UNIT-2

Initial Response:

An initial live response is usually performed when you have decided to conduct a forensic duplication of the media. In-depth response This goes beyond obtaining merely the volatile data. The CSIRT obtains enough additional information from the target/victim system to determine a valid response strategy.

The goal of initial response is :

1.Confrom there is an incidence

2.Retrive the system volatile data.

WHAT ARE THE GOALS OF INCIDENT RESPONSE?

In our incident response methodology, we emphasize the goals of corporate security professionals with legitimate business concerns, but we also take into consideration the concerns of law enforcement officials.

Thus, we developed a methodology that promotes a coordinated, cohesive response and achieves the following:

▼ Prevents a disjointed, noncohesive response (which could be disastrous)

■ Confirms or dispels whether an incident occurred

■ Promotes accumulation of accurate information

■ Establishes controls for proper retrieval and handling of evidence

■ Protects privacy rights established by law and policy

■ Minimizes disruption to business and network operations

■ Allows for criminal or civil action against perpetrators

■ Provides accurate reports and useful recommendations

■ Provides rapid detection and containment

■ Minimizes exposure and compromise of proprietary data

■ Protects your organization’s reputation and assets

■ Educates senior management

▲ Promotes rapid detection and/or prevention of such incidents in the future (via lessons learned, policy changes, and so on)

WHO IS INVOLVED IN THE INCIDENT RESPONSE PROCESS?

Incident response is a multifaceted discipline. It demands a myriad of capabilities that usually require resources from several different operational units of an organization. Human resources personnel, legal counsel, technical experts, security professionals, corporate security officers, business managers, end users, help desk workers, and other employees may find themselves involved in responding to a computer security incident. Most organizations establish a team of individuals, often referred to as a Computer Security Incident Response Team (CSIRT), to respond to any computer security incident. The CSIRT is a multi disciplined team with the appropriate legal, technical, and other.

INCIDENT RESPONSE METHODOLOGY:

We are always on a quest for the perfect way to organize a process. We search for the right way to define phases of the process, look for bright-line separation of phases to avoid murky areas, try to make the perfect flowchart to illustrate the process, and organize the phases so the process can be applied to the widest range of possible scenarios. Since the incident response process can involve so many variables and factors that affect its flow, it is quite a challenge to create a simple picture of the process while maintaining a useful level of accuracy. However, we feel that we have developed an incident response process that is both simple and accurate.

Computer security incidents are often complex, multifaceted problems. Just as with any complex engineering problem, we use a "black box" approach. We divide the larger problem of incident resolution into components and examine the inputs and outputs of each component. Figure 2-1 illustrates our approach to incident response.

In our methodology, there are seven major components of incident response:

▼ **Pre-incident preparation** :Take actions to prepare the organization and the CSIRT before an incident occurs.

■ **Detection of incidents:** Identify a potential computer security incident.

■ **Initial response:** Perform an initial investigation, recording the basic details surrounding the incident, assembling the incident response team, and notifying the individuals who need to know about the incident.

■ **Formulate response strategy:** Based on the results of all the known facts, determine the best response and obtain management approval. Determine what civil, criminal, administrative, or other actions are appropriate to take, based on the conclusions drawn from the investigation.

■ **Investigate the incident:** Perform a thorough collection of data. Review the data collected to determine what happened, when it happened, who did it, and how it can be prevented in the future.

■ **Reporting:** Accurately report information about the investigation in a manner useful to decision makers.

▲ **Resolution:** Employ security measures and procedural changes, record lessons learned, and develop long-term fixes for any problems identified.

Forensic Duplication:

A forensic duplication is an accurate copy of data that is created with the goal of being admissible as evidence in legal proceedings. Furthermore, we define forensic duplication as an image of every accessible bit from the source medium.

The data may consist of single file, a group of files, a partition on a hard drive, an entire Harddrive, on other elements of data storage devices and the information stored on them.

A forensic duplication is an accurate copy of data that is created with the goal of being admissible as evidance in the legal procedings.

What is a Forensic Duplicate?

A file that contains every bit of informationv from the source in a raw bitstream format.

Tools that create forensic duplicates:

1. dd
2. FTK Imager, Access Data
3. Dfcldd, US DOD Computer Forensics Lab version of the dd comand.

Qualified Forensic Duplicate?

- A file that contains every bit of informationv from the source, but may be stored in a altered form.
- Tools that create qualified forensic duplicatev output files:
  1. SafeBack
  2. EnCase
  3. FTK Imager

Initial Response & Volatile Data Collection from Windows system:

Volatile Data Collection Strategy:

Step 1: Incident Response Preparation.
Step 2: Incident Documentation.
Step 3: Policy Verification.
Step 4: Volatile Data Collection Strategy

Volatile data collection from Window system:

Volatile data is the data that is usually stored in cache memory or RAM. This volatile data is not permanent this is temporary and this data can be lost if the power is lost i.e., when computer looses its connection.
During any cyber crime attack, investigation process is held in this process data collection plays an important role but if the data is volatile then such type of data should be collected immediately. Volatile information can be collected remotely or onsite. If there are many number of systems to be collected then remotely is preferred rather than onsite.

It is very important for the forensic investigation that immediate state of the computer is recorded so that the data does not lost as the volatile data will be lost quickly. If the volatile data is lost on the suspects computer if the power is shut down, Volatile information is not crucial but it leads to the investigation for the future purpose. To avoid this problem of storing volatile data on a computer we need to charge continuously so that the data isn't lost. So that computer doesn't loose data and forensic expert can check this data sometimes cache contains Web mail.

Live Response:

Investigators today face a number of issues where unplugging a system (or several systems) and acquiring an image of the hard drive(s) might not be an option. As the use of e-commerce continues to grow, system downtime is measured in hundreds or thousands of dollars per minute, based on lost transactions. Therefore, taking a system down to acquire a hard-drive image has a serious effect on the bottom line. Also, some companies have service-level agreements (SLAs) guaranteeing "five nines" of uptime—that is, the company guarantees to its customers that the systems will be up and operational 99.999 percent of the time (outside of maintenance windows, of course). Taking a system with a single hard drive offline to perform imaging can take several hours, depending on the configuration of the system.
The Information Superhighway is no longer just a place for joy riders and pranksters. A great deal of serious crime takes place in cyberspace, and criminal activities are becoming increasingly sophisticated. Software programs can get into your computer system and steal your personal information (passwords, personal files, income tax returns, and the like), yet the code for some of

these programs is never written to the hard drive; the programs exist only in memory. When the system is shut down, all evidence of the program disappears.

In April 2006, Seagate introduced the first 750GB hard drives. Today, I regularly see external hard drives available in sizes greater than 1.5 terabytes (TB), and I see multiterabyte storage systems on customer networks. Imagine a RAID 5 system with eight 1TB hard drives, topping out at 8 TB of storage. How long would it take you to image those hard drives? With certain configurations, it can take investigators four or more hours to acquire and verify a single 80GB hard drive. And would you need to image the entire system if you were interested in only the activities of a single process and not in the thousands of files resident on the system?

In some cases**,** we might want to collect some information about the live system before shutting it down, acquiring a bit-stream image of the hard drive or drives, and performing a more traditional computer forensic investigation. The information you would be most interested in is volatile in nature, meaning that it ceases to exist when power is removed from the system. This volatile information usually exists in physical memory, or RAM, and consists of such things as information regarding processes, network connections, the contents of the Clipboard, and so on. This information describes the state of the system at the time you are standing in front of it or sitting at the console or accessing it remotely. As an investigator, you could be faced with a situation in which you must quickly capture and analyze (covered in the next topic) data to determine the nature and scope of the incident. When power is removed from the system in preparation for imaging the hard drive in the traditional manner, this information simply disappears. However, you also need to keep in mind that any actions you take (e.g., running antivirus scans, searching for files or credit card data, reconfiguring the system, etc.) on a live system are going to leave artifacts of their own, and possibly will overwrite useful or pertinent data. Therefore, collecting and preserving this volatile data should be your first concern.

We do have options available to us—tools and techniques we can use to collect this volatile information from a live system, giving us a better overall picture of the state of the system as well as providing us with a greater scope of information. This is what "live response" entails: accessing a live, running system and collecting volatile (and in some cases, nonvolatile) information.

There is another term you might hear that is often confused with live response: live acquisition. Live response deals with collecting volatile information from a system; live acquisition describes acquiring the hard drive while the system is still running and creating an image of that hard drive. In this topic, we'll start by discussing tools, techniques, and methodologies for performing live response. When we talk about performing live response, we need to understand what information we want to collect from the system and how we should go about collecting it. In this topic, we will walk through the what and how of collecting volatile information from a system; in the next topic, we will discuss how to analyze this data. Following that, we will examine some solutions for performing a live acquisition.

Before we start discussing live-response tools and activities, we need to address two important topics: Locard's Exchange Principle and the order of volatility. These concepts are the cornerstones of this topic and live response in general, and we will discuss them in detail.

This volatile data may contain crucial information.so this data is to be collected as soon as possible. This process is known "Live Forensics".
This may include several steps they are:

1. Initially create response tool kit.
2. Storing in this information which is obtained during initial response.
3. Moving of data using netcat
    - Netcat is a freely available tool that can be used to establish a communication between hosts.
    - Use netcat to establish connection between the forensic workstation and target system.

4. Then obtain volatile data
5. Then after that performing in in-depth live response.
6. Documenting and managing the investigation.
7. Collecting temporary data.

Live Investigation Goals Obtain enough information to determineν appropriate response. Considerations include totality of theν circumstances Learn before respondingθ Two goals:
1. Confirm there is an incident
2. Retrieve volatile system data

Won't be there after system powered off
4. Creating a Response Toolkit Without affecting any potential evidence, planν to obtain all relevant information.
By collecting trusted files on a CD, you arεν better equipped to respond: Quicklyν Professionallyν Successfully
5. Some Common Tools and Sources Cmd.exeν PsLoggedOn SysIntν rasusers NTRK netstat fport FS PsList SysIntν ListDLLs FS nbstat arp kill NTRK md
5.sum etree.org rmtshare NTRK netcat atstakeν cryptcat sourceforget PsLogList FS ipconfig PsInfo SysInt PsFile SysInt PsService SysInt auditpol NTRK doskeyν
6. Tool Interface Categories Graphical or command line GUI or CLI Since GUI programs create windows, havεν pull down menus, and generally do "behind the scenes" interaction, the text authors advise against using them during an investigation.
7. Preparing the Toolkit Label response toolkit media with: Case numberθ Time and dateθ Name of investigatorθ Presence of output files?θ Check for dependencies (Filemon)ν Create toolkit checksumν Write protect any toolkit floppies.

8. Storing Information Obtained During the Initial Response Live refers to a currently powered on system. Environment untrusted Unexpected should be anticipated.
Four options :
1. Save the retrieved data to a hard dive
2. Record data in a notebook by hand
3. Save data onto the response floppy disk or other removable storage medium
4. Save data on a remote system using net or cryptcat 9 Transferring Data with Netcat .
Netcat can create a connection between thev target system and the forensic workstation. Allows you to review information offline.
After the data transfer is complete, you will need to break the connection.
On the forensic workstation, press CTRL-C.θ
Integrity with md5sum Protect the integrity of retrieved files.
Among other places, you can get md5sum for windowsθ from etree.org
Perform the md5sum in the front of witnesses.
Process Summary Run trusted commands on NT Server.
Send output to forensics box with NetCat Md5sum files Perform off-line review.

Data to Collect:

- System date and time
- Users currently logged on
- Time/date stamps for the entire files system
- Currently running processes
- Currently open sockets
- Applications listening on open sockets
- Systems that have current or recent system connections

Sample Data Collection Process:

1. Execute trusted shell

2. Record system time and date

3. Determine who is logged on

4. Record modification, creation, and access times of all files

5. Determine open ports

6. List applications associated with open ports

7. Determine running processes

8. List current and recent connections

9. Record the system time

10. Record the steps taken

11. Record cryptographic checksums

Encrypting Data with Cryptcat :

Cryptcat has the same syntax and functionsν as netcat Encrypted data transfer. Encrypting files means that: Attacker's sniffer cannot compromise your information (Unless your passphrase is compromised.)

Encryption nearly eliminates risk of data contamination or injection.

Volatile Data for Live Response:

Only available prior to system power off. Possible data items include:

1. System date and time
2. Currently logged on users
3.Time/date stamps for entire file system
4. Currently running processes
5.Currently open sockets
6. Applications listening on open sockets
7. Systems that have current or recent connections to the system.

Collecting Volatile Data :

1. Execute trusted cmd.exe
2. Record system time and date
3. Determine logged users
4. For all files, record modification, creation, and access times.
5. Determine open ports.
6. List applications associated with open ports
7. List all running processes
8. List current and recent connections
9. Document commands used during initial response.

Gathering Data One:

For all files, record modification, creation, andν access times

Direct Determine open ports Fport.

Enumerate all running processes on the target system PsList.

Note, to identify abnormal processes, you first need to have identified normal processes i.e. done a baseline.

Gathering Data Two :

- ✓ List current and recent connections
- ✓ Netstat can determine current connections as well as the remote IP address of those connections
- ✓ Arp cache contains IP addresses mapped to MAC addresses
- ✓ Use nbtstat to access the remote NetBIOSv name cache

In Depth Live Response:

- ❖ Date and time commands
- ❖ PsLoggedOn
- ❖ Netstat
- ❖ PsList
- ❖ Fport
- ❖ Safeback or EnCase.

In Depth Response Tools :

- ❖ Auditpol NTRK
- ❖ Reg NTRK
- ❖ Regdump NTRK
- ❖ Pwdump3e
- ❖ NTLast FS
- ❖ Sfind FS
- ❖ Afind FS
- ❖ Dumpel NTRK

Collecting Live Response Data:

- ❖ Review
  - Event logs
  - Registry
- ❖ Obtain system passwords
- ❖ Dump system RAM.

Obtaining Event Logs during Live Response:

1. Auditpol discovers which audit policies exist

2.NTLast allows you to monitor successful andv failed system logons

3.Dumpel can retrieve remote logs

Initial Response & Volatile Data Collection from Unix system:

The initial response to prospective incidents on Unix systems is similar to the initial re- sponse for incidents on Windows systems. Your goal is to obtain the volatile system data before forensic duplication. You can expand the scope of your initial response to obtain log files, configuration files, system files, and relevant files (such as hacker tools and suspicious programs) to rapidly confirm whether or not an incident occurred.

One difference between working with Windows and Unix systems is the difficulty of recovering deleted files on some Unix variants. When you execute a process in the Win- dows environment, you cannot delete the file corresponding to the running process from the hard drive. However, the Unix operating system allows you to delete a program after it has been executed—the process is running, yet the program's file has been deleted from the hard drive. In this chapter, we discuss why you should recover these files before shut- ting down the system, as well as how to create your response toolkit, obtain volatile data, and conduct a live response.

With the rapid development of information technology, the computer continuously spread to people's work and life, it brings more and more for the convenience of the people at the same time, also becomes a powerful tool for criminals.

A presence on the computer and related peripheral devices has become a new form of digital evidence.

Digital evidence in itself has many characteristics different from traditional physical evidence.

From the computer system to extract the required data as evidence in court has raised new challenges to the law and computer science.

"Computer forensics" the term comes from the IACIS (International Association of Computer Specialists) the International Conference which was first held in 1991, and it was called at the time the main topic at the annual meeting of the 13 session of the International FIRST (Forum of Incident Response and Security Teams) in 2001.

As the computer field and legal field of an interdisciplinary science, computer forensics is gradually becoming the focus of research and attention.

This paper includes the computer forensics technology, Forensic analysis on Windows Forensic analysis on Unix.

The basic method of preserving, detecting and obtaining the electronic evidences was described .

A working definition of Computer Forensics can be formulated as the pursuit of knowledge by uncovering elemental evidence extracted

Conducting an investigation on Unix systems is very similar to conducting one on Windows systems. The forensic analyst must understand how Unix allocates and deletes files in order to know where to look for the contents and attributes of files that exist (and potentially hidden) and are deleted.

But the idiosyncrasies of Unix provide the investigator with different approaches to analyzing the data on Unix systems versus windows systems. Unix and Windows view files very differently.

Unix uses the concept of inodes (index nodes) to represent files.

Each inode contains the pointers to the actual data on the disk as well as file attributes useful to the investigator; these include the owner ID, access Permissions (read, write, execute), the number of links (number of directories referencing the file), the MAC times which are the last modification, access, and change of status (change of owner, permission or number of links), and file size.

Note that the filename is not included with the inode. Instead the file name is stored as an entry in the directory structure along with the location of the actual inode.

Like the NTFS on a Windows system, the Unix file system allocates data in fixed sized pieces called blocks.

This is analogous to the clusters used by the NTFS.

Therefore, file slack, the space between the end of a file and the end of the cluster, is also found on unix systems as well as Windows systems because not all files fit exactly into the blocks on the disk.

Forensic analysts can examine the file slack for remnants of deleted files and attributes.

File deletion in Unix involves marking the directory entry for that file name to marked as unused, resulting in the disconnection of the file name with the actual file data and attributes.

The inode of the file is marked as unused and some but not all of attribute information is lost.

The file data blocks are marked as unused according to the creators of the Unix forensics toolkit, The Coroner's Toolkit (TCT), the deleted file data and attributes remain for long periods of time such as hundreds of days for heavily used systems because Unix has good file system locality files tend to be clustered together instead of randomly space apart.

Unix file systems avoid fragmentation as much as possible to achieve this locality, allowing deleted files and attributes to remain much longer on the disk since chances are slim that the new files to be written to the disk are the same size as these deleted files.

So, deleted files may be easier to recover on Unix systems than on Windows. The Coroner's Toolkit is widely used to examine Unix systems and contains many useful utilities for forensic analysts.

One such tool is the unrm, a tool that un deletes files. Deleted file attributes can be recovered using the ils tool in the TCT.

Remember that file attributes are very important to investigators, especially the MAC times. Even TCT includes a tool called mactime that neatly displays the MAC times of a file.

Everything in Unix is a file. So any transactions done within Unix will leave evidence of that the transaction occurred because the MAC times for the associated files will be altered.

Analysts can examine the MAC times of files in Unix like the MAC times of files in Windows to show that the suspect had knowledge of the existence and contents of a file.

However, skilled hackers can alter the MAC times to hide their tracks within the file system since inode information is stored in the file system. So investigators should not completely trust the MAC times of files.

Unix tools can be used to examine the contents of the hard drive. Commonly used commands include find, grep, and strings.

Analysts can use these tools to form keywords to search for a specific piece of data like an email or pornography.

The TCT includes a tool called lazarus that attempts to classify the blocks of data as text files or binaries.

With text files, lazarus checks for the keywords that the analyst has requested in the form of regular expressions.

Places on the hard drive that the analyst could look for remnants of files are nearly the same as those on Windows systems.

In addition to the file slack mentioned earlier, investigators can search through the Unix swap file (similar to the Windows swap file), and of course, the unallocated space occupied by unused and deleted files. In addition, for each user in Unix there is a directory named /tmp that holds temporary application files.

This is similar to the situation in Windows with temporary application files being created; the contents of these temporary files may still exist in the /tmp directory at the time of the investigation and may be used as evidence against the suspect.

Unix gives the users the ability to repeat commands used in previous sessions.

In order to do this, the commands are saved in a shell history file.

Thus the shell history file can be examined to trace the steps of a hacker or to show that the suspect knowingly created, modified, accessed, and/or deleted a specific file. However, a user (or hacker) can clean out the shell history file to cover his tracks.

So, the shell history file can be useful only some of the time, especially if no attempt has been made at modifying it.

Forensic analysis of a Unix system shares some characteristics with that of a Windows system.

The search for deleted data involves looking in the same kinds of spaces like the unallocated space, file slack, and swap space.

But investigation of Unix systems can involve the use of Unix tools that help in the search for certain patterns among the contents of the disk. In addition, unix forensics

CREATING A RESPONSE TOOLKIT:

Preparing your trusted toolkit is more difficult and time-consuming than it sounds, because practically every variant of Unix requires a unique toolkit. Since many of the tools we rec-ommend are not included with the standard release of all Unix operating systems, you must compile the source code on your own. For example, if the victim machine is a Sparc server running Solaris 2.8, you need to compile your tools on a clean copy of Solaris 2.8 on a system with the same architecture.

When we refer to Unix, we are collectively referring to all Unix variants. Specifically, we are most famil- iar with Sun Solaris, Hewlett-Packard's HP-UX, FreeBSD, and Linux (RedHat, SuSE, and Corel). Our examples and response strategies are based on our experiences with these operating systems, which are the most common. If you know how to respond to incidents of these Unix flavors, you should be able to handle any other variants that you may encounter (such as IBM's AIX).

To complicate matters further, many Unix versions are not backward or forward compatible. For example, programs compiled to run on a Solaris 2.6 system may not work correctly on Solaris 2.7, and vice versa.

All these issues increase the amount of resources and time required for creating your Unix response toolkits. Therefore, it is essential to create the response toolkits prior to an incident. You may not have the time to create one after an incident occurs.

When you respond to an incident, you must choose where to store information retrieved during the initial response. You have the following storage options:

▼ Store the data on the local hard drive.

■ Store the data to remote media such as floppy disks, USB drives, or tape drives.

■ Record the information by hand.

▲ Use netcat(or cryptcat)to transfer the retrieved data to a forensic workstation over the network.

Storing data on the local hard drive should be avoided whenever possible. If data re- covery or forensic analysis is required, the data you store on the local hard drive will overwrite deleted data that was in unallocated space that may be of investigative and/or evidentiary value.

Since only newer versions of Linux support USB drives, they are not as useful for data collection by direct physical connection. However, you can overcome this limitation by us- ing netcat transfer the data over the network to a forensic workstation equipped with a USB drive or other adequate storage. We use Linux on our forensic workstations to provide a faster response. This way, we are rarely impeded by limitations of storage space. We use netcat to transfer the information across the network, and "pipe" the netcat stream through des to encrypt the transfer. The crypt cat command offers an encrypted TCP channel in a single step. (See Chapter 5 for details on using netcat and crypt cat.)

After selecting how you will retrieve the data from the target system, you must con- sider the best time to respond (usually when the attacker or most users are not online). You will also want to determine whether the target system must maintain network con- nectivity or if you will pull the network cable to prevent users and attackers from con- necting to the system during your initial response. When these issues have been resolved.

Initial Response & Volatile Data Collection from Unix system Steps:

1. **Creating response tool kit:**
   - Preparing your trusted toolkit is more difficult and time-consuming than it sounds, because practically every variant of Unix requires a unique toolkit.
   - Since many of the tools we rec- ommend are not included with the standard release of all Unix operating systems.

2.Saving information obtained at the time of initial response:

- You must choose where to save information retrive at the time of intial response.
- Saving the data on local drives should be avoided.
- The information you save on the local hard drive will distroy the deleted data.

3.Obtaining voltile data before forensic duplication:

- Run a trusted shell.
- Record the time and date of the system.
- Identify who is currently logged on the system.
- Record creation ,alteration and access time of each file.
- Identify open port.
- Enlist application associated with open port.
- Identify the running process.
- List of the current and recent connections.
- Record the time of the system.
- Record the steps taken.
- Record cryptography checksum.

Forensic Duplication

Forensic duplication:

A forensic duplication is an accurate copy of data that is created with the goal of being admissible as evidence in legal proceedings.

A file that contains every bit of information from the source in a raw bitstream format.

• Some data on a hard disk or SSD isn't normally used to store user data

• It contains firmware

• "Host Protected Area" (HPA)

• Not normally included in a forensic image

Tools that create forensic duplicates:

1. dd

2. FTK Imager, Access Data

3. Dfcldd,

US DOD Computer Forensics Lab version of the dd comand.

Furthermore, we define forensic duplication as an image of every accessible bit from the source medium.

We encourage you to consider all data you collect as evidence that may contribute to a legal process. To that end, you should perform duplication with methods that are generally accepted in the forensic community.

Type of image formats are:

1. Complete image
2. Partition
3. Logical

Three Data Types:

• Active data

• Files and folders in use, in the directory

• Unallocated Space

• Remnants of deleted files

• File slack

• Fragments of data left at the end of other files Partition Image

• Not a common technique

• May be required because of limited scope of authority, or an excessively large disk

• All allocation units from a partition

• Allows recovery of deleted files on that partition only

• But not unpartitioned space, reserved areas, or other partitions

Types of Duplication:

• Simple duplication

• Copy selected data; file, folder, partition...

• Forensic duplication

• Every bit on the source is retained

• Including deleted files

• Goal: act as admissible evidence in court proceedings

Forensic Duplicates as Admissible Evidence:

Existing legal standards define minimumv criteria for an item to be admitted into evidence.

Collection process usually under scrutiny as well.

Federal Rules of Evidence:

Federal Rules of Evidence (FRE) 1002 state that the item or information presented in court must be the original.

Exceptions: Definitions and Duplicates

If data are stored by computer or similar device, anyv printout or other output readable by sight, shown to reflect the data accurately, is an original.

Admissibility of Duplicates A duplicate is admissible to the same extent as anν original unless:

• A genuine question is raised as to the authenticity of the original, or

• In the circumstances it would be unfair to admit the duplicate in lieu of the original

Legal Issues :

Tools used for forensic duplication must passν the legal tests for reliability.

Note, when tool is generally accepted by others in the field, it is easier to prove that information was gathered in a reliable, accurate manner.

- Forensics Duplicates as Admissible Evidence As familiarity with digital data increases, behavior of the judicial system will increase in rationality.
- Reasons for Forensics Duplication The examination can destroy evidence inadvertently. The original computer system might only be available for capturing.
- Definition of Forensic Duplication Able to produce identical byte stream from duplicate as from the original.
- Definitions Forensic Duplicate: File that contains every bit of information from the source in a raw bitstream format. Qualified Duplicate: Same as above, but allows embedded metadata or certain types of compression.
- Definitions Restored Image: A forensic duplicate or qualified forensic duplicate restored to another storage medium. Difficult to do if second hard drive does not have the same geometry as the previous one.
- Definitions Mirror Image created from hardware that does a bit- to-bit copy from one hard drive to another. Issue with disk and file system metadata such as boot sectors.
- Creating a Forensics Duplicate of a Hard Drive Hardware Mirroring. Can be done in the field.
- Creating a Forensics Duplicate of a Hard Drive Software tools: Unix dd Tested and proven. Runs on Unix/Linux/Mac OS X which can recognize almost any hardware. Free.
- Creating a Forensics Duplicate of a Hard Drive Software tools: Encase Expensive. Full Suite of Forensics Tools. Great Market Penetration. Based on Windows, which can be a problem, since Windows might “discover” a drive connected to the system.
- Creating a Forensics Duplicate of a Hard Drive Software Tools: Safeback Specialized Imaging Tool. Uses DOS Target Drive needs FAT 32.

- Creating a Forensics Duplicate of a Hard Drive FTK Drive Duplication tool included in the Forensic Tool Kit
- Write-blocking Software or hardware tool that prevents writes to a disk. Software tools are hard to validate. All forensics tools need to be validated before use. Manufacturers offer expert testimony when tools are challenged Forensics institutes publish test results Test images at Purdue Examiners might to do some testing as well. Publication in peer-reviewed journals increases value of testimony

Frye and Daubert :

- 1993, Daubert . Merrell Dowν Pharmaceuticals shifted the focus from a test for general acceptance.
- 1923, Federal Court decided on set ofν evidence standards called the Frye test
- A test of "reliability and relevance".

Lead to the Daubert Criteriaθ Four Daubert Factors

1. Has scientific theory or technique been empirically tested?

2. Has scientific theory or technique been subjected to peer review and publication?

3. Is there a known or potential error rate?

• Do standards exist that control the technique's operation?

4. Is there a general acceptance of the methodology or technique in the relevant scientific community?

Forensic Duplication Tool Requirements:

Forensic duplication tools must satisfy the following criteria:
I. The tool shall make a bitstream duplicate or an image of an original disk or partition.
2. The tool shall not alter the original disk.
3. The tool will be able to verify the integrity of a disk image file.
4. The cool shall log I/O errors.
5. The tool's documentation shall be correct.
6. The tool should create a mirror image or forensic du1licaie of the original storage media.
7. The tool must be able handle read errors.
8. The tool should not make any changes to the source mediLlrn.
9. The tool mu,st have the capability to be held ur to scientific review. Results must be verifiable by a third party.

10. If there are no errors accessing the source, then shall create bitstream duplicate or image of the source.
11. If there are I/O errors accessing the source, then the tool shall ***create*** a qualified bistreaiii duplicate or image of the source.
12. tool shall log I/O errors n n acccssil)lC and readable forni, including the type of error and location of the error.
13. Th tool shall be able to access disk drives through w or more wilde1int'd interfaces.
14 Documentation shall be correct, insofar as the mandaory and any implemented optional requirement are concerned,that is. if a nscr following the tools suit, then the document is deemed correct.
15. if the tool copies a source to a dcc,inaunn that is larger than the sourL.c, then it will destination that are not part of the copy.
16. If the tool copies a source to a that **is** smaller than the source, then the tool will truncate the copy, anti log this IC non.

Some Exampies are:
1. SafeBack (www.forensits-intl.cnlfl)
2. Ghost (svww.symantec .uml)
3. DD (standard UNIX/I inux utility)
4. InCase (ww.cncasc.com)
5. Mareware
6. FTK

7. ProDiscoverBasic

Tool must:

Create a forensic duplicate or mirror image of theν original.

Handle read errors in a robust and graceful manner.

Not make any changes to source medium.

Capable of scientific and peer review.

Results must be third party repeatable andν verifiable.

Creating a Forensic Duplicate:

A Forensic Image is most often needed to verify the integrity of the image after an acquisition of a Hard Drive has occurred. This is usually performed by law enforcement for court because, after a forensic image has been created, its integrity can be checked to verify that it has not been tampered with. Forensic Imaging is defined as the processes and tools used in copying an electronic media such as a hard-disk drive for conducting investigations and gathering evidence that will be presentable in the law of court. This copy not only includes files that are visible to the operating system but every bit of data, every sector, partition, files, folders, master boot records, deleted files, and unallocated spaces. The image is an identical copy of all the drive structures and contents.

Further, a forensic image can be backed up and/or tested on without damaging the original copy or evidence.

It should be obvious that dd operates with files rather than directly on physical devices.

However, open -source Unix operating systems such as Linux and FreeBSD implement devices as files.

These special files, located in the /dev directory, allow direct access to devices mediated by the operating system.

Therefore, input files to dd can be entire hard drives, partitions of hard drives , or other devices. To create a forensic duplication of a hard drive, the hard drive device file (that is, /dev/hdb in Linux or /dev/ad1 in FreeBSD) will be the input file.

To create a forensic duplication of a single partition, the input file will be the partition device file (that is, /dev/hdb1 in Linux or /dev/ad1s1 in FreeBSD).

Naturally, the next consideration is what the destination will be for the duplication.

The destination could be another hard drive (using the device files mentioned), which is called a *bit-for-bit copy* of the source hard drive.

We could extend this idea beyond using hard drives as the destination media and use a tape drive instead, albeit a far slower method.

The destination could also be a regular file (also denoted as an *evidence file*), saved on any file system as a logical file.

This is typically the way most modern forensic duplications are stored, because of the ease of manipulation when moving the evidence file between storage devices.

Lastly, the destination could be the standard output (that is, output to the display).

Although we cannot do anything with the data being output directly to the screen (standard out) at this point, later in this section we will examine a method of duplication that will rely on this method.

All three of these output destinations have been successfully used in the past for one reason or another when creating a forensic duplication.

The type (also known as the method) of duplication is typically dictated by the problems encountered during the duplication attempt that are often out of the investigator 's control.

For instance, if it is impossible to remove the hard drive from the source computer during a duplication and no other connectors are available to attach an additional storage hard drive, it would be difficult to save the hard drive's contents directly to another hard drive.

Similarly, you could not save the duplication to a regular file because it would have to be copied to media already in the source computer, therefore overwriting potential evidence.

The only choice in such a case would be to image over a network, as will be discussed in upcoming sections.

Many options in dd can make forensic duplication more efficient.

For instance, you can manipulate the block size that is copied to make the process faster for the host that dd is running onthe bs switch is typically chosen to be 1KB or 1MB at a time.

Another option you should utilize is the conv switch, which allows extra optional parameters to dictate the copying process.

Two highly recommended options are the noerror and notrunc parameters.

These switches will ignore the occurrence of bad blocks read from the source media, so the copy will continue without truncating the output to the evidence media.

An additional option of sync used with noerror will make those bad blocks from the input turn into zeros in the output.

Note When duplicating CD-ROMs, be sure to use a block size that is a multiple of 2048 bytes.

It is always a good idea to generate a log when you're performing a forensic duplication so that you can refer to it in the future or make it available for legal proceedings .

The script command in Unix will capture the input and output of a Unix console or xterm session and save it to a file.

It's a good idea to run the following command before you start your duplication. You should type exit after you finish duplication.

forensic# script /root/disk.bin.duplication

Forensic Duplication #1: Exact Binary Duplications of Hard Drives

To create a mirror image copy of a hard drive using dd, you must tell the utility which source hard drive will be the input file and which will be the output (the evidence) hard drive where you will store the image.

You can determine which hard drive is the source and which is the destination by studying the output of the dmesg command.

In both Linux and FreeBSD, the dmesg command will present information that appeared on the console as the machine was booted (and any other console messages that appeared since bootup).

Determining which hard drive is which isn't a scientific process; rather, you might want to connect to a storage hard drive created by a manufacturer different from that of the source hard drive, which makes it obvious which is the source and which is the destination.

After you have cleansed the destination hard drive at /dev/hdd (discussed later in the section "dd: A Hard Drive Cleansing Tool"), the following syntax can be used to create a forensic duplication from a source hard drive attached to /dev/hdc in Linux:

forensic# dd if=/dev/hdc of=/dev/hdd bs=1024 conv=noerror,notrunc,sync

Forensic Duplication #2: Creating a Local Evidence File

In the first method, we processed a bit-for-bit copy from the source hard drive and laid it on top of the destination hard drive.

Using this method, we cannot simply copy the evidence from one media to another.

A method that facilitates simpler management of the evidence is to create a logical file that is a bit-for-bit representation of the source hard drive.

Obviously, we should never save the evidence file to the source hard drive or we may destroy evidence.

The following command demonstrates the creation of a forensic duplication from a source hard drive on /dev/hdc to a regular file located at /mnt/storage/disk.bin in Linux.

Also, you can create a forensic image from a running or dead machine. It is a literal snapshot in time that has integrity checking.

Never boot from evidence drive.

In preparation, create a bootable disk.

To prevent compressed disks from loadingν and changing time stamps, disable the DRVSPACE.BIN driver file Hack IO.SYS 4 instances need to be changed.

Need for a Forensic Image:

1. In today's world of crime, many cases have been solved by using this technique, as evidence apart from what is available through an operating system, has been found using this technique, as incriminating data might have deleted to prevent discovery during the investigation. Unless that data is overwritten and deleted securely, it can be recovered.
2. One of the advantages includes the prevention of the loss of critical files.
3. When you suspect a custodian of deleting or altering files. A complete forensic image will, to a certain extent, allow you to recover deleted files. It can also potentially be used to identify files that have been renamed or hidden.
4. When you expect that the scope of your investigation could increase at a later date. If you aren't sure about the scope of your project, ALWAYS OVER COLLECT. It's better to have too much data than not enough, and you can't get much more data than a forensic image.
5. When you expect that you or someone in your organization may need to certify or testify to the forensic soundness of the collection. In most cases, this need will never arise, but will almost certainly come into play in any criminal or potential criminal proceedings.
6. The Imaging of random access memory (RAM) can be enabled by using Live imaging. Live imaging can bypass most encryption.

Response Strategy :

Decision of when to perform a forensicν duplication based is based, in part, on existing response strategy for the instant situation.

For example, many organizations have a policy ofθ creating forensic HD duplicates of all PCs used by executives that leave the organization.

Qualified Forensic Duplicate of a Hard Drive:

A Forensic Duplicate is a file that contains every bit of information from the source, in a raw bitstream format. A Qualified Forensic Duplicate is a file that contains every bit of information from the source in a raw bitstream format, but stored in an altered form.

A file that contains every bit of information from the source, but may be stored in a altered form.

Tools that create qualified forensic duplicateν output files:

1. SafeBack
2. EnCase
3. FTK Imager

- dd, part of the GNU software suite. dcfldd, from the DODν dd utility the most reliable tool for creating aν true forensic duplicate image.
- Dd a tool that you should be intimatelyν familiar with before you need to use it on a real investigation.
- Process Creating Linux boot mediaν Start with a precompiled version of Linux.
- Once you have the basic package up and running, disassemble the packages and add your own binaries, such as dcfldd.
- In certain situations, duplications will be stored in aν series of files that are sized to fit on a particular media type (such as CDs or DVDs) or file system type (such as files under 2.1 GB).
- Called a segmented image.
- Most commercial forensic packages have the ability toθ process segmented images.
- Creating A Qualified Forensic Duplicate Never boot from evidence drive.ν In preparation, create a bootable disk
- To prevent compressed disks from loadingν and changing time stamps, disable the DRVSPACE.BIN driver file Hack IO.SYS
- 4 instances need to be changed

SafeBack:

- SafeBack, a small application that isν designed to run from a DOS boot floppy Requires a clean DOS environment ready on aθ boot floppy.
- Offered by New Technologies Inc. (NTI)θ SafeBack Four operating modes Backup function.
- Produces a forensically sound image file for the source media.
- Restore functionν Restores forensically sound image files
- Verify functionν Verifies the checksum values within an image file.
- Copy functionν Performs the Backup and Restore operations in one action.

- Text authors prefer to use the Backupν function to create an image file for creating a qualified forensic duplicate.
- SafeBack includes a logging function thatν records options used for each session.

Restored Image :

A restored image is what you get when you restore a forensic duplicate or a qualified forensic duplicate to another storage medium.

Mismatched drive geometries can cause problems.

For example, partition table or mbr problems

HD Development:

When hard drives grew beyond 512MB, the PC-BIOSν needed to be updated (to recognize larger drives). …software emulated a modern BIOS.

Software pushed all of the real data on the drive down one sector and stored its program and information in sector 2.

The real partition table would be at cylinder 0, head 0, sector2.

Safeback, EnCase, FTK Imager, and dd will create aν restored image from the qualified forensic duplicate.

EnCase and dd images may not need to be restored.

Treat images as virtual disks, eliminating the need for restoration.

Note, FTK Imager can create images in the EnCase Format.

Mirror Image:

Created from hardware that does at bit for bit copy from one hard drive to another.

Requires two identical hard drives.

Doesn't happen very often.

Forensic imaging of hard drive:

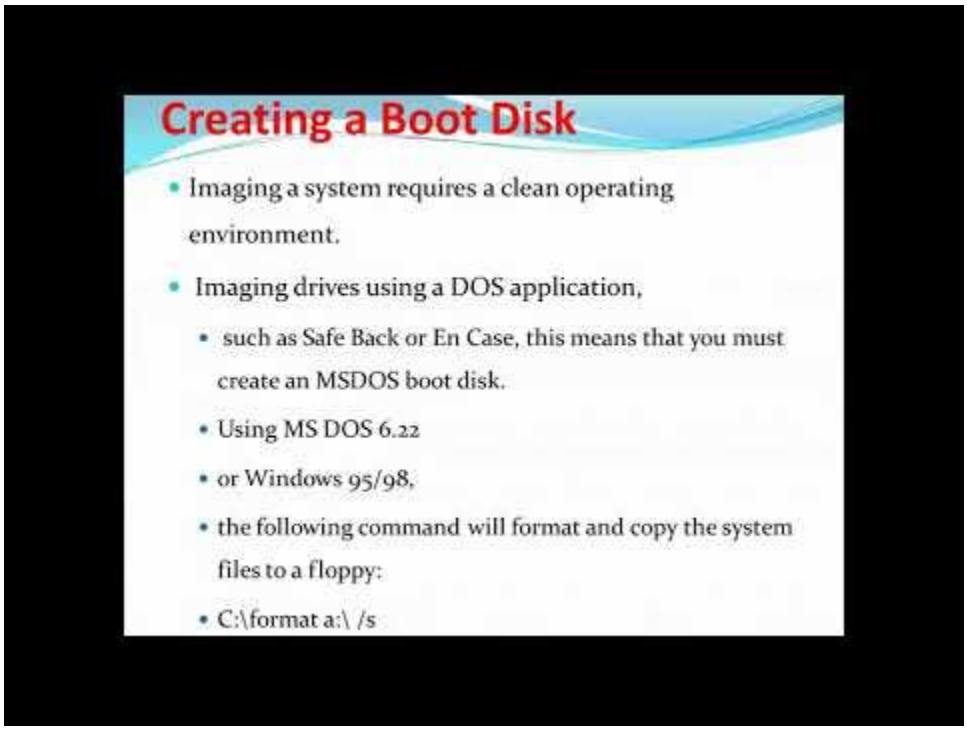
A forensic image of a hard drive captures everything on the hard drive, from the physical beginning to the physical end.

Performing a "copy and paste" via the operating system is not the same as a forensic clone.

A true forensic image captures both the active and latent data.

Cloning a hard drive legal:

If you are cloning your own drive or cloning someone else's drive with permission, yes, it is legal. As long as after the fact, you are not using software on both drives without the appropriate number of licenses.



First type of forensic tool:

Identification. It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format). Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

2 types of write blocking:

Write Blockers are basically of 2 types: Hardware Write Blocker and Software Write Blocker. Both types of write blockers are meant for the same purpose that is to prevent any writes to the storage devices.

Free forensic disk examination tools:

22 FREE Forensic Investigation Tools for IT Security ExpertAutopsy.Encrypted Disk Detector.Wireshark.Magnet RAM Capture.Network Miner.NMAP.RAM Capturer.Forensic Investigator.

Chain of custody in criminal investigation:

The chain of custody is a tracking record beginning with detailed scene notes that describe where the evidence was received or collected. … The chain of custody is established whenever an investigator takes custody of evidence at a crime scene.

Forensic image capture utility:

A forensic image (forensic copy) is a bit-by-bit, sector-by-sector direct copy of a physical storage device, including all files, folders and unallocated, free and slack space. … Some disk imaging utilities not marketed for forensic use also make complete disk images.

Rule of digital forensics:

The first rule of digital forensics is to preserve the original evidence. During the analysis phase, the digital forensics analyst or computer hacking forensics investigator (CHFI) recovers evidence material using a variety of different tools and strategies.

Computer forensic investigators :

As the name implies, forensic computer investigators and digital forensic experts reconstruct and analyze digital information to aid in investigations and solve computer-related crimes. They look into incidents of hacking, trace sources of computer attacks, and recover lost or stolen data.

Digital forensic tools:

Digital forensics tools can fall into many different categories, some of which include database forensics, disk and data capture, email analysis, file analysis, file viewers, internet analysis, mobile device analysis, network forensics, and registry analysis.

At which stage of the digital forensics process would a write blocker be used

A write blocker, which is designed to prevent the alteration of data during the copying process (Cybercrime Module 4 on Introduction to Digital Forensics), should be used before extraction whenever possible in order to prevent the modification of data during the copying process (SWGDE Best Practices for Computer