Forensic Collection and Analysis of Persistent Data

Persistent data is the data on a host that remains unchanged if the host has been powered off. This can be any data that is held on the hard disk. Examples of persistent data include e-mails, deleted files, web browsing history and documents. It is important to remember that even though this information is more stable than volatile data, you must still take precautions when collecting it. You do not want to invalidate your evidence!

Much information related to a security incident may be found on the hard disk, but because it is evidence you need to do everything possible to preserve it. This lab will walk you through the steps of collecting an image of a hard disk partition and moving it to another location for analysis. By taking these steps you can ensure that anything you do to gather evidence will not alter the original state of the actual hard disk.

This lab consists of 2 components. The first is imaging a partition for analysis and the second is setting up and using a forensic analysis tool called Autopsy. Autopsy is a GUI for the popular (and free) forensic analysis toolkit called “The Sleuth Kit.” This tool allows you to build a case file for your analysis and contains tools for logging your steps during the analysis, calculating an MD5 hash of the partition for integrity and looking at deleted files.

Your lab environment consists of three virtual computer systems.
1. A Windows 2003 Server launchpad system that will allow you to remotely access a server running Autopsy and the compromised host. This system’s hostname is: **VTE-Launchpad** and its IP address is **10.0.254.254**.

2. A Windows 2003 Server machine that has been booted from a Knoppix STD CDROM. It will serve as a compromised host from which you will gather forensic data. This system’s hostname is: **Win Compromised** and its IP address is **10.0.4.50**.

3. A Linux workstation that will serve as the collection point for your forensic data. It has been preloaded with the forensic analysis tool Autopsy. This system’s hostname is: **Chamberlain** and its IP address is **10.0.4.40**.

### Establishing a Forensic Collection System

#### 1.1 Configuring the Collection Workstation (Chamberlain)

1. From the desktop of the VTE-Launchpad, locate and double-click the VNC Client icon to open a ‘VNC client’. In the Server field, ‘type: 10.0.4.40:2.’ For encryption choose, “Let Server Choose (Default)”. Click OK.

   ![VNC Viewer Connection Details](image)

   **Figure 1**

2. Enter the password “tartans” and click OK.

   ![VNC Authentication](image)

   **Figure 2**

3. From the VNC terminal you now have access to the desktop of Chamberlain. Locate and double-click the Terminal icon to open ‘a terminal screen’.

4. From the command line create a directory to hold the forensic data. At the command line type:

   ```bash
   # mkdir -p /mnt/data/evidence_locker/
   ```
5. For this exercise you will need two Netcat listening sessions to receive transferred data from the target system (Win Compromised).

6. First, verify and make a note of the IP Address of the collection host (Chamberlain) as it will be needed in a later task. At the command line type:

```
# ifconfig
```

7. Next, establish the two Netcat listening sessions on ports 9000 and 9001. Type the following commands, one at a time separated by a hard return <Enter> :  
   * note: Do NOT type the # sign; it is in these instructions to represent the command prompt on your Linux system). Remember to try to use the Tab complete (tab button) and previous command (up arrow button) features within Linux, as this can save you on time and typing errors.

```
# nc –l –p 9000 > /mnt/data/evidence_locker/partitionhash.txt &
# nc –l –p 9001 > /mnt/data/evidence_locker/partitionE.dd &
```

8. You will need to confirm that both occurrences of Netcat are running. To do this type:

```
# ps -a
```

You should see two instances of Netcat running as separate processes.

2 Forensically Imaging a Windows Partition

The Windows 2003 host that you will be imaging has been pre-configured to boot from a Knoppix STD CDROM. When performing forensic imaging on other computers you will want to make sure that the boot sequence checks the CDROM first. When performing this same operation on other computers this may need to be configured.

The Knoppix disk you are using for gathering forensic data has been preconfigured to assign the compromised host an IP address of 10.0.4.50. Also, Knoppix has been customized to start the SSH service. This is necessary since when the computer is booted you will need to know its IP address and have the ability to connect via Secure Shell.

2.1 Identifying and Hashing the Partition to be Forensically Imaged

1. From within the VNC terminal you will enter the following commands. When collecting forensic evidence it is important to log all of the activities performed on the compromised host. To do this you will use the script
1. From the command line on Chamberlain you will make a connection to the Windows compromised host. Type:

```
# ssh –l knoppix 10.0.4.50
```

When prompted to accept the certificate type: yes. You will then be prompted for a password. Type: tartans.

2. You are now connected to Win Compromised as user knoppix, but in order to perform the forensic operations you will need to be operating as a user with root privileges. At the command line type: su. This causes all commands typed to be executed as root.

```
# su
```

3. Next, determine the partitions on the target host (Win Compromised). At the command line type: fdisk –l for a list of the partitions. You will be imaging and analyzing sdb1.

```
# fdisk -l
```

4. Before imaging a partition, calculate an md5 hash to later confirm the integrity of the captured image. Enter the following command to send the hash to the Linux Workstation:

```
# md5deep /dev/sdb1 | nc 10.0.4.40 9000 &
```

```
root@0[knoppix]# fdisk -l

Disk /dev/sda: 4294 MB, 4294967296 bytes
255 heads, 63 sectors/track, 522 cylinders
Units = cylinders of 16065 * 512 = 62914560 bytes

Device Boot Start   End   Blocks  Id  System
/dev/sda1   * 1 521  4184901  7  HPFS/NTFS

Disk /dev/sdb1: 107 MB, 1073741880 bytes
255 heads, 63 sectors/track, 13 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot Start   End   Blocks Id  System
/dev/sdb1   1 13 104991  42  ESP
```

```
root@0[knoppix]# md5deep /dev/sdb1 | nc 10.0.4.40 9000 &
```

Figure 3
Netcat may take several seconds to transfer this data and does not report its status. You will need to check the destination file on the Linux Workstation to determine if the data has been received.

### 2.2 Forensically Imaging and Transferring the Target Partition

Now that the partition has been identified and hashed, the next step is to create a forensic image of the partition and transfer it to the Linux Workstation.

1. You will use `dcfldd` (a Department of Defense version of `dd.exe`) to make an image of the partition and then use Netcat to transfer the image to the “Linux Workstation”. At the command line type:

   ```
   # dcfldd if=/dev/sdb1 bs=512 | nc 10.0.4.40 9001 &
   ```

   Once the “records out” count is equal to the “records in” count, press the ‘Enter’ key.

   ![Figure 4](image)

   2. Now that you have imaged the partition and collected it on the listening Linux Workstation you will want to end your SSH connection and shutdown the compromised host. To do this type:

   ```
   # shutdown -h now
   ```

   You will see a message that read “The system is going down for system halt NOW!” Followed by “Connection to 10.0.4.50 closed.”

2. Close the session log that you started earlier by typing:

   ```
   # exit
   ```

   You will see the notice “Script done, file is sessionlog.txt”

### 2.3 Confirm the Integrity of the Forensically Imaged Partition.

Now that you have closed your SSH connection to the compromised host you are back at a command prompt for the collection workstation (chamberlain). You can confirm this because the command prompt is “root@chamberlain #”.

```
Any commands you type will be executed on this machine where you collected your forensic data.

In order to complete the collection of the evidence you will want to confirm the integrity by calculating a hash of the image that you made of the hard drive and compare it with the MD5 hash that you calculated on the compromised host at the beginning of the lab.

1. Navigate to the evidence locker directory. At the command line type:

```
# cd /mnt/data/evidence_locker/
```

2. Now calculate an md5 hash on the partition image in the evidence_locker directory. At the command line type:

```
# md5sum partitionE.dd > partitionhashDD.txt
```

3. At this point compare the md5 hash taken before the partition was imaged to the md5 hash that was just calculated. At the command line type:

```
# diff partitionhash.txt partitionhashDD.txt
```

![Comparison](image.png)

**Figure 5**

### 3 Open and Prepare an Autopsy Case File for Examination

#### 3.1 Starting the Autopsy Server

You will need to launch the Autopsy server which will allow you to connect from the VTE-Launchpad in order to perform your forensic analysis.

1. First, navigate to the directory that contains the autopsy application. At the command line type:

```
# cd /usr/local/src/autopsy-2.05/
```

2. To start the application type:

```
# ./autopsy
```
3. Autopsy will provide a URL: “http://chamberlain:9999/autopsy”

   Note: Make sure to keep the autopsy process running in the terminal window while using the browser.

4. Minimize the terminal window on Chamberlain.

### 3.2 Creating a New Autopsy Case

1. Through the VNC console open a browser on Chamberlain by clicking Application > Internet > Firefox Web Browser at the top left-hand corner of the VNC window.

   ![Figure 6](image_url)

   Type: http://localhost:9999/autopsy in the address bar to access Autopsy’s web interface.

2. Click on the ‘New Case button’.

3. Enter the requested information below and click the ‘New Case button’:

   - Case Name: *Forensic_lab*
   - Description: *Windows_Compromised*
   - Investigator Names: *Student*

4. Information on the location of the new case directory will be displayed. Click ‘Add Host’.

5. Enter the appropriate information below and click ‘Add Host’ at the bottom of the screen:
   - Host Name: *Partition_E*
   - Description: *Windows_Compromised*
   - For this exercise, leave the remainder of the entries unchanged.
6. Information on the location of the case files will be displayed. Click ‘Add Image’.

7. Now you need to add the image that was collected earlier to the Autopsy case file. Click ‘Add Image File’.

8. At this point, you will need to enter the location of the image to be examined, as well as the following information. Once entered click the ‘Next button’.

Location: /mnt/data/evidence_locker/partitionE.dd
Type: Partition
Import Method: Copy

9. Make the following changes to the Image File Details. Once entered click the ‘Add button’:

   Data Integrity: Calculate the hash value for this image
   Mount Point: E:\
   File System Type: ntfs

Figure 7
10. Information concerning the location of the newly added host will be displayed. Review the confirmation information with the md5 hash of the newly copied partition. (This hash should match the hash values calculated during the early portion of the lab). Click 'OK'.

If multiple images existed for a host, this process would be repeated for each image. Partition E is made up of only one image.

3.3 Analyze a Forensic Image using Autopsy

1. Now that the image has been imported and the case has been defined you can begin your analysis. Click 'Analyze' to begin.

2. First, you will explore the existing file structure looking for useful information. To begin click the 'File Analysis' tab located on the top left side of the page.
From the File Browsing Mode, examine the following common locations bulleted below: What suspicious files and or information can you find? The default path “E:\” is displayed in your browser. Navigate to the directories listed below and see what you can discover.

- **Outlook**
  E:\Documents and Settings\Student System\Local Settings\Application Data\Microsoft\ Outlook

- **My Documents**
  E:\Documents and Settings\Student System\My Documents

- **Bookmarks**
  E:\Documents and Settings\Student System\Favorites

- **Cookies**
  E:\Documents and Settings\Student System\Cookies

- **History**
  E:\Documents and Settings\Student System\Local Settings\History

- **Temporary Internet Files**
  E:\Documents and Settings\Student System\Local Settings\Temporary Internet Files

- **Program Files**
  E:\Program Files

3. Next, Autopsy has a feature that allows the user to view all deleted files at once. In the left hand frame, click the **ALL DELETED FILES** tab. What can you find?

   - This is a convenient way to check for deleted documents that may have been in directories the student did not examine.

   - Notice also that in addition to deleted documents, there are deleted Windows shortcut links. These can tip off an investigator to documents or programs that have otherwise been cleaned from the system.

4. Autopsy will also sort by file types and look for any anomalies. To do this, click the ‘File Type’ tab at the top of the browser window.
Figure 12

- Click **Sort Files by Type** in the left hand frame.

- Select “Sort Files into categories by type” and “Extension and File Type Validation” boxes and click ‘OK’ *(It will take a minute to finish sorting files)*

Figure 13

- Scroll down and locate the “Output can be found by viewing:*” (which is just above the Results Summary page break). Copy this path into a new browser window which can be opened by selecting File > New Tab.

- From within this new browser, click the **Extension Mismatches** (16) link, to view files that do not match their extension.

  ✓ The 4th entry from the bottom is of particular interest. The student will see that the file log.dll is located in the E:\Documents and Settings\Student System\PrintHood directory. Autopsy, however, reports that this is a JPEG image despite the .dll extension.

Figure 14

- Return to the original browser, and select the “Forensic_Lab:partitionE:vol1” tab. Click the **File Analysis** button, and navigate to the E:\Documents and Settings\Student System\PrintHood directory. Click the ‘log.dll link’.

- In the bottom frame click the link, **View Full Size Image**, to open the JPEG. A new browser window will open displaying the JPEG. Aside from the incorrect file extension, is there anything suspicious about the image? Close the browser showing the JPEG.
5. Autopsy is a multi-featured tool. This exercise has merely touched the surface of its functionality. Take a few minutes to explore some of the other features.

- When finished close the browser.
- In the terminal window enter ‘Ctrl C’ to stop the Autopsy process.