Unit III

CHAPTER 6

Investigation, Evidence Presentation and Legal Aspects of Digital Forensics

All investigations into computer security incidents require you to collect information. Especially, you will accumulate host-based evidence, network-based evidence, and different nontechnical evidence so that you can determine what happened and the way the incident might be resolved. An investigation is needed if any cybercrime takes place like online fraud, child abuse, Electronic tampering, Violation of security policies or procedures etc.

6.1 Evidence

Q. 6.1.1 What is mean by Evidence ? *(Ref. Sec. 6.1)* **(5 Marks)**

- The evidence is any information of supporting value, that means which proves something or helps to prove something relevant to the case.
- The digital evidence consists of the data on a computer, images audio and video files. It is a data and information of value to an investigation that is stored on an electronic device, received or transmitted by an electronic machine.
- You can acquire the evidence when data or electronic machines are seized /in custody and secured for the examination. Examples of evidence are a fingerprint, DNA, files on system etc.
- The problems in acquiring digital evidence are
  (a) Digital Evidences can be easily modified, damaged or destroyed.
  (b) Digital Evidences are time sensitive

The places from where you can get the digital evidence are :

i. Computers
ii. External hard drives
iii. Floppy disks
iv. Pen drive
v. CDs and DVDs
vi. Thumb drives
vii. Cell phones and mobile devices
viii. Voice over IP phones
ix. Answering machines
x. iPods
xi. PDAs
xii. Electronic game devices
xiii Digital video recorders (Tivos)
xiv. Digital cameras
xv. PDAs
xvi. GPSs
xvii. Servers
xviii. Routers
xix. Switches
xx. Wireless access points
xxi. Fax machines
xxii. Printers that buffer files
xxiii. Photo-copiers that buffer files
xxiv. Scanners that buffer files

6.1.1 Types of Evidence

Q. 6.1.2 What are the types of evidence ? *(Ref. Sec. 6.1.1)* **(5 Marks)**

The types of evidence are:

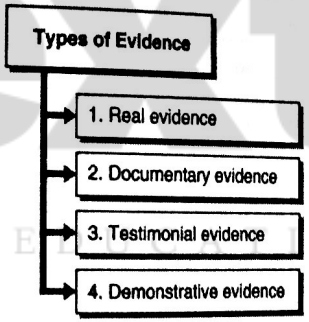

Fig. 6.1.1 : Types of Evidence

➜ **1. Real evidence :**

Real evidence are something that one can carry into a courtroom and show it in front of the jury. Real evidence is the most powerful evidence. This evidence typically "speaks for itself."

➜ **2. Documentary evidence :**

The evidence which is in the written form is nothing but the documentary evidence. For example server logs, email, database document etc. Documentary evidence might be faked via a professional pc user and therefore must be authenticated to be admissible in a courtroom. Continually produce the original document, do not use the copy.

3. Testimonial evidence :

Testimonial evidence is nothing but the statement of a witness, underneath oath, either in court or by deposition. This sort of evidence normally helps or validates alternative types.

4. Demonstrative evidence :

Demonstrative evidence recreates or explains the different evidence. Demonstrative evidence does not "talk for itself" and is used to demonstrate and make clear previous points. This sort of evidence is maximum helpful in explaining technical topics to non-technical audiences.

6.1.2 Evidence Characteristics

Q. 6.1.3 Explain the characteristics of the evidence? *(Ref. Sec. 6.1.2)* **(5 Marks)**

There are five characteristics of evidence. They are as follow:

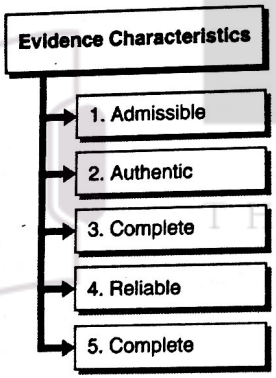

Fig. 6.1.2 : Evidence Characteristics

1. Admissible

Evidence ought to be acceptable, if the proof you reveal won't stand up in court, you have squandered your time and conceivably allowed a guilty party to go unpunished.

2. Authentic

Evidence ought to be Authentic. Authentication is directly related to the incident being investigated. The investigation may reveal evidence that is interesting but not relevant.

3. Complete

Evidence ought to be Complete. The specialist ought to approach the case with no assumptions about somebody's blame or blamelessness. Criminological routines ought to take out option Suspects and clarifications until an unmistakable conclusion is come to.

4. Reliable

Evidence ought to be Reliable. There ought to be no doubt about the reality of the specialist's decisions. Reliability originates from standardized and verified forensic tools and techniques. Qualification of a specialist as an expert witness for a case will set up believability and reliability.

5. Complete

Evidence ought to be acceptable. The investigator must create results that are clear and straightforward, even among the most nontechnical individuals from a jury. Have different agents have used the same forensic techniques and reached similar conclusions?

Syllabus Topic : Authorization to Collect the Evidence

6.2 Authorization to Collect the Evidence

Q. 6.2.1 Write a short note on Authorization to collect the evidence. *(Ref. Sec. 6.2)* **(5 Marks)**

- Digital evidence can be fragile and exceedingly delicate. Cyber security experts understand the estimation of this data and regard the way that it very well may be effectively compromised if not appropriately handled and ensured.
- Therefore, it is basic to set up and pursue strict guidelines and procedures for exercises identified with computer forensic investigations. Such procedures can incorporate detailed instructions about when computer forensics agents are authorized to recuperate potential digital evidence, how to appropriately prepare systems for evidence recovery, where to store any recovered evidence, and how to record these exercises to help guarantee the authenticity of the information.
- In Criminal cases, Law enforcement agencies train the persons as technicians to make sure the preservation of the evidence.

- They follow strict procedures for forensic cyber security divisions have to set forth rules of governance for all other digital activity inside an organization.
- Actions for collecting the evidence are defined by the law enforcement, such as where to look for said evidence and how to handle it once it has been retrieved. Before the investigation, it is important to understand the warrant and authorization. In criminal matters, there are laws related to search warrants.
- In the civil matters, the company officer has the right to collect the evidence. The company officers are not trained one. In civil proceedings, it is assumed that a company is able to investigate their own equipment without a warrant. Providing the privacy and human rights of employees are observed.
- *Any individual* who is using a computer system can collect the data from the system, for example, a wife can collect data from the husband's computer or vice versa.

Syllabus Topic : Acquisition of Evidence

6.3 Acquisition of Evidence

Q. 6.3.1 Write and explain the steps taken to collect the live data. *(Ref. Sec. 6.3)* **(10 Marks)**

- Once exhibits have been seized an accurate sector level duplicate (or "forensic duplicate" of the media is created, usually via a write blocking device, a process referred to as Imaging or Acquisition. Obtaining Volatile Data Prior to Forensic Duplication.
- Data which is in a state of change is called volatile data. The data in the computer system will get lost as the power loss. Volatile data is present in the active physical memory. We will find the volatile data in physical memory, registers, virtual memory in the file system and in the peripheral device memory.
- To ensure all relevant data are collected, you should prepare an order of volatility while gathering evidence, the Order of Volatility (OoV) should be from the most volatile to the least.
- When you acquire volatile data, you'll want to respond to the target device at the console in preference to getting access to it over the network. This eliminates the possibility of the attacker monitoring your response and ensures that you are running trusted commands.

- If you are certain that you may be doing a forensic duplication of the target device, you have to focus on obtaining the volatile system data before powering down the system. The risky information consists of presently open sockets, strolling approaches, the contents of system RAM, and the location of unlinked documents.
- The unlinked files are documents marked for deletion while processes that get entry to it to terminate. The documents marked for deletion will "disappear" while the system is powered down. Therefore, the preliminary reactions have to get better, each type of unstable proof inclusive of the documents marked for deletion! This could save you some grief because getting a deleted report in maximum flavours of UNIX isn't as simple as running a report undeletion device or tool.

Collecting the Data

1. Date and time of the system.
2. Currently logged on the user's list.
3. Entire file systems time and date stamp.
4. Currently running processes list.
5. Currently, open sockets list.
6. The applications listening on open sockets.
7. A list of the systems that have current or had recent connections to the system.

The following steps are taken to collect the live data :

1. Execute a trusted shell.
2. Record the system time and date.
3. Determine who is logged on to the system.
4. Record modification, creation, and access times of all files.
5. Determine open ports.
6. List applications associated with open ports.
7. Determine the running processes.
8. List current and recent connections.
9. Record the system time.
10. Record the steps taken.
11. Record cryptographic checksums.

Remember that the steps we outline are just a game plan. You need to modify the order and the tools used based on the whole of the circumstances. You may choose to include tools we do not mention, as well as carry out your steps in a different manner:

➜ 1. Executing a Trusted Shell

- When you are responding to a targeted system on which UNIX operating system is running, you will come across one of two scenarios :
  1. The system runs in console mode.
  2. The system runs X Windows, a GUI like to the Windows desktop.
- Exit the X windows prior to you begin your response; it helps to avoid common X Windows-based vulnerabilities that permit the attacker to log keystrokes. If you are responding to a Linux system, you possibly able to switch to another virtual console by pressing ALT-F2.
- To avoid generating traffic Log on locally at the victim console with root privileges. Now mount the trusted toolkit and respond with trusted tools. The following is the command syntax to mount a floppy drive when responding to a Linux system:

```
mount /dev/fd0 /mnt/floppy
```

- This command mounts your trusted toolkit on the mount point /mnt/floppy. To access the trusted file change the directory to /mnt/floppy.
- The first step in all response is to be certain you are executing a trusted command shell.
- The Unix shells can be trojaned by attackers to log all the commands executed or to perform immoral and evil operations invisible to the investigator.
- Therefore, you will want to execute your own trusted shell. Once you have executed your trusted shell, set your PATH environment variable equal to dot (.).
- This will decrease the chances of someone accidentally executing untrusted commands that are in the target system's PATH.

➜ 2. Recording the System Time and Date

- The local date and time settings are important for later correlation of time/date stamps, and they also show when you were on the system.

- To capture this information, use the date command :

```
[root@conan /root]# date
Tue Dec 17 16:12:43 UTC 2003
```

➜ 3. Determining Who Is Logged on to the S...

- The ...

(mtime), and the inod...
which ...

```
ls -alR / > /flo...
```

➜ 5. Determining Which Ports are Open

- The netstat command is used to determine the open ports. By using *netstat – a* command is used to view all open ports.
- The *-n* option tells netstat to not resolve hostnames, which reduces the impact on the system and speeds the execution of the command.

➜ 6. Listing Applications Associated with Open Ports

With the netstat command *–p* option is used which maps the name of the application and its Process ID (PID) to the open ports.

Remember that the steps we outline are just a game plan. You need to modify the order and the tools used based on the whole of the circumstances. You may choose to include tools we do not mention, as well as carry out your steps in a different manner:

➜ 1. Executing a Trusted Shell

- When you are responding to a targeted system on which UNIX operating system is running, you will come across one of two scenarios :
  1. The system runs in console mode.
  2. The system runs X Windows, a GUI like to the Windows desktop.
- Exit the X windows prior to you begin your response; it helps to avoid common X Windows-based vulnerabilities that permit the attacker to log keystrokes. If you are responding to a Linux system, you possibly able to switch to another virtual console by pressing ALT-F2.
- To avoid generating traffic Log on locally at the victim console with root-level privileges. Now mount the trusted toolkit and respond with trusted tools. The following is the command syntax to mount a floppy drive when responding to a Linux system:

```
mount /dev/fd0 /mnt/floppy
```

- This command mounts your trusted toolkit on the mount point /mnt/floppy. To access the trusted file change the directory to /mnt/floppy.
- The first step in all response is to be certain you are executing a trusted command shell.
- The Unix shells can be trojaned by attackers to log all the commands executed or to perform immoral and evil operations invisible to the investigator.
- Therefore, you will want to execute your own trusted shell. Once you have executed your trusted shell, set your PATH environment variable equal to dot (.).
- This will decrease the chances of someone accidentally executing untrusted commands that are in the target system's PATH.

➜ 2. Recording the System Time and Date

- The local date and time settings are important for later correlation of time/date stamps, and they also show when you were on the system.

- To capture this information, use the date command :

```
[root@conan /root]# date
Tue Dec 17 16:12:43 UTC 2003
```

➜ 3. Determining Who Is Logged on to the System

- The (what) command determines who is logged on. It displays the logged on user IDs, and from which system they have logged on.
- It also shows what they are currently executing on the system with the date and system time.

➜ 4. Recording File Modification, Access, and Inode Change Times

- You may need to retrieve all of the time/date stamps at the file device. As with home windows structures, Unix structures have 3 time/date stamps to collect for every file and listing: get right of entry to time (atime), amendment or modification time (mtime), and the inode alternate time (ctime). An inode is a data structure in Unix which is used to represent file system objects.
- You can use a depended on ls command with the proper command-line arguments to obtain those times for every file. The subsequent strains show the way to obtain the time/date stamps and show the output on a trusted floppy disk :

```
ls -alRu / > /floppy/atime
ls -alRc / > /floppy/ctime
ls -alR / > /floppy/mtime
```

➜ 5. Determining Which Ports are Open

- The netstat command is used to determine the open ports. By using *netstat – a* command is used to view all open ports.
- The *-n* option tells netstat to not resolve hostnames, which reduces the impact on the system and speeds the execution of the command.

➜ 6. Listing Applications Associated with Open Ports

With the netstat command *–p* option is used which maps the name of the application and its Process ID (PID) to the open ports.

7. Determining the Running Processes

- Taking a snapshot of all the running processes during the initial response is critical. This can be done by using the standard ps (process status) command.
- The output varies a bit among the different UNIX flavors.
  1. Use ps -eaf on Solaris systems,
  2. Use ps -aux on FreeBSD and Linux systems.

8. Listing Current and Recent Connections

- The netstat command provides information about another aspect of live response: current and recent connections.
- The command usage is identical for determining which ports are open.

9. Recording System Time

- Use the date command again (repeat step 2) to record the current system time. The reason for another timestamp is so that you will know the exact time window during which you manipulated the system.
- Thus, any changes that take place outside this time window are not due to your investigation.

10. Recording the Steps Taken

- Finally, record all of the commands you have issued to the system. There are several possibilities here: use script, history, or even vi if you performed your live response from the editor.
- Since you issued all commands from a trusted shell, using the history command will record all of the commands you've executed. However, a better choice is the script command, which will record your keystrokes and the output. If you choose to use the script command, you'll need to run this command before you perform the live response.

11. Recording Cryptographic Checksums

- Finally, record the cryptographic checksums of all recorded data.
- Simply run the md5sum program against all files in the data directory, as shown here :


```
[root@conan /root]# md5sum * > md5sums.txt
```

12. Scripting the Initial Response

- Write a simple shell script to automate the live data collection.
- Steps of a UNIX system are same as windows system. Place your script in the same directory as the response toolkit and it calls the local tools.

6.4 Forensic Duplication

Q. 6.4.1 What is forensic duplicate? When forensic duplicate is admissible? *(Ref. Secs. 6.4 and 6.4.1)* **(5 Marks)**

- In the previous sections, we have seen how to obtain volatile data from Windows and Unix systems. In many cases, the data collection process is a start for performing a forensic duplication.
- Forensic duplication decision of when to perform is based on the response strategy that which is already formulated. In this section we will first see the terms related to forensic duplication, then how forensic duplication data can be used as legal evidence and define related terms and some generally accepted tools and techniques used to obtain a forensically sound duplicate image.

6.4.1 Forensic Duplicates as Admissible

- It is very necessary to know that,
  1. What requirements need to be met by a tool before it becomes a part of your investigative process ?
  2. The tool or process must ultimately provide you with evidence that may be presented at a trial.
- There is a set of acknowledged or legal standards that define the minimum criteria to be met for an item or writing to be accepted into evidence. Furthermore, due to the manner in which we access the data, the action of accumulating also falls under inspection. Inattention to forensic duplicates, the best evidence rule comes into play. This applies to any information on which the facts of the case or issues are based.
- The rule, U.S. Federal Rules of Evidence (FRE) §1002, states that the item or information presented in court must be the original. Fortunately for us, as with most rules governing legal issues, there are always exceptions.

- Quite often, the originals themselves cannot be obtained due to business needs.
- The exceptions pertinent for our purposes are defined in two rules :
  1. FRE §1001-3, Definitions and Duplicates : "If information is stored by the computer or like device, any printout or other output readable by sight, shown to reflect the data accurately, is an original."
  2. FRE §1003, Admissibility of Duplicates : A duplicate is admissible to the similar level as an original unless
     (a) A authentic question is raised as to the authenticity of the original.
     (b) In the situations, it would be unjust to admit the duplicate in lieu of the original.
- This concept of figurative accuracy permits investigators to collect forensic duplicates, qualified forensic duplicates, mirror images, and to a level, logical copies of the computer and data storage systems involved.
- Here, "logical copy" is referred to the act of copying discrete files from the logical file system onto media in the collection process. Let's have a look at the related terms to forensic duplication.

6.4.1.1 Forensic Duplicate

A forensic duplicate is a file that includes every bit of information from the source, in a raw bitstream format. A 5GB hard drive would result in a 5GB forensic duplicate. No additional data is stored within the file, apart from in the case where errors occurred in a read operation from the original. When this occurs, a placeholder is put where the bad data would have been. A forensic duplicate may be compressed following the duplication process. The tools that create a forensic duplicate are :

1. Unix dd command
2. dfcldd (U.S. Department of Defence (DoD) Computer Forensics Lab version of the dd command).
3. open-source Open Data Duplicator (ODD) e.g. FTK Imager.

6.4.1.2 Qualified Forensic Duplicate

Q. 6.4.2 Write short note on Qualified Forensic Duplicate ? *(Ref. Sec. 6.4.1.2)* **(5 Marks)**

- A qualified forensic duplicate is a file that contains every bit of information from the source but may be stored in an altered or changed form. Two examples of altered paperwork are in-band hashes and Empty Quarter compression.

- A few types of equipment will examine in some of the sectors from the supply, generate a hash from that group of sectors, and write the world organization, accompanied via the hash value to the output document.
- This approach works very well if something is going wrong in the course of the duplication or recovery of the reproduction. If a quarter groups fail to fit the hash cost generated for it, the recovery can continue, and the analyst is conscious that records from that area organization may be invalid. If a similar state of affairs came about with a forensic duplicate file, the place of the mistake may be unknown, probable invalidating the entire reproduction.
- Empty Quarter compression is a not unusual technique for minimizing the dimensions of the output document. If the tool comes throughout 500 sectors, all filled with zeros, it will make a unique entry inside the output file that the healing application will recognize.
- Three tools that create qualified forensic duplicate output files are :
  1. SafeBack
  2. EnCase.
  3. FTK Imager.

6.4.1.3 Restored Image

Q. 6.4.3 Write short note on Restored Image ? *(Ref. Sec. 6.4.1.3)* **(5 Marks)**

- A restored image is what you get when you restore a forensic duplicate or a qualified forensic duplicate to another storage medium. The restoration process is more complicated than it sounds.
- For example, one method involves a blind sector-to-sector copy of the duplicate file to the destination hard drive. If the destination hard drive is the same as the original hard drive, everything will work fine. The information in the partition table will match the geometry of the hard drive.
- Partition tables will be accurate; if the table says that partition 2 starts on cylinder 20, head 3, and sector 0 that is where the data actually resides. But what if the destination hard drive is not the same as the original hard drive? If you restore the forensic duplicate of a 2.1GB drive to a 20GB drive, then the geometries do not match.
- In fact, all of the data from the original drive may occupy only three cylinders of the 20GB destination drive. The partition that started on cylinder 20, head 3, and sector 0 on the original drive may actually start on cylinder 2, head 9, and sector 0.

- The software would look in the wrong location and give inaccurate results. How does the restoration software compensate for this? As the forensic duplicate is restored to the destination hard drive, the partition tables (in the master boot record and partition boot sectors) are updated with the new values. Is the restored image an exact duplicate of the original? If the analyst generates hashes of the restored image, will they match the original? The answer is no in both cases. Is the data on the restored image still a true and accurate representation of the original? For the purposes of analysis, yes.
- The method of updating the partition tables on the destination hard drive is not reliable. When hard drives grew beyond 512MB, the PC-BIOS manufacturers were scrambling to update their software to recognize such huge drives. Hard drive manufacturers came up with a way around the problem.
- Instead of forcing everyone to buy new motherboards with updated BIOS code, they released software that emulated modern BIOS. This software would "push" all of the real data on the drive down one sector and store its program and information in sector 1. The real partition table would be at cylinder 0, head 0, and sector 2.
- When the software restored the forensic duplicate to a large destination drive, it would not update the correct table, leaving the restored image relatively useless. Most forensic processing software will detect this drive overlay software and create a valid restored image.
- The following tools are used to create a restored image from the qualified forensic duplicate :
  1. SafeBack,
  2. EnCase,
  3. dd
- Depending on your method of analysis, EnCase and dd images may not need to be restored. EnCase, the Forensic Toolkit, treats the images as virtual disks, eliminating the need for restoration.

6.4.1.4 Mirror Image

- A mirror image is created from hardware that does a bit-by-bit copy from one hard drive to another. Hardware solutions are very fast, pushing the theoretical maximum data rate of the IDE or SCSI interfaces.
- Investigators do not make a mirror image very often, because it introduces an extra step in the forensic process, requiring the examiner to create a working copy in a forensically sound manner. If your organization has the ability to keep the original drive, seized from the computer system being investigated, you can easily make working copies. If the

original drive must be returned (or never taken offsite), the analyst will still be required to create a working copy of the mirror image for analysis.

- The small amount of time saved onsite is overshadowed by the overhead of making a second working copy. We will not cover the process of creating a mirror image of evidence here. Most hardware duplicators are relatively simple to set up and operate.
- Two such duplicators are Log cube's Forensic SF-5000 and Intelligent Computer Solutions' Image MASSter Solo-2 Professional Plus. You do need to ensure that the hardware duplicator actually creates a true mirror image.
- Many duplicating machines on the market are made for systems integration companies who use them for installing operating systems on large numbers of hard drives. When used in this capacity, the hardware device will typically alter items in the boot and partition blocks to ensure that the partitions fall on cylinder boundaries.
- This alters the resulting image, which means that you do not walk offsite with an exact duplicate of the original. As with any process, test it thoroughly before you need to rely on it.

6.4.2 Forensic Duplication Tool Requirements

Q. 6.4.4 What are the forensic duplication tool requirements ? *(Ref. Sec. 6.4.2)* **(5 Marks)**

- Expanding on the legal standards that are set up to control the tolerability of expert affirmation, we trust that a legal duplication tool must prove itself in the accompanying areas :
  1. The tool must be able to image all of the information on the storage medium.
  2. The tool must make a forensic duplicate or mirror image of the original storage medium.
  3. The tool must handle read errors in a vigorous and elegant way. In the event that a process fails after repeated endeavors, the error is noted and the imaging process proceeds. A placeholder might be placed in the output file with the same dimensions as the portion of the input with errors. The contents of this placeholder must be archived in the tool's documentation.
  4. The tool must not make any changes to the source medium.
  5. The tool must be able to be involved to scientific and peer review. Results must be repeatable and certain by a third party, if essential.

- Action and error logs are crucially important also. The more data logged by the tool amid operation, the less demanding your occupation will be the point at which you record the procedure.

6.4.3 Creating a Forensic Duplicate of Hard Drive

Q. 6.4.5 How to create a forensic duplicate of a hard drive ? *(Ref. Sec. 6.4.3)* **(5 Marks)**

To create the forensic duplicate of hard drive the following tools are used.

1. dd and dcfldd
2. ODD (Open Data Duplicator)

➜ 1. Creating forensic duplicate using dd and dcfldd

- The dd tool is the part of the GNU software suite, afterward, dd was improved by the programmers and re-released as dcfldd. The dd tool is very reliable to create the true forensic duplicate.
- The dd tool performs a complete bit-by-bit copy of the original. While using the dd tool simply transposing a single character may destroy evidence, so one must have to be familiar with the dd tool before using it as well as with the Unix environment address storage devices.
- The steps required for duplicating hard drive using dd are :
  1. Create a boot media
  2. Perform the duplication with dd. In some situations the duplication is stored in the series of the files which are sized to fit on a specific media type or file system type, we call this as a segmented image. So do the following things to perform the duplication.
     - Write the script to perform hard drive duplication.
     - Write down the source device name.
     - Write down the output file name and set the output file size.
     - Use the dd command.
- It is also possible to create the duplicate without splitting the output file in Linux. To create such type of duplicate calculate the MD5 sum of the entire drive in one pass over the source hard drive.

➜ 2. Creating forensic duplicate with Open Data Duplicator (ODD)

- The Open Data Duplicator (ODD) is an open-source tool which follows the client-server model. This client-server model allows the investigator to perform forensic duplications on a number of computer systems simultaneously over a local LAN.
- We can use the software on a single forensic system because both halves can be run on the same computer system. ODD can perform additional functions on the data as it is being processed. ODD includes modules (plug-ins) that will calculate checksums and hashes, perform string searches, and extract files based on the file headers.
- The ODD package is having three portions :
  - **Bootable CD-ROMs :** These are similar to the Trinux Linux distribution.
  - **Server-side application :** The server will perform most of the processing of the duplicate image, including the calculation of hashes, string searches, and the storage of the true forensic duplication.
  - **Client-side application :** This portion may be run locally if you are duplicating drives on a forensic workstation.
- When we perform the forensic duplication of a hard drive using ODD. Firstly it detects the location of the ODD server. Then the ODD server detects the device and files which we can use to direct ODD for the duplication of some portions. After detecting the device the next step is processing.
- The process stores the forensic image and performs simple string searches and extracts certain types of files based on their file headers. We also manage some notes using the Notes plugin which gives the information like the case number, the computer's date and time, the actual date and time, and the system description.
- Then we use the Carv plug-in to extract a certain number of bytes from the incoming data stream, based on file headers. For example, we have selected gif and jpg for extraction, once the duplication has completed, the carved files may be found in a directory on the ODD server.

6.4.4 Creating Qualified Forensic Duplicate of a Hard Drive

Q. 6.4.6 How to create a qualified forensic duplicate of a hard drive? **(5 Marks)**
(Ref. Sec. 6.4.4)

- It is must to know as an investigator that never boot from the evidence drive. Many items on the evidence media can be altered; starting from the moment the BIOS executes the boot block on the hard drive.
- In the initial boot process, file access timestamps, partition information, the Registry, configuration files, and important log files may be changed in a matter of seconds. The qualifier "forensic" implies that the copy is a true copy, that is, the bit stream from the original and the duplicate are the same.
- In order to certify this, one can compare the original and duplicate bit-by-bit, or one can speed up the process by using signatures, also known as a hash. A signature is a small piece of data, typically between 4 and 22 bytes long calculated from the contents of a sector, a track, a file, or a whole hard drive.
- 32-bit cyclic redundancy codes SHA1 use an algorithm to generate the signatures that are so complicated that it is computationally impossible (i.e. it just takes too long) to generate a sector, block, track, or file that has the same signature as a given sector, block, track, or file. A good duplication tool will have some way of proving that the duplicate is true, typically by calculating the signature.

1. Creating a Boot Disk

- A clean operating environment is required for imaging a system. For doing the imaging DOS applications like SafeBack or EnCase is used it means that you must create an MS-DOS boot disk. The following command will format and copy the system files to a floppy :

```
C:\format a:\ /s
```

- There should be four files in the root directory of the floppy. These files contain the code to get the computer running a minimal operating system and these four files are IO.SYS, MSDOS.SYS, and COMMAND.COM. DRVSPACE.BIN.
- The computer first process the IO.SYS file and then the code in IO.SYS loads the contents of MS-DOS.SYS and begins to initialize device drivers, tests and resets the hardware, and loads the command interpreter, COMMAND.COM.
- During the process of loading device drivers, if a disk or partition connected to the machine uses compression software then IO.SYS loads the DRVSPACE.BIN driver file. When the driver loads it mount the compressed volume and present the operating system with an uncompressed view of the file system. When it mounts the compressed volume, it changes the time/date stamps on the compressed file; it means that the evidence will be altered. These files are not required to you.

- When you boot from your clean boot disk, you want to make sure that the loading of the DRVSPACE.BIN driver file fails. Simply removing the file is a good start, but IO.SYS is smart enough to check the root directories of all active partitions for the file.
- The most effective way to prevent the loading of DRVSPACE.BIN is to load IO.SYS into a hex editor and alter the strings manually. Perform the string search operation in word space.
- Notice that the period in the filename is not represented in the executable file. Continue to search the file for the SPACE string. There are four instances in IO.SYS that will need to be changed. When you are finished, save the file and exit the hex editor.
- On the safer side remove the DRVSPACE.BIN file from the floppy as well. After you've created the clean boot floppy, copy over any DOS mode drivers that you will need to access the hard drives on the computer system under investigation.
- The best source for DOS drivers is the website for each hardware manufacturer, rather than on the driver CD that ships with the product.

2. Use the Encase tool

- Encase is a totally high-priced, but very surprising window based Forensics suite that consists of the making of certified forensics duplicates. Being home windows based totally makes Encase easy to apply, however, it additionally introduces a few issues, approximately the OS spotting suspect drives and inside the procedure changing their contents. This doesn't imply - of direction - that Encase should ever generate person information.
- Encase strength lies in their seamless integration of all forensics investigation obligations. Encase generates a certified forensics duplicate.

3. Use Safe back tool

- The safe back is small software program software that is positioned on a DOS boot disk (normally a floppy, however, this could be changing as floppy drives die out).
- It offers options on the kind of duplicate, a real forensics duplicate or a reflection. We will need to have a clean DOS environment ready on a boot floppy.

Syllabus Topic : Authentication of the Evidence

6.5 Authentication of the Evidence

Q. 6.5.1 Explain what is mean by authentication of evidence ? *(Ref. Sec. 6.5)* **(5 Marks)**

- Authentication of evidence means, providing the proof that the data which is collected is not altered after the computer came into possession of the investigation team.
- Every time when any document introduced and material recorded should be authenticated. Authentication means that whoever gathered the evidence should testify during direct examination that the information is what the defender claims.
- To authenticate evidence is to have a witness who has personal knowledge as to the origins of that piece of evidence provide testimony.
- The evidence is inadmissible if it cannot be authenticated. Such inadmissible evidence cannot be presented to the judging body.
- To meet the demands of authentication it is necessary to ensure that whoever collected the evidence is a matter of record. For this purpose develop some type of internal document that records the way in which evidence is collected.
- Another way to authenticate the document is to use mathematical forensic tools. For example, MD5 and hash algorithm. It is important to preserve the integrity of the files which are retrieved during the response using md5sum. Run the md5sum on the files stored on the forensic workstation in the presence of witnesses, which is also known as the two-man integrity.
- The hash algorithm and MD5 create the hashes of the original evidence. As we know, no two files create the same hash value. At the time of authentication if the hash values match then the evidence is not altered and are authenticated.

Syllabus Topic : Analysis of the Evidence

6.6 Data Analysis Techniques

Q. 6.6.1 What are the steps for preparing the forensic analysis ? *(Ref. Sec. 6.6)* **(5 Marks)**

In data analysis techniques, we discuss how to locate and organize all of the pieces of computer media and assemble them before you begin any interpretation of the contents.

We cover the following topics :

1. Restoring a forensic duplication
2. Restoring a qualified forensic image
3. Recovering previously deleted files
4. Recovering unallocated space and slack space
5. Generating file lists
6. Performing string searches.

Preparation for Forensic Analysis

Forensic duplicates and qualified forensic duplicates of hard drives may require additional planning in order to make the information they contain usable.

The restoration of the duplicate or analysis of that it is in its native format or not is depends on several factors :

1. Your organization's analysis procedure.
2. Original data format.
3. The original data condition.
4. Is there any need to review the client's working surroundings in its local state?
5. In some cases, there is a need to see the environment that the user was exposed to before the system was duplicated. Apply the rules to the native file system to the image file before you can analyze a forensic duplication. These rules, normally utilized by the local operating system, permit access to the logical file system. At the point when working with forensic duplicates, this can be done in three ways.
   (a) The duplicate image can be restored to another medium, resulting in a mirror or restored image.
   (b) You can analyze the duplicate image in Unix, allowing Unix to apply the local file system rules to the duplicate image.
   (c) You can allow a forensic tool suite to perform the functions of interpreting, presenting, and examining the forensic duplication.

In this section, we will see how to restore duplicate images, prepare a duplicate image for analysis under Linux, and load a forensic duplicate into Encase and the Forensic Toolkit.

6.6.1 Restoring a Forensic Duplicate

Q. 6.6.2 Explain the process of restoring the forensic duplicate ? *(Ref. Sec. 6.6.1)* **(5 Marks)**

When you restore a forensic duplicate :

1. Assure that you have a hard drive with a capacity greater than the original drive. It is possible to use a drive that is of equal size.
2. Assure that the two drives are from the same manufacturer. If the drives are from the different manufacturer there are chances of a handful of sectors short. This happens because of the specification differences or physical defects.
3. It is necessary to wipe the destination hard drive clean at the time of restoring drive.

☛ Restoring a Forensic Duplication of a Hard Disk

As we know that the dd command is to create a forensic duplicate of a hard drive. To restore a forensic duplication of a Hard Disk performs the following steps :

1. Run the script against the suspect drive. It gives a quick review of the total records read in and records readout reveals that no blocks were lost or corrupted.
2. Use a md5sum command to verify that the duplication was successful and accurate.
3. Use cat command to restore the forensic duplicate. You can re-assemble the segmented forensic duplicate to a single file or restore it to a hard drive.
4. In three separate IDE hard drives we will receive the output :
   (a) The first drive hosts the local operating system for the forensic workstation.
   (b) The second drive is a storage drive to store forensic images.
   (c) The third drive is the new drive, planned for the restoration.
5. Now we can restore the forensic image to the new hard drive for analysis. Use the *cat* command to concatenate the multiple segments of the forensic duplicate to the new hard drive.
6. We now use a ***md5sum*** command on the restored image to once again verify that the operation was completed accurately or not. If the hash values matches, it means duplication and restoration operations were successful.

6.6.2 Restoring a Qualified Forensic Duplication of a Hard Disk

Q. 6.6.3 Explain the process of restoring the forensic duplicate ? *(Ref. Sec. 6.6.2)* **(5 Marks)**

A clean wiped hard drive of equal or greater capacity is required for restoring a qualified forensic duplication. The destination drive should be completely clear of any data before you restore any type of forensic duplicate.

It is important to restore the following evidence file :

1. EnCase evidence file 2. SafeBack evidence file.

➜ 1. EnCase Evidence File

EnCase evidence file restoration to a clean hard drive is relatively simple. EnCase does not provide the means to convert their proprietary image file format to a true forensic image.

➜ 2. SafeBack Evidence File

SafeBack operates entirely in DOS mode. It is better than working in Windows. It is risky for an operating system to recognize the restored image if you restore a duplicate of an evidence drive in EnCase. If Windows recognizes a valid file system, it will modify files and file system structure tables.

6.6.3 Recovering Previously Deleted Files

6.6.3.1 Recovering Deleted Files on Windows Systems

Q. 6.6.4 How to Recover Deleted Files on Windows Systems? *(Ref.Sec. 6.6.3.1)* **(5 Marks)**

- Many times you want to clear the unallocated space on a restored forensic image in order to undelete or recover as many files or file fragments as possible. You also want to recover the evidence which was deleted by an attacker.
- In this section, we going to study e the different ways to obtain files that, for all intents and purposes, suspects would believe no longer exist. As you probably know, deleted files are not truly deleted; they are merely *marked* for deletion.
- For example, when a file or directory is deleted from a FAT file system, the first letter of its filename is set to the sigma character (Ó), or, in hex, 0xE5. This means that these files will remain intact until new data has overwritten the physical area where these deleted files are located on the hard drive. Special tools can find these "intact" deleted files and recover them for review. After a file has been marked for deletion, each hard drive I/O could overwrite the data you want to recover.

- To recover the file on windows system we use the following tools :

1. Windows-based tools: Encase, FTK
2. Linux tools: Fatback, TASK, and Foremost.

1. Windows-Based Tools to Recover Files on FAT File Systems

EnCase and FTK is the tools of the windows system for recovering files on FAT filesystems. Both EnCase and FTK have this capability built-in, and they automatically recover any files they can.

2. Linux Tools to Recover Files on FAT File Systems

Three Linux utilities that can recover data: Fatback, TASK, and Foremost.

(i) FatBack to Recover Deleted Files

Fatback is used to recover the deleted files from the Fat System. Fatback also performs file recovery on FAT12, FAT16, and FAT32 file systems from a Linux forensics platform. Following are the features of Fatback :

(a) It supports the Long filename.

(b) There is recursive undeletion of directories.

(c) Lost cluster chain recovery.

(d) It can work within single partitions or entire disks.

Fatback is flexible because it works on image files as well as devices Fatback installation is easily on Linux and FreeBSD systems.

To recover the deleted file from an image of an evidence floppy, the following Fatback command-line options are used :

(a) -a - This option runs Fatback in automatic undelete mode.

(b) -o - This option places recovered files into the specified directory

(c) -s - This option tells Fatback to treat the input file *evidencefloppy.bin* as a single Partition since all floppy drives have only one partition.

(ii) Using TASK to Recover Deleted Files

- TASK is a tool used to recover the deleted files. It is an open-source forensic toolkit. It is used to analyze Microsoft and Unix file systems. TASK can recover files from different

file systems, including FAT, FAT12, FAT16, FAT32, FreeBSD, EXT2, EXT3, OpenBSD, and UFS.

- TASK can work on binary images which do not have embedded checksum values. TASK cannot work on EnCase evidence files and SafeBack files. TASK works with only a single partition so image each partition on a drive separately in order to use this tool. TASK is used to recover previously deleted files in your binary image file created by dd.
- One can also use autopsy forensic browser for analyzing allocated files, previously deleted files, directories, data units, and metadata of forensic images in a read-only environment.

(iii) Using Foremost to Recover Lost Files

- Foremost is a Linux program used to recover or files based on the file headers and footers. Foremost is a portable, exceptional tool for data recovery. Foremost can work on forensic image files such as those generated by dd, SafeBack, and Encase, or act directly on a device.
- Foremost consults a configuration file at runtime. This configuration file specifies the headers and footers that Foremost is looking for so you can choose which ones you want to look for simply by editing the ***foremost.conf*** file.
- The Foremost can find GIF files, JPG files, common Microsoft Office documents, email repositories, HTML pages, PDF files, ZIP files, Windows Registry files, WordPerfect files, and even America Online (AOL) mail files.

6.6.3.2 Recovering Deleted Files on Unix Systems

- Recovering previously deleted files on Unix systems can be quite a challenge. Since most of the files you attempt to recover on Unix systems are flat text files. For recovering previously deleted files in Unix system you can use **debugfs** on files stored on the ext2 (second extended file system) file system.
- Debugfs is a very powerful tool in the hands of the computer forensic examiner. It is an interactive file debugger used to examine and to change the state of the ext2 file systems. The debugfs provides the best means for recovering files on media using the ext2 file system.

6.6.4 Recovering Unallocated Space, Free Space, and Slack Space

After doing the forensic duplication of media and recovering as many files as you can, there is still data left on the evidence media that you will want to review. The remaining data is

stored in ***slack space***, ***unallocated space***, and ***free space***. In order to understand slack space and unallocated space, we must first review what an ***allocation unit*** or ***cluster*** is.

Cluster

- Operating systems arrange all data stored on a hard drive into segments called allocation units (also called ***clusters***). For example, an operating system that uses 32K clusters reads and writes data from a hard drive 32K at a time. It cannot read less than 32K of data from a hard drive, and it cannot write less than 32K at a time to the hard drive.
- However, very few files have the exact amount of data to occupy an entire cluster or set of clusters. Therefore, when an operating system that writes 32K clusters to a hard drive is being asked to save a 20K Microsoft Word document, there is 12K of unused space called ***file slack***. In our example, there may be remnants of previous files in this 12K of file slack.

Unallocated space

- Unallocated space is the area of the hard drive which is not currently allocated to a file. Sections of deleted files are frequently scattered crosswise over unallocated space on a hard drive. ***Free space*** is the segment of the hard drive media that is not inside of any currently active partition.
- MS-DOS tools have been written that examine the information on a hard drive and create files that contain all the information inside of the unallocated space, free space, and slack space on a drive. To write the contents of slack space and free space to a file the NTI'S tools are used.
- These tools are powerful and simple. The tools EnCase and FTK automatically uncover slack space and unallocated space on the qualified forensic duplication. The advantage of these tools is there is no need to restore the original evidence to its own hardware.

6.6.5 Generating File Lists

- It is a very risky step to create informative file listings. The following information is contained by a listing of these files: Full path of each file found on the evidence media.
  1. Last written and modified time/date stamps for each file.
  2. Time or date stamp generation.
  3. Date/time stamps of last access.
  4. The logical size of each file.
  5. An MD5 hash of each file.

- Comparing the MD5 hashes of "known-good" files with all the files on the evidence media is the investigative step. It is not exceptional to take out more than 50 percent of the files on a Windows system from your analysis in light of the fact that the files have a known-good reason.
- For instance, you might find that the files are operating system files or application files that probably won't add to your case. On the rear side, it is not uncommon to utilize the MD5 hashes of "known-awful" files with an end goal to rapidly find files that are pointers of malicious intent. For the listing, metadata file use Encase, FTK and CATALOG (a command line Linux tool) tools.

Identifying Known System Files

- It is important to identify the known file system as a large amount of data on any hard drive consists of known files, such as operating system and application files, which are usually not of probative value to any case. So to reduce the number of files to review, it is very helpful to identify and exclude from review the known operating system files.
- It is achieved by getting the hash values of the known files. MD5 file signature algorithm is used to create hash values for the known files. Forensic examiners compare the known hash values to the hash values of unknown files on a seized computer system.
- Where those values match, the examiner can say, with statistical certainty, that the unknown files on the seized system have been authenticated and therefore do not need to be examined. Another idea is to create hash sets of your own by using the md5sum command.

6.6.6 Performing String Searches

- The challenges in properly string search the media are :
  1. Numerous compressed file formats render conventional string searching ineffective.
  2. Compressed files, for example .tgz, .rar, .jar, .Z, .gz, .zip, arj, .lzh, packed files, and self-extracting archives all foil conventional string searching utilities.
  3. Encrypted files or password-protected files can't be audited until un-encrypted.
  4. There are some file formats with additional complexity when trying to perform string searches on the contents of a hard drive. For example Outlook's ".pst" and ".ost" files, Outlook Express's ".dbx" files, the Windows Registry files, the Windows event log files, the browser history files, and many other files all require special tools for proper forensic analysis.

- Before conducting the effective and complete string searches, you must :
  1. Discover all compressed files and decompress them.
  2. Discover all encrypted files and un-encrypt them.
  3. Discover all compressed files in email stores and decompress them.
- After you are certain that your string searches will be thorough by decompressing files and unencrypting everything you can, it is time to choose your string search criteria wisely and begin searching. grep, EnCase, and Autopsy tools are used string searches. The standard Unix tool "grep" is one of the most useful forensic tools.

Syllabus Topic : Reporting on the Findings

6.7 Reporting on the Findings

Q. 6.7.1 What are the goals of report ? *(Ref. Sec. 6.7)* **(5 Marks)**

Q. 6.7.2 Explain the report writing guidelines. *(Ref. Sec. 6.7)* **(5 Marks)**

Q. 6.7.3 Explain template for computer forensic report. *(Ref. Sec. 6.7)* **(5 Marks)**

The investigation will not be effective if the documentation is terrible. A forensic report has to document facts and offer opinions with a style of communication that gives decision-makers with useful, accurate information. In other words, a poorly written report hinders the progress of your case.

Report Goals

- Your report should meet some standards established by the organization. So, it is necessary that your forensic report should achieve the following goals:
  1. Details of the incident should be accurately described.
  2. A report should be understandable to decision-makers.
  3. A report should withstand a barrage of legal examination.
  4. A report should be clear and not open to misunderstanding.
  5. A report should be easily referenced (using paragraph numbers for the report and Bates numbers for attached documents).
  6. A report should Contain all data needed to explain your conclusions.

  7. A report should Offer valid conclusions, opinions, or recommendations when required.
  8. A report should be created in a timely manner.
- When you write a report, that report should meet the given goals and it is a very difficult challenge of doing incident response and computer forensics.

REPORT WRITING GUIDELINES

There are following incident reports writing guidelines :

1. Document Investigative Steps Immediately and Clearly
2. Know the Goals of Your Analysis
3. Organize Your Report
4. Follow a Template
5. Use Consistent Identifiers
6. Use Attachments and Appendices
7. Have Co-workers Read Your Reports
8. Use MD5 Hashes
9. Include Metadata.

1. Document Investigative Steps Immediately and Clearly

- This step needs discipline and organization for successful report writing. Write everything down in a way that it is understandable to you and others; do not use shorthand or shortcuts. Such unclear notations, incomplete scribbling, or unclear documentation will eventually lead to redundant efforts, forced translation of notes, confirmation of notes, and a failure to comprehend notes by yourself or others.
- Writing something clearly and concisely at the moment you discover evidence saves time and promotes accuracy. It also ensures that the details of the investigation can be communicated more clearly to others at any moment, which is critical should new personnel become involved or assigned to lead the investigation. This is known as the "write it tight" philosophy

2. Know the Goals of Your Analysis

- It is important to know what the goals of your examination are before you begin your analysis. It helps to foster a focused report. For law enforcement examiners, every crime

has elements of proof. Your report should unearth evidence that confirms or dispels these elements. It means that the more focused your reports are, the more effective they are.

- While hashing out the objectives of your forensic examination, you should also address issues such as the following :
- Does the client of your report need a single forensics report for each piece of media examined or a report of the investigation that encompasses all media analyzed?
- How does the client wish you to communicate your findings: verbally or in written form?
- How often does the client want a status report of your forensic examination?
- Should the interim status reports be verbal or written?
- Which examiner should sign as the provider or author of the forensic report?

➜ 3. Organize Your Report

- Write "macro to micro." Organize your forensic report to start at a high level, and have the complexity of your report increase as your audience continues to read it. This way, the high-level executives need to read only the first page or so to get the idea of your conclusions, and they should not need to understand the low-level details that support your claims. Include a table of contents for your longer reports.
- The table of contents enforces a logical approach to documenting your findings, and it helps the reader understand what your report accomplishes.

➜ 4. Follow a Template

Follow a standardized report template. The template makes your report writing scalable, establishes a repeatable standard, and saves time.

➜ 5. Use Consistent Identifiers

- In a report, instead of referring to an item in a different way like referring to the same computer as a system, PC, box, web server, victim system, and so on can create confusion. Developing a consistent, unwavering way to reference each item throughout your report is critical to eliminate such ambiguity or confusion. P:\010Comp\Hacking\696-x\ch17.vp Monday, June 23, 2003, 2:09:13 PM Color profile: Generic CMYK printer profile Composite Default screen It is a good idea to create a unique identifier or reference tag for each person, place, and thing (nouns) referred to repeatedly in your report. That label will identify the corresponding item for the remainder of the report.

- For example, if the report is a summary of your forensic analysis of a laptop system belonging to a suspect named John, you could reference the items in capital letters in the following manner: "We performed a forensic duplication to the laptop system belonging to John (JOHN), an employee of ABC Corporation.
- The system was a Dell laptop, SN 141607, hereafter referred to as the JOHN LAPTOP. An in-depth review of the JOHN LAPTOP revealed ...." We have reviewed expert forensic reports that refer to items in the report as tag 1 or evidence tag 2. Using descriptive labels such as JOHN LAPTOP the reader know precisely which piece of evidence you're talking about.

➜ 6. Use Attachments and Appendices

- Use attachments or appendices to maintain the flow of your report. Any information, files, and file fragments that you cite in your report that are over a page long should be included as appendices or attachments. Then, you can include a brief reference to the appendix in the report. For example, you might say, "A printout of the information is included as Appendix A."
- Consider including every file that contributes to your conclusions as an appendix to your report. It is also a great idea to Bates number any files you reference in your report so that every document that you cite in your report has a unique reference number.
- You should also provide an electronic copy of every file or file fragment you cite in your report which is too big or simply impossible to provide in a printed format. For example, large database files, lengthy source code files, and spreadsheets. For this type of reference, we provide an electronic copy instead of the printed copy and call it an eAppendix (electronic appendix).
- Simply burn a CD-ROM that contains all files that we cited in the report, and we append it as the last attachment in the report.

➜ 7. Have Co-workers Read Your Reports

- Employ other co-workers to read your forensic reports. This helps develop reports that are comprehensible to nontechnical personnel who have an impact on your incident response strategy and resolution. Write your reports at the appropriate level of the client of your report.
- Take into consideration the technical capability and knowledge of your audience. For example, if you are providing a computer forensics report to a nontechnical lawyer, it is a good idea to provide a glossary of terms tailored specifically for that report.

8. Use MD5 Hashes

- Create and record the MD5 hashes of your evidence, whether it is an entire hard drive or specific files.
- Performing MD5 hashes for all evidence provides support to the claim that you are diligent and attentive to the special requirements of forensic examination. If your evidence is handled properly and remains tamper-proof, the MD5 hashes calculated for a given set of data will always remain the same. By recording these MD5 values, your audience becomes confident that you are handling the data in the appropriate manner.

9. Include Metadata

Record and include the metadata for every file or file fragment cited in your report. This metadata includes the time/date stamps, full path of the file, the file size, and the file's MD5 sum.

This will help to remove any ambiguity about which files you reference during testimony. For example, the following table shows the files cited in the report. Specifically, it provides the file metadata for a Windows IIS web access log found on the C: partition (C:\WINNT\system32\LogFiles\W3SVC3\ex001215.log).

File Created	12/15/00 09:16:26AM
Last Accessed	11/14/01 08:47:11AM
Last Written	04/06/01 04:26:05AM
Logical Size	2,034,833
Hash Value	eb40d0678cd9cdfbf22d2ef7ce093273

We frequently add a Comment field to our file tables to provide a quick reference and reminder of why we cited the file in the report. It is shown as follows :

File Created	02/14/01 01:24:02AM
Last Accessed	11/14/01 04:41:11AM
Logical Size	208,144
Hash value	25d1ee046ebf4a758148f92cc39a8e7e
Comment	A copy of cmd, exe in a browser accessible directory. The MD5 sum is identical to c:\winnt\system32\cmd.exe.

When a single report includes data from multiple pieces of media (evidence), we need to include additional data in our file tables. This table includes an extra row illustrating the source media for the file.

Item :	Foundstone Evidence Tag#1, JOHN LAPTOP		
Directory :	\hda1\var\log		
File Name	Messages		
Creation Date :	N/A	Time :	N/A
Modification Date :	02/04/00	Time :	02:32:42 AM
Access Date :	01/29/00	Time :	09:39:00 AM
File Size :	2,400,995		
MD5 Checksum :	Afdf51b0af89efa754ff646626b55ba0		

There are chances of complexity to the metadata if the file you are citing was originally contained within a zip file or some other archive file. So in such cases provide the metadata for both the original zip file and the metadata for the cited file contained within that zip file.

A TEMPLATE FOR COMPUTER FORENSIC REPORTS

Any of the following sections could include in each forensic report by Your organization:

1. Executive Summary
2. Objectives
3. Computer Evidence Analyzed
4. Relevant Findings
5. Supporting Details
6. Investigative Leads
7. Additional subsections, such as Attacker Methodology, User Applications, Internet Activity, and Recommendations

1. Executive Summary

The Executive Summary section gives the background data of the conditions that realized the requirement for an investigation. The senior management reads translation summary, they do not go into the detailed report. So, this section should include short details (under a page long) i.e. only the things that matter.

The "Executive Summary" section is used to do the following :

1. Take account of who authorized the forensic examination
2. Describe why a forensic examination of computer media was necessary
3. List what the significant findings were (in short detail)
4. Include a signature block for the examiner(s) who performed the work.

Include the full and proper name of the all people who are involved in the case, a name of their employer, job titles, and the dates of initial communications.

The following are the few examples of significant findings which are the part of an Executive Summary section :

1. Three days before to leaving employment, Employee C emailed ten company confidential documents to Company B, a competitor.
2. Employee C did not have authorized access to these documents, but on his computer password cracking tools, along with "cracked" executive user passwords, were found.

➜ 2. Objectives

- In some cases, it may happen that the forensic examination may not do the full-scale investigation or fishing expedition when reviewing the contents of the media. The Objective section is used to outline all the tasks that our investigation planned to complete.
- The prepared plan list should be discussed and approved by legal counsel, decision-makers, the client before any forensic analysis. The task list should include the tasks undertaken and the method undertook by an examiner for each task and the status of each task at the end of the report.

➜ 3. Computer Evidence Analyzed

In the Computer Evidence Analyzed section, all the collected evidence and their interpretations are introduced. This section gives detailed information about the assignment of evidence tag numbers, media serial numbers, and descriptions of the evidence.

➜ 4. Relevant Findings

- The Relevant Findings section gives a summary of the findings of probative value. The answers to the questions are given, like "What related items were found in the investigation?"

- The relevant findings have to list in order of relevance to the case. In this section, findings are described in a logical and organized way. This section gives quick reference needed to high-level decision-makers and it is used at the time of describing the results of the investigation.

➜ 5. Supporting Details

- The in-depth analysis of the relevant findings is done in supporting details section. This section outlines how we found the conclusions outlined in the Relative Findings section. This section contains the table of important files with the full pathname, number of files reviewed, results of string searches, Emails/ URLs reviewed, and any other significant information.
- The Supporting Details section is used to outline all the tasks undertook to meet the objectives. In this section, we go into technical depth. It includes charts, tables, and illustrations as it conveys much more than written text.
- Many subsections are also included to meet the outlined objectives. This section is the longest section of our report.
- The supporting details section always starts by giving background details of the actual media analyzed. It is difficult to report the number of files reviewed and the size of the hard drive in human understandable language. So, your client must have to know how much information you wanted to review to arrive at your conclusions.
- The following table shows, how to report the size of the media inspected:

Size	6.8 GB
Files	~9828
Directories	~500

- The geometry of the evidence media is also given in the report. The following table illustrates it.

Partition	File system	Size	Logical drive
1	FAT32	3.00GB	C:\
2	Extended	12.15GB	N/A
5	NTFS	3.1GB	D:\
6	NTFS	5.6GB	E:\

We also include a table of string search results in the report. The following is the example:

Keyword	Number of hits reviewed
pornography	0
Client name	456
Source code	988
Rotation Raja	14

➜ 6. Investigative Leads

- This section outlines action items that could be carried out to discover additional information related to the investigation. Investigator performs all the outstanding tasks if more time and extra information resources are there.
- The investigative leads section is very critical to law enforcement. It is also necessary to document which is beyond the scope o forensic report for more generating compelling evidence and successful resolution of a case. This section is also important to a hired forensic consultant.
- The investigative leads section suggest the extra task that discover the information needed to move on the case. The example of investigative leads is, finding out whether there are any firewall logs that date far enough into the past to give a correct picture of any attacks that took place.

➜ 7. Additional Report Subsections

- There are numerous additional subsections included in forensic reports.
- The following subsections are useful in specific cases. These subsections are depended on the need and want of the client.

➜ 8. Attacker Methodology

This section gives the additional briefing to help the reader understand the general or exact attacks performed. This section is useful in computer intrusion cases. Here, you can inspect how the attacks are done and what the bits and pieces of the attacks look like in standard logs.

➜ 9. User Applications

- It is observed that in many cases the applications present on the system are very relevant, so in this section, we discuss the relevant applications that are installed on the media analyzed.

- Outline where the applications were found and what they do. If you are investigating any system that is used by the attacker then give a title to this section, for example, "Cyber-Attack Tools". This section is used in cases like accounting software on frauds, credit card number generation software on credit card fraud, and image viewing applications on a child pornography.

➜ 10. Internet Activity or Web Browsing History

- This section gives the web surfing history of the user of the media analyzed. This section included in administrative cases where an employee all day surfing the web.
- The browser history is also useful to suggest intent, downloads of malicious tools, unallocated space, and online research, downloads of secure delete programs, or evidence-removal type programs that wipe files slack, and temporary files that often harbor evidence very important to an investigation.

➜ 11. Recommendations

- Recommendation section gives the recommendation to posture the client to be more prepared and trained for the next computer security incident.
- To reduce or eliminate the risk of incident security we investigated, some host-based, network-based and procedural countermeasures are given to the clients.

Syllabus Topic : Testimony

6.8 Testimony

6.8.1 Preparing for Testimony

Q. 6.8.1 Explain how to prepare a testimony ? *(Ref. Sec. 6.8.1)* **(5 Marks)**

- When your case goes to court then the forensic examiner play 2 roles. One is the technical or scientific witness and second is an expert witness.
- As a technical or scientific witness, the forensic examiner gives only the information which is found in an investigation-any evidence that meets the relevance standard and is more probative than prejudicial.
- After giving the technical/scientific testimony, present this evidence and explain what it is and how it was acquired.

- As an expert witness, do not offer conclusions, but you can give your opinion about the findings. These opinions are formed from the experience and deductive reasoning based on information found in an investigation. Your (forensic experts) opinion makes him an expert witness.
- For any type of testimony in a computer forensics case, you have to prepare in detail. Establish communication before time with your lawyer.
- Before you begin to process the evidence, do the of the victim, the petitioner, opposing technical or scientific witnesses, and the opposing lawyer as soon as possible.
- Do the proper study of the basic points of the dispute.
- Prepare the notes about the case but keep the notes in rough draft form and record only the information, keep minimum opinions.
- In your preparation, verify your findings with your own documentation and by confirming with other computer forensics professionals.
- Return to the notes which you have prepared during your investigation. If you are working on electronic notes then store them carefully.
- Develop and maintain a standard procedure of processing in your analysis and report. It will minimize the confusion and help to prepare for testimony later.
- Perform the peer review process, to get the peer review search outside your region. Use your professional network and ask for peer reviews to help support your findings.
- Make use of the internet to study the strengths and weaknesses of opposing experts in previous testimony. If possible review their curriculum vitae and how they present themselves.
- Your lawyer might be able to get copies of statements they have given in other cases, typically from the deposition banks.
- There are few organizations of forensics investigators which maintain electronic mailing lists that you can utilize to query members about other expert witnesses.
- While preparing the testimony review the following questions :
  - What is my story of the case (the central facts relevant to my testimony)?
  - What can I say with confidence?
  - What is the client's overall theory of the case?
  - How does my opinion support the case?

  - What is the scope of the case? Have I gone too far?
  - Have I identified the client's needs for how my testimony fits into the overall theory of the case?

6.8.2 Documenting and Preparing Evidence

- It is important to document steps in gathering and preserving evidence to ensure that they are repeatable, in case you are challenged. If your findings are not repeated, then it results in losing the credibility as evidence. Additionally, ensure the integrity of your evidence by using the hashing algorithms and validate your tools.
- The following are the guidelines to ensure the integrity of your evidence:
  - Create a checklist to analyze evidence for a specific case. Your checklist should not be formal which is applied to your all cases. If your opposing counsel will get this checklist through discovery then you might be get challenged in cross-examination about variations in your performance, if you deviate from the checklist.
  - Collect the evidence and record the tools you used in chosen file folders or container of the evidence. Due to this method, your evidence and tools are organized properly.
  - Chain of custody of evidence supports the integrity of evidence. Prevent the evidence from contamination. So, document the lapse and the gaps in evidence preservation as this lapses or gaps may affect the power given to the evidence.
  - While gathering the evidence, be careful not to get too little or extra information. For court case, only collect the information what is asked for, not more than that. In some situations, if you collect and identify evidence which is not related to the case would create the problem for your lawyer.
  - Ensure that the date and time of the forensic computer are noted by you before you start the analysis. Consider the internet clock to avoid the correct time issue, for example, www.time.gov or you can also use the atomic clock.
  - Record the successful output when running analysis tools; discard the previous runs, for example, those missing necessary switch or output settings. Keep in mind that due to these missing settings you are not able to create output although you are using the tool.
  - When you perform the search for keyword results, rerun searches with clear keywords and search parameters. It may be possible that you want to relate the search result to your case, for example, personal names or business names. Try to narrow down your search to avoid the false hit and eliminate the false positive hits.

- Keep your finding notes simple and specific to the investigation. Avoid personal comments so that you do not have to give the explanation to opposing counsel.
- In report writing consider the evidence related to a case only, do not include unrelated findings.
- If you are using any method for conducting analysis as scientific and in compliance with your profession's standards then describe that procedure or method. If you are taking and listing the reference of textbooks, technical books, articles by renowned experts, and procedures from trustworthy organizations during your examination, it is a typical way to prove your conformity with scientific and professional standards.

6.8.3 Reviewing Your Role as a Consulting Expert or an Expert Witness

Q .6.8.2 Review the role of expert witness or consulting expert? *(Ref. Sec. 6.8.3)* (5 Marks)

- Based on your lawyer's requirement, you may give only your opinion and technical expertise to him instead of testifying in court; this role is known as a consulting expert. If your role changes from consulting the expert to expert witness afterward, but, your earlier work as a consulting expert is dependent on a discovery by opposing counsel.
- Due to this reason, do not record the telephone calls and conversations.whn you present yourself in front of a federal court as an expert witness, as per the Federal Rules of Civil Procedure (FRCP) 26 (2) (B) requires that you give the following information:
  - Other cases in which you have testified as an expert at trial in the preceding 4 years.
  - Ten years of any published writings.
  - Previous compensation you have received when giving testimony.
- Additionally, a court can also appoint its own expert witnesses. These appointed witnesses have to be neutral in their opinions, and knowledgeable in their field. You have to evaluate the court's expert as it is hired by the defense or claimant; ensure that you have briefed your findings and opinion of the court's expert so it will help your lawyer deal with any testimony the court-appointed expert provides.

6.8.4 Creating and Maintaining Your CV

- It is important to maintain the updated curriculum vitae (CV) for forensics specialists, as it lists your professional experience. It is also used to qualify your testimony and your role as an expert.

- The updated CV shows your constant enhancements in your skills through training, teaching, and experience. It also shows the tasks you have done that describe your particular accomplishments and your basic and advanced skills.
- Describe your general and professional education and profession training in the CV. If the training list is long then use heading as "Selected Training Attended."
- Ensure that you have included coursework sponsored by government agencies that train government agency personnel and courses sponsored or approved by professional associations, for instance, bar associations. As well, note any professional training you gave or contributed to.
- Also, include a testimony log. This log reflects each testimony you have given as an expert. Ensure that your CV reflects your professional background; it should not gear toward a particular trial.
- Update your CV till current date for version control, if it is more than three months old, update it.

6.8.5 Preparing Technical Definitions

- Prepare the technical definitions of the concepts before you testify in court. These definitions can be used when your layer or the opposing lawyer question. Ensure that you have used your own words, and remember that you are explaining these concepts for a nontechnical audience. You just have to explain the meaning of the terms.
- The following are the examples of the definitions which you have to prepare for your testimony :
  - Computer forensics
  - hashing algorithms: CRC-32, MD5, and SHA-1
  - Image and bit-stream backups
  - File slack and unallocated space
  - File timestamps
  - Computer log files
  - Folder or directory
  - Operating system
  - Hardware
  - Software.

6.8.6 Preparing to Deal with the News Media

– There are some legal actions that attract the news media, but you should avoid contact with news media, particularly throughout a case, for the following reasons :

- Your comments may harm the case and make a record that can be used against you.
- You have no control over the context of the information a journalist publishes.
- You cannot rely on a journalist's promises of privacy. Journalists are violent in getting information, and their interests do not match with yours or your client's.
- Be cautious all times as your remarks could be deciphered in a way that pollutes your impartiality for this situation and future cases.
- Indeed, even after the case is settled, abstain from examining subtle elements with the press. In case you're requested for data or conclusions by journalists (or any other person), abstain from saying anything, and allude them to your customer (the lawyer who held you). *In the event that you* can't avoid a journalist, counsel with your lawyer and decide how to deal with the circumstance. Plan to record any endeavored meetings with the goal that you have your own record of what happened. (Note, in any case, that state law on assent for account change).
- This chronicle can be vital in case you're misquoted or cited outside of any relevant connection to the issue at hand. Columnists frequently search for an incredible Sound nibble or dubious statement.

6.9 Exam Pack (Review Questions)

Q. 1 What is mean by Evidence? *(Refer section 6.1)* **(5 Marks)**

Q. 2 What are the types of evidence ? *(Refer section 6.1.1)* **(5 Marks)**

Q. 3 Explain the characteristics of the evidence ? *(Refer section 6.1.2)* **(5 Marks)**

☛ Syllabus Topic : Authorization to collect the evidence

Q. 4 Write a short note on Authorization to collect the evidence. *(Refer section 6.2)* **(5 Marks)**

☛ Syllabus Topic : Acquisition of Evidence

Q. 5 Write and explain the steps taken to collect the live data *(Refer section 6.3)* **(10 Marks)**

Q. 6 What is forensic duplicate ? When forensic duplicate is admissible ? *(Refer sections 6.4 and 6.4.1)* **(5 Marks)**

Q. 7 Write short note on Qualified Forensic Duplicate? *(Refer section 6.4.1.2)* **(5 Marks)**

Q. 8 Write short note on Restored Image ? *(Refer section 6.4.1.3)* **(5 Marks)**

Q. 9 What are the forensic duplication tool requirements ? *(Refer section 6.4.2)* **(5 Marks)**

Q. 10 How to create a forensic duplicate of a hard drive ? *(Refer section 6.4.3)* **(5 Marks)**

Q. 11 How to create a qualified forensic duplicate of a hard drive ? *(Refer section 6.4.4)* **(5 Marks)**

☛ Syllabus Topic : Authentication of the Evidence

Q. 12 Explain what is mean by authentication of evidence ? *(Refer section 6.5)* **(5 Marks)**

☛ Syllabus Topic : Analysis of the evidence

Q. 13 What are the steps for preparing the forensic analysis ? *(Refer section 6.6)* **(5 Marks)**

Q. 14 Explain the process of restoring the forensic duplicate ? *(Refer section 6.6.1)* **(5 Marks)**

Q. 15 Explain the process of restoring the forensic duplicate ? *(Refer section 6.6.2)* **(5 Marks)**

Q. 16 How to Recover Deleted Files on Windows Systems? *(Refer section 6.6.3.1)* **(5 Marks)**

☛ Syllabus Topic : Reporting on the findings

Q. 17 What are the goals of report? *(Refer section 6.7)* **(5 Marks)**

Q. 18 Explain the report writing guidelines? *(Refer section 6.7)* **(5 Marks)**

Q. 19 Explain template for computer forensic report? *(Refer section 6.7)* **(5 Marks)**

☛ Syllabus Topic : Testimony

Q. 20 Explain how to prepare a testimony? *(Refer section 6.8.1)* **(5 Marks)**

□□□

Chapter Ends...