------------------------------------------------------------
#
# Windows NT registry
dat  y  4000000regf
# Windows 95 registry
dat  y  4000000CREG
#
#
#-----------------------------------------------------------------
# MISCELLANEOUS
#-----------------------------------------------------------------
#
  zip  y  10000000  PK\x03\x04  \x3c\xac
  java y  1000000\xca\xfe\xba\xbe
#
#-----------------------------------------------------------------
# ScanSoft PaperPort "Max" files
#-----------------------------------------------------------------
      max   y     1000000    \x56\x69\x47\x46\x6b\x1a\x00\x00\x00\x00
\x00\x00\x05\x80\x00\x00
#-----------------------------------------------------------------
# PINs Password Manager program
#-----------------------------------------------------------------
#      pins  y     8000     \x50\x49\x4e\x53\x20\x34\x2e\x32\x30\x0d
#
###############-------Foremost.conf----CUT LINE-------
################################
```

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

14 Index.

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

Attachment A. Investigation Activity Spreadsheet.

Type of Activity	Criminal	Liturgical	Non-liturgical
Child Exploitation	x	x	
Child Pornography	x	x	
Company policy abuse		x	x
Computer abuse	x	x	x
Viruses, Trojans, Worms	x	x	x
hacking/intrusion	x	x	x
password trafficking	x	x	x
Denial of Service	x	x	x
Web site defacement	x	x	x
Discrimination	x	x	x
Electronic Mail Spam	x	x	x
Electronic tampering			
Medical Records	x	x	x
Finanical Records	x	x	x
Commerical Business	x	x	x
Private Business		x	x
HIPAA	x	x	x
Intellectual Property	x	x	x
Trade Secrets	x	x	x
Copyright piracy	x	x	x
Counterfeiting	x	x	
Currency	x	x	x
Credit Cards	x	x	x
Software	x	x	
Inapproriate E-mail	x	x	x
Inapproriate E-mail use		x	x
Information Theft	x	x	x
Internet Fraud	x	x	x
Internet Gambling	x	x	x
Internet Harassment	x	x	x
Internet Usage - Extreme		x	x
Non-work related use of computer resource		x	x
Sarbanes-Oxley	x	x	x
Sexual Harassment	x	x	
Use of computer in any criminal crime	x	x	

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

Attachment B. Master Crime Category Matrix Spreadsheet.

Internet Computer Fraud

- **Advance Fee Fraud Schemes**
- **Business/Employment Schemes**
- **Counterfeit Check Schemes**
- **Credit/Debit Card Fraud**
- **Freight forwarding/Reshipping**
- **Identity theft**
- **Investment Fraud**
- **Non-delivery of Goods/Services**
- **Phony Escrow Services**
- **Ponzi/Pyramid Schemes**
- **Spoofing/Phishing**
- **Online Auction fraud**
- **Identity theft**
- **Financial**
- **Telecommunications fraud,**

Traditional Crimes

- **Fraud**
- **Theft**
  - **Monetary**
  - **Service**
  - **Data/Information**
- **Harassment**
- **Child Pornography.**
- **Counterfeiting of currency**
- **Internet bomb threats**
- **Solicitation to commit crime.**

Harassment Offenses

- **Online Harassment**
- **Cyberstalking**
  - **Sending harassing or threatening messages**
    - **E-mail**
    - **Instant Messaging**
    - **Posting messages on websites or chat rooms.**
- **Spam – unwanted and uninvited electronic communications**

Child Pornography

- **Transmission of media that exploits children.**
- **Solicitation to commit sexual crimes against minors**

Online Pornography

- **Using computer resources to distribute illegal media of and to minors**
- **Engaging in actions to sexually exploit children**

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

	Distributing child pornography of any form to a minor.
Crimes involving Use of Computer	
	Phishing
	Unauthorized Access
	Denial of Service
	Computer Invasion of Privacy
	Spam
	Malicious Programs/Viruses
	Cyberterrorism
	Computer Intrusion (i.e. hacking)
	Malicious Programs and Computer Resource Use
	Unauthorized Use of a Computer, Computer System, or Computer Network
	Trademark counterfeiting
	Child Exploitation and Internet Fraud matters that have a mail nexus
	Trafficking in explosive or incendiary devices or firearms over the Internet
	Wirtetapping/sniffing
Theft Computer Crimes	
	Password Trafficking
	Copyright (software, movie, sound recording) piracy
	Theft of trade secrets
	See Internet Computer Fraud
	Intellectual Property
Harmful Content Crimes	
	Child Pornography
	Exploitation Crimes
	Harassment
	Stalking
	Malicious programs
	Use of computer resources.
States with Computer Crime Laws	**Computer Crime Laws**
Arizona	
	• Computer tampering
	• Interception of wire, electronic and oral communications; installations of pen register or trap and trace device
	• Divulging communication service information
	• Possession of interception devices

© SANS Institute 2006, Author retains full rights.

	• Stored oral, wire and electronic communications; agency access; backup preservation; delayed notice; records preservation request
	• Cyberstalking
California	
	• Unauthorized access to computers
	• Cyberfraud
	• Cyberstalking
Connecticut	
	• Unauthorized access to a computer system
	• Interruption of computer services
	• Misuse of computer system information
	• Destruction of computer equipment
	• Cyberstalking
Florida	
	• Offenses against intellectual property
	• Offenses against computer equipment or supplies
	• Offenses against computer users
	• Cyberstalking
	• Using the Internet in dealing stolen property
Iowa	
	• Unauthorized access
	• Computer damage
	• Computer theft
	• Cyberstalking
Maryland	
	• False entry in public record; altering, defacing, destroying, removing or concealing public record; accessing public record
	• Credit Card Fraud
	• Unauthorized access to computers
	• Cyberstalking
Massachusetts	
	• Larceny
	• Fraudulent obtaining of commercial computer service
	• Stolen trade secrets; buying or selling
	• Unauthorized accessing of computer systems
	• Cyberstalking

New York	
	• Unauthorized use of a computer
	• Computer Trespass
	• Computer tampering
	• Unlawful duplication of computer related material
	• Criminal possession of computer related material
	• Cyberstalking
Texas	
	• Breach of Computer Security

© SANS Institute 2006, Author retains full rights.

	• **Cyberstalking** • **Assistance by Attorney General**
Virginia	• **Computer fraud** • **Transmission of unsolicited bulk electronic mail** • **Computer trespass** • **Computer invasion of privacy** • **Theft of computer services** • **Personal trespass by computer** • **Computer as instrument of forgery** • **Cyberstalking**

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.

Attachment C. Software Tool-Kit License and Version Listing Spreadsheet.

Software License and Versions

Software	Version	License
Autopsy	2.06	GPL Version 2.
SleuthKit	2.03	Common Public License Agreement
Foremost	1.10	Author - Jesse Kornblum - Government Work under "17 '
TASK	1.60	GPL Version 2.
The Coroner's Toolkit (TCT)	1.15	Copyright 1999 Dan Farmer -- distribution and use are l provided copyright notice is duplicated in all copies.
cabextract	1.10	Copyright 2000-2004 Stuart Caie - GPL Version 2.
comeforth	1.12	Copyright 2003-2004 Danamis Associates - software is free; 'edistribute or modify under the terms of the GNU Lesser ion 2.1
dcfldd	1.3.4	Author - Nicholas Harbour -- GPL Version 2
galleta	No version number.	Copyright 2003 by Keith J. Jones -- distribution an use are l provided the redistribution maintains the copyright notice er name or product name or contributors may be used to he or promote products derived from this software.
md5deep	1.5	Author - Jesse Kornblum - Government Work under "17 '
mscompress	0.3	Copyright 2000 Martin Hinner -GPL Version 2
pasco	No version number.	Copyright 2003 by Keith J. Jones -- distribution an use are l provided the redistribution maintains the copyright notice er name or product name or contributors may be used to he or promote products derived from this software.
rifiuti	No version number.	Copyright 2003 by Keith J. Jones -- distribution an use are l provided the redistribution maintains the copyright notice er name or product name or contributors may be used to he or promote products derived from this software.
Fedora Core	4.00	Releases of software from The Fedora Project are covered d User License Agreement. Copyright © 2003 Fedora Project. reserved. "Red Hat" and “Fedora” are trademarks of Red 'Linux" is a registered trademark of Linus Torvalds. All other ks are the property of their respective owners.

© SANS Institute 2006, Author retains full rights.

Attachment D Graphic File Types

Attachment D GraphicFileTypes.zip

The attachment can be obtained by clicking on the following URL:
http://members.cox.net/gerryking/Attachment_D_GraphicFileTypes.xls

© SANS Institute 2006, Author retains full rights.

Attachment E Document Types

Attachment E DocumentTypes.zip

The attachment can be obtained by clicking on the following URL:
http://members.cox.net/gerryking/Attachment_E_DocumentTypes.xls

© SANS Institute 2006, Author retains full rights.

© SANS Institute 2006, Author retains full rights.