*NIST SP800-86 Notes*

# Guide to
# Integrating Forensic Techniques into Incident Response

Authors: Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, August 2006

Computer Forensics
The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

Organizations utilize an ever-increasing amount of data from many sources.

Digital forensic techniques can be used for many purposes including
- Investigating crimes and internal policy violations
- Reconstructing computer security incidents
- Troubleshooting operational problems
- Recovering from accidental system damage

Practically every organization needs a digital forensics capability.
- To determine what events have occurred within its systems and networks

Digital forensics process
1. Collection
2. Examination
3. Analysis
4. Reporting

Computer Forensics provides detailed information concerning the analysis of :
1. Files
2. Operating systems
3. Network traffic
4. Applications.

Organizations should ensure that their policies contain clear statements addressing major forensic issues, including
- Law enforcement liaison
- System and network monitoring
- Conducting regular reviews of forensic policies and procedures.

Organizations should create and maintain procedures and guidelines for performing forensic tasks based on:

- Organization's policies
- Applicable laws and regulations,

Organizations should ensure that their
- Policies and procedures support reasonable and appropriate use of forensic tools.
- IT professionals are prepared to participate in forensic activities.

1. Establishing and Organizing a Forensics Capability

An increasing variety of data sources has helped spur the development and refinement of forensics tools and techniques. Such tools and techniques can be used for many purposes, including:
- Investigating crimes
- Reconstructing computer security incidents
- Troubleshooting operational problems
- Recovering from accidental system damage.

Over the last decade, the number of crimes that involve computers has grown, spurring an increase in companies and products that aim to help determine the who, what, where, when, and how for crimes.

However, forensic tools and techniques are also useful for many other types of tasks, such as:
- Operational Troubleshooting.
- Log Monitoring.
- Data Recovery.
- Data Acquisition
- Due Diligence/Regulatory Compliance.

Forensic process comprises the following phases:
- Collection
- Examination
- Analysis
- Reporting

Forensic Staffing
Practically every organization needs to have some capability to perform computer and network forensics. Job categories include:
- Investigators
- IT Professionals
- Incident Handlers

To perform forensic tasks, many organizations rely on a combination of their own staff and external parties.

When deciding which internal or external parties should handle each aspect of forensics, organizations should consider:

- Cost.
- Response Time
- Data Sensitivity

Incident handlers performing forensic tasks need to have a reasonably comprehensive knowledge of:

- Forensic principles
- Guidelines
- Procedures
- Tools
- Techniques
- Anti-forensic tools and techniques that could conceal or destroy data.

Each incident handling team person should be cross trained.

- Absence of any single team member should not impact the team's abilities.

Interactions with Other Teams

Individuals performing forensic actions should be able to reach out to other teams and individuals as needed for additional assistance.

To facilitate inter-team communications, each team should designate one, or more, points of contact.

Policies

Organizations should ensure that their policies contain clear statements addressing all major forensic considerations

- Contacting law enforcement
- Performing monitoring
- Conducting regular reviews of forensic policies, guidelines, and procedures.

Defining Roles and Responsibilities

Forensic policy should clearly define the roles and responsibilities of all people performing or assisting with the organization's forensic activities.

- Provides Guidance for Forensic Tool Users and Incident handlers

Supporting Forensics in the Information System Life Cycle

Many incidents can be handled more efficiently and effectively if forensic considerations have been incorporated into the information system life cycle. Examples include

- Regular system backups
- Enabling auditing on workstations, servers, and network devices
- Forwarding audit records to secure centralized log servers
- Configuring mission-critical applications to perform auditing, including recording all authentication attempts

- Maintaining a database of file hashes for the files of common OS and application deployments, and using file integrity checking software on particularly important assets
- Maintaining records (e.g., baselines) of network and system configurations
- Establishing data retention policies.

Guidelines and Procedures
An organization should create and maintain guidelines and procedures for performing forensic tasks, based on:

- Organization's policies
- Incident response staffing models
- Other teams identified as participants in forensic activities.

Goal for guidelines and procedures is to facilitate consistent, effective, and accurate forensic actions.

- The use of sound, documented, and reasonably explicable forensic techniques coupled with other methods (such as log retention and analysis).

Recommendations

- Organizations should have a computer and network forensics capability.
- Organizations should determine which parties should handle each aspect of forensics.
- Incident handling teams should have robust forensic capabilities.
- Many teams within an organization should participate in forensics.
- Forensic considerations should be clearly addressed in policies.
- Forensic policy should clearly define the roles and responsibilities of all people performing or assisting with the organization's forensic activities.
    - Organizational policies, guidelines, and procedures should clearly explain what forensic actions should and should not be performed under normal and special circumstances and should address the use of anti-forensic tools and techniques.
- Incorporating forensic considerations into the information system life cycle can lead to more efficient and effective handling of many incidents.

Performing the Forensic Process
The most common goal of performing forensics is to gain a better understanding of an event of interest by finding and analyzing the facts related to that event.

Basic forensic process phases:

| **Phase** | **Activities** |
|---|---|
| Collection | Data related to a specific event is identified, labeled, recorded, and collected, and its integrity is preserved |
| Examination | Forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity. |

| | |
|---|---|
| | Examination may use a combination of automated tools and manual processes. |
| Analysis | Involves analyzing the results of the examination to derive useful information that addresses the questions that were the impetus for performing the collection and examination. |
| Reporting | May include describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process. |

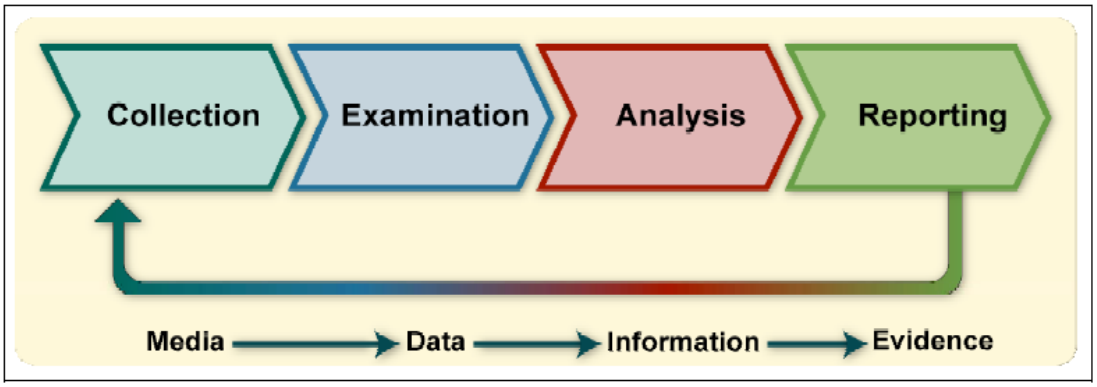



Figure 3-1. Forensic Process

Forensic process transforms media into evidence.

- Evidence could be used for law enforcement or for an organization's internal usage.

| | Transformation |
|---|---|
| First | Collected data is examined. Extracts data from media. Transforms it into a format that can be processed by forensic tools. |
| Second | Through analysis, data is transformed into information. |
| Final | Information transformation into evidence analogous to transferring knowledge into action using the information produced by the analysis in one or more ways during the reporting phase |

Data Collection

The first step in the forensic process is to identify potential sources of data and acquire data from them.

Common data sources include desktop computers, servers, network storage devices, and laptops with internal drives that accept media, such as CDs and DVDs, and also have several types of ports (e.g., Universal Serial Bus [USB], Firewire,

Personal Computer Memory Card International Association [PCMCIA]) to which external data storage media and devices can be attached.

External storage examples include

- Thumb drives
- Memory and flash cards
- Optical discs
- Magnetic disks.

Standard computer systems also contain volatile data that is available until the system is shut down or rebooted.

In addition to computer-related devices, many types of portable digital devices (e.g., PDAs, cell phones, digital cameras, digital recorders, audio players) may also contain data.

Analysts should be able to survey a physical area, such as an office, and recognize the possible sources of data.

Organizations can take proactive measures to collect data for forensic purposes.

- Most OSs can be configured to audit and record certain event types, such as authentication attempts and security policy changes, as part of normal operations.

Another helpful action is to implement centralized logging

- Certain systems and applications forward copies of their logs to secure central log servers.

Performing regular system backups allows analysts to view the contents of the system as they were at a particular time.

In addition, security monitoring controls such as intrusion detection software, antivirus software, and spyware detection and removal utilities can generate logs that show when and how an attack or intrusion took place.

Acquiring Data

After identifying potential data sources, the analyst needs to acquire the data from the sources.

Data acquisition should be performed using a three-step process:

- Develop a plan to acquire data
- Acquire data
- Verify integrity of acquired data.

Create a plan that:

Prioritizes the sources

Establishes the order in which the data should be acquired.

Important factors for prioritization include the following:

- Likely Value.

- Volatility.
- Amount of Effort Required.

Before the analyst begins to collect any data, a decision should be made by the analyst or management (in accordance with the organization's policies and legal advisors) on the need to collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings.

- Clearly defined chain of custody should be followed.
- Involves keeping a log of every person who had physical custody of the evidence, documenting the actions that they performed on the evidence and at what time, storing the evidence in a secure location when it is not being used, making a copy of the evidence and performing examination and analysis using only the copied evidence, and verifying the integrity of the original and copied evidence.

Analysts should take into account what will be done with the collected data and plan for the potential ramifications.

- In some cases, the data may be turned over to a LE or another external party for examination and analysis.
- Could result in the collected hardware being unavailable for an extended period of time. If the original media needs to be kept secured for legal proceedings, it could be unavailable for years.

Incident Response Considerations
How and when should the incident should be contained?

- Isolating the pertinent systems from external influences may be necessary to prevent further damage to the system and its data or to preserve evidence.

The organization should also consider in advance the impact that various containment strategies may have on the ability of the organization to operate effectively.

- Care should be taken to minimize disruptions to an organization's operations.

Examination
Assessing and extracting the relevant pieces of information from the collected data.

Analysis
Once the relevant information has been extracted, the analyst should study and analyze the data to draw conclusions from it.

- The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet be drawn.
- Analysis should include identifying people, places, items, and events, and determining how these elements are related so that a conclusion can be reached.
- Often, this effort will include correlating data among multiple sources.

Reporting

Process of preparing and presenting the information resulting from the analysis phase. Many factors affect reporting, including the following:

- Alternative Explanations.
- Audience Consideration.
- Actionable Information.

Recommendations

The key recommendations presented in this section for the forensic process are as follows:

- Organizations should perform forensics using a consistent process.
- Analysts should be aware of the range of possible data sources.
- Implementing centralized logging, performing regular system backups, and using security monitoring controls can all generate sources of data for future forensic efforts.
- Analysts should perform data collection using a standard process.
- Analysts should use a methodical approach to studying the data.
- Analysts should review their processes and practices.

Using Data from Data Files

A data file (also called a file) is a collection of information logically grouped into a single entity and referenced by a unique name, such as a filename.

File Basics

Before attempting to collect or examine files, analysts should have a reasonably comprehensive understanding of files and filesystems.

File Storage Media

The widespread use of computers and other digital devices has resulted in a significant increase in the number of different media types that are used to store files

**Table 4-1. Commonly Used Media Types**

| Media Type | Reader | Typical Capacity[16] | Comments |
|---|---|---|---|
| **Primarily Used in Personal Computers** | | | |
| Floppy disk | Floppy disk drive | 1.44 megabytes (MB) | 3.5-inch disks; decreasing in popularity |
| CD-ROM | CD-ROM drive | 650 MB–800 MB | Includes write-once (CD-R) and rewritable (CD-RW) disks; most commonly used media |
| DVD-ROM | DVD-ROM drive | 1.67 gigabytes (GB)–15.9 GB | Includes write-once (DVD±R) and rewritable (DVD±RW) single and dual layer disks |
| Hard drive | N/A | 20 GB–400 GB | Higher capacity drives used in many file servers |
| Zip disk | Zip drive | 100 MB–750 MB | Larger than a floppy disk |
| Jaz disk | Jaz drive | 1 GB–2 GB | Similar to Zip disks; no longer manufactured |
| Backup tape | Compatible tape drive | 80 MB–320 GB | Many resemble audio cassette tapes; fairly susceptible to corruption from environmental conditions |
| Magneto optical (MO) disk | Compatible MO drive | 600 MB–9.1 GB | 5.25-inch disks; less susceptible to environmental conditions than backup tapes |
| Advanced Technology Attachment (ATA) flash card | PCMCIA slot | 8 MB–2 GB | PCMCIA flash memory card; measures 85.6 x 54 x 5 mm |
| **Used by Many Types of Digital Devices** | | | |
| Flash/Jump drive | USB interface | 16 MB–2 GB | Also known as thumb drives because of their size |
| CompactFlash card | PCMCIA adapter or memory card reader | 16 MB–6 GB | Type I cards measure 43 x 36 x 3.3 mm; Type II cards measure 43 x 36 x 5 mm |
| Microdrive | PCMCIA adapter or memory card reader | 340 MB–4 GB | Same interface and form factor as CompactFlash Type II cards |
| MultiMediaCard (MMC) | PCMCIA adapter or memory card reader | 16 MB–512 MB | Measures 24 x 32 x 1.4 mm |
| Secure Digital (SD) Card | PCMCIA adapter or memory card reader | 32 MB–1 GB | Compliant with Secure Digital Music Initiative (SDMI) requirements; provides built-in data encryption of file contents; similar in form factor to MMCs |
| Memory Stick | PCMCIA adapter or memory card reader | 16 MB–2 GB | Includes Memory Stick (50 x 21.5 x 2.8 mm), Memory Stick Duo (31 x 20 x 1.6 mm), Memory Stick PRO, Memory Stick PRO Duo; some are compliant with SDMI requirements and provide built-in encryption of file contents |
| SmartMedia Card | PCMCIA adapter or memory card reader | 8 MB–128 MB | Measures 37 x 45 x 0.76 mm |
| xD-Picture Card | PCMCIA adapter or xD-Picture card reader | 16 MB–512 MB | Currently used only in Fujifilm and Olympus digital cameras; measures 20 x 25 x 1.7 mm |

Filesystems

Before media can be used to store files, the media must usually be partitioned and formatted into logical volumes.

Partitioning is the act of logically dividing a media into portions that function as physically separate units.

A logical volume is a partition or a collection of partitions acting as a single entity that has been formatted with a filesystem.
The format of the logical volumes is determined by the selected filesystem.

A filesystem defines the way that files are named, stored, organized, and accessed on logical volumes. Many different filesystems exist, each providing unique features and data structures.

All filesystems share some common traits.
First, they use directories and files to organize and store data. Directories are organizational structures that are used to group files together.
In addition to files, directories may contain other directories called subdirectories.
Second, filesystems use some data structure to point to the location of files on media. In addition, they store each data file written to media in one or more file allocation units. These are referred to as clusters by some filesystems (e.g., File Allocation Table [FAT], NT File System [NTFS]) and as blocks by other filesystems (e.g., UNIX and Linux). A file allocation unit is simply a group of sectors, which are the smallest units that can be accessed on media. Some commonly used filesystems

| FS | File System Description |
|---|---|
| FAT12 | FAT12 is used only on floppy disks and FAT volumes smaller than 16 MB. FAT12 uses a 12-bit file allocation table entry to address an entry in the filesystem. |
| FAT16 | MS-DOS, Windows 95/98/NT/2000/XP, Windows Server 2003, and some UNIX OSs support FAT16 natively. FAT16 is also commonly used for multimedia devices such as digital cameras and audio players. FAT16 uses a 16-bit file allocation table entry to address an entry in the filesystem. FAT16 volumes are limited to a maximum size of 2 GB in MS-DOS and Windows 95/98. Windows NT and newer OSs increase the maximum volume size for FAT16 to 4 GB. |
| FAT32 | 18 Windows 95 Original Equipment Manufacturer (OEM) Service Release 2 (OSR2), Windows 98/2000/XP, and Windows Server 2003 support FAT32 natively, as do some multimedia devices. FAT32 uses a 32-bit file allocation table entry to address an entry in the filesystem. The maximum FAT32 volume size is 2 terabytes (TB). |
| NTFS | Windows NT/2000/XP and Windows Server 2003 support NTFS natively. NTFS is a recoverable filesystem, which means that it can automatically restore the consistency of the filesystem when errors occur. In addition, NTFS supports data compression and encryption, and allows user and group-level access permissions to be defined for data files and directories.19 The maximum NTFS volume size is 2 TB. |
| HPFS | High-Performance File System (HPFS). is supported natively by OS/2 and can be read by Windows NT 3.1, 3.5, and 3.51. HPFS builds on the directory organization of FAT by providing automatic sorting of directories. In addition, HPFS reduces the amount of lost disk space by |

| | |
|---|---|
| | utilizing smaller units of allocation. |
| ext2fs | Second Extended Filesystem (ext2fs). is supported natively by Linux. It supports standard UNIX file types and filesystem checks to ensure filesystem consistency. The maximum ext2fs volume size is 4 TB. |
| ext3fs | Third Extended Filesystem (ext3fs). is supported natively by Linux. It is based on the ext2fs filesystem and provides journaling capabilities that allow consistency checks of the filesystem to be performed quickly on large amounts of data. The maximum ext3fs volume size is 4 TB. ! ReiserFS.21 ReiserFS is supported by Linux and is the default filesystem for several common versions of Linux. It offers journaling capabilities and is significantly faster than the ext2fs and ext3fs filesystems. The maximum volume size is 16 TB. |
| HFS | Hierarchical File System (HFS) is supported natively by Mac OS. HFS is mainly used in older versions of Mac OS but is still supported in newer versions. The maximum HFS volume size under Mac OS 6 and 7 is 2 GB. The maximum HFS volume size in Mac OS 7.5 is 4 GB. Mac OS 7.5.2 and newer Mac OSs increase the maximum HFS volume size to 2 TB. |
| HFS Plus. | HFS Plus is supported natively by Mac OS 8.1 and later and is a journaling filesystem under Mac OS X. It is the successor to HFS and provides numerous enhancements, such as long filename support and Unicode filename support for international filenames. The maximum HFS Plus volume size is 2 TB. |
| UFS | UNIX File System (UFS) is supported natively by several types of UNIX OSs, including Solaris, FreeBSD, OpenBSD, and Mac OS X. However, most OSs have added proprietary features, so the details of UFS differ among implementations. |
| CDFS | Compact Disk File System  As the name indicates, the CDFS filesystem is used for CDs. |
| ISO 9660 | International Organization for Standardization (ISO) 9660 and Joliet filesystem is commonly used on CD-ROMs. Another popular CD-ROM filesystem, Joliet, is a variant of ISO 9660. ISO 9660 supports filename lengths of up to 32 characters, whereas Joliet supports up to 64 characters. Joliet also supports Unicode characters within filenames. |
| UDF | Universal Disk Format (UDF) is the filesystem used for DVDs and is also used for some CDs. |
| | |

Filesystems may also hold data from deleted files or earlier versions of existing files. erased data can still exist on various media:

- Deleted Files.
- Slack Space.
- Free Space.

Another way in which data might be hidden is through Alternate Data Streams (ADS) within NTFS volumes.

- NTFS has long supported multiple data streams for files and directories.

- Each file in an NTFS volume consists of an unnamed stream that is used to store the file's primary data, and optionally one or more named streams (i.e., file.txt:Stream1, file.txt:Stream2) that can be used to store auxiliary information, such as file properties and picture thumbnail data.

Collecting Files During data collection, the analyst should make multiple copies of the relevant files or filesystems

- typically a master copy and a working copy.

Copying Files from Media Files can be copied from media using two different techniques:

- Logical Backup.
- Bit Stream Imaging.

Organizations should have policy, guidelines, and procedures that indicate the circumstances under which bit stream images and logical backups (including those from live systems) may be performed for forensic purposes and which personnel may perform them.

- The policy, guidelines, or procedures should also identify which individuals or groups have the authority to perform the backup or imaging for each type of system.

Data File Integrity
During backups and imaging, the integrity of the original media should be maintained.

- analysts can use a write-blocker while backing up or imaging the media.

it is important to verify that the copied data is an exact duplicate of the original data.

- Two most commonly used are MD5 and Secure Hash Algorithm 1 (SHA-1). Because SHA-1 is a Federal Information Processing Standards (FIPS)–approved algorithm and MD5 is not, Federal agencies should use SHA-1 instead of MD5.

When a bit stream image is performed, the message digest of the original media should be computed and recorded before the image is performed.

File Modification, Access, and Creation Times
It is often important to know when a file was created, used, or manipulated, and most OSs keep track of certain timestamps related to files. The most commonly used timestamps are the modification, access, and creation (MAC) times, as follows:

- Modification Time.
- Access Time.
- Creation Time.

Different types of filesystem may store different types of times.

Bit stream images can preserve file times because a bit-for-bit copy is generated; performing a logical backup using some tools may cause file creation times to be altered when the data file is copied.

File times may not always be accurate. Among the reasons for such inaccuracies are

- Computer's clock does not have the correct time.
- Time may not be recorded with the expected level of detail, such omitting the seconds or minutes.
- An attacker may have altered the recorded file times.

Technical Issues
Collection of hidden data.
Many OSs permit users to tag certain files, directories, or even partitions as hidden

- by default they  not displayed in directory listings.
- Some applications and OSs hide configuration files to reduce the chance that users will accidentally modify or delete them.

Users may create hidden partitions by altering the partition table to disrupt disk management and prevent applications from seeing that the data area exists.

- Hidden data can also be found within ADSs on NTFS volumes, in the end-of-file slack space and free space on a medium, and in the Host Protected Area (HPA) on some hard drives, which is a region of a drive intended to be used by vendors only.

Another issue is collection of data from RAID arrays

Examining Data Files

- After a logical backup or bit stream imaging has been performed, the backup or image may have to be restored to another media before the data can be examined.

Locating the Files
First step in the examination is to locate the files.

Several tools are available that can automate the process of extracting data from unused space and saving it to data files as well as recovering deleted files and files within a recycling bin.

Analysts can also display the contents of slack space with hex editors or special slack recovery tools.

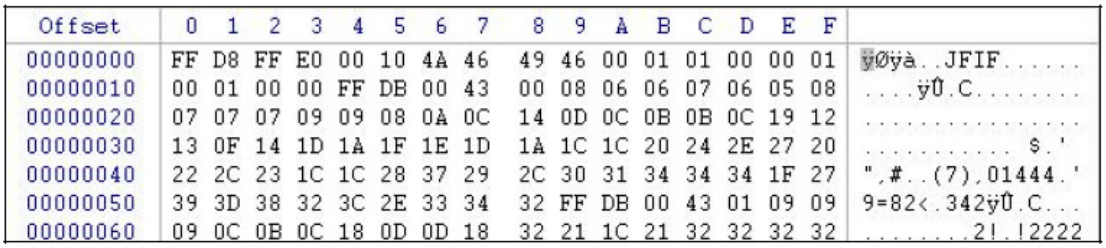
Extracting Data

Analysts can more accurately identify the type of data stored in many files by examining file headers.

- A file header contains identifying information about a file and possibly metadata that provides information about the file's contents.
- As shown in Figure 4-1, file header contains a signature that identifies the type of data that particular file contains.

Another effective technique for identifying the type of data in a file is a simple histogram showing the distribution of ASCII values as a percentage of total characters in a file.

- For example, a spike in the 'space', 'a', and 'e' lines generally indicates a text file, while consistency across the histogram indicates a compressed file. Other patterns are indicative of files that are encrypted or that were modified through steganography.



| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | FF | D8 | FF | E0 | 00 | 10 | 4A | 46 | 49 | 46 | 00 | 01 | 01 | 00 | 00 | 01 | ÿØÿà..JFIF..... |
| 00000010 | 00 | 01 | 00 | 00 | FF | DB | 00 | 43 | 00 | 08 | 06 | 06 | 07 | 06 | 05 | 08 | ....ÿÛ.C..... |
| 00000020 | 07 | 07 | 07 | 09 | 09 | 08 | 0A | 0C | 14 | 0D | 0C | 0B | 0B | 0C | 19 | 12 | ..... |
| 00000030 | 13 | 0F | 14 | 1D | 1A | 1F | 1E | 1D | 1A | 1C | 1C | 20 | 24 | 2E | 27 | 20 | ..... $.' |
| 00000040 | 22 | 2C | 23 | 1C | 1C | 28 | 37 | 29 | 2C | 30 | 31 | 34 | 34 | 34 | 1F | 27 | ",#..(7),01444.' |
| 00000050 | 39 | 3D | 38 | 32 | 3C | 2E | 33 | 34 | 32 | FF | DB | 00 | 43 | 01 | 09 | 09 | 9=82<.342ÿÛ.C... |
| 00000060 | 09 | 0C | 0B | 0C | 18 | 0D | 0D | 18 | 32 | 21 | 1C | 21 | 32 | 32 | 32 | 32 | ........2!.!2222 |

**Figure 4-1. File Header Information**

Encryption often presents challenges.

- Although an analyst can detect the presence of encrypted data rather easily, the use of steganography is more difficult to detect.

Analysts may also need to access non-stegged files that are protected by passwords.

- Passwords are often stored on the same system as the files they protect, but in an encoded or encrypted format.
- Various utilities are available that can crack passwords placed on individual files, as well as OS passwords.

Using a Forensic Toolkit

Analysts should have access to various tools that enable them to perform examinations and analysis of data, as well as some collection activities.

- Fforensic toolkit should contain applications that can accomplish data examination and analysis in many ways and can be run quickly and efficiently from floppy disks, CDs, or a forensic workstation. The following processes are among those that an analyst should be able to perform with a variety of tools:
  - Using File Viewers.
  - Uncompressing Files.
  - Graphically Displaying Directory Structures.
  - Identifying Known Files.
  - Performing String Searches and Pattern Matches.
  - Accessing File Metadata.

Analysis
After the examination has been completed, next step is to analyze extracted data.

Analysts can use special tools that can generate forensic timelines based on event data.
- Such tools typically give analysts a graphical interface for viewing and analyzing sequences of events.
- A common feature of these tools is to permit analysts to group related events into meta-events.

In many cases, forensic analysis involves not only data from files, but also data from other sources, such as the OS state, network traffic, or applications.

Recommendations
Analysts should examine copies of files, not original files.
Analysts should preserve and verify file integrity.
Analysts should rely on file headers, not file extensions, to identify file content types.
Analysts should have a forensic toolkit for data examination and analysis.

**Using Data from Operating Systems**
Logs.
OS log files contain information about various OS events, and may also hold application-specific event information. OS data exists in both non-volatile and volatile states.
- Non-volatile data refers to data that persists even after a computer is powered down, such as a filesystem stored on a hard drive.
- Volatile data refers to data on a live system that is lost after a computer is powered down, such as the current network connections to and from the system.

Non-Volatile Data
The primary source of non-volatile data within an OS is the filesystem.
- Configuration Files. The OS may use configuration files to store OS and application settings
- Users and Groups. The OS keeps a record of its user accounts and groups. Account information may include group membership, account name and description, account permissions, account status (e.g., active, disabled), and the path to the account's home directory.
- Password Files.
- Scheduled Jobs.
- Logs. OS log files contain information about various OS events, and may also hold application-specific event information.
    - System Events.
    - Audit Records.
    - Application Events.
    - Command History.
    - Recently Accessed Files.
- Application Files.

- Data Files.
- Swap Files.
- Dump Files.
- Hibernation Files.
- Temporary Files

Volatile Data
While OS is functioning, RAM contents are constantly changing.
At any given time, RAM might contain many types of data and information that could be of interest.

Slack Space.
Memory slack space is much less deterministic than file slack space.

Free Space.
Memory pages are allocated and deallocated much like file clusters.

Some other significant types of volatile data that might exist within an OS are:
- Network Configuration.
- Network Connections.
- Running Processes.
- Open Files.
- Login Sessions.
- Operating System Time.

Collecting Volatile OS Data
Volatile OS data involving an event can be collected only from a live system that has not been rebooted or shut down since the event occurred.
- Every action performed on the system, whether initiated by a person or by the OS itself, will almost certainly alter the volatile OS data in some way.
- Therefore, analysts should decide as quickly as possible whether the volatile OS data should be preserved.
- Ideally, the criteria for making this decision should have been documented in advance so that the analyst

Forensic Tool Preparation
When collecting volatile OS data, all forensic tools that might be needed should be placed on a floppy disk, CD-ROM, or USB flash drive, from which the tools should be executed.
- Enables analysts to collect OS data with the least amount of disturbance to the system.
- Only forensic tools should be used, since a user might have replaced system commands with malicious programs, such as one to format a hard disk or return false information.
- However, use of forensic tools is no guarantee that the data retrieved will be accurate. If a system has been fully compromised, it is possible that rootkits and

other malicious utilities have been installed that alter the system's functionality at the kernel level. This can cause false data to be returned to user-level tools.

When creating a collection of forensic tools, statically linked binary files should be used. Such an executable file contains all of the functions and library functions that it references, so separate dynamic link libraries (DLL) and other supporting files are not needed.

- Eliminates need to place the appropriate versions of DLLs on the tool media and increases the reliability of the tools.
- Analyst should know how each tool affects or alters the system before collecting the volatile data.
- Message digest of each tool should be computed and stored safely to verify file integrity.

The media containing the tools should protect them from changes.

- Because the media containing the tools should be write-protected, the results produced by the tools cannot be placed onto the tool media.
- Specially prepared CDs and USB flash drives containing a Windows or Linux-based environment can be used to gather output without changing the state of the system and typically direct the output to another USB flash drive, external hard drive, or other writable media, or to a remote system.

On the other hand, collecting volatile OS data from a running computer has inherent risks.

- For instance, the possibility always exists that files on the computer might change and other volatile OS data might be altered.
- In addition, a malicious party might have installed rootkits designed to return false information, delete files, or perform other malicious acts.

Types of Volatile OS Data
Several types of volatile OS data

- Contents of Memory.
- Network Configuration.
- Network Connections.
- Running Processes.
- Open Files.
- Login Sessions.
- Operating System Time.

It is often useful to include some general-purpose tools in the forensic toolkit, such as:

- OS Command Prompt.
- SHA-1 Checksum.
- Directory List.
- String Search.
- Text Editor.

Prioritizing Data Collection
The types of volatile data that should be collected with the toolkit depend on the specific need.

- If a network intrusion is suspected, it might be useful to collect network configuration information, network connections, login sessions, and running processes to determine how someone gained access to a system.
- If an investigation concerns identity theft, then the contents of RAM, the list of running processes, the list of open files, network configuration information, and network connections might reveal social security and credit card numbers, programs used to obtain or encrypt data, password hashes, and methods that might have been used to obtain the information over a network.
- When in doubt, it is usually a good idea to collect as much volatile data as possible

An automated script on a toolkit CD can be used for consistency in collecting volatile data.

- The script can include ways to transfer the collected information to local storage media, such as a thumb drive, and to networked drive locations.

Because volatile data has a propensity to change over time, the order and timeliness with which volatile data is collected is important.

- In most cases, analysts should first collect information on network connections and login sessions, because network connections may time out or be disconnected and the list of users connected to a system at any single time may vary.
- Volatile data that is less likely to change, such as network configuration information, should be collected later.
- Recommended order from first to last:
  1. Network connections
  2. Login sessions
  3. Contents of memory
  4. Running processes
  5. Open files
  6. Network configuration
  7. Operating system time.

Collecting Non-Volatile OS Data
After obtaining volatile OS data, analysts often should collect non-volatile OS data.

Perform a Graceful OS Shutdown.
Remove Power from the System.

After the computer has been powered off, all components, storage devices, media, and peripheral devices connected to the computer should be inventoried and labeled if they are needed as evidence.

Once the filesystem data has been collected, tools can be used to acquire specific types of data from the filesystem.

- Users and Groups.
- Passwords.
- Network Shares.
- Logs.

Occasionally, analysts may need to collect data from the BIOS, such as system date and time or processor type and speed.

Technical Issues with Collecting Data

OS Access.
Log Modification.
Hard Drives with Flash Memory.
Key Remapping.

Examining and Analyzing OS Data
Various tools and techniques can be used to support the examination process.

- Many previously examined tools and techniques for examining collected data files can also be used with collected OS data.
- In addition, security applications, such as file integrity checkers and host IDSs, can be very helpful in identifying malicious activity against OSs.
- For instance, file integrity checkers can be used to compute the message digests of OS files and compare them against databases of known message digests to determine whether any files have been compromised. If intrusion detection software is installed on the computer, it might contain logs that indicate the actions performed against the OS.

Recommendations

- Analysts should act appropriately to preserve volatile OS data.
    - The criteria for determining whether volatile OS data must be preserved should be documented in advance so that analysts can make informed decisions as quickly as possible.
    - To determine whether the effort required to collect volatile OS data is warranted, the risks associated with such collection should be weighed against the potential for recovering important information.
- Analysts should use a forensic toolkit for collecting volatile OS data.
    - Use of a forensic toolkit enables accurate OS data to be collected while minimizing the disturbance to the system and protecting the tools from changes.
    - The analyst should know how each tool is likely to affect or alter the system during collection of data.
- Analysts should choose the appropriate shutdown method for each system.

- Each method of shutting down a particular OS can cause different types of data to be preserved or corrupted; analysts should be aware of the typical shutdown behavior of each OS.

Using Data From Network Traffic

Data from network traffic can be used to reconstruct and analyze network-based attacks and inappropriate network usage, as well as to troubleshoot various types of operational problems.

Recommendations

Key recommendations presented in this section for using data from network traffic are:

- Organizations should have policies regarding privacy and sensitive information. The use of forensic tools and techniques might inadvertently disclose sensitive information to analysts and others involved in forensic activities.
  - Long-term storage of sensitive information inadvertently captured by forensic tools might violate data retention policies.
  - Policies should address the monitoring of networks, as well as requiring warning banners on systems that indicate activity may be monitored.
- Organizations should provide adequate storage for network activity–related logs.
  - Organizations should estimate typical and peak log usage, determine how many hours' or days' worth of data should be retained based on the organization's policies, and ensure that systems and applications have sufficient storage available.
  - Logs related to computer security incidents might need to be kept for a substantially longer period of time than other logs.
- Organizations should configure data sources to improve the collection of information.
- Analysts should have reasonably comprehensive technical knowledge.
  - Experienced, and knowledgeable in networking principles, common network and application protocols, network and application security products, and network-based threats and attack methods.
- Analysts should consider the fidelity and value of each data source.
  - Analysts should have more confidence in original data sources than in data sources that receive normalized data from other sources.
  - Analysts should validate any unusual or unexpected data that is based on interpretation of data, such as IDS and SEM alerts.
- Analysts should generally focus on the characteristics and impact of the event.