

## UNIT-II

### **Initial Response and forensic duplication:**

#### **Initial Response:**

One of the first steps of any preliminary investigation is to obtain enough information to determine an appropriate response.

The goal of an initial response is twofold: Confirm there is an incident, and then retrieve the system's volatile data that will no longer be there after you power off the system.

Initial response is an investigative as well as a technical process.

#### **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.

We also define forensic duplication as an image of every accessible bit from the source medium.

### **Volatile Data Collection:**

Two basic types of data are collected in computer forensics. Those are,

**Persistent (Non-Volatile)** data is the data that is stored on a local hard drive (or another medium) and is preserved when the computer is turned off.

**Volatile data** is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM).

The investigation of this volatile data is called “**live forensics**”

It is essential to the forensic investigation that the immediate state of a computer is recorded before shutting it down. Volatile information is lost once the suspect's computer is powered down and this may be crucial to the claim.

When collecting data for a computer forensic investigation you want to collect the most volatile data first as it will be lost the quickest.

To avoid losing this volatile storage on a mobile device, keep this continuously charged to avoid losing volatile memory. A computer system will lose volatile memory when this is powered down, so the only way to safeguard this evidence is to leave the system powered up until a forensics expert can salvage this memory.

## **Live Data/ Volatile Data Collection from Windows System:**

The main goal of the live data collection is to obtain temporal or volatile data before forensic duplication. The scope of initial response can be expanded by obtaining configuration files, system files, files that contain attacker's tools and suspicious programs, and log files to confirm quickly whether the event has occurred or not.

Here, the first step is to determine whether the system was used by the victim or the attacker. After that we need to create a Response Toolkit.

**Creating a Response Toolkit:** A response toolkit is a collection of tools which are helpful to extract or read the information from the system was used by the victim or the attacker. We have to be careful about not destroying or altering the evidence and to do this we need to create a response toolkit.

An Investigator should maintain a CD or a floppy that involves a minimum of the tools described in the following table.

| <b>Tool</b>       | <b>Description</b>                                                                                                               | <b>Source</b>                                    |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| <b>cmd.exe</b>    | The command prompt for Windows NT and Windows 2000                                                                               | Built in                                         |
| <b>PsLoggedOn</b> | A utility that shows all users connected locally and remotely                                                                    | www.foundstone.com                               |
| <b>rasusers</b>   | A command that shows which users have remote access privileges on the target system                                              | NT Resource Kit (NTRK)                           |
| <b>netstat</b>    | A system tool that enumerates all listening ports and all current connections to those ports                                     | Built in                                         |
| <b>Fport</b>      | A utility that enumerates all processes that opened and TCP/IP ports on a Windows NT/2000 system                                 | www.foundstone.com                               |
| <b>PsList</b>     | A utility that enumerates all running processes on the target system                                                             | www.foundstone.com                               |
| <b>nbstat</b>     | A system tool that lists the recent NetBIOS connections for approximately the last 10 minutes.                                   | Built in                                         |
| <b>ipconfig</b>   | A system tool that displays interface configuration information.                                                                 | Built in                                         |
| <b>Arp</b>        | A system tool that shows the MAC addresses of systems that the target system has been communicating with, within the last minute | Built in                                         |
| <b>doskey</b>     | A system tool that displays command history for Built in open cmd.exe shell                                                      | Built in                                         |
| <b>netcat</b>     | A utility used to create a communication channel between two different system                                                    | www.atstake.com/research/tools/network_utilities |

There are two types of applications/tools available in windows:

1. Based on GUI (Graphical User Interface)
2. Based on CUI (Control User Interface)

GUI involves pull-down menus and usually works in the background or “behind the scene” interactions. However, experts advised to avoid GUI for investigation.

### **Obtaining Volatile Data**

We collect the following temporal/volatile data before forensic duplication:

- The date and the time of the system.
- List of users that are currently logged on.
- Entire file system’s time and date stamp.
- List of sockets/ports that are open currently.
- Applications that are listening on the open sockets.
- List of processes that are currently running.
- List of systems that have current or had recent connections to the system.

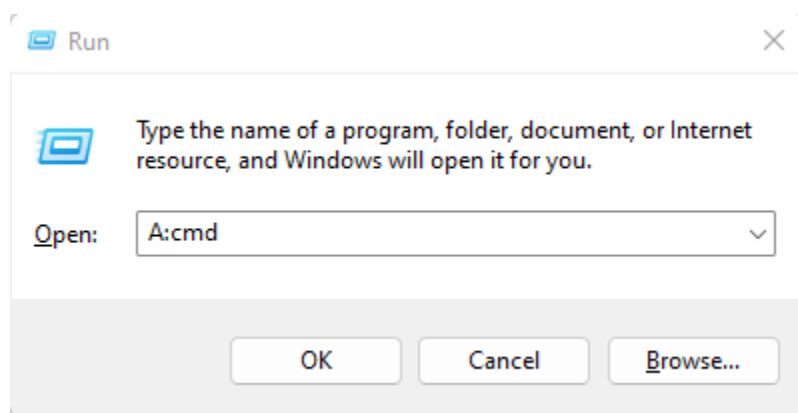
Following are the steps used for collecting the data:

#### **1. Run a Trusted cmd.exe:**

As discussed earlier, investigators should be careful about the traps that have been implemented by an attacker, which will mislead the investigator to place wrong incident response.

Running trusted version of cmd.exe from your own toolkit will be the best solution for this problem.

To open trusted cmd.exe on floppy drive of windows system,



## 2. Recording the system time and date:

After executing the trusted command shell, it is a good idea to capture the local system date and time settings. This is important to correlate the system logs, as well as to mark the times at which you performed your response. The time and date commands are a part of the cmd.exe application.

```
D:\>date >date.txt

D:\>time >> date.txt

D:\>type date.txt
The current date is: Thu 02/02/2023
Enter the new date: (mm-dd-yy) The current time is:  9:56:58.92
Enter the new time:
D:\>
```

The above figure illustrates the execution of the date command, redirecting the output to a file called date.txt. The second command in the figure uses the append operator (>>) to add the output to the time command to the date.txt file.

To indicate that you do not want to change the setting, press the "enter" key.

## 3. Identify who has logged on to the system and who are the remote access users:

It is necessary to identify which user accounts have remote access rights on the target system, in order to respond to a system that offers remote access via modem. You need to decide if you want to pull the telephone lines from the system at the time of response, if several accounts access systems via Remote Access Services (RAS).

You may not want to allow any access to the target system while you are responding.

The commands to determine the number of the users who logged into the system (via RAS) is called rasusers.

```
C:\Users\CC3>psloggedon

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
      2/2/2023 9:53:34 AM      DESKTOP-GE6GVHE\CC3
      <unknown time>         DESKTOP-GE6GVHE\Student

No one is logged on via resource shares.

C:\Users\CC3>
```

#### 4. Record creation, access time, and all the modifications made to the files:

To get the list of all the directory files on the target machine, "dir" command is used. It includes the size, access, and alteration and creation time.

The time and date stamps become the evidence, if the significant information about the time frame when an event occurred is identified. Windows system performs the task of collecting time and date stamps very quickly.

An example of using "**dir**" command to gain access, modification, and time of creation:

**dir/t:a/a/s/o** Provides a recursive directory listing of all the access times on the drive

**dir/t:w/a/s/o** Provides a recursive directory listing of all the modification times on the drive

**dir/t:c/a/s/o** Provides a recursive directory listing of all the creation times on the drive

```
D:\CF-Lecture Notes>dir/t:a/a/s/o
Volume in drive D is New Volume
Volume Serial Number is 502A-3B47

Directory of D:\CF-Lecture Notes

02/02/2023  10:49 AM    <DIR>          .
02/02/2023  09:57 AM    <DIR>          ..
02/01/2023  02:18 PM    <DIR>          CF PPT
02/02/2023  09:54 AM             162 ~$-UNIT-2.docx
02/02/2023  10:06 AM          27,593 ~WRL0005.tmp
02/01/2023  12:04 PM        2,528,442 CF-LectureNotes.pdf
02/02/2023  09:37 AM        334,634 CF-UNIT-1.docx
02/01/2023  11:04 AM        384,318 CF-UNIT-1.pdf
02/02/2023  10:48 AM         72,801 CF-UNIT-2.docx
02/02/2023  09:38 AM         17,932 CYBER_FORENSICS_Syllabus.pdf
02/01/2023  11:03 AM        3,205,342 UNIT-I_PART_1_CF.pptx
02/02/2023  09:37 AM        1,705,224 UNIT-I_PART_2_CF.pptx
               9 File(s)          8,276,448 bytes
```

#### 5. Identifying open ports:

There are several networking commands available, out of which **Netstat** can be used to determine which ports are open. It also enlists all listening port and currents connections to those ports. Volatile data, such as recently terminated connections and current connections, can be recorded using Netstat.

```
C:\>netstat
```

Active Connections

| Proto | Local Address       | Foreign Address                | State       |
|-------|---------------------|--------------------------------|-------------|
| TCP   | 10.100.203.72:53648 | 20.198.119.84:https            | ESTABLISHED |
| TCP   | 10.100.203.72:54335 | whatsapp-cdn-shv-02-bom1:https | ESTABLISHED |
| TCP   | 10.100.203.72:54624 | bs:https                       | ESTABLISHED |
| TCP   | 10.100.203.72:55128 | 108:https                      | ESTABLISHED |
| TCP   | 10.100.203.72:55134 | a184-86-248-168:https          | CLOSE_WAIT  |
| TCP   | 10.100.203.72:55135 | a184-86-248-168:https          | CLOSE_WAIT  |
| TCP   | 10.100.203.72:55136 | a184-86-248-168:https          | CLOSE_WAIT  |
| TCP   | 10.100.203.72:55137 | a184-86-248-168:https          | CLOSE_WAIT  |
| TCP   | 10.100.203.72:55138 | a184-86-248-168:https          | CLOSE_WAIT  |
| TCP   | 10.100.203.72:55139 | a184-86-248-168:https          | CLOSE_WAIT  |
| TCP   | 10.100.203.72:55207 | 52.143.86.214:https            | TIME_WAIT   |
| TCP   | 10.100.203.72:55211 | 52.231.199.126:https           | ESTABLISHED |
| TCP   | 10.100.203.72:55212 | 49.44.205.119:https            | ESTABLISHED |
| TCP   | 10.100.203.72:55213 | 52.113.194.132:https           | TIME_WAIT   |

The above figure illustrates the execution of Netstat command window machine. There are several local host connections in the output. The applications on the local host 127.0.0.1 will always be displayed by Netstat command.

## 6. List of applications that are associated with those ports:

Knowing which services listen on which ports is helpful. A free tool **fport** is used to enlist listening ports for all the processes.

## 7. List of all running processes:

It is necessary to record all the processes that are currently executing on the system before turning off the target system. Unplugging the power cable will destroy this information. The executable code that resides in address space has been created when a process is created on the Windows system. To manage the process and maintain statistical information about the process, the kernel object is created by the operating system.

## 8. List of current and recent connections:

To know who is connected or who has connected recently, the networking commands like *Netstat*, *ARP*, and *Nbstat* are useful. For many Windows system, these utilities might be the only way to determine a remote system connecting to workstation. Many experts refer *Netstat* command to enlist the ports that are opened on a system.

As previously discussed, *fport* lists open ports and application listening to them, so also can *Netstat* be used to identify IP address of remote system and current connections of the systems. *ARP* networking command is used to map IP address to the MAC address. The utility named *nbtstat* is used to access the remote NetBIOS (Network Basic Input/output System) name cache, listing NetBIOS connections for approximately the last 10 minutes.

```
C:\>nbtstat -c

Ethernet:
Node IpAddress: [10.100.203.72] Scope Id: []

    No names in cache
```

### **Live Data/Volatile Data Collection from UNIX System:**

The main goal of the live data collection is to obtain temporal or volatile data before forensic duplication. The scope of initial response can be expanded by obtaining configuration files, system files, files that contain attacker's tools and suspicious programs, and log files to confirm quickly whether the event has occurred or not.

Here, the first step is to determine whether the system was used by the victim or the attacker. After that we need to create a Response Toolkit.

***Creating a Response Toolkit:*** It is difficult to create a trusted toolkit as it takes a lot of time; the reason behind this is that every variable in UNIX requires a UNIX toolkit. In some cases, you may need to compile a source code on your own because some recommended tools are not included with the official UNIX system.

### **Obtaining Volatile Data**

We collect the following temporal/volatile data before forensic duplication:

- The date and the time of the system.
- List of users that are currently logged on.
- Entire file system's time and date stamp.
- List of sockets/ports that are open currently.
- Applications that are listening on the open sockets.
- List of processes that are currently running.
- List of systems that have current or had recent connections to the system.

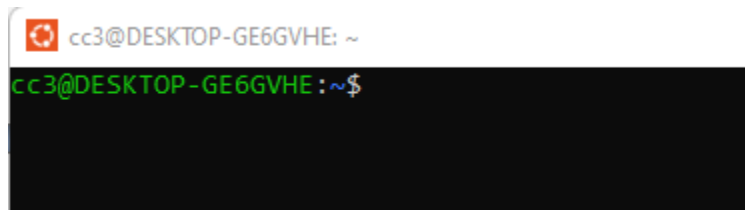
Following are the steps used for collecting the data:

### 1. Run a trusted shell:

As discussed earlier, investigators should be careful about the traps that have been implemented by an attacker, which will mislead the investigator to place wrong incident response.

Running trusted command shell is the first step in all response. Bash shell can be used for this purpose.

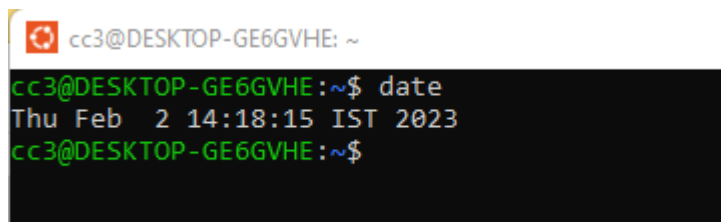
By pressing ctrl + alt + T, we get the following terminal.

A terminal window with a black background. The prompt is 'cc3@DESKTOP-GE6GVHE: ~' in green. Below it, the prompt is 'cc3@DESKTOP-GE6GVHE:~\$' in green.

### 2. Recording the system time and date:

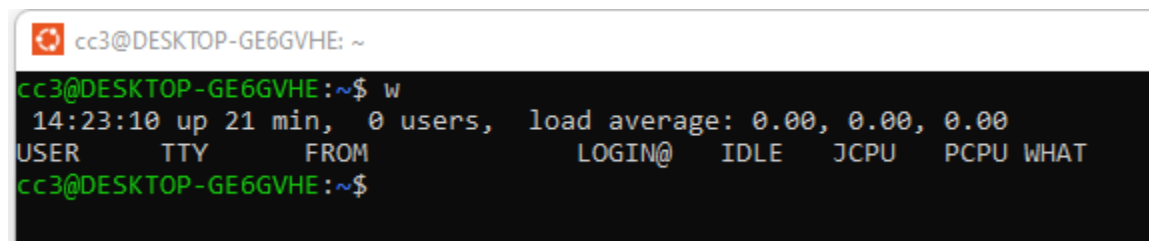
After executing the trusted command shell, it is a good idea to capture the local system date and time settings. This is important to correlate the system logs, as well as to mark the times at which you performed your response.

The following command can be used to capture this information.

A terminal window with a black background. The prompt is 'cc3@DESKTOP-GE6GVHE: ~' in green. Below it, the prompt is 'cc3@DESKTOP-GE6GVHE:~\$' in green. The command 'date' has been executed, and the output is 'Thu Feb 2 14:18:15 IST 2023' in green.

### 3. Identify who has logged on to the system:

It is easy to identify who is logged on. We just need to execute the w command. The user IDs of logged on users, the system they logged on from, and what they are currently executing can be displayed by using this **w** command.

A terminal window with a black background. The prompt is 'cc3@DESKTOP-GE6GVHE: ~' in green. Below it, the prompt is 'cc3@DESKTOP-GE6GVHE:~\$' in green. The command 'w' has been executed, and the output is '14:23:10 up 21 min, 0 users, load average: 0.00, 0.00, 0.00' in green. Below this, a table is displayed with columns: USER, TTY, FROM, LOGIN@, IDLE, JCPU, PCPU, WHAT. The prompt 'cc3@DESKTOP-GE6GVHE:~\$' is at the bottom.

#### 4. Record creation, access time, and all the modifications made to the files:

You have to obtain all the time and date stamps on the file system. There are three time/date stamps available for each file in windows and UNIX system – atime (i.e., access time), mtime (i.e., modification time), and ctime (i.e., creation time).

With the use of following command line arguments to obtain these times for each file.

|                 |                   |
|-----------------|-------------------|
| <b>ls -alRu</b> | Access Time       |
| <b>ls -alRc</b> | Creation Time     |
| <b>ls -alR</b>  | Modification Time |

```
cc3@DESKTOP-GE6GVHE: ~  
cc3@DESKTOP-GE6GVHE:~$ ls -alRc  
.:  
total 28  
drwxr-x--- 3 cc3 cc3 4096 Feb  2 14:37 .  
drwxr-xr-x 3 root root 4096 Feb  2 14:02 ..  
-rw-r--r-- 1 cc3 cc3  220 Feb  2 14:02 .bash_logout  
-rw-r--r-- 1 cc3 cc3 3771 Feb  2 14:02 .bashrc  
-rw-r--r-- 1 cc3 cc3   0 Feb  2 14:02 .motd_shown  
-rw-r--r-- 1 cc3 cc3  807 Feb  2 14:02 .profile  
-rw-r--r-- 1 cc3 cc3   0 Feb  2 14:04 .sudo_as_admin_successful  
-rw-r--r-- 1 cc3 cc3  12 Feb  2 14:34 cfunit.txt  
drwxr-xr-x 2 cc3 cc3 4096 Feb  2 14:37 floppy  
  
./floppy:  
total 1204  
drwxr-xr-x 2 cc3 cc3  4096 Feb  2 14:37 .  
drwxr-x--- 3 cc3 cc3  4096 Feb  2 14:37 ..  
-rw-r--r-- 1 cc3 cc3 1222822 Feb  2 14:38 atime
```

```
cc3@DESKTOP-GE6GVHE: ~  
cc3@DESKTOP-GE6GVHE:~$ ls -alRc  
.:  
total 28  
drwxr-x--- 3 cc3 cc3 4096 Feb  2 14:37 .  
drwxr-xr-x 3 root root 4096 Feb  2 14:02 ..  
-rw-r--r-- 1 cc3 cc3  220 Feb  2 14:02 .bash_logout  
-rw-r--r-- 1 cc3 cc3 3771 Feb  2 14:02 .bashrc  
-rw-r--r-- 1 cc3 cc3   0 Feb  2 14:02 .motd_shown  
-rw-r--r-- 1 cc3 cc3  807 Feb  2 14:02 .profile  
-rw-r--r-- 1 cc3 cc3   0 Feb  2 14:04 .sudo_as_admin_successful  
-rw-r--r-- 1 cc3 cc3  12 Feb  2 14:34 cfunit.txt  
drwxr-xr-x 2 cc3 cc3 4096 Feb  2 14:37 floppy  
  
./floppy:  
total 1204  
drwxr-xr-x 2 cc3 cc3  4096 Feb  2 14:37 .  
drwxr-x--- 3 cc3 cc3  4096 Feb  2 14:37 ..  
-rw-r--r-- 1 cc3 cc3 1222822 Feb  2 14:38 atime
```

## 5. Identify open ports:

The most widely used command for listing open ports on a UNIX system is **netstat**. To view all open ports use **-an** command line argument along with **netstat** command.

```
cc3@DESKTOP-GE6GVHE: ~  
cc3@DESKTOP-GE6GVHE:~$ netstat -an  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
udp        0      0 127.0.0.1:323           0.0.0.0:*  
udp6       0      0 :::1:323                :::*  
Active UNIX domain sockets (servers and established)  
Proto RefCnt Flags       Type       State      I-Node  Path  
unix    2      [ ACC ]     STREAM    LISTENING   19583   /run/WSL/1_interop  
unix    2      [ ACC ]     STREAM    LISTENING   19562   /run/WSL/1_interop  
unix    2      [ ACC ]     STREAM    LISTENING   17623   /var/run/dbus/system_bus_socket  
unix    2      [ ACC ]     SEQPACKET LISTENING   19567   /mnt/wslg/weston-notify.sock  
unix    2      [ ACC ]     STREAM    LISTENING   20537   /run/WSL/56_interop  
unix    2      [ ACC ]     STREAM    LISTENING    71      /mnt/wslg/runtime-dir/wayland-0  
unix    2      [ ACC ]     STREAM    LISTENING    72      /tmp/.X11-unix/X0  
unix    2      [ ACC ]     STREAM    LISTENING   17789   /run/WSL/193_interop  
unix    2      [ ACC ]     STREAM    LISTENING   18580   /mnt/wslg/runtime-dir/pulse/native  
unix    2      [ ]       DGRAM          19469   /var/run/chrony/chronyd.sock  
unix    2      [ ACC ]     STREAM    LISTENING   18586   /mnt/wslg/PulseServer  
unix    2      [ ACC ]     STREAM    LISTENING   21526   /mnt/wslg/PulseAudioRDPSource  
unix    2      [ ACC ]     STREAM    LISTENING   19593   /mnt/wslg/PulseAudioRDPSink  
unix    2      [ ACC ]     STREAM    LISTENING   23598   @/tmp/dbus-z84mvzBqc2  
unix    3      [ ]       STREAM    CONNECTED   18551  
unix    3      [ ]       STREAM    CONNECTED   19578  
unix    3      [ ]       STREAM    CONNECTED    82      /mnt/wslg/PulseAudioRDPSink  
unix    3      [ ]       STREAM    CONNECTED   19577
```

## 6. Enlist applications associated with open ports:

The **-p** option of **netstat** command used to map the name of the application and its process identification number (i.e., PID) to open ports.

```
cc3@DESKTOP-GE6GVHE: ~  
cc3@DESKTOP-GE6GVHE:~$ netstat -anp  
(No info could be read for "-p": geteuid()=1000 but you should be root.)  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State      PID/Program name  
udp        0      0 127.0.0.1:323           0.0.0.0:*               -  
udp6       0      0 :::1:323                :::*                    -  
Active UNIX domain sockets (servers and established)  
Proto RefCnt Flags       Type       State      I-Node  PID/Program name  Path  
unix    2      [ ACC ]     STREAM    LISTENING   19583   -                 /run/WSL/1_interop  
unix    2      [ ACC ]     STREAM    LISTENING   19562   -                 /run/WSL/1_interop  
unix    2      [ ACC ]     STREAM    LISTENING   17623   -                 /var/run/dbus/system_bus_socket  
unix    2      [ ACC ]     SEQPACKET LISTENING   19567   -                 /mnt/wslg/weston-notify.sock  
unix    2      [ ACC ]     STREAM    LISTENING   20537   -                 /run/WSL/56_interop  
unix    2      [ ACC ]     STREAM    LISTENING    71      -                 /mnt/wslg/runtime-dir/wayland-0  
unix    2      [ ACC ]     STREAM    LISTENING    72      -                 /tmp/.X11-unix/X0  
unix    2      [ ACC ]     STREAM    LISTENING   17789   -                 /run/WSL/193_interop  
unix    2      [ ACC ]     STREAM    LISTENING   18580   -                 /mnt/wslg/runtime-dir/pulse/native  
unix    2      [ ]       DGRAM          19469   -                 /var/run/chrony/chronyd.sock  
unix    2      [ ACC ]     STREAM    LISTENING   18586   -                 /mnt/wslg/PulseServer  
unix    2      [ ACC ]     STREAM    LISTENING   21526   -                 /mnt/wslg/PulseAudioRDPSource  
unix    2      [ ACC ]     STREAM    LISTENING   19593   -                 /mnt/wslg/PulseAudioRDPSink  
unix    2      [ ACC ]     STREAM    LISTENING   23598   -                 @/tmp/dbus-z84mvzBqc2  
unix    3      [ ]       STREAM    CONNECTED   18551   -  
unix    3      [ ]       STREAM    CONNECTED   19578   -  
unix    3      [ ]       STREAM    CONNECTED    82      -                 /mnt/wslg/PulseAudioRDPSink
```

## 7. Identify the running processes:

Taking snapshots of **ps** command, the processes that are running during the initial response is difficult; but by using **ps** command we can achieve this. Output will be different on different UNIX flavors. The following command shows the running processes.

 cc3@DESKTOP-GE6GVHE: ~

```
cc3@DESKTOP-GE6GVHE:~$ ps -aux
```

| USER | PID | %CPU | %MEM | VSZ  | RSS  | TTY   | STAT | START | TIME | COMMAND  |
|------|-----|------|------|------|------|-------|------|-------|------|----------|
| root | 1   | 0.0  | 0.0  | 2276 | 1548 | ?     | S1   | 14:02 | 0:00 | /init    |
| root | 4   | 0.0  | 0.0  | 2292 | 68   | ?     | S1   | 14:02 | 0:00 | plan9 -- |
| root | 55  | 0.0  | 0.0  | 2284 | 104  | ?     | Ss   | 14:02 | 0:00 | /init    |
| root | 56  | 0.0  | 0.0  | 2300 | 108  | ?     | S    | 14:02 | 0:00 | /init    |
| cc3  | 57  | 0.0  | 0.0  | 6084 | 5112 | pts/0 | Ss+  | 14:02 | 0:00 | -bash    |
| root | 192 | 0.0  | 0.0  | 2284 | 104  | ?     | Ss   | 14:13 | 0:00 | /init    |
| root | 193 | 0.0  | 0.0  | 2300 | 108  | ?     | S    | 14:13 | 0:00 | /init    |
| cc3  | 194 | 0.0  | 0.0  | 6080 | 5172 | pts/1 | Ss   | 14:13 | 0:00 | -bash    |
| cc3  | 235 | 0.0  | 0.0  | 7784 | 3280 | pts/1 | R+   | 15:02 | 0:00 | ps -aux  |

## **Forensic Duplication:**

Forensic duplication is the copying of the contents of a storage device completely and without alteration. The technique is sometimes known as bitwise duplication, sector copying, or physical imaging. Forensic duplication is the primary method for collecting hard disk, floppy, CD/DVD, and flash-based data for the purpose of evidence gathering.

A simple duplication consists of making a copy of specific data. The data may consist of a single file, a group of files, a partition on a hard drive, an entire hard drive, or 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 evidence in legal proceedings.

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

### **Rules of Forensic Duplication:**

1. Make two copies of the original media (digital evidence).
  - (a) One copy becomes the working copy on which investigation will be done.
  - (b) One copy is a library/control copy for future reference.
  - (c) Verify the integrity of the copies.
2. The working copy is used for the analysis.
3. The library copy is stored for disclosure purposes or in the event that the working copy becomes corrupted.
4. If performing a drive to drive imaging (not an image file), use clean media to copy to.
5. Verify the integrity of all images using hash values.

### **Necessity of Forensic Duplication:**

- After securing the computer, we should make a complete bit stream backup of all Computer data before it is reviewed or processed.
- Bit stream backups are much more thorough than standard backups.
- They involve copying of every bit of data on a storage device, and it is recommended that two such copies be made of the original when hard disk drives are involved.
- Any processing should be performed on one of the backup copies.
- IMDUMP was the first software for taking bit stream back-ups developed by Michael White.

Forensic duplication importance can be summarized as:

1. Working from a duplicate image provides following features:
  - (a) Preserves the original digital evidences.
  - (b) Prevents inadvertent alteration of original digital evidence during examination.
  - (c) Allows recreation of the duplicate image, if necessary.
2. Digital evidence can be duplicated with no degradation from copy to copy:
  - (a) This is not the case with most other forms of evidence.

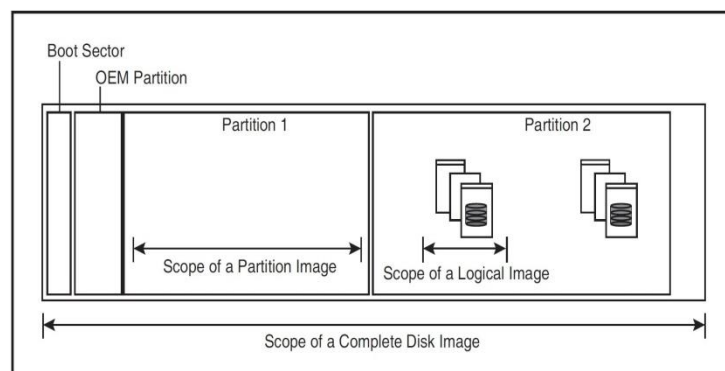
### **Forensic Duplicates as Admissible Evidence:**

Digital evidence should satisfy minimum criteria of legal standards. Some standards are given by the United States, known as Federal Rules of Evidence (FRE).

1. FRE §1001 states that if data are deposited in a computer or alike device, any printout or other output readable by sight, shown to reflect the data precisely is an “original.”
2. FRE §1002 requires an original to prove the content of a writing, record, or photograph. This means the item or information presented in court must be original. It follows from the best evidence rule: Copying can introduce errors.
3. FRE §1003 states that a duplicate is admissible to the same extent as an original if:
  - (a) An honest question is elevated to the authenticity of the original or
  - (b) In the circumstances, it would be partial to confess the identical in lieu of the original.

### **Forensic Image Formats:**

1. **Complete Disk Image:** The process for getting a “complete disk image” is meant to duplicate each addressable computer memory unit on the medium. This includes Host Protected Areas (HPAs) and Drive Configuration Overlays (DCOs).
2. **Partition Image:** Most forensic imaging tools permit you specifies a personal partition, or volume, as the source for a picture. A partition image may be a set of a whole disk image and contains all of the allocation units from a personal partition on a drive. This includes the unallocated space and file slack present within that partition.



**3. Logical Image:** A logical image is a smaller amount of Associate in Nursing “image” and additional of a straightforward copy. A logical image is less of an “image” and more of a simple copy.

**4. Image Integrity:** When a forensic image is formed, cryptologic checksums are generated for two reasons. First, once the image is taken from a drive, which is offline (static) and preserved, the hash is employed to verify and demonstrate that the forensic image could be a true and correct illustration of the initial. Second, the hash is employed to sight if the info was changed since the purpose of your time at which the image was created.

### **Traditional Duplication:**

1. **Hardware Write Blockers:** The write blockers are generally protocol bridges that contain changed code or an ASIC designed to intercept a set of the protocol’s commands. With these in your kit, you will faithfully duplicate SATA, PATA, SCSI, SAS, and USB devices.

2. **Image Creation Tools:** The three main tools we tend to use are a unit DC3dd, AccessData’s FTK Imager, and steering Software’s incase. Each has its pros and cons that build it additional or less appropriate for a given scenario.

### **Forensic Duplication Tool Requirements:**

Forensic duplication tools must satisfy the following criteria:

1. The tool shall make a bit stream 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 tool shall log I/O errors.
5. The tool’s documentation shall be correct.
6. The tool should create a mirror image or forensic duplicate 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 medium.
9. The tool must have the capability to be held up to scientific review. Results must be verifiable by a third party.
10. If there are no errors accessing the source, then the tool shall create a bitstream duplicate or image of the source.
11. If there are I/O errors accessing the source, then the tool shall create a qualified bitstream duplicate or image of the source.
12. The tool shall log I/O errors in an accessible and readable form, including the type of error and location of the error.
13. The tool shall be able to access disk drives through one or more well-defined interfaces.
14. Documentation shall be correct, insofar as the mandatory and any implemented optional requirements are concerned, that is, if a user following the tool’s documented procedures produces the expected result, then the documentation is deemed correct.

15. If the tool copies a source to a destination that is larger than the source, then it will document the contents of the areas on the destination that are not part of the copy.

16. If the tool copies a source to a destination that is smaller than the source, then the tool will notify the user, truncate the copy, and log this action.

Some Examples of forensic duplication tools are:

- a. SafeBack ([www.forensics-intl.com](http://www.forensics-intl.com))
- b. Ghost ([www.symantec.com](http://www.symantec.com))
- c. DD (standard UNIX/Linux utility)
- d. Encase ([www.encase.com](http://www.encase.com))
- e. Mareware
- f. FTK ([www.accessdata.com](http://www.accessdata.com))
- g. ProDiscover Basic

### **Creating a Forensic Duplicate of a Hard Drive:**

1. **Duplicating with dd and dcfldd:** For creating a true forensic duplicate image, dd utility is the most efficient tool. dd will perform bit-for-bit copy of the original, as long as the operating system kernel recognizes the storage medium. However, it is expensive.

2. **Creating a Linux Boot Media:** Preparation for duplication using Linux is difficult from the methods that we discuss in this section. But using Linux is worthy, as it can be the most flexible boot environment in the toolbox.

3. **Performing Duplication with dd:** Sometimes, to fit on a specific media type, such as CD/DVD or file systems with files fewer than 2.1 GB, duplication will be stored in a series of files. This is usually referred to as segmented image.

4. **Duplicating with the Open Data Duplicator:** The new open source tool is ODD. To perform forensic duplication simultaneously on a number of computers over a Local LAN, the client-server model is followed by this tool. To use the software on single forensic workstations, you need to run both halves on the same computer.

Three portions of ODD are:

- 1. *Bootable CD-ROMs:* This is similar to Trinux Linux Distributions;
- 2. *Server-side applications:* Most of the duplications, such as string searches, calculation of hashes, and storage of true forensic duplications, will be done by the server.
- 3. *Client-side applications:* If you are duplicating drives on forensic workstations, this portion may be run locally.

## **Creating a 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 duplicate output files:

1. SafeBack
2. EnCase
3. FTK Imager

### **1. Creating a Boot Disk :**

Clean operating environment is required for imaging a system. You must create an MS DOS boot disk when imaging drives using DOS applications such as SafeBack or EnCase.

### **2. Creating a Qualified Forensic Duplicate with SafeBack :**

New Technology Inc. (NTI) offers SafeBack. It is used to make qualified forensic duplication of any hard drive. You need to have a clear environment ready on the floppy for SafeBack application because it runs from DOS boot floppy.

### **3. Creating a Qualified Forensic Duplicate with EnCase :**

The most popular commercially available forensic tool is EnCase from Guidance Software. It provides 'easy-to-navigate' GUI. Allowing the examiner to customize the types of searches performed by the tool, a flexible scripting language is included. Preview option is the most significant feature of EnCase. You can use the preview function to quickly ascertain whether a computer system is material to the issue being investigated, during the first stages of the investigation.

## **Creating a Forensic Duplicate**

In today's digital era, the indulgence of devices is increasing more and more and with-it cybercrime is also on the rise. When such a crime occurs, the hard drive becomes an important part as it is crucial evidence. Therefore, during investigation one cannot directly perform various tasks on the hard drive as it is considered tempered. Also, one can lose data by mistake while performing tasks on it. Hence, the necessity of disk image. Now that we have understood the importance and use of disk image, let us now understand that what exactly a forensic image is.

### **What is a Forensic image?**

A Forensic image is an exact copy of hard drive. This image is created using various third-party tools which can easily capture the image of a hard drive bit by bit without changing even a shred of data. Forensic software copies data by creating a bitstream which is an exact duplicate. The best thing about creating a forensic image is that it also copies the deleted data, including files that are left behind in swap and free spaces. Now that we have understood all about the forensic

imaging, let us now focus on the practical side of it. We will learn and understand how to create such image by using five different tools which are:

FTK Imager

Belkasoft acquisition tool

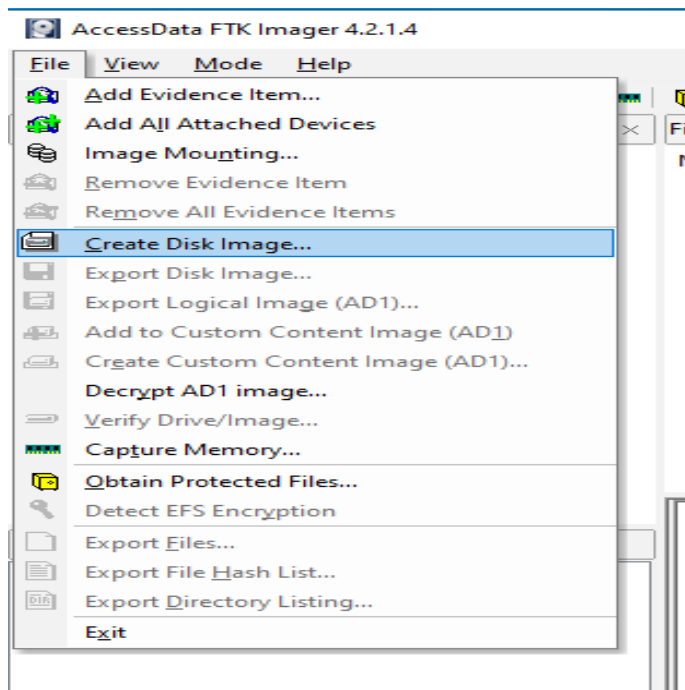
Encase imager

Forensic imager

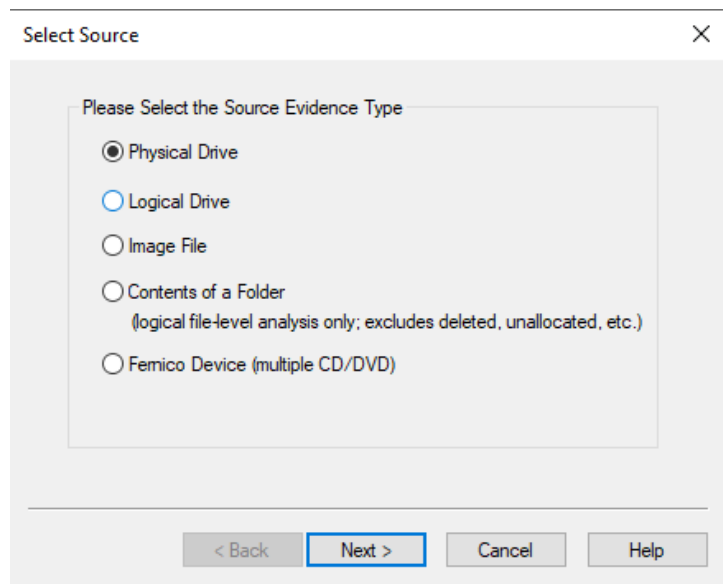
### **FTK Imager:**

FTK imager can create an image and paging file for windows; along with capturing volatile memory for analysis purpose.

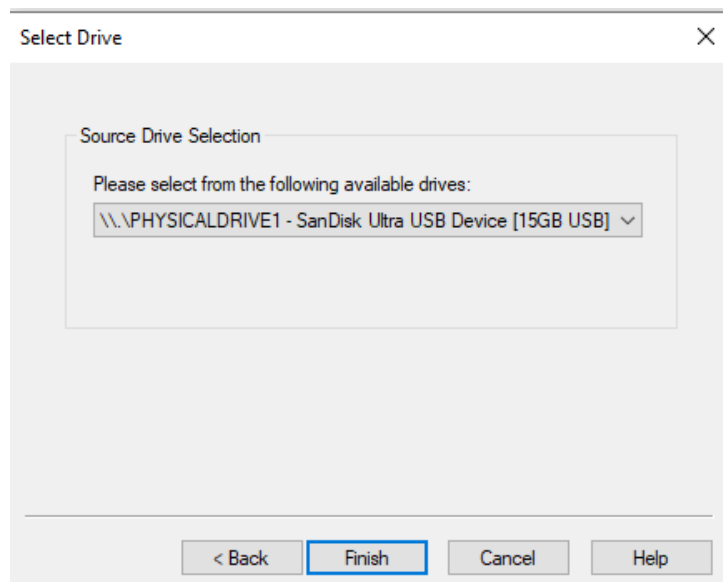
After installing the FTK imager we can start by creating an image and to do so, we have to go to the file button and from the drop-down menu, select the Create Disk Image option.



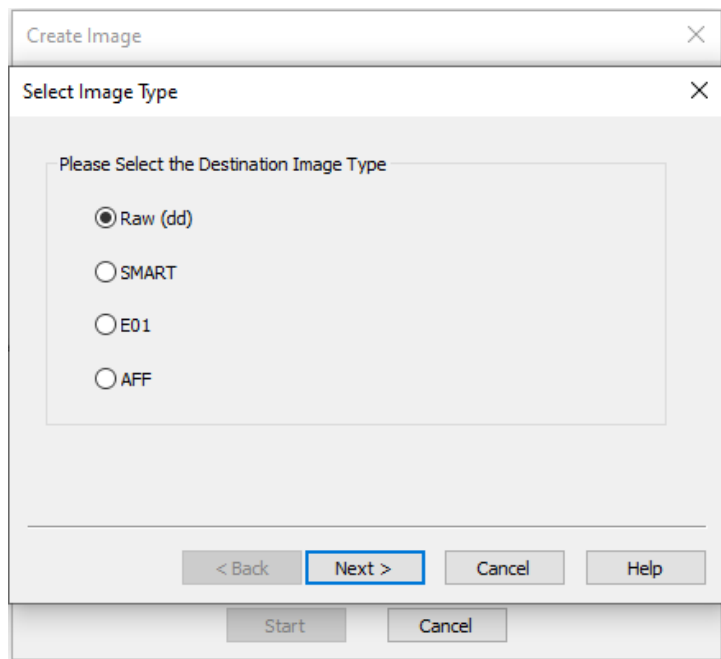
After selecting the create disk image it will ask you the evidence type whether i.e. physical drive, logical drive, etc. and once you have selected the evidence type then press the next button to move further in the process.



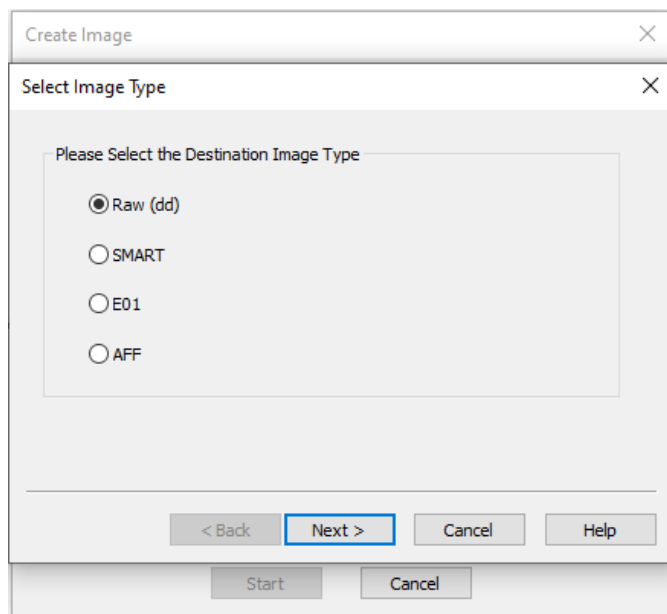
Now it will ask for the drive of which you want to create the image. Select that drive and click on Finish button.



Now, we need to provide the image destination i.e. where we want our image to be saved. And to give the path for the destination, click on Add button.



Then select the type you want your image to be i.e. raw or E01, etc. Then click on Next button.



Further it will ask you to provide details for the image such as case number, evidence number, unique description, examiner, notes about the evidence or investigation. Click on Next button after providing all the details.

The screenshot shows the 'Create Image' dialog box with the 'Evidence Item Information' tab selected. The fields are as follows:

| Field               | Value          |
|---------------------|----------------|
| Case Number:        | 001            |
| Evidence Number:    | 001            |
| Unique Description: |                |
| Examiner:           | Shubham Sharma |
| Notes:              |                |

At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'. Below the dialog box, there are 'Start' and 'Cancel' buttons.

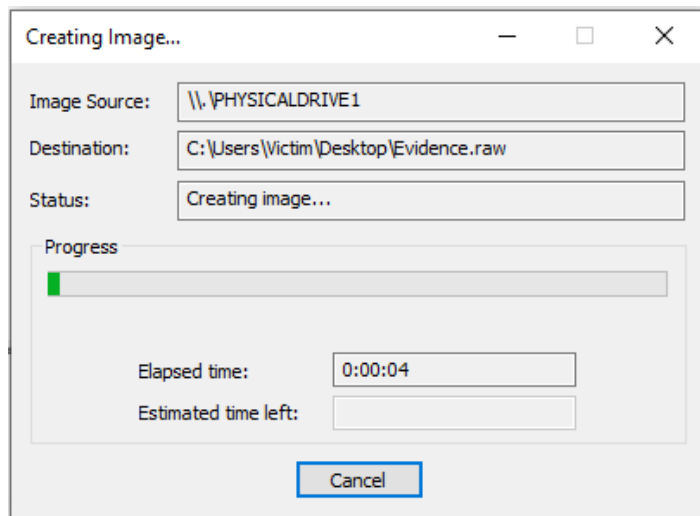
After this, it will ask you for the destination folder i.e. where you want your image to be saved along with its name and fragment size. Once you fill up all the details, click on the Finish button.

The screenshot shows the 'Create Image' dialog box with the 'Select Image Destination' tab selected. The fields are as follows:

| Field                                            | Value                    |
|--------------------------------------------------|--------------------------|
| Image Destination Folder                         | C:\Users\Victim\Desktop  |
| Image Filename (Excluding Extension)             | Evidence.raw             |
| Image Fragment Size (MB)                         | 1500                     |
| Compression (0=None, 1=Fastest, ..., 9=Smallest) | 0                        |
| Use AD Encryption                                | <input type="checkbox"/> |

At the bottom, there are buttons for '< Back', 'Finish', 'Cancel', and 'Help'. Below the dialog box, there are 'Start' and 'Cancel' buttons.

And now the process to create the image will start and it will simultaneously inform you about the elapsed time, estimated time left, image source, destination and status.



After the progress bar completes and status shows Image created successfully then it means our forensic image is created successfully.

