EC-Council

codered
FROM EC-COUNCIL

CHAPTER 20

COMPUTER FORENSICS

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 20:
Computer Forensics

SCENARIO

Ever-increasing instances of cybercrime and the rise in computing technology have made an efficient and effective information security program essential for organizations. With the rapid change in technology and threat landscape, it is important for organizations to incorporate ongoing and proactive computer investigations into their current information security programs to thwart and prevent evolving threats.

To implement these programs, organizations need to adapt current information security best practices to include certain aspects of digital forensic readiness into their current cybersecurity programs.

OBJECTIVE

The objective of this lab is to provide expert knowledge in conducting computer forensics. This includes knowledge of the following tasks:

- Creating a disk image file of a hard disk partition
- Acquiring RAM and volatile information from a Windows system
- Analyzing file system of a Linux image using tools such as Autopsy
- Capturing and analyzing memory dump on Linux System
- Viewing contents of forensics image file

OVERVIEW INTERRUPTED SESSIONS

Computer forensics is a part of digital forensics that deals with crimes committed across computing devices such as networks, computers, and digital storage media. It refers to a set of methodological procedures and techniques to identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment such that the discovered evidence is acceptable during a legal and/or administrative proceeding in a court of law.

An exponential increase in the number of cybercrimes and civil litigations involving large organizations has emphasized the need for computer forensics. It has become a necessity for organizations to employ the service of a computer forensics agency or to hire a computer forensics expert to solve cases involving the use of computers and related technologies. The staggering financial losses caused by cybercrimes have also contributed to renewed interest in computer forensics.

LAB TASKS

A cyber security professional or a security professional use numerous tools and techniques to investigate evidence related to cyber-attacks. The recommended labs that will assist you in learning the process of computer forensics include the following:

01 Create a Disk Image File of a Hard Disk Partition

02 Acquire RAM from Windows Workstation

03 Acquire Volatile Information from a Live Windows System

04 Analyze File System of a Linux Image using Autopsy

05 Capture and Analyse Memory Dump on Linux

06 View Contents of Forensic Image File

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: CREATE A DISK IMAGE FILE OF A HARD DISK PARTITION

A disk image is a bit-by-bit copy of a hard disk or a disk partition, which includes all the files/folders, deleted files, files left in the slack space and unallocated space, file system information, etc.

LAB SCENARIO

An investigator was performing forensics on a hard disk copy when he triggered a pre-loaded process that deleted the entire disk data leading to loss of evidence. However, he had already created a forensic copy of the disk, and this gave him the option to work on the same data again. Therefore, investigators should always create duplicates of the hard disk and perform the forensics process on the copy.
An expert investigator must have sound knowledge of the various disk imaging tools used for forensics investigation.

OBJECTIVE

The objective of this lab is to learn how to create a disk image file of a hard disk partition using R-Drive Image.

OVERVIEW OF TROJAN

This lab helps you learn how to create the disk image file of a hard-disk partition. Imaging of a hard disk or a hard disk partition helps you create the forensic copy of the disk or a partition on it so that you can use the forensic copy for investigation purposes.

EXERCISE 1: CREATE A DISK IMAGE FILE OF A HARD DISK PARTITION

Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on the Admin Machine-1 virtual machine.
2. Log in with the credentials Admin and admin@123.

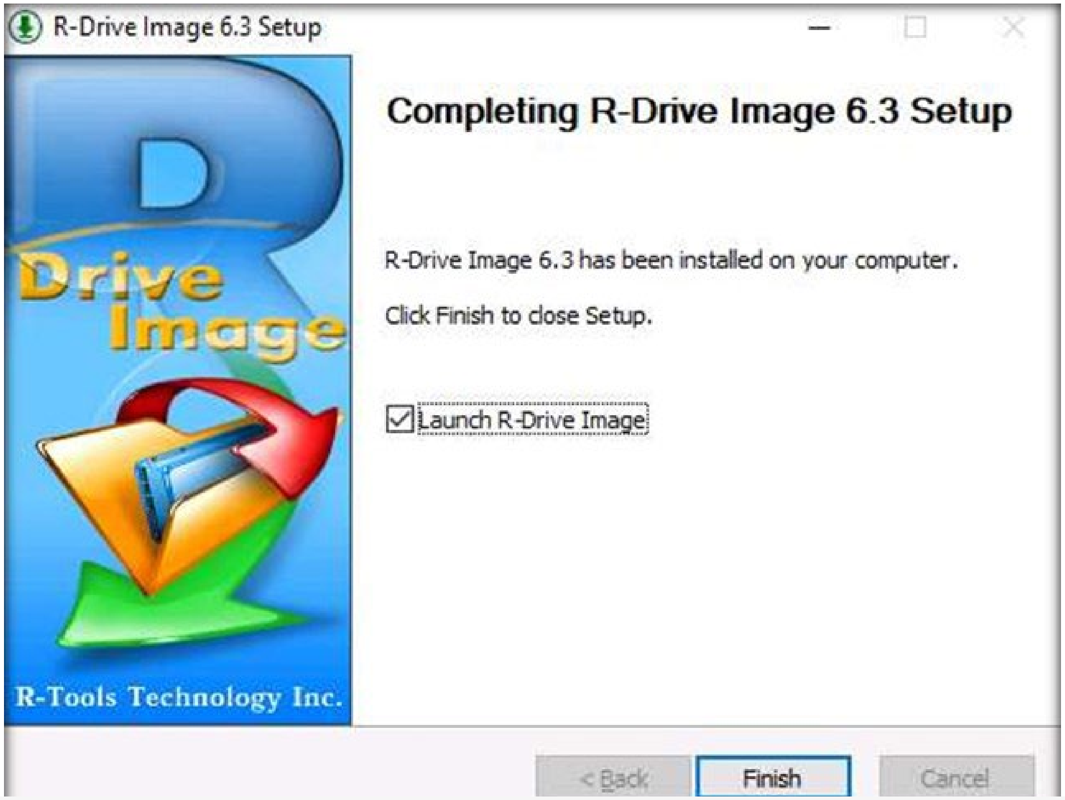
Note: If Networks pane appears, click Yes to allow your PC to be discoverable by other PCs and devices on this network.

3. Navigate to Z:\CCT-Tools\CCT Module 20 Computer Forensics\Computer Forensics Software\R-drive Image.
4. Double-click RDriveImage6.exe to launch the setup, select the language (here, English) and click OK.

Note: If an Open File - Security Warning pop-up appears, click Run.

Note: If a User Account Control pop-up appears, click Yes.

5. Follow the wizard-driven installation steps to install the application.
6. On completing the installation, ensure that Launch R-Drive Image option is checked and



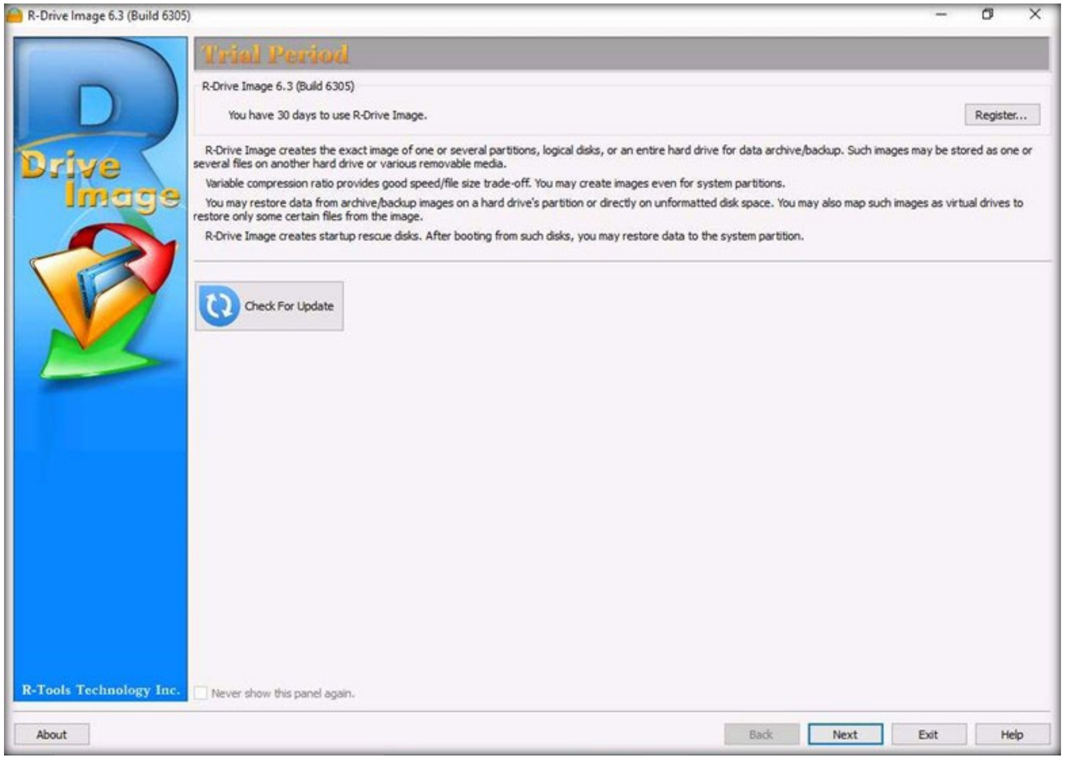
Completing R-Drive Image 6.3 Setup

R-Drive Image 6.3 has been installed on your computer.

Click Finish to close Setup.

☑ Launch R-Drive Image

7. The R-Drive Image GUI appears, click Next.



R-Drive Image 6.3 (Build 6305)

You have 30 days to use R-Drive Image.

R-Drive Image creates the exact image of one or several partitions, logical disks, or an entire hard drive for data archive/backup. Such images may be stored as one or several files on another hard drive or various removable media.

Variable compression ratio provides good speed/file size trade-off. You may create images even for system partitions.

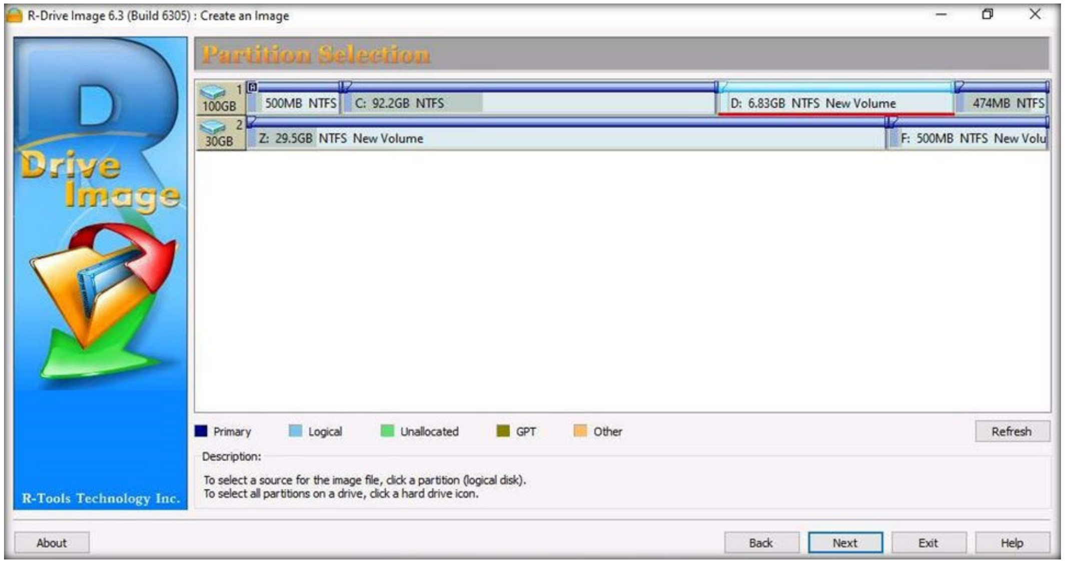
You may restore data from archive/backup images on a hard drive's partition or directly on unformatted disk space. You may also map such images as virtual drives to restore only some certain files from the image.

R-Drive Image creates startup rescue disks. After booting from such disks, you may restore data to the system partition.

□ Never show this panel again.

8. In the Action Selection window, Create an Image option is selected by default. Click Next to continue.
9. In this lab, we will be creating an image for D:. Therefore, in the Partition Selection window, select D drive to create a drive image file of the drive. Click Next.

EXERCISE 1: CREATE A DISK IMAGE FILE OF A HARD DISK PARTITION

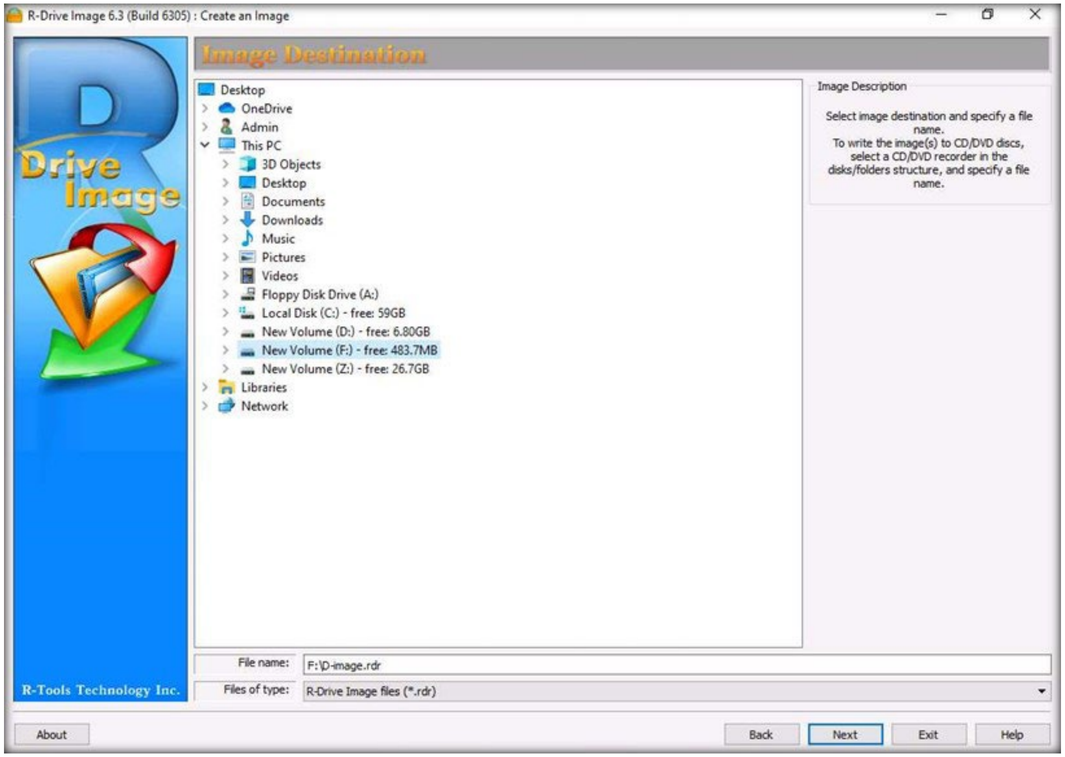


Description:

To select a source for the image file, click a partition (logical disk).
To select all partitions on a drive, click a hard drive icon.

10. In the Image Destination panel:

- Expand This PC and select the New Volume (F:) (F drive) to save the file in this drive.
- The filename will be automatically taken by the application.
- Select R-Drive Image files (*.rdr) in the Files of type field and click Next.



Select image destination and specify a file name.
To write the image(s) to CD/DVD discs, select a CD/DVD recorder in the disks/folders structure, and specify a file name.

File name: F:\D-image.rdr

Files of type: R-Drive Image files (*.rdr)

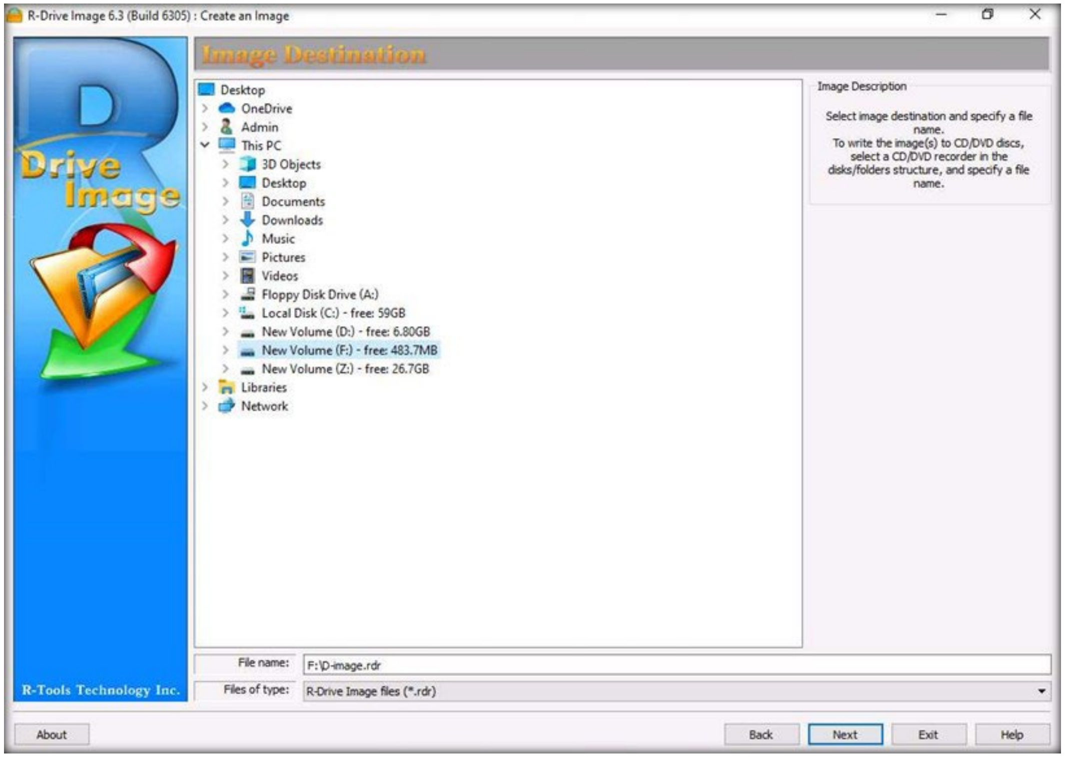
EXERCISE 1: CREATE A DISK IMAGE FILE OF A HARD DISK PARTITION

11. In the Image Options panel, click Next.

Note: Providing a password is optional.

12. In the Backup Options panel, click Next.

13. The Processing panel displays the summary of all the processes. Click Start to start the disk partition imaging process.



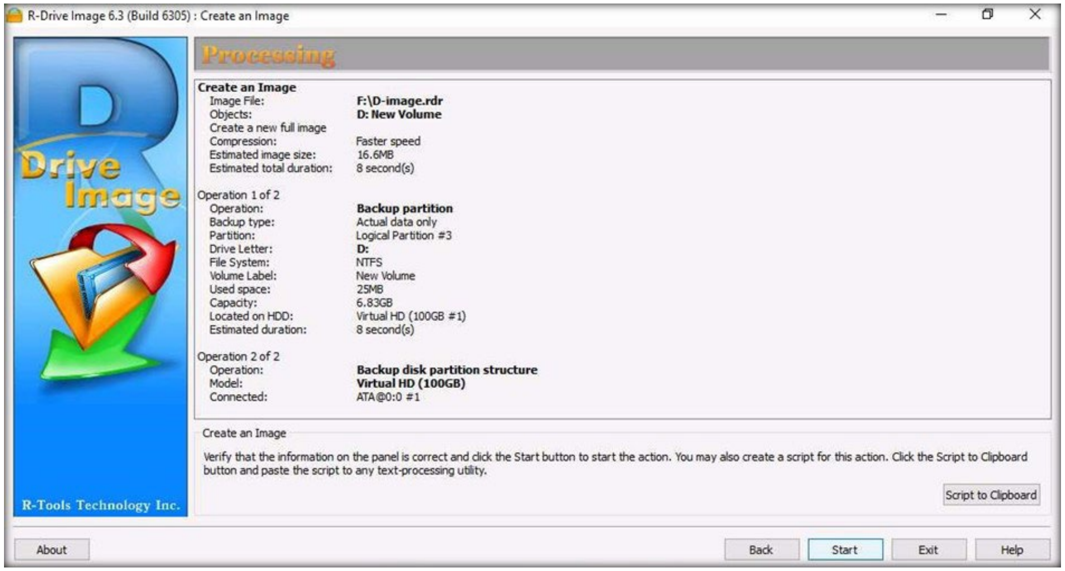
Select image destination and specify a file name.
To write the image(s) to CD/DVD discs, select a CD/DVD recorder in the disks/folders structure, and specify a file name.

File name: F:\D-image.rdr

Files of type: R-Drive Image files (*.rdr)

EXERCISE 1: CREATE A DISK IMAGE FILE OF A HARD DISK PARTITION

11. In the Image Options panel, click Next.
Note: Providing a password is optional.
12. In the Backup Options panel, click Next.
13. The Processing panel displays the summary of all the processes. Click Start to start the disk partition imaging process.



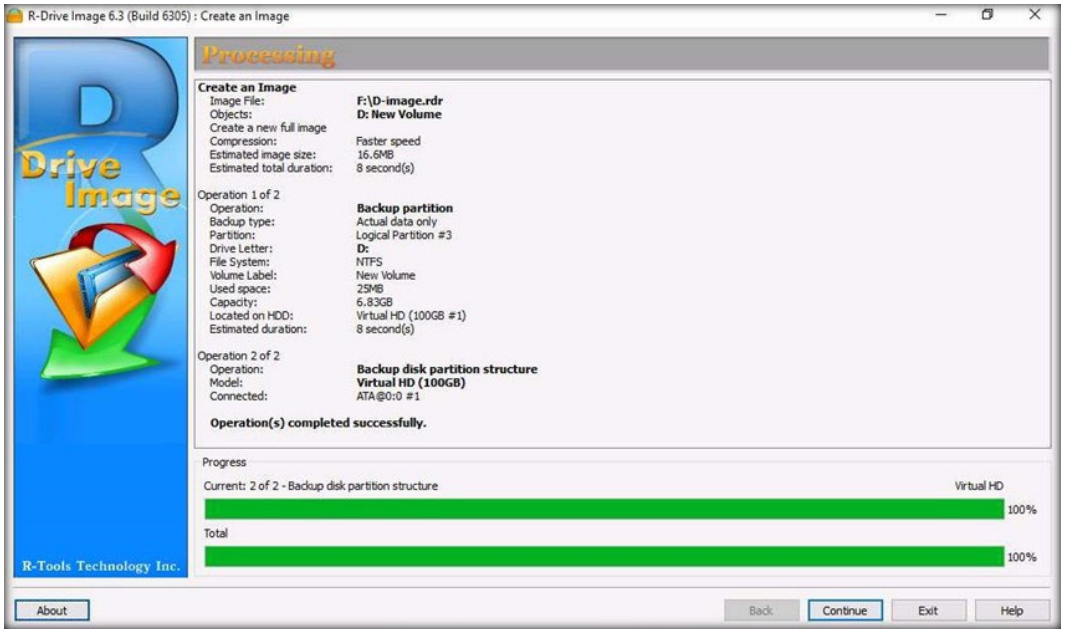
```
Create an Image
   Image File:                    F:\D-image.rdr
   Objects:                       D: New Volume
   Create a new full image
   Compression:                   Faster speed
   Estimated image size:          16.6MB
   Estimated total duration:      8 second(s)

Operation 1 of 2
   Operation:                     Backup partition
   Backup type:                   Actual data only
   Partition:                     Logical Partition #3
   Drive Letter:                  D:
   File System:                   NTFS
   Volume Label:                  New Volume
   Used space:                    25MB
   Capacity:                      6.83GB
   Located on HDD:                Virtual HD (100GB #1)
   Estimated duration:            8 second(s)

Operation 2 of 2
   Operation:                     Backup disk partition structure
   Model:                         Virtual HD (100GB)
   Connected:                     ATA@0:0 #1
```

Create an Image

Verify that the information on the panel is correct and click the Start button to start the action. You may also create a script for this action. Click the Script to Clipboard button and paste the script to any text-processing utility.

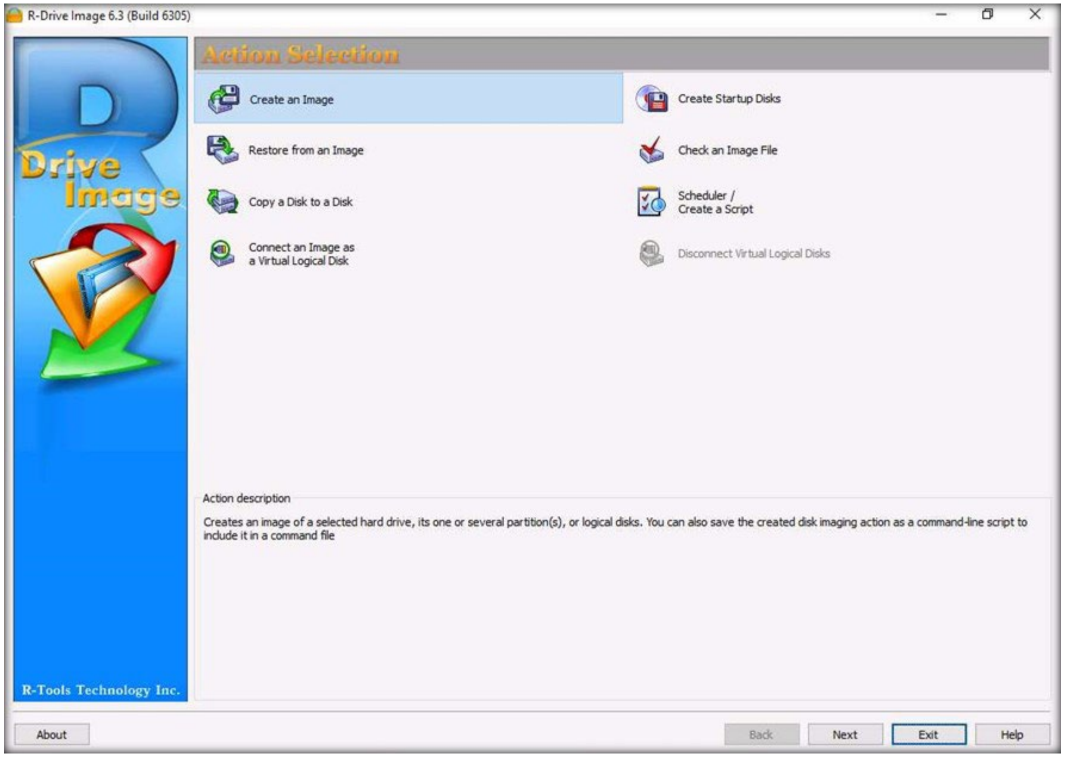
14. The Progress bar in the Processing panel will show the percentage of task completed. Once the processing is done, a pop-up will appear displaying Image created successfully. Click OK.
15. In the Processing panel, click Continue to complete the process.

EXERCISE 1:
CREATE A DISK IMAGE FILE OF A HARD DISK PARTITION



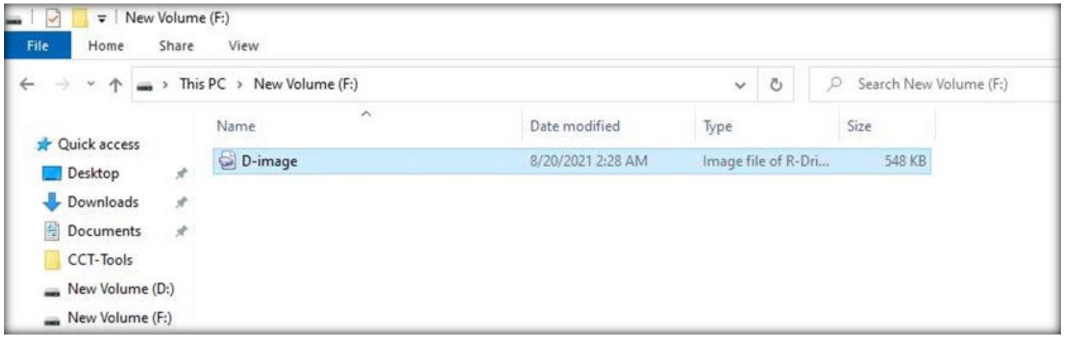
```
Create an Image
  Image File:                F:\D-image.rdr
  Objects:                   D: New Volume
  Create a new full image
  Compression:               Faster speed
  Estimated image size:      16.6MB
  Estimated total duration:  8 second(s)

Operation 1 of 2
  Operation:                 Backup partition
  Backup type:               Actual data only
  Partition:                 Logical Partition #3
  Drive Letter:              D:
  File System:               NTFS
  Volume Label:              New Volume
  Used space:                25MB
  Capacity:                  6.83GB
  Located on HDD:            Virtual HD (100GB #1)
  Estimated duration:        8 second(s)

Operation 2 of 2
  Operation:                 Backup disk partition structure
  Model:                     Virtual HD (100GB)
  Connected:                 ATA@0:0 #1

  Operation(s) completed successfully.

Progress
Current: 2 of 2 - Backup disk partition structure          Virtual HD
                                                            100%
Total
                                                            100%
```

16. In the R-Drive Image window that reads Action Selection at the top, click the Exit button to close the application.



Creates an image of a selected hard drive, its one or several partition(s), or logical disks. You can also save the created disk imaging action as a command-line script to include it in a command file

17. Now, navigate to the New Volume (F:) (F Drive) to view the created disk partition image file.



Name	Date modified	Type	Size
D-image	8/20/2021 2:28 AM	Image file of R-Dri...	548 KB

Note: The size of the image file depends on the space filled in the drive. Since we are imaging D drive, which is currently empty, the size of the generated image file is relatively less.

18. Delete the image file upon finishing this lab.
19. This concludes the demonstration showing how to create a disk image file of a hard disk partition.
20. Close all open windows.

EXERCISE 1:
CREATE A DISK
IMAGE FILE OF
A HARD DISK
PARTITION

EXERCISE 2: **ACQUIRE RAM FROM WINDOWS WORKSTATION**

RAM (Random Access Memory) is a volatile-memory storage found in computing devices that temporarily holds the data your device needs to access.

LAB SCENARIO

James, a forensics investigator, is performing live analysis on a suspect's computer. In this process, he needs to primarily capture the RAM dump of the machine as it contains volatile data that is lost when the machine loses power. In this scenario, the investigator performs RAM acquisition on Windows workstation.
An expert investigator must understand how to acquire a RAM dump from Windows and Linux OSes.

OBJECTIVE

The objective of this lab is to learn how to perform RAM acquisition on Windows workstation.

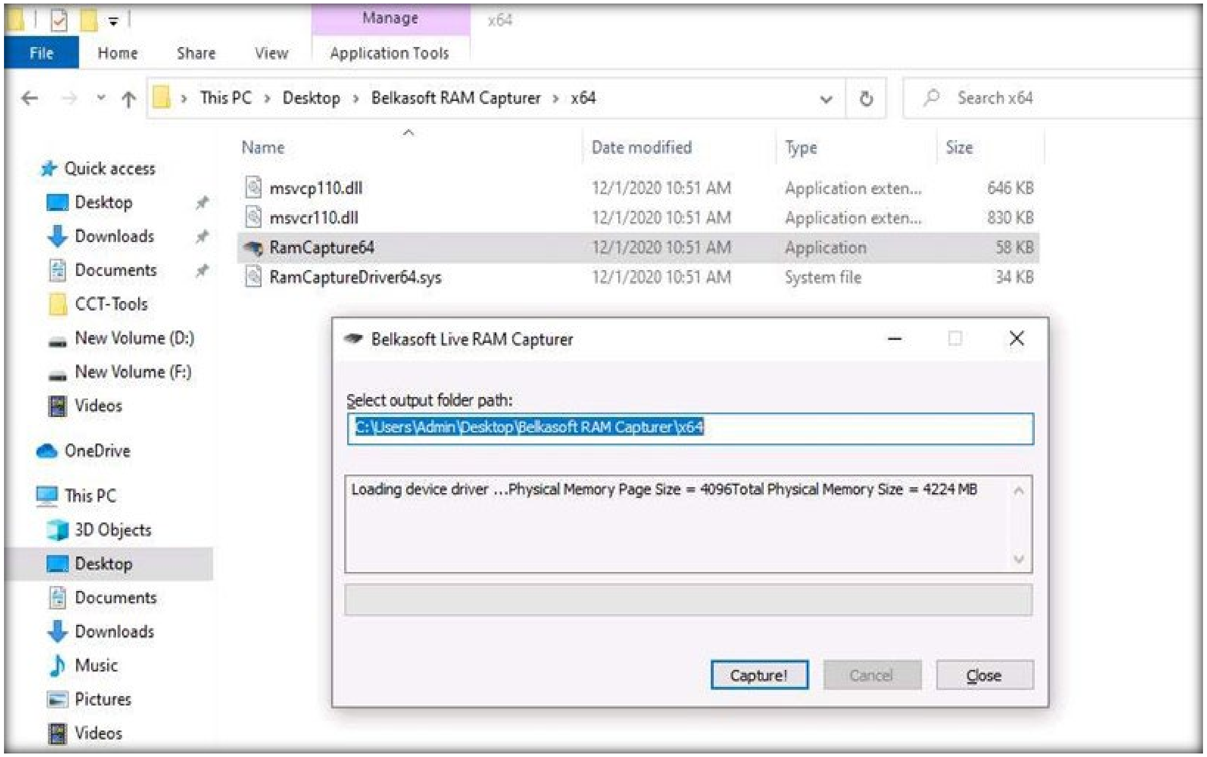
OVERVIEW OF TROJAN

This lab familiarizes you with the Belkasoft RAM Capturer tool, which helps perform RAM acquisition on Windows systems; LiME and fmem do the same on Linux systems.

EXERCISE 2: ACQUIRE RAM FROM WINDOWS WORKSTATION

Note: Ensure that the Admin Machine-1 and PfSense Firewall virtual machine is running.

1. In the Admin Machine-1 virtual machine, navigate to the directory Z:\CCT-Tools\CCT Module 20 Computer Forensics\Data Acquisition Tools, copy Belkasoft RAM Capturer folder and paste it onto Desktop.
2. Now navigate to the directory Desktop →Belkasoft RAM Capturer → x64 and double-click RamCapture64.exe to launch the application.



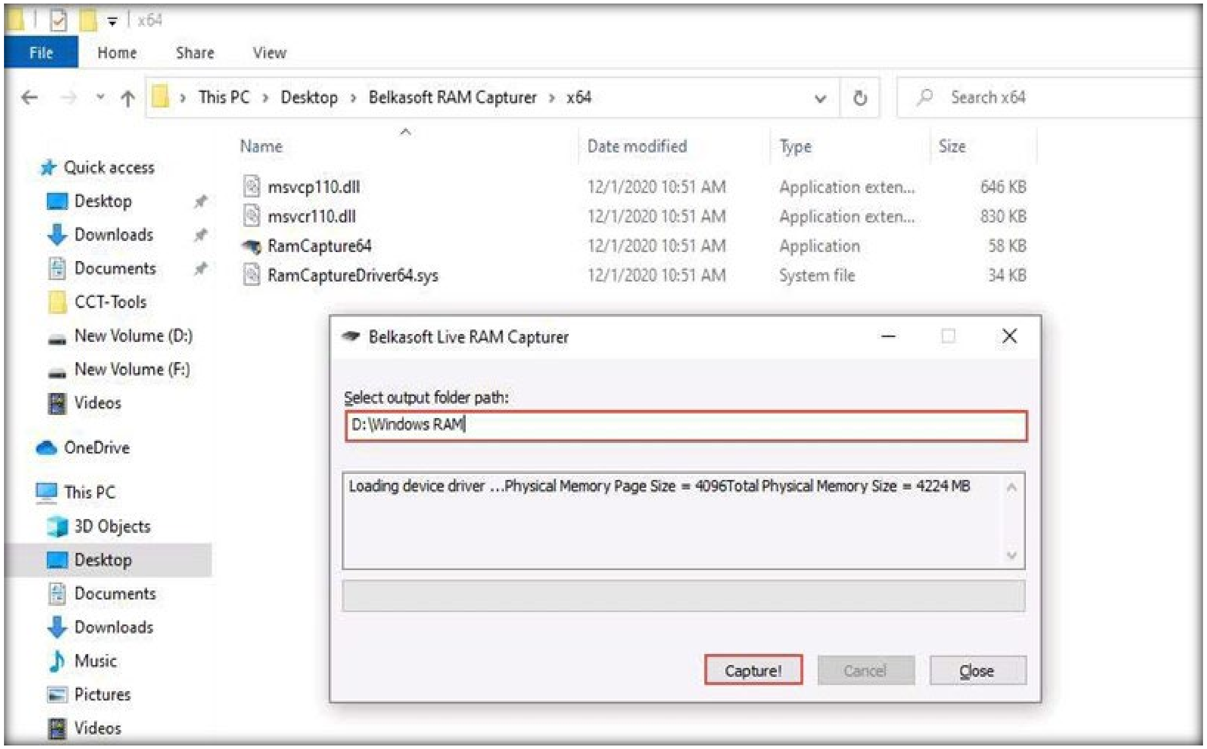
Name	Date modified	Type	Size
msvcp110.dll	12/1/2020 10:51 AM	Application exten...	646 KB
msvcr110.dll	12/1/2020 10:51 AM	Application exten...	830 KB
RamCapture64	12/1/2020 10:51 AM	Application	58 KB
RamCaptureDriver64.sys	12/1/2020 10:51 AM	System file	34 KB

Select output folder path: C:\Users\Admin\Desktop\Belkasoft RAM Capturer\x64

```
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 4224 MB
```

Note: If an Open File - Security Warning pop-up appears, click Run.
Note: If a User Account Control pop-up appears, click Yes.

3. You need to assign a folder to store the captured RAM. Therefore, navigate to the New Volume (D:) (D Drive) and create a folder named Windows RAM.
4. Now, enter the path for the output (here, D:\Windows RAM) under Select output folder path field and click Capture!.



Name	Date modified	Type	Size
msvcp110.dll	12/1/2020 10:51 AM	Application exten...	646 KB
msvcr110.dll	12/1/2020 10:51 AM	Application exten...	830 KB
RamCapture64	12/1/2020 10:51 AM	Application	58 KB
RamCaptureDriver64.sys	12/1/2020 10:51 AM	System file	34 KB

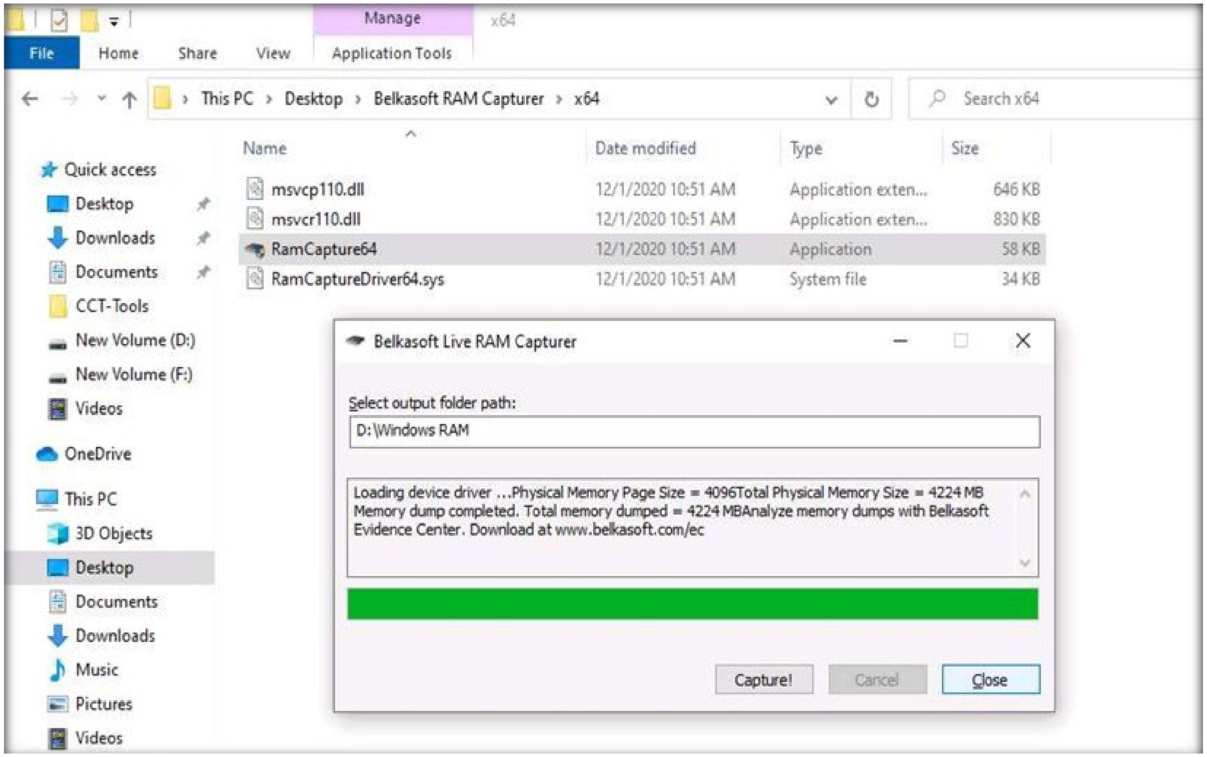
Belkasoft Live RAM Capturer

Select output folder path:
D:\Windows RAM

```
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 4224 MB
```

EXERCISE 2: ACQUIRE RAM FROM WINDOWS WORKSTATION

5. The application begins to capture the RAM.
6. Once the memory dump is successfully created, click Close to close the application.



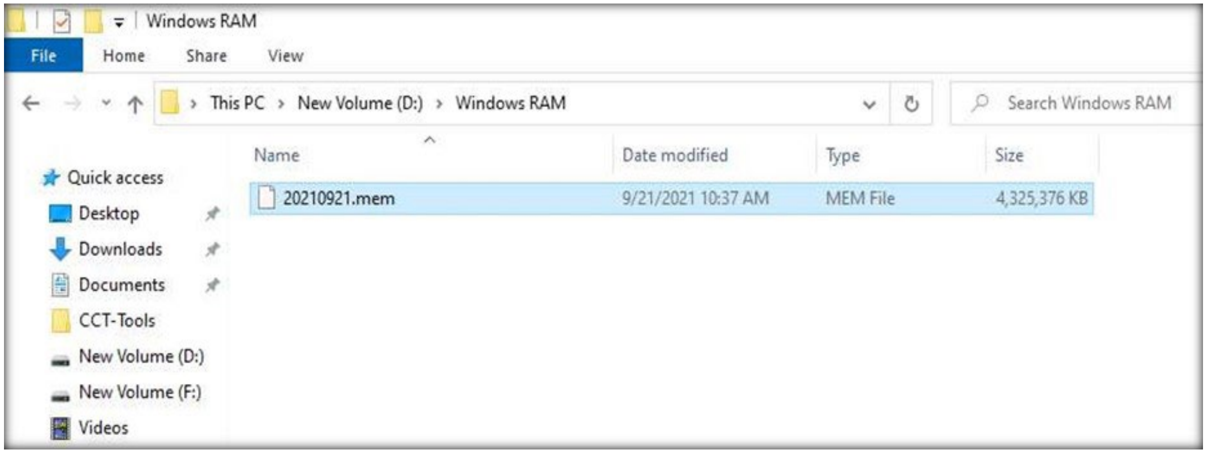
Name	Date modified	Type	Size
msvcp110.dll	12/1/2020 10:51 AM	Application exten...	646 KB
msvcr110.dll	12/1/2020 10:51 AM	Application exten...	830 KB
RamCapture64	12/1/2020 10:51 AM	Application	58 KB
RamCaptureDriver64.sys	12/1/2020 10:51 AM	System file	34 KB

Belkasoft Live RAM Capturer

Select output folder path: D:\Windows RAM

```
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 4224 MB
Memory dump completed. Total memory dumped = 4224 MBAnalyze memory dumps with Belkasoft
Evidence Center. Download at www.belkasoft.com/ec
```

7. Navigate to D:\Windows RAM to view the created memory dump. The dump is saved in the yyyymmdd.mem format, where yyyy refers to the year, mm refers to the month, and dd refers to the date.



Name	Date modified	Type	Size
20210921.mem	9/21/2021 10:37 AM	MEM File	4,325,376 KB

8. This way, you can capture the memory dump of a suspect Windows machine. These dumps act as important source of evidence for the investigators while investigating volatile memory.
9. This concludes the demonstration showing how to acquire RAM from Windows machine.
10. Close all open windows.

EXERCISE 2:
ACQUIRE RAM
FROM WINDOWS
WORKSTATION

EXERCISE 3: ACQUIRE VOLATILE INFORMATION FROM A LIVE WINDOWS SYSTEM

Acquiring volatile information from a live system involves obtaining information such as network information and process information about an OS.

LAB SCENARIO

For forensics investigation, an investigator often needs to gather data from a live Windows system to analyze details such as network information and process information by using different tools (command-line tools as well as GUI-based tools). Performing a thorough analysis will enable the investigator to obtain vital evidence, which helps them solve cases related to digital forensics.
An expert investigator should know how to collect volatile information from a live system.

OBJECTIVE

The objective of this lab is to help you collect volatile information from a live Windows system

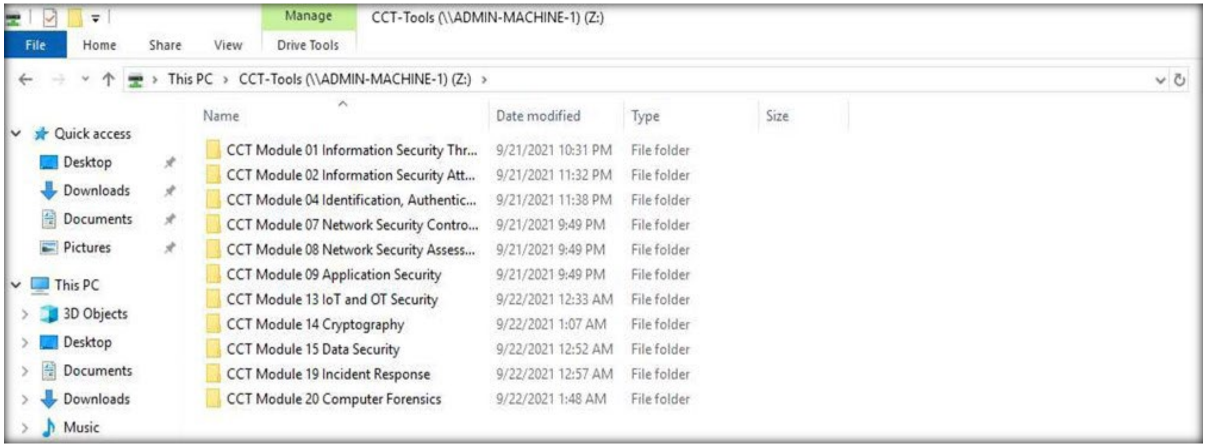
OVERVIEW OF THE LAB

This lab familiarizes you with the procedures to collect volatile information from a host computer running on a Windows OS by using tools such as PsTools and LogonSessions.

EXERCISE 3: ACQUIRE VOLATILE INFORMATION FROM A LIVE WINDOWS SYSTEM

Note: Ensure that the PfSense Firewall and Admin Machine-1 virtual machine is running.
1. Turn on the AD Domain Controller virtual machine.
2. Log in with the credentials CCT\Administrator and admin@123.
Note: If Networks pane appears, click Yes to allow your PC to discoverable by other PCs and Devices on this network.

3. Now, connect to the network drive CCT-Tools (Z:) as shown in the below screenshot.

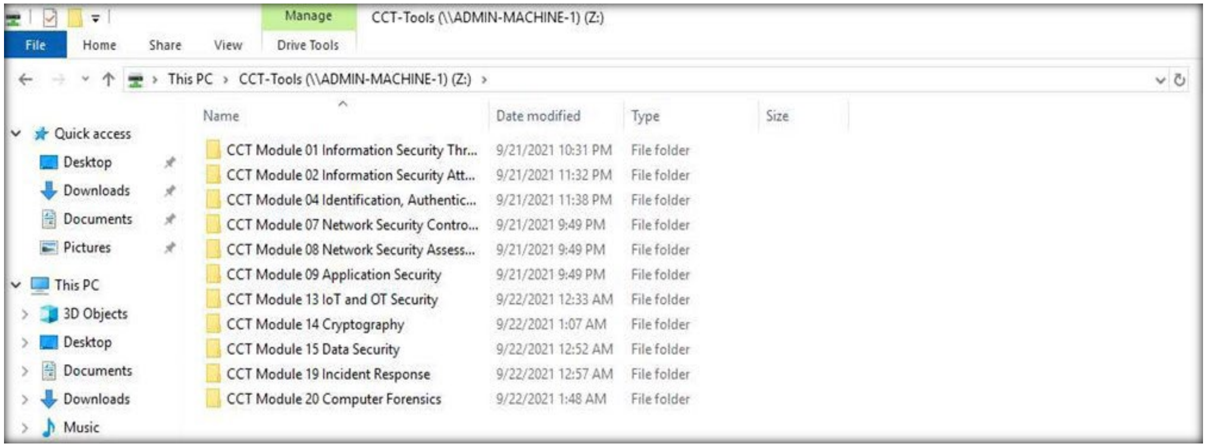


Name	Date modified	Type	Size
CCT Module 01 Information Security Thr...	9/21/2021 10:31 PM	File folder	
CCT Module 02 Information Security Att...	9/21/2021 11:32 PM	File folder	
CCT Module 04 Identification, Authentic...	9/21/2021 11:38 PM	File folder	
CCT Module 07 Network Security Contro...	9/21/2021 9:49 PM	File folder	
CCT Module 08 Network Security Assess...	9/21/2021 9:49 PM	File folder	
CCT Module 09 Application Security	9/21/2021 9:49 PM	File folder	
CCT Module 13 IoT and OT Security	9/22/2021 12:33 AM	File folder	
CCT Module 14 Cryptography	9/22/2021 1:07 AM	File folder	
CCT Module 15 Data Security	9/22/2021 12:52 AM	File folder	
CCT Module 19 Incident Response	9/22/2021 12:57 AM	File folder	
CCT Module 20 Computer Forensics	9/22/2021 1:48 AM	File folder	

EXERCISE 3: ACQUIRE VOLATILE INFORMATION FROM A LIVE WINDOWS SYSTEM

Note: Ensure that the PfSense Firewall and Admin Machine-1 virtual machine is running.
1. Turn on the AD Domain Controller virtual machine.
2. Log in with the credentials CCT\Administrator and admin@123.
Note: If Networks pane appears, click Yes to allow your PC to discoverable by other PCs and Devices on this network.

3. Now, connect to the network drive CCT-Tools (Z:) as shown in the below screenshot.



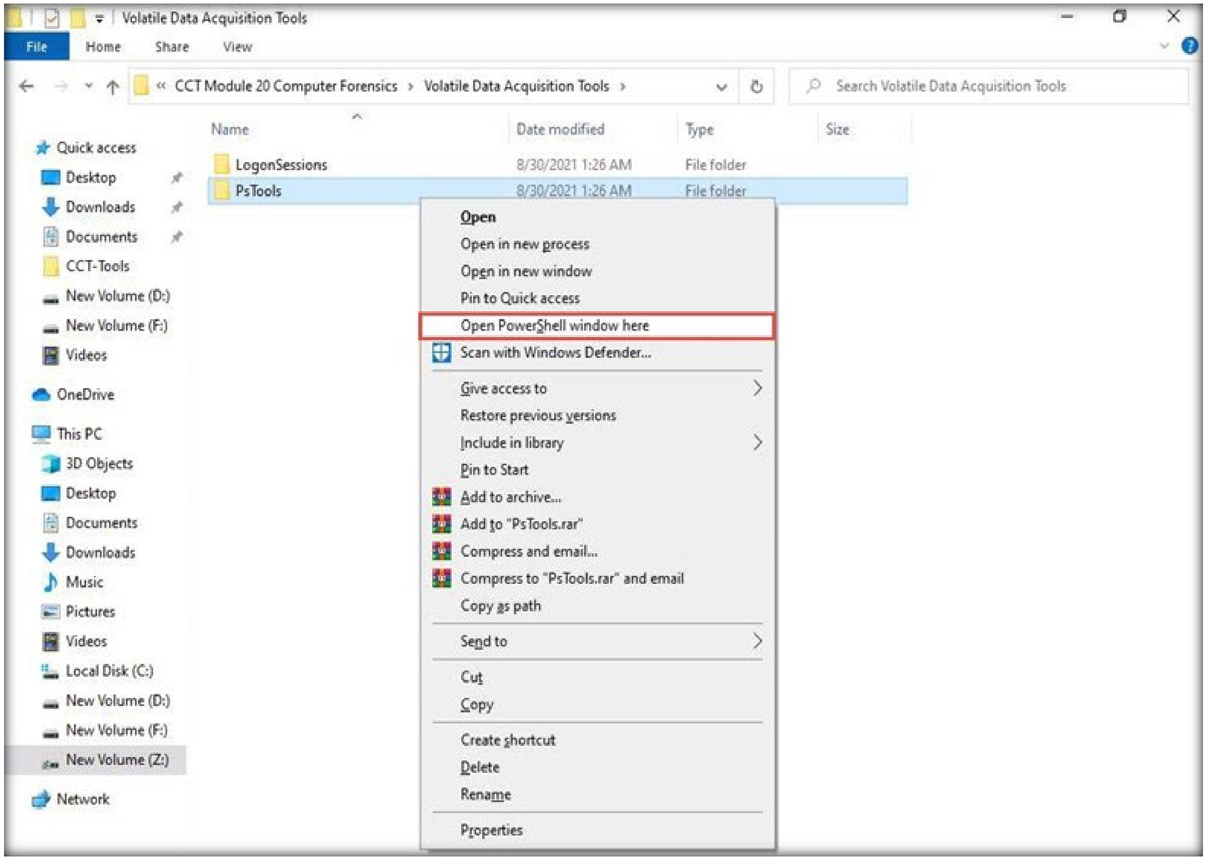
Name	Date modified	Type	Size
CCT Module 01 Information Security Thr...	9/21/2021 10:31 PM	File folder	
CCT Module 02 Information Security Att...	9/21/2021 11:32 PM	File folder	
CCT Module 04 Identification, Authentic...	9/21/2021 11:38 PM	File folder	
CCT Module 07 Network Security Contro...	9/21/2021 9:49 PM	File folder	
CCT Module 08 Network Security Assess...	9/21/2021 9:49 PM	File folder	
CCT Module 09 Application Security	9/21/2021 9:49 PM	File folder	
CCT Module 13 IoT and OT Security	9/22/2021 12:33 AM	File folder	
CCT Module 14 Cryptography	9/22/2021 1:07 AM	File folder	
CCT Module 15 Data Security	9/22/2021 12:52 AM	File folder	
CCT Module 19 Incident Response	9/22/2021 12:57 AM	File folder	
CCT Module 20 Computer Forensics	9/22/2021 1:48 AM	File folder	

EXERCISE 3: ACQUIRE VOLATILE INFORMATION FROM A LIVE WINDOWS SYSTEM

Note: Our task in this lab is to collect volatile information from a host machine. We will be using Admin Machine-1 machine as the host machine and AD Domain Controller machine as a locally connected machine.

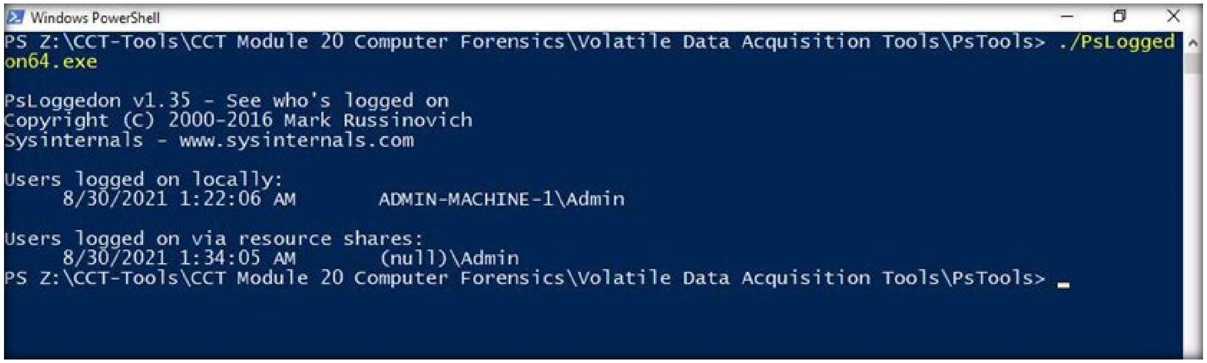
Note: If you are already logged into the Admin Machine-1, then skip to Step#6.

4. Now, switch to the Admin Machine-1 virtual machine.
5. In the Admin Machine-1 virtual machine, navigate to Z:\CCT-Tools\CCT Module 20 Computer Forensics\Volatile Data Acquisition Tools.
6. Select the PsTools folder, hold the Shift key on the keyboard, right-click on the selected folder, and then select Open PowerShell window here from the context menu.



7. The above operation will launch PowerShell displaying the path of PsTools. Type ./PsLoggedon64.exe and press Enter.
8. The PsLoggedon License Agreement window will appear. Click Agree to continue.
9. The PowerShell window will now display two results: Users Logged on locally (here, the local user is the Administrator of the local machine) and Users Logged on via resource shares (in this case, no user is logged on through resource shares; hence, the result displays null in the Users logged on via resource shares section)

EXERCISE 3: ACQUIRE VOLATILE INFORMATION FROM A LIVE WINDOWS SYSTEM



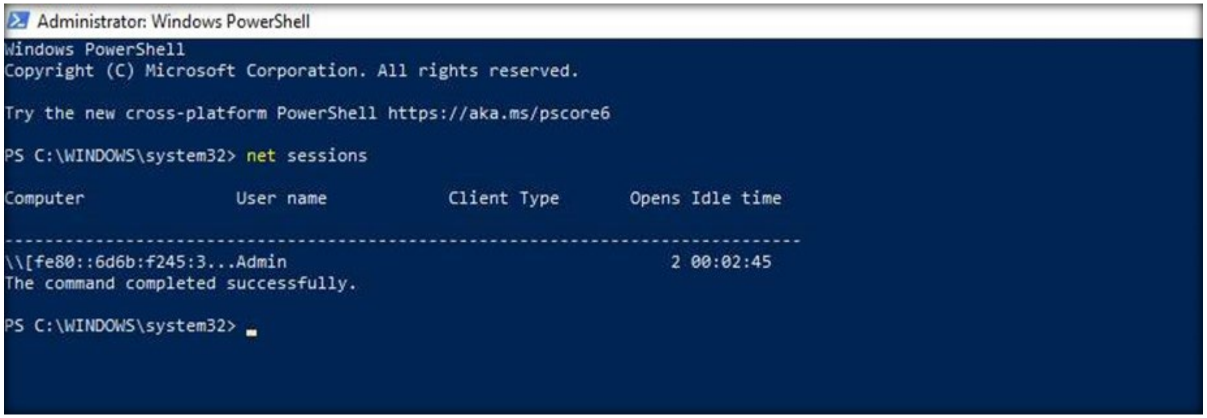
```
PS Z:\CCT-Tools\CCT Module 20 Computer Forensics\Volatile Data Acquisition Tools\PsTools> ./PsLogged
on64.exe

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

Users logged on locally:
     8/30/2021 1:22:06 AM       ADMIN-MACHINE-1\Admin

Users logged on via resource shares:
     8/30/2021 1:34:05 AM       (null)\Admin
PS Z:\CCT-Tools\CCT Module 20 Computer Forensics\Volatile Data Acquisition Tools\PsTools> _
```

10. Now, close the PowerShell window and launch PowerShell window with Administrator privileges by right clicking the Start button (Windows icon button) and then clicking on Windows PowerShell (Admin).

Note: If a User Account Control pop-up appears, click Yes.

11. We will now run the net sessions command, which will list all the connected sessions on the host machine (here, Admin Machine-1), the command has listed the username of the Admin Machine-1 machine as shown in the following screenshot:

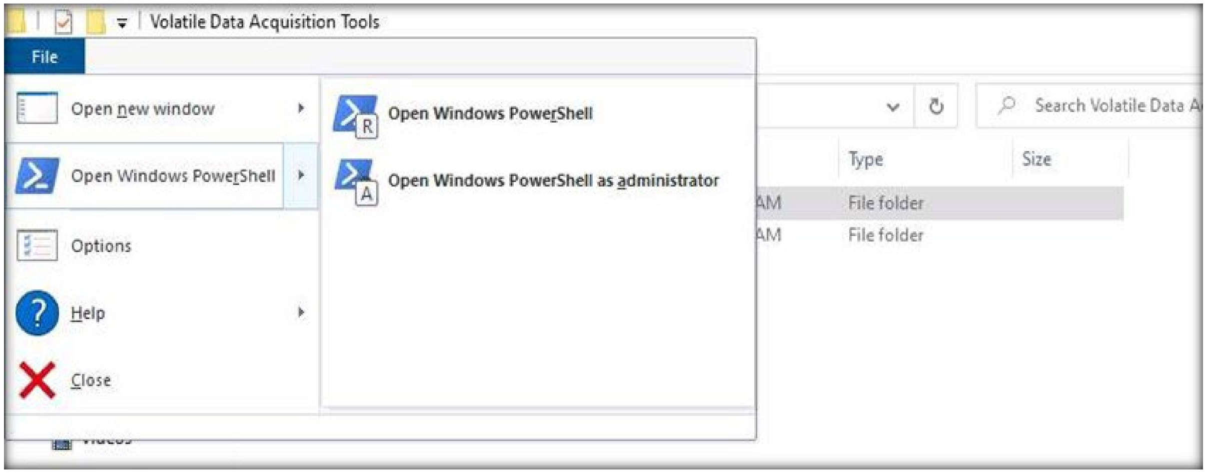
Note: The net sessions command can be run only on Admin Machine-1 machine.



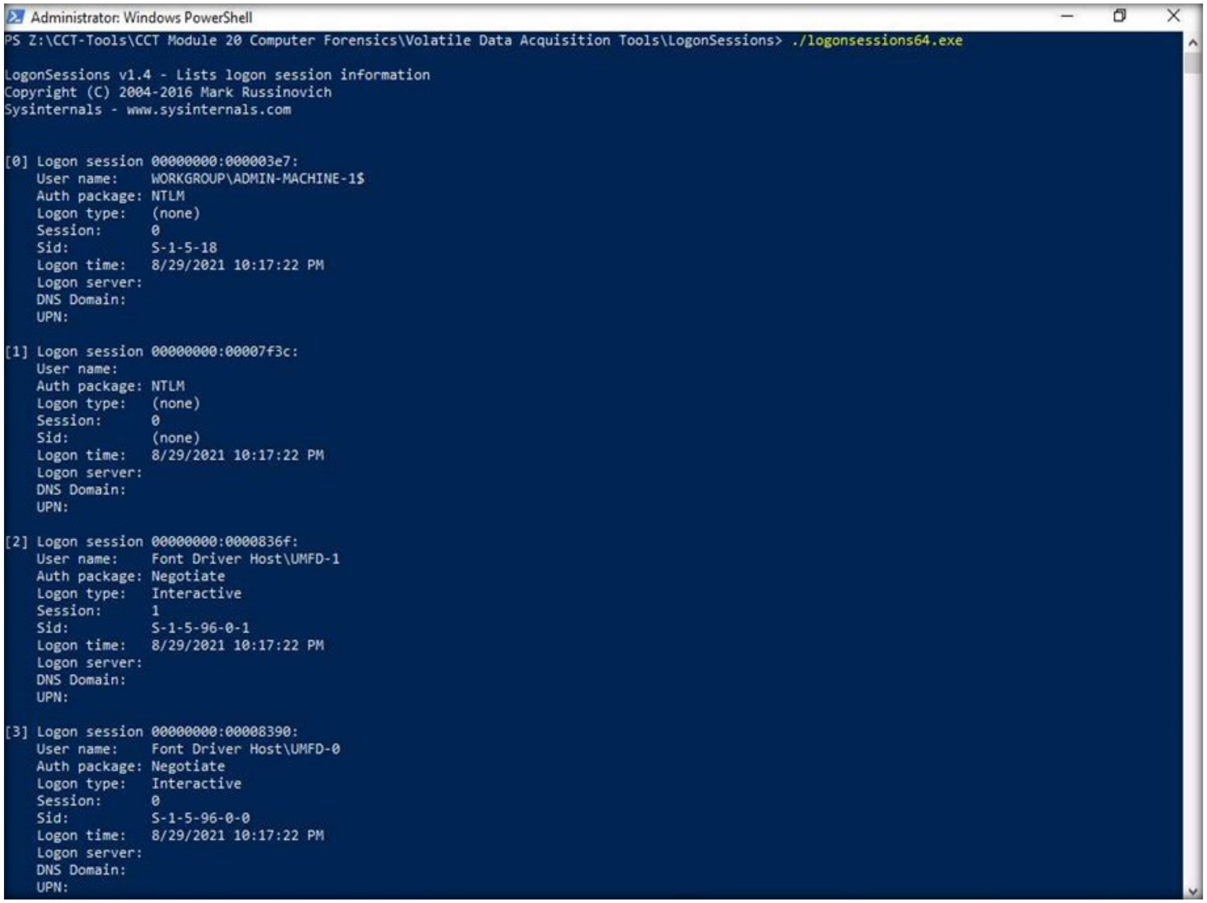
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> net sessions

Computer               User name            Client Type       Opens Idle time

-------------------------------------------------------------------------------
\\[fe80::6d6b:f245:3...Admin                                      2 00:02:45
The command completed successfully.

PS C:\WINDOWS\system32> _
```

12. Navigate to Z:\CCT-Tools\CTT Module 20 Computer Forensics\Volatile Data Acquisition Tools, select the LogonSessions folder, and press Alt, F, S, A keys on the keyboard one after the other, to open PowerShell window with Administrator privileges.

Note: If a User Account Control pop-up appears, click Yes.

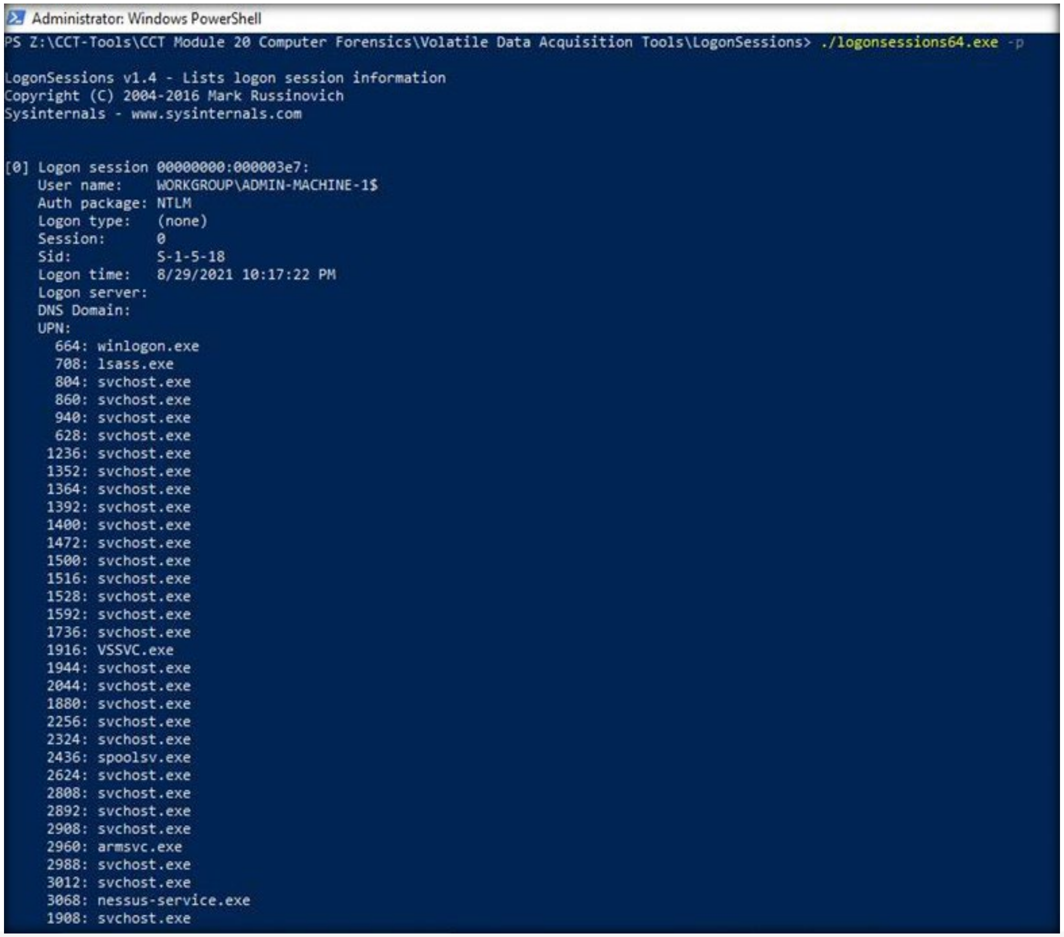


13. The above operation will launch PowerShell with the path of LogonSessions. Type ./logonsessions64.exe and press Enter.
14. The LogonSessions License Agreement window will appear. Click Agree to continue.
15. The utility will now list the currently active logon sessions.



```
PS Z:\CCT-Tools\CCT Module 20 Computer Forensics\Volatile Data Acquisition Tools\LogonSessions> ./logonsessions64.exe

LogonSessions v1.4 - Lists logon session information
Copyright (C) 2004-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
    User name:    WORKGROUP\ADMIN-MACHINE-1$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   8/29/2021 10:17:22 PM
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:00007f3c:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          (none)
    Logon time:   8/29/2021 10:17:22 PM
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:0000836f:
    User name:    Font Driver Host\UMFD-1
    Auth package: Negotiate
    Logon type:   Interactive
    Session:      1
    Sid:          S-1-5-96-0-1
    Logon time:   8/29/2021 10:17:22 PM
    Logon server:
    DNS Domain:
    UPN:

[3] Logon session 00000000:00008390:
    User name:    Font Driver Host\UMFD-0
    Auth package: Negotiate
    Logon type:   Interactive
    Session:      0
    Sid:          S-1-5-96-0-0
    Logon time:   8/29/2021 10:17:22 PM
    Logon server:
    DNS Domain:
    UPN:
```

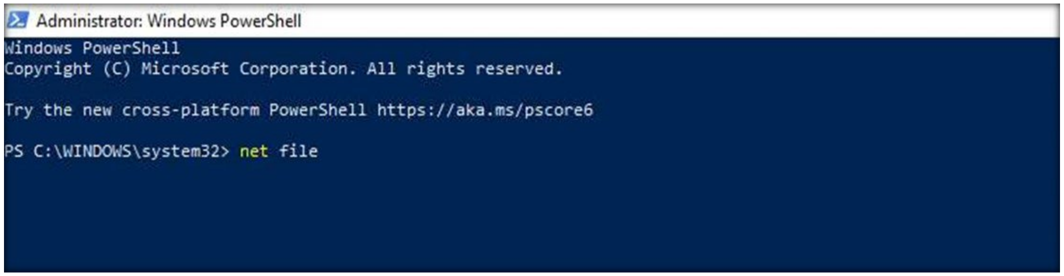
16. To list the logon sessions, their types, and the processes running under them, use the -p switch in combination with ./logonsessions64.exe. All the running processes associated with each session will be displayed under the UPN section as shown in the screenshot below.



```
PS Z:\CCT-Tools\CCT Module 20 Computer Forensics\Volatile Data Acquisition Tools\LogonSessions> ./logonsessions64.exe -p

LogonSessions v1.4 - Lists logon session information
Copyright (C) 2004-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


[0] Logon session 00000000:000003e7:
    User name:    WORKGROUP\ADMIN-MACHINE-1$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   8/29/2021 10:17:22 PM
    Logon server:
    DNS Domain:
    UPN:
      664: winlogon.exe
      708: lsass.exe
      804: svchost.exe
      860: svchost.exe
      940: svchost.exe
      628: svchost.exe
     1236: svchost.exe
     1352: svchost.exe
     1364: svchost.exe
     1392: svchost.exe
     1400: svchost.exe
     1472: svchost.exe
     1500: svchost.exe
     1516: svchost.exe
     1528: svchost.exe
     1592: svchost.exe
     1736: svchost.exe
     1916: VSSVC.exe
     1944: svchost.exe
     2044: svchost.exe
     1880: svchost.exe
     2256: svchost.exe
     2324: svchost.exe
     2436: spoolsv.exe
     2624: svchost.exe
     2808: svchost.exe
     2892: svchost.exe
     2908: svchost.exe
     2960: armsvc.exe
     2988: svchost.exe
     3012: svchost.exe
     3068: nessus-service.exe
     1908: svchost.exe
```

17. Close the PowerShell.
18. Now, we will use the net file utility to retrieve information pertaining to all the open shared files with respect to Admin Machine-1 virtual machine.
19. To run the net file command, launch it by right clicking the Start button and then clicking Windows PowerShell (Admin). In the PowerShell window, type net file and press Enter.

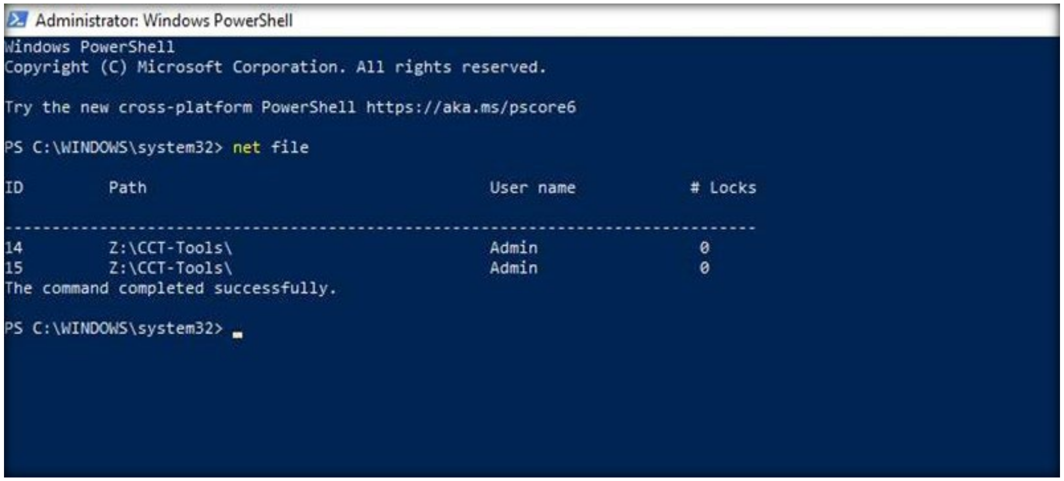
Note: If a User Account Control pop-up appears, click Yes.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> net file
```

20. The net file command will now display the Path of the shared folder from the local machine which is accessed by other machines (here, AD Domain Controller machine); it also displays the Username of the user account that is remotely accessing the shared folder along with the ID and Locks that are associated with the shared folder as shown in the screenshot below.

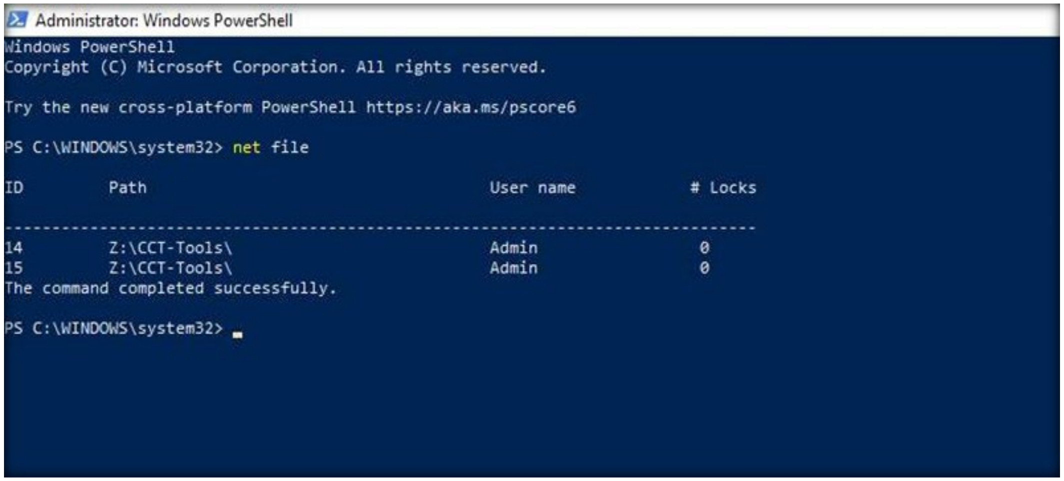
EXERCISE 3: ACQUIRE VOLATILE INFORMATION FROM A LIVE WINDOWS SYSTEM



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> net file

ID         Path                                    User name            # Locks

-------------------------------------------------------------------------------
14         Z:\CCT-Tools\                           Admin                0
15         Z:\CCT-Tools\                           Admin                0
The command completed successfully.

PS C:\WINDOWS\system32> _
```

Note: The output of the command shown in the screenshot below, might vary in your lab environment.

21. This concludes the demonstration showing how to acquire volatile information from a live Windows machine.
22. Close all open windows.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> net file

ID         Path                                    User name            # Locks

-------------------------------------------------------------------------------
14         Z:\CCT-Tools\                           Admin                0
15         Z:\CCT-Tools\                           Admin                0
The command completed successfully.

PS C:\WINDOWS\system32> _
```

EXERCISE 4: **ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY**

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other such digital forensics tools.

LAB SCENARIO

An inspector, who is probing a murder incident, has found a dead system in a crime scene and suspects that the system is related to the incident and could provide clues about it. When the inspector brings the system to the cyber forensics department, he/she creates an image of the hard disk and begins to analyze the image using Autopsy. On further analysis of the file systems, the investigator finds some crucial evidence that might help in solving the case.

In order to investigate a hard disk, as an investigator, you must know the types of file systems and how to analyze them using various tools.

OBJECTIVE

The objective of this lab is to learn and perform file system analysis using Autopsy. Performing file system analysis allows an investigator to determine the following information:

- File system type
- Metadata information
- Content information

OVERVIEW OF THE LAB

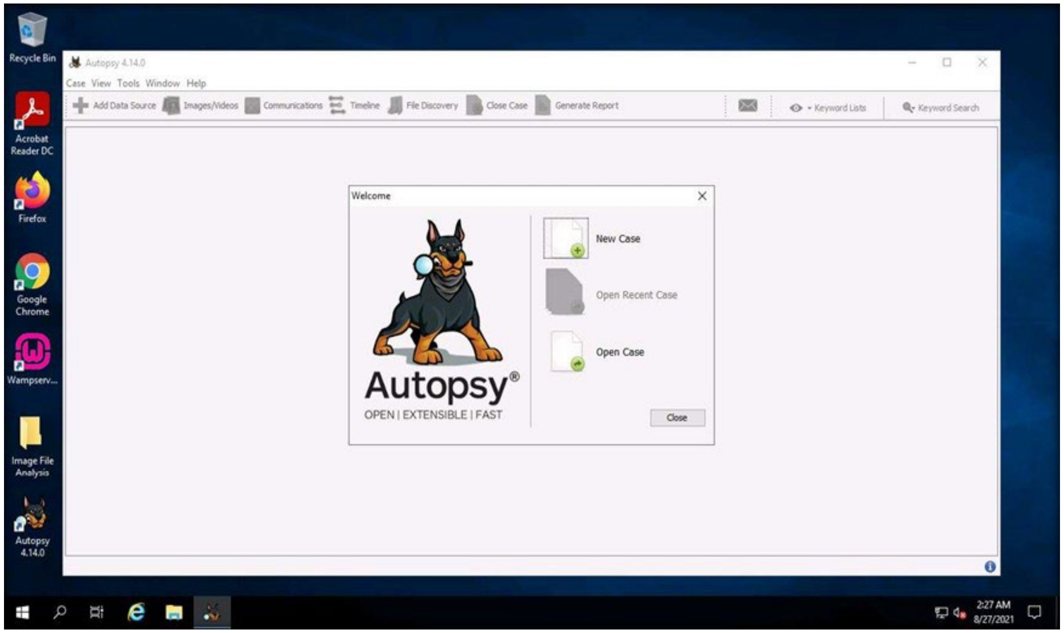
Forensics analysis tools help investigators in collecting, managing, transferring, and storing necessary information required during forensics investigation. Using these tools, an investigator can act quickly when investigating a security incident.

This lab familiarizes you with file system analysis using Autopsy. It helps you understand how to create a case in Autopsy and then examine the file system using the application.

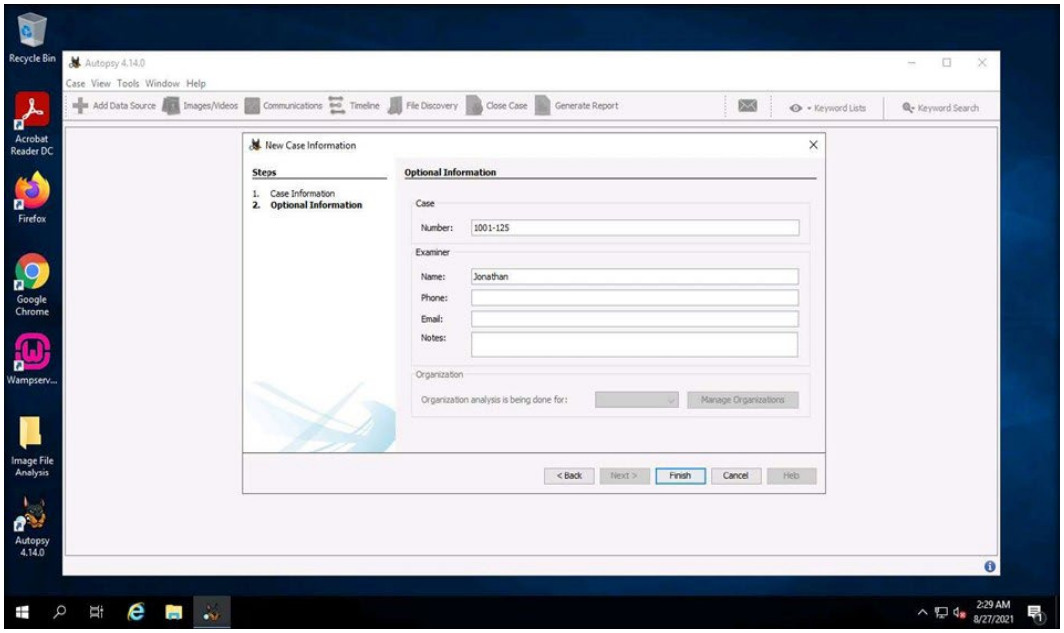
EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY

Note: Ensure that PfSense Firewall and Admin Machine-1 and AD Domain Controller virtual machines are running.

1. In this lab, we will be using Autopsy tool to examine the filesystem of a Linux image.
2. In the AD Domain Controller virtual machine, double-click the Autopsy 4.14.0 shortcut icon on the Desktop.
3. Autopsy Welcome window will appear along with Autopsy main window in the background. In the Welcome window, click New Case.



4. A New Case Information window opens asking you to input the base Case Name and the Base Directory. The base directory is the location where the case data will get stored. The case name may be entered according to your identification purpose. In this lab, we are assigning the case name as Linux_Analysis.
5. Before specifying the base directory, we will be creating a folder on the Desktop with the name Image File Analysis and setting the path of the Base directory to this folder.
6. Upon setting the base directory, click Next.
7. The New Case Information window now shows the Optional Information section where you can specify details such as name of the examiner and case number. For this lab, let us enter the name of the examiner as Jonathan and the case number as 1001-125. You may also fill out the other optional fields. Click Finish after entering the details for optional fields.



New Case Information

Steps
1. Case Information
2. Optional Information

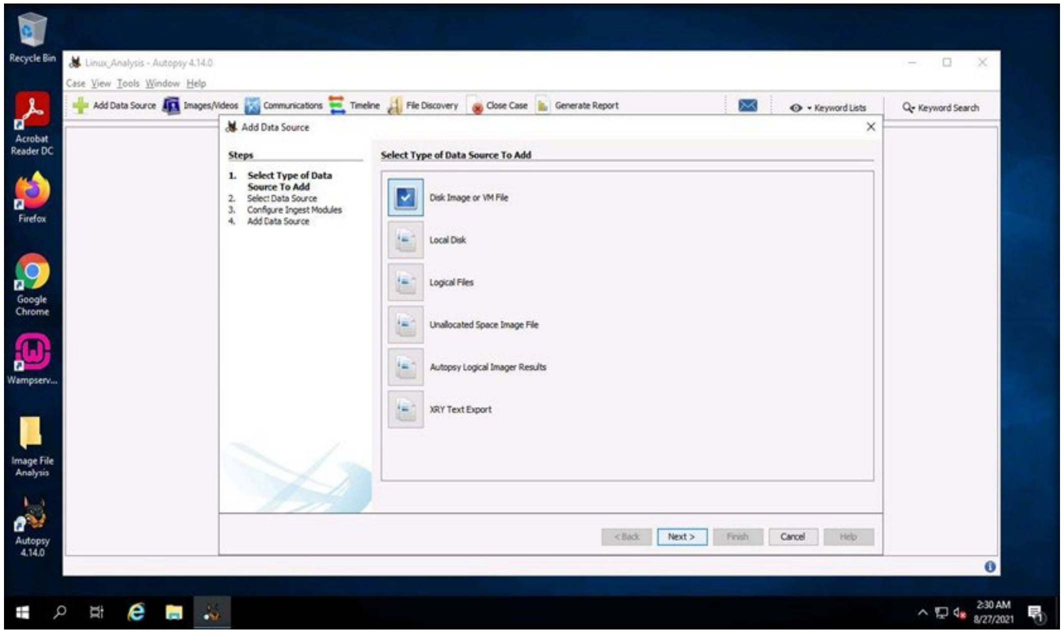
Optional Information

Case
Number: 1001-125

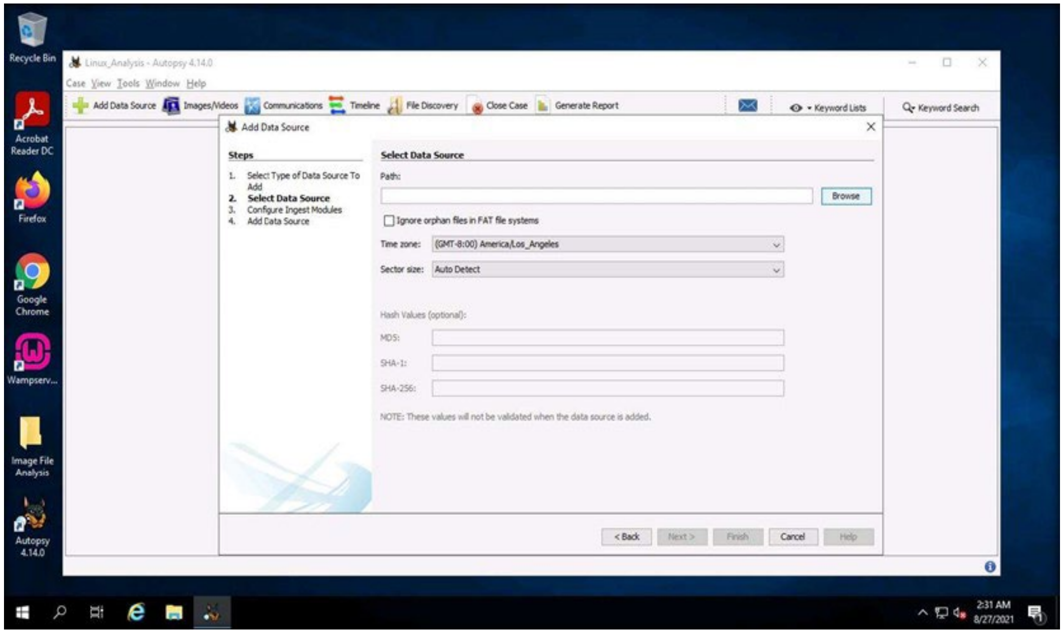
Examiner
Name: Jonathan
Phone:
Email:
Notes:

Organization
Organization analysis is being done for:

8. The Add Data Source window now appears displaying the section Select Type of Data Source To Add. Here, you need to select the type of data source to be provided as an input. In this lab, we will be analyzing a disk image; therefore, select the option Disk Image or VM File and click Next.



9. The Add Data Source window now displays the section Select Data Source where you need to select the location of the Image that you are going to examine. Click Browse.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path:

Browse

□ Ignore orphan files in FAT file systems

Time zone: (GMT-8:00) America/Los_Angeles

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

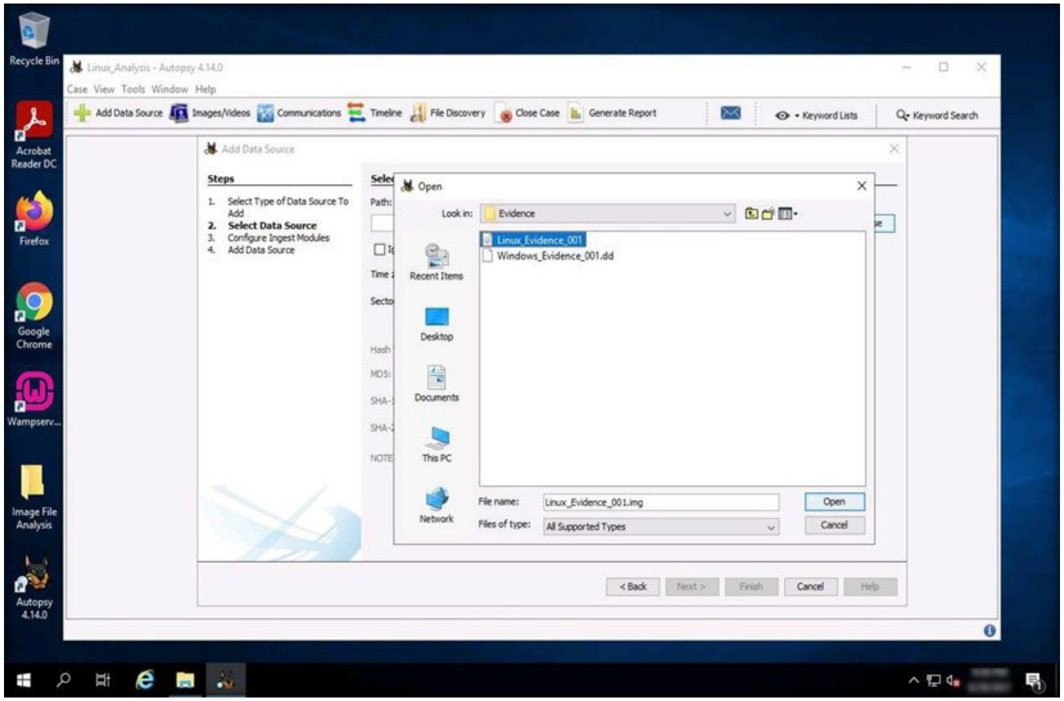
SHA-256:

NOTE: These values will not be validated when the data source is added.

< Back   Next >   Finish   Cancel   Help

EXERCISE 4:
ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY

10. An Open window will appear where you need to specify the forensic image. Navigate to Z:\CCT Module 20 Computer Forensics\Evidence, select Linux_Evidence_001.img and click Open.



Linux_Analysis - Autopsy 4.14.0

Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Open

Look in: Evidence

Linux_Evidence_001

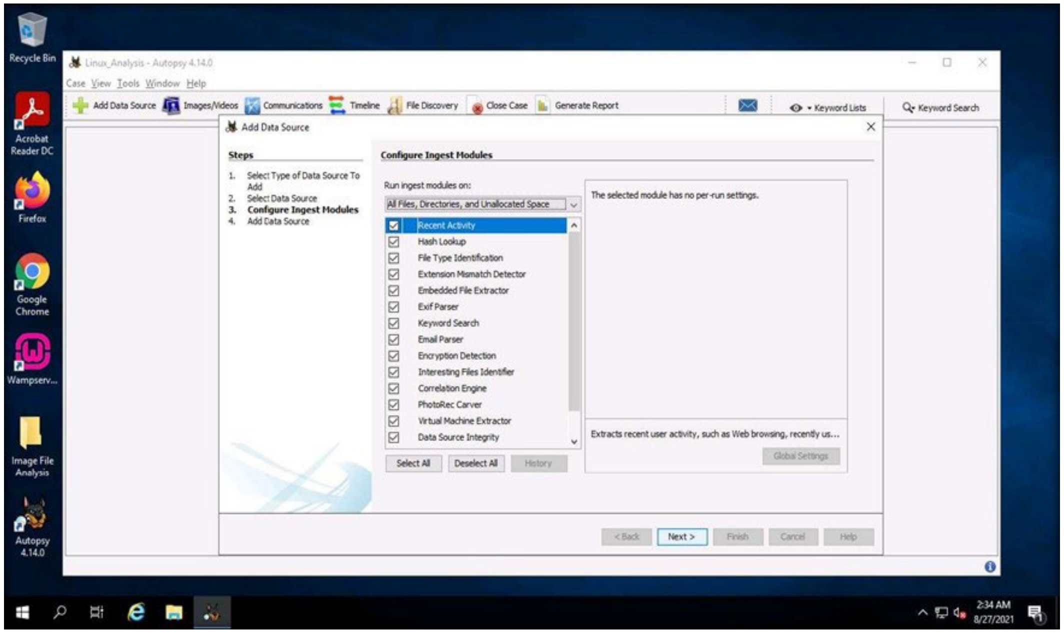
Windows_Evidence_001.dd

File name: Linux_Evidence_001.img

Files of type: All Supported Types

11. Once you set the path of the image file, click Next.
12. The Add Data Source window now displays the Configure Ingest Modules section, which contains lists of options that are checked. Select the options according to your requirement and click Next.

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY



Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

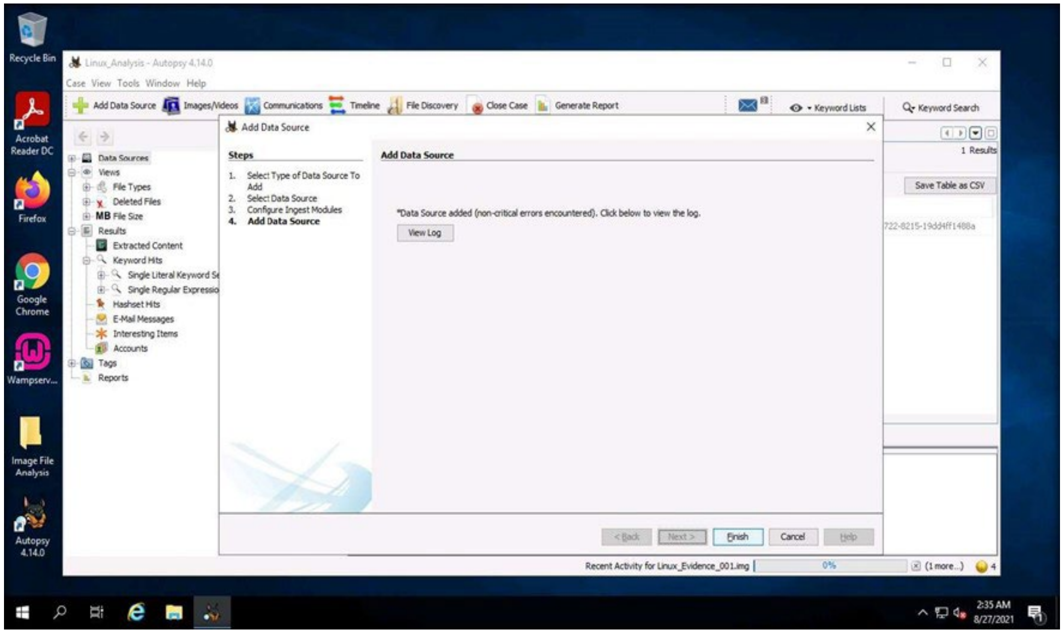
- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Correlation Engine
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor
- ☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

13. The Add Data Source window now displays the Add Data Source section, stating that the data source is successfully added. Click Finish.

Note: Autopsy will take some time to completely analyze the evidence file. You can proceed to the next steps of this lab even when the analysis of the evidence file is still in progress.



Add Data Source

Steps

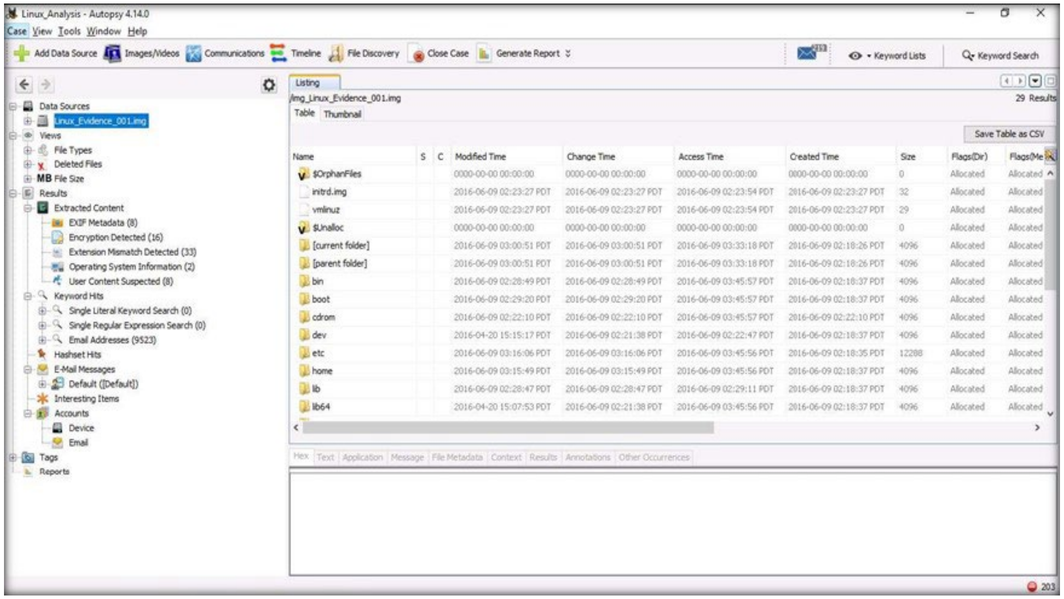
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

*Data Source added (non-critical errors encountered). Click below to view the log.

View Log

14. The application now displays the result in the Autopsy main window. Expand the Data Sources node in the left pane and click on the image file i.e., Linux_Evidence_001.img. This will show the contents of the image file, as shown in the following screenshot:

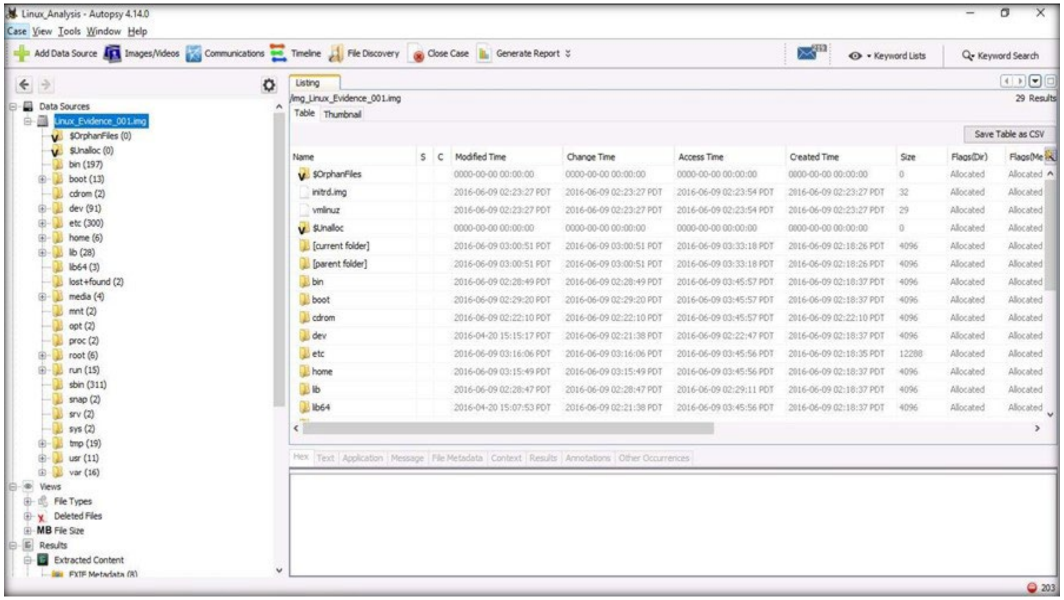


/img_Linux_Evidence_001.img

29 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Me
$OrphanFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
initrd.img			2016-06-09 02:23:27 PDT	2016-06-09 02:23:27 PDT	2016-06-09 02:23:54 PDT	2016-06-09 02:23:27 PDT	32	Allocated	Allocated
vmlinuz			2016-06-09 02:23:27 PDT	2016-06-09 02:23:27 PDT	2016-06-09 02:23:54 PDT	2016-06-09 02:23:27 PDT	29	Allocated	Allocated
$Unalloc			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
[current folder]			2016-06-09 03:00:51 PDT	2016-06-09 03:00:51 PDT	2016-06-09 03:33:18 PDT	2016-06-09 02:18:26 PDT	4096	Allocated	Allocated
[parent folder]			2016-06-09 03:00:51 PDT	2016-06-09 03:00:51 PDT	2016-06-09 03:33:18 PDT	2016-06-09 02:18:26 PDT	4096	Allocated	Allocated
bin			2016-06-09 02:28:49 PDT	2016-06-09 02:28:49 PDT	2016-06-09 03:45:57 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
boot			2016-06-09 02:29:20 PDT	2016-06-09 02:29:20 PDT	2016-06-09 03:45:57 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
cdrom			2016-06-09 02:22:10 PDT	2016-06-09 02:22:10 PDT	2016-06-09 03:45:57 PDT	2016-06-09 02:22:10 PDT	4096	Allocated	Allocated
dev			2016-04-20 15:15:17 PDT	2016-06-09 02:21:38 PDT	2016-06-09 02:22:47 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
etc			2016-06-09 03:16:06 PDT	2016-06-09 03:16:06 PDT	2016-06-09 03:45:56 PDT	2016-06-09 02:18:35 PDT	12288	Allocated	Allocated
home			2016-06-09 03:15:49 PDT	2016-06-09 03:15:49 PDT	2016-06-09 03:45:56 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
lib			2016-06-09 02:28:47 PDT	2016-06-09 02:28:47 PDT	2016-06-09 02:29:11 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
lib64			2016-04-20 15:07:53 PDT	2016-06-09 02:21:38 PDT	2016-06-09 03:45:56 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated

15. Expand the image file Linux_Evidence_001.img to see its contents. Upon expanding the image, Autopsy displays the filesystem of the Linux image as shown in the following screenshot:

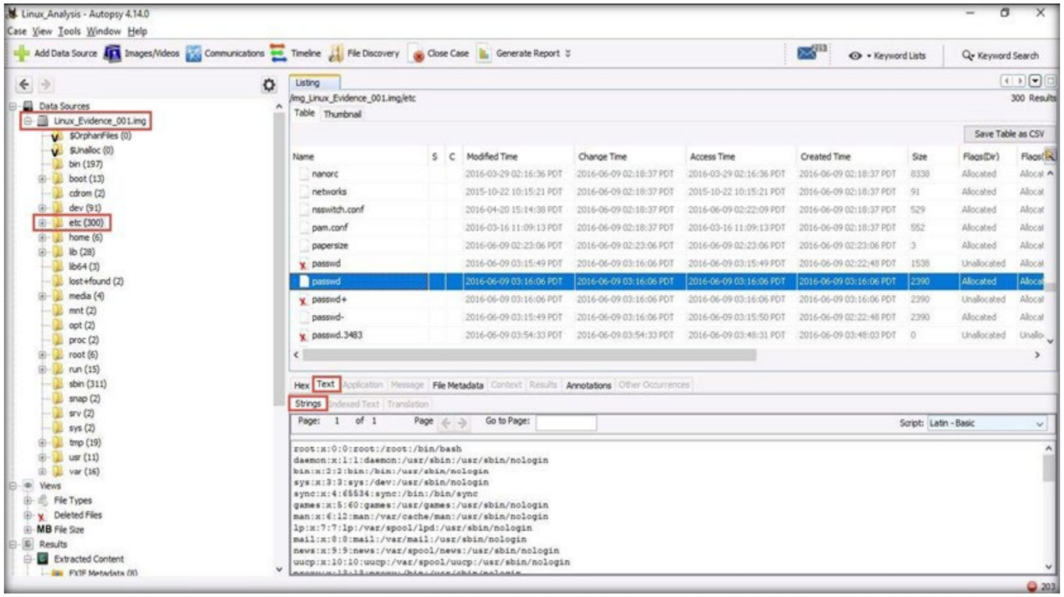


/img_Linux_Evidence_001.img

29 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Me
$OrphanFiles			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
initrd.img			2016-06-09 02:23:27 PDT	2016-06-09 02:23:27 PDT	2016-06-09 02:23:54 PDT	2016-06-09 02:23:27 PDT	32	Allocated	Allocated
vmlinuz			2016-06-09 02:23:27 PDT	2016-06-09 02:23:27 PDT	2016-06-09 02:23:54 PDT	2016-06-09 02:23:27 PDT	29	Allocated	Allocated
$Unalloc			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated
[current folder]			2016-06-09 03:00:51 PDT	2016-06-09 03:00:51 PDT	2016-06-09 03:33:18 PDT	2016-06-09 02:18:26 PDT	4096	Allocated	Allocated
[parent folder]			2016-06-09 03:00:51 PDT	2016-06-09 03:00:51 PDT	2016-06-09 03:33:18 PDT	2016-06-09 02:18:26 PDT	4096	Allocated	Allocated
bin			2016-06-09 02:28:49 PDT	2016-06-09 02:28:49 PDT	2016-06-09 03:45:57 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
boot			2016-06-09 02:29:20 PDT	2016-06-09 02:29:20 PDT	2016-06-09 03:45:57 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
cdrom			2016-06-09 02:22:10 PDT	2016-06-09 02:22:10 PDT	2016-06-09 03:45:57 PDT	2016-06-09 02:22:10 PDT	4096	Allocated	Allocated
dev			2016-04-20 15:15:17 PDT	2016-06-09 02:21:38 PDT	2016-06-09 02:22:47 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
etc			2016-06-09 03:16:06 PDT	2016-06-09 03:16:06 PDT	2016-06-09 03:45:56 PDT	2016-06-09 02:18:35 PDT	12288	Allocated	Allocated
home			2016-06-09 03:15:49 PDT	2016-06-09 03:15:49 PDT	2016-06-09 03:45:56 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
lib			2016-06-09 02:28:47 PDT	2016-06-09 02:28:47 PDT	2016-06-09 02:29:11 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated
lib64			2016-04-20 15:07:53 PDT	2016-06-09 02:21:38 PDT	2016-06-09 03:45:56 PDT	2016-06-09 02:18:37 PDT	4096	Allocated	Allocated

16. You may examine all the required files stored in the image as a part of filesystem analysis. In this lab, we are going to view the passwd file that is stored in \etc location. Therefore, select the etc folder from the left pane.
17. Upon selecting the folder, all the files and folders present in etc are displayed in the right pane of the window.
18. Scroll down the window and select the passwd file.
19. Click the Text tab.
20. Autopsy displays all the text (user account information) present in the passwd file, under the Strings tab, as shown in the following screenshot:

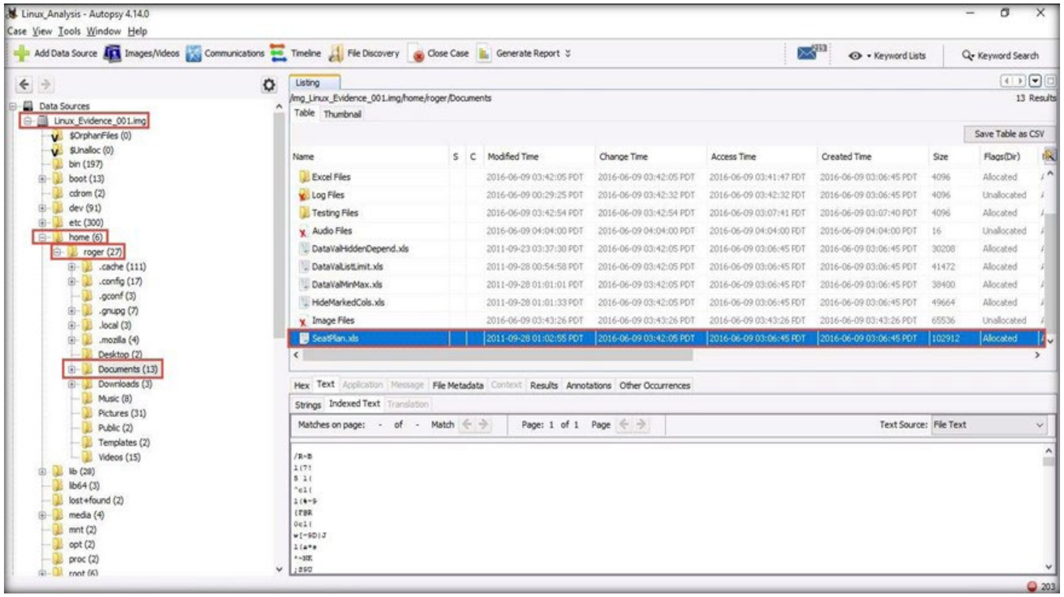


Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(
nanorc			2016-03-29 02:16:36 PDT	2016-06-09 02:18:37 PDT	2016-03-29 02:16:36 PDT	2016-06-09 02:18:37 PDT	8338	Allocated	Allocat
networks			2015-10-22 10:15:21 PDT	2016-06-09 02:18:37 PDT	2015-10-22 10:15:21 PDT	2016-06-09 02:18:37 PDT	91	Allocated	Allocat
nsswitch.conf			2016-04-20 15:14:38 PDT	2016-06-09 02:18:37 PDT	2016-06-09 02:22:09 PDT	2016-06-09 02:18:37 PDT	529	Allocated	Allocat
pam.conf			2016-03-16 11:09:13 PDT	2016-06-09 02:18:37 PDT	2016-03-16 11:09:13 PDT	2016-06-09 02:18:37 PDT	552	Allocated	Allocat
papersize			2016-06-09 02:23:06 PDT	2016-06-09 02:23:06 PDT	2016-06-09 02:23:06 PDT	2016-06-09 02:23:06 PDT	3	Allocated	Allocat
passwd			2016-06-09 03:15:49 PDT	2016-06-09 03:16:06 PDT	2016-06-09 03:15:49 PDT	2016-06-09 02:22:48 PDT	1538	Unallocated	Allocat
passwd			2016-06-09 03:16:06 PDT	2016-06-09 03:16:06 PDT	2016-06-09 03:16:06 PDT	2016-06-09 03:16:06 PDT	2390	Allocated	Allocat
passwd+			2016-06-09 03:16:06 PDT	2016-06-09 03:16:06 PDT	2016-06-09 03:16:06 PDT	2016-06-09 03:16:06 PDT	2390	Unallocated	Allocat
passwd-			2016-06-09 03:15:49 PDT	2016-06-09 03:16:06 PDT	2016-06-09 03:15:50 PDT	2016-06-09 02:22:48 PDT	2390	Allocated	Allocat
passwd.3483			2016-06-09 03:54:33 PDT	2016-06-09 03:54:33 PDT	2016-06-09 03:48:31 PDT	2016-06-09 03:48:03 PDT	0	Unallocated	Unallo

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

21. Similarly, click on the File Metadata, Hex, and Annotations tabs to view other details pertaining to the selected file.
22. This way, you can analyze all the other files and folders of your choice to get detailed information on them.
23. Apart from examining the file system, you can also calculate the hashes of the files that you examine, which helps in validating the integrity of the evidence. In this lab, we will be calculating the MD5 hash of a file named SeatPlan.xls, which is located within /home/roger/Documents.
24. To view the MD5 hash value of this file, expand home → roger → Documents in the left pane. The SeatPlan.xls file appears in the right pane of the Autopsy window. Click the file.

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY

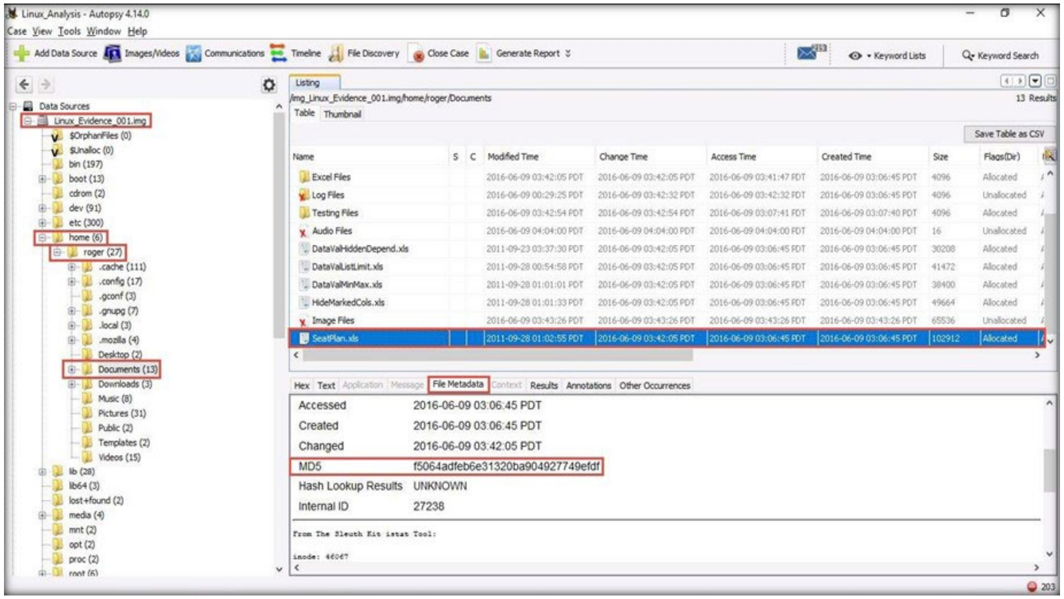


/img_Linux_Evidence_001.img/home/roger/Documents 13 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Excel Files			2016-06-09 03:42:05 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:41:47 PDT	2016-06-09 03:06:45 PDT	4096	Allocated
Log Files			2016-06-09 00:29:25 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:06:45 PDT	4096	Unallocated
Testing Files			2016-06-09 03:42:54 PDT	2016-06-09 03:42:54 PDT	2016-06-09 03:07:41 PDT	2016-06-09 03:07:40 PDT	4096	Allocated
Audio Files			2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	16	Unallocated
DataValHiddenDepend.xls			2011-09-23 03:37:30 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	30208	Allocated
DataValListLimit.xls			2011-09-28 00:54:58 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	41472	Allocated
DataValMinMax.xls			2011-09-28 01:01:01 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	38400	Allocated
HideMarkedCols.xls			2011-09-28 01:01:33 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	49664	Allocated
Image Files			2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	65536	Unallocated
SeatPlan.xls			2011-09-28 01:02:55 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	102912	Allocated

25. The File Metadata section displays the selected folder/file's metadata information such as the file's created, modified, and accessed times followed by its MD5 hash value.
26. Click on File Metadata and scroll down the section to find the MD5 value for the SeatPlan.xls file.

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY



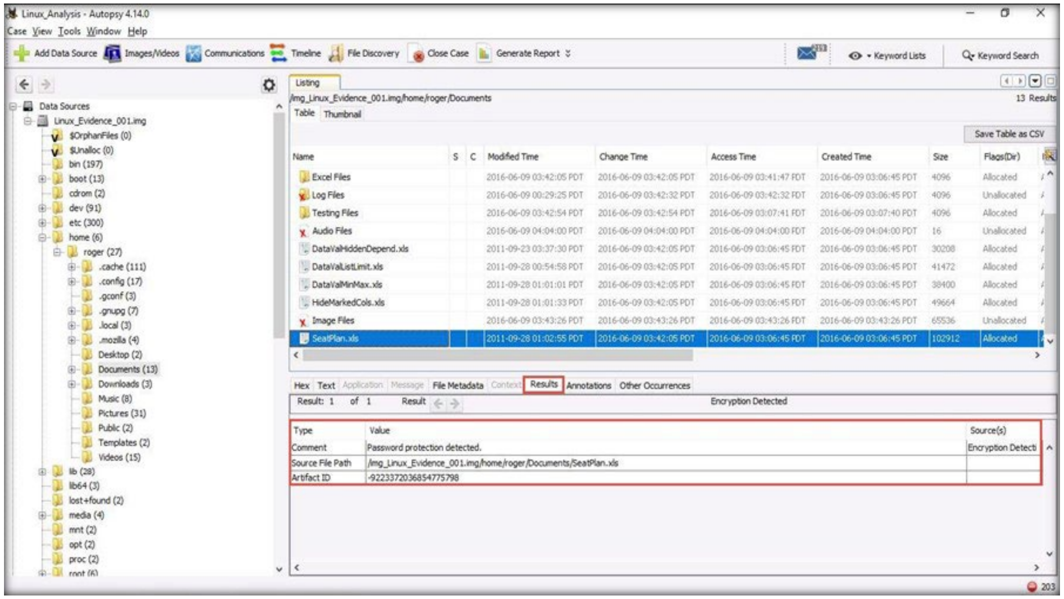
/img_Linux_Evidence_001.img/home/roger/Documents 13 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Excel Files			2016-06-09 03:42:05 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:41:47 PDT	2016-06-09 03:06:45 PDT	4096	Allocated
Log Files			2016-06-09 00:29:25 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:06:45 PDT	4096	Unallocated
Testing Files			2016-06-09 03:42:54 PDT	2016-06-09 03:42:54 PDT	2016-06-09 03:07:41 PDT	2016-06-09 03:07:40 PDT	4096	Allocated
Audio Files			2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	16	Unallocated
DataValHiddenDepend.xls			2011-09-23 03:37:30 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	30208	Allocated
DataValListLimit.xls			2011-09-28 00:54:58 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	41472	Allocated
DataValMinMax.xls			2011-09-28 01:01:01 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	38400	Allocated
HideMarkedCols.xls			2011-09-28 01:01:33 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	49664	Allocated
Image Files			2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	65536	Unallocated
SeatPlan.xls			2011-09-28 01:02:55 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	102912	Allocated

Accessed	2016-06-09 03:06:45 PDT
Created	2016-06-09 03:06:45 PDT
Changed	2016-06-09 03:42:05 PDT
MD5	f5064adfeb6e31320ba904927749efdf
Hash Lookup Results	UNKNOWN
Internal ID	27238

```
From The Sleuth Kit istat Tool:

inode: 46067
```

27. Click on Results tab and you can view information such as Source File Path, Artifact ID and it shows that the file is password protected.



/img_Linux_Evidence_001.img/home/roger/Documents

13 Results

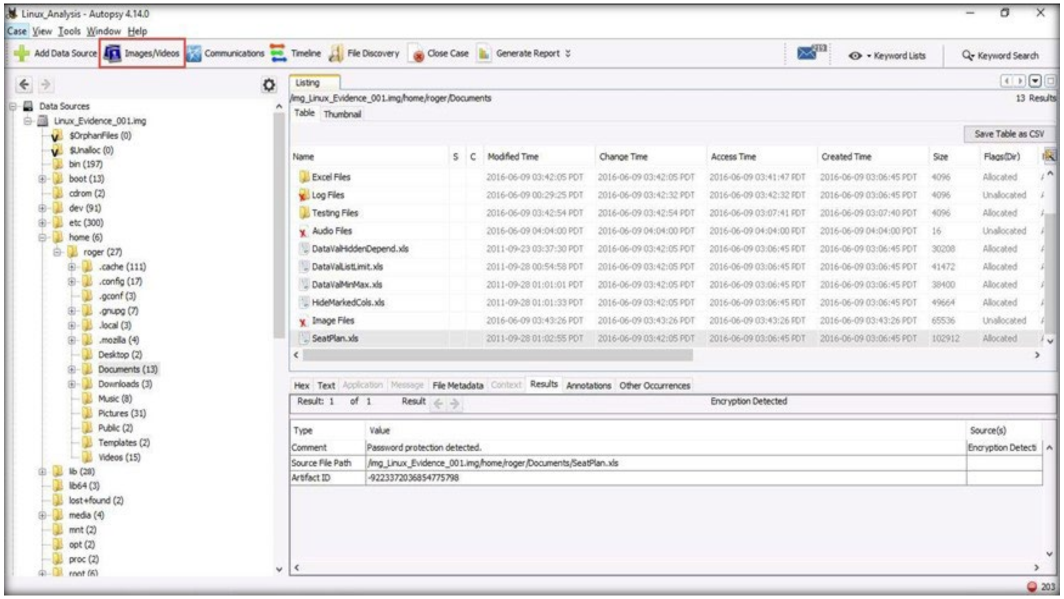
Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Excel Files			2016-06-09 03:42:05 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:41:47 PDT	2016-06-09 03:06:45 PDT	4096	Allocated
Log Files			2016-06-09 00:29:25 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:06:45 PDT	4096	Unallocated
Testing Files			2016-06-09 03:42:54 PDT	2016-06-09 03:42:54 PDT	2016-06-09 03:07:41 PDT	2016-06-09 03:07:40 PDT	4096	Allocated
Audio Files			2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	16	Unallocated
DataValHiddenDepend.xls			2011-09-23 03:37:30 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	30208	Allocated
DataValListLimit.xls			2011-09-28 00:54:58 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	41472	Allocated
DataValMinMax.xls			2011-09-28 01:01:01 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	38400	Allocated
HideMarkedCols.xls			2011-09-28 01:01:33 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	49664	Allocated
Image Files			2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	65536	Unallocated
SeatPlan.xls			2011-09-28 01:02:55 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	102912	Allocated

Result: 1 of 1 Result

Encryption Detected

Type	Value	Source(s)
Comment	Password protection detected.	Encryption Detecti
Source File Path	/img_Linux_Evidence_001.img/home/roger/Documents/SeatPlan.xls	
Artifact ID	-9223372036854775798	

28. Now, click on Images/Videos option from the toolbar to view all the images and videos present in the evidence file.



/img_Linux_Evidence_001.img/home/roger/Documents

13 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
Excel Files			2016-06-09 03:42:05 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:41:47 PDT	2016-06-09 03:06:45 PDT	4096	Allocated
Log Files			2016-06-09 00:29:25 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:06:45 PDT	4096	Unallocated
Testing Files			2016-06-09 03:42:54 PDT	2016-06-09 03:42:54 PDT	2016-06-09 03:07:41 PDT	2016-06-09 03:07:40 PDT	4096	Allocated
Audio Files			2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	16	Unallocated
DataValHiddenDepend.xls			2011-09-23 03:37:30 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	30208	Allocated
DataValListLimit.xls			2011-09-28 00:54:58 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	41472	Allocated
DataValMinMax.xls			2011-09-28 01:01:01 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	38400	Allocated
HideMarkedCols.xls			2011-09-28 01:01:33 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	49664	Allocated
Image Files			2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	65536	Unallocated
SeatPlan.xls			2011-09-28 01:02:55 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	102912	Allocated

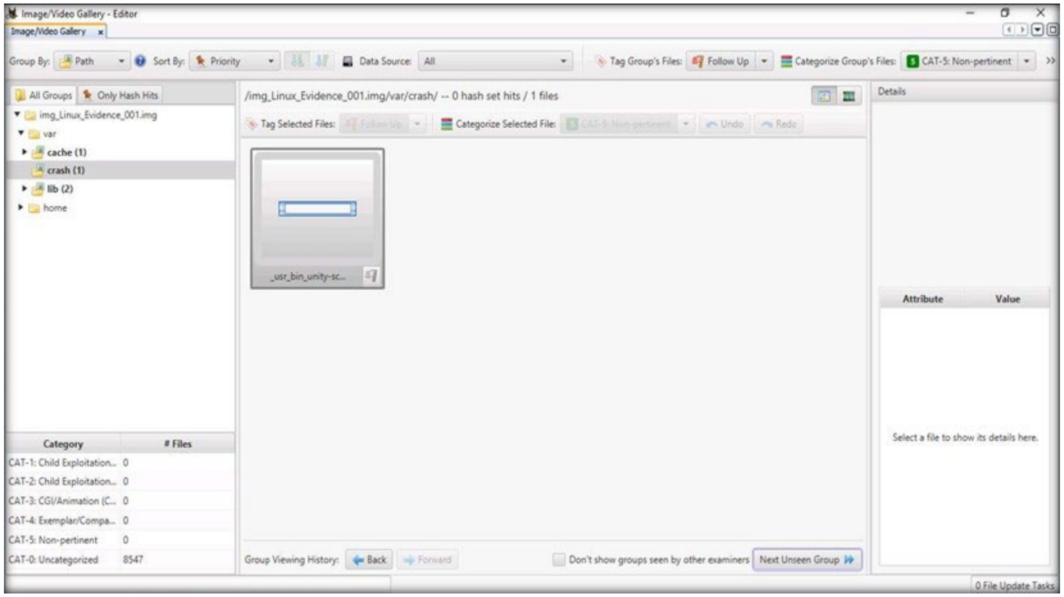
Result: 1 of 1 Result

Encryption Detected

Type	Value	Source(s)
Comment	Password protection detected.	Encryption Detecti
Source File Path	/img_Linux_Evidence_001.img/home/roger/Documents/SeatPlan.xls	
Artifact ID	-9223372036854775798	

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY

29. Image/Video Gallery - Editor window appears, maximize the window. It displays only image and video files.


Image/Video Gallery - Editor
Image/Video Gallery
Group By: Path
Sort By: Priority
Data Source: All
Tag Group's Files: Follow Up
Categorize Group's Files: CAT-5: Non-pertinent
All Groups
Only Hash Hits
img_Linux_Evidence_001.img
var
cache (1)
crash (1)
lib (2)
home
Tag Selected Files: Follow Up
Categorize Selected File: CAT-5: Non-pertinent
Undo
Redo
_usr_bin_unity-sc...
Details
Attribute
Value
Group Viewing History:
Back
Forward
Don't show groups seen by other examiners
Next Unseen Group
0 File Update Tasks

/img_Linux_Evidence_001.img/var/crash/ -- 0 hash set hits / 1 files

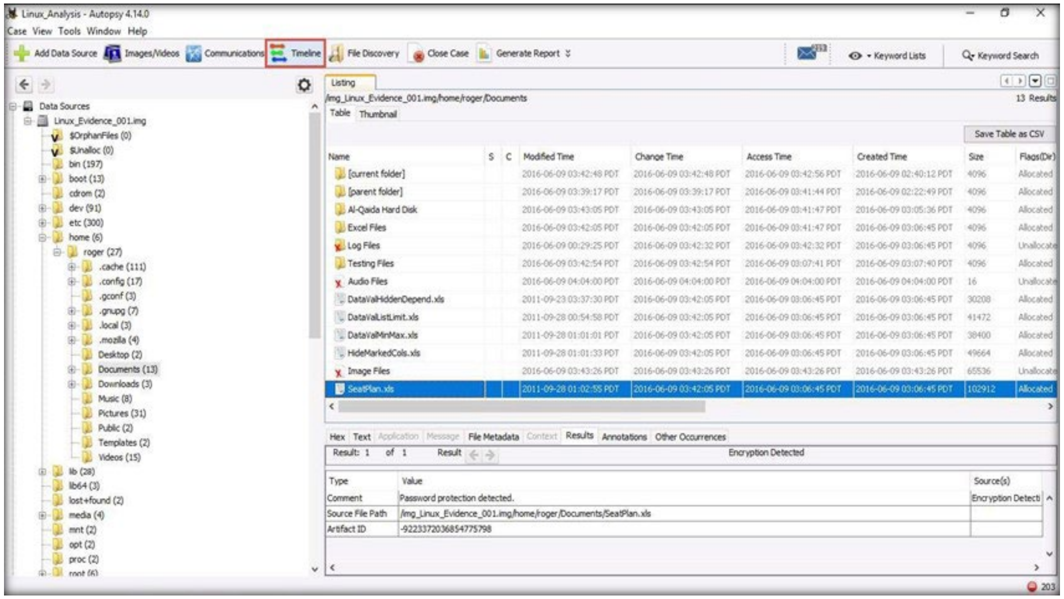
Category	# Files
CAT-1: Child Exploitation...	0
CAT-2: Child Exploitation...	0
CAT-3: CGI/Animation (C...	0
CAT-4: Exemplar/Compa...	0
CAT-5: Non-pertinent	0
CAT-0: Uncategorized	8547

Select a file to show its details here.

30. Close the Image/Video Gallery - Editor window to navigate back to Autopsy main window.

31. Now, click on Timeline from the menu bar.

EXERCISE 4:
ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY



/img_Linux_Evidence_001.img/home/roger/Documents

13 Results

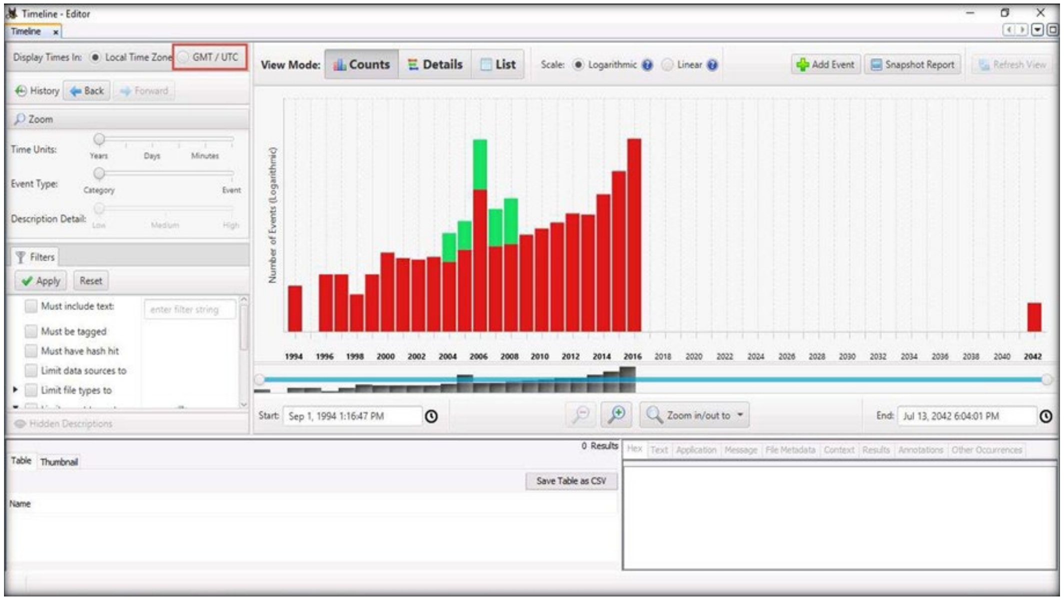
Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]			2016-06-09 03:42:48 PDT	2016-06-09 03:42:48 PDT	2016-06-09 03:42:56 PDT	2016-06-09 02:40:12 PDT	4096	Allocated
[parent folder]			2016-06-09 03:39:17 PDT	2016-06-09 03:39:17 PDT	2016-06-09 03:41:44 PDT	2016-06-09 02:22:49 PDT	4096	Allocated
Al-Qaida Hard Disk			2016-06-09 03:43:05 PDT	2016-06-09 03:43:05 PDT	2016-06-09 03:41:47 PDT	2016-06-09 03:05:36 PDT	4096	Allocated
Excel Files			2016-06-09 03:42:05 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:41:47 PDT	2016-06-09 03:06:45 PDT	4096	Allocated
Log Files			2016-06-09 00:29:25 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:06:45 PDT	4096	Unallocate
Testing Files			2016-06-09 03:42:54 PDT	2016-06-09 03:42:54 PDT	2016-06-09 03:07:41 PDT	2016-06-09 03:07:40 PDT	4096	Allocated
Audio Files			2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	16	Unallocate
DataValHiddenDepend.xls			2011-09-23 03:37:30 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	30208	Allocated
DataValListLimit.xls			2011-09-28 00:54:58 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	41472	Allocated
DataValMinMax.xls			2011-09-28 01:01:01 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	38400	Allocated
HideMarkedCols.xls			2011-09-28 01:01:33 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	49664	Allocated
Image Files			2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	65536	Unallocate
SeatPlan.xls			2011-09-28 01:02:55 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	102912	Allocated

Result: 1 of 1 Result Encryption Detected

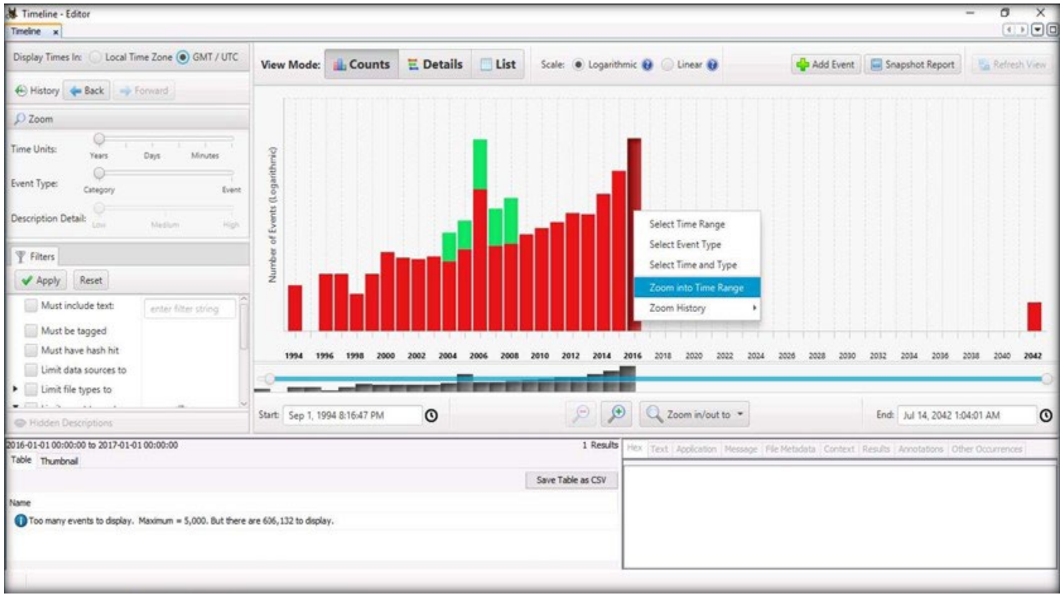
Type	Value	Source(s)
Comment	Password protection detected.	Encryption Detecti
Source File Path	/img_Linux_Evidence_001.img/home/roger/Documents/SeatPlan.xls	
Artifact ID	-9223372036854775798	

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY

32. The Timeline-Editor window opens, displaying a bar graph. Click on GMT/UTC radio button from the left pane under Display Times In section.



33. Now, right click on the longest bar (here 2016) and select Zoom into Time Range option from the context menu.



Display Times In: ○ Local Time Zone ● GMT / UTC

View Mode: Counts

Scale: ● Logarithmic ○ Linear

Start: Sep 1, 1994 8:16:47 PM

End: Jul 14, 2042 1:04:01 AM

2016-01-01 00:00:00 to 2017-01-01 00:00:00

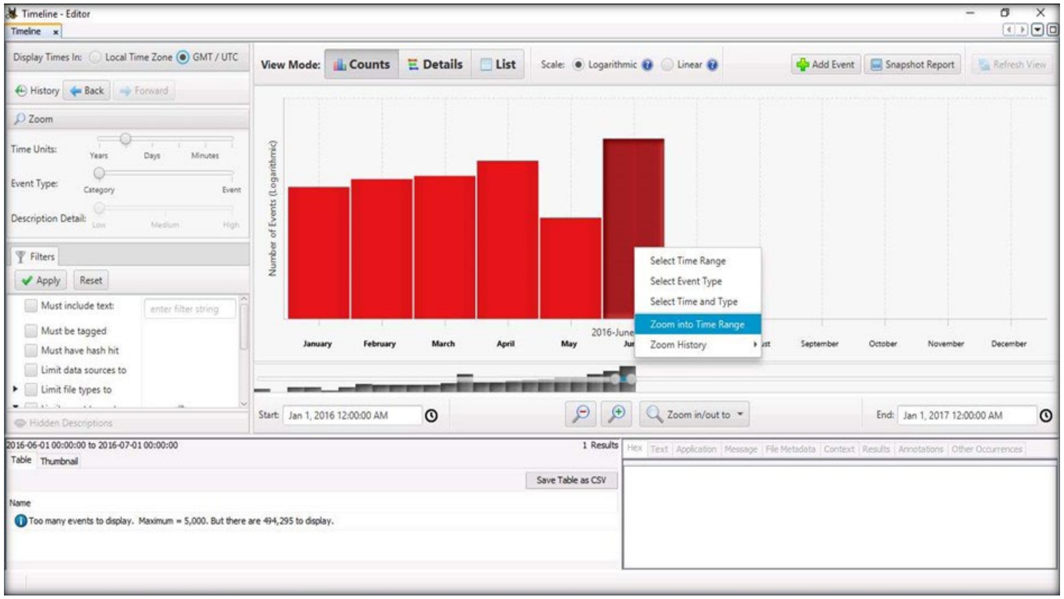
1 Results

Name

Too many events to display. Maximum = 5,000. But there are 606,132 to display.

34. vIn the next window, right click on a bar (here June) and click on Zoom into Time Range option from the context menu.

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY



Start: Jan 1, 2016 12:00:00 AM

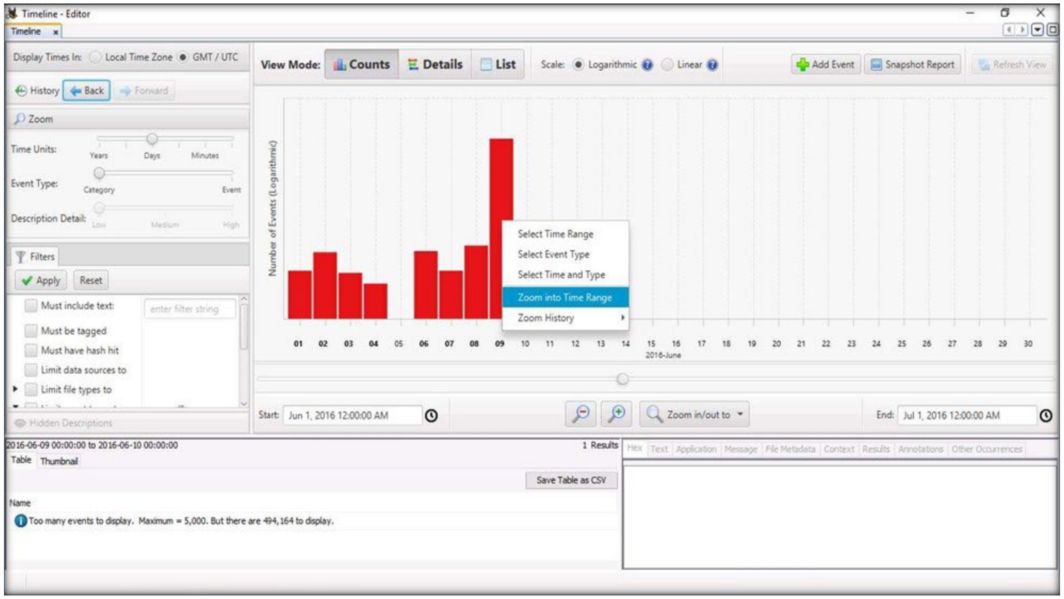
End: Jan 1, 2017 12:00:00 AM

2016-06-01 00:00:00 to 2016-07-01 00:00:00

1 Results

Too many events to display. Maximum = 5,000. But there are 494,295 to display.

35. In the next window, right click on a date (here 09) and click on Zoom into Time Range option from the context menu. In the following window, right click on a time interval (here 09) and select Zoom into Time Range option from the context menu.



Display Times In: ○ Local Time Zone ● GMT / UTC

Scale: ● Logarithmic ○ Linear

Start: Jun 1, 2016 12:00:00 AM

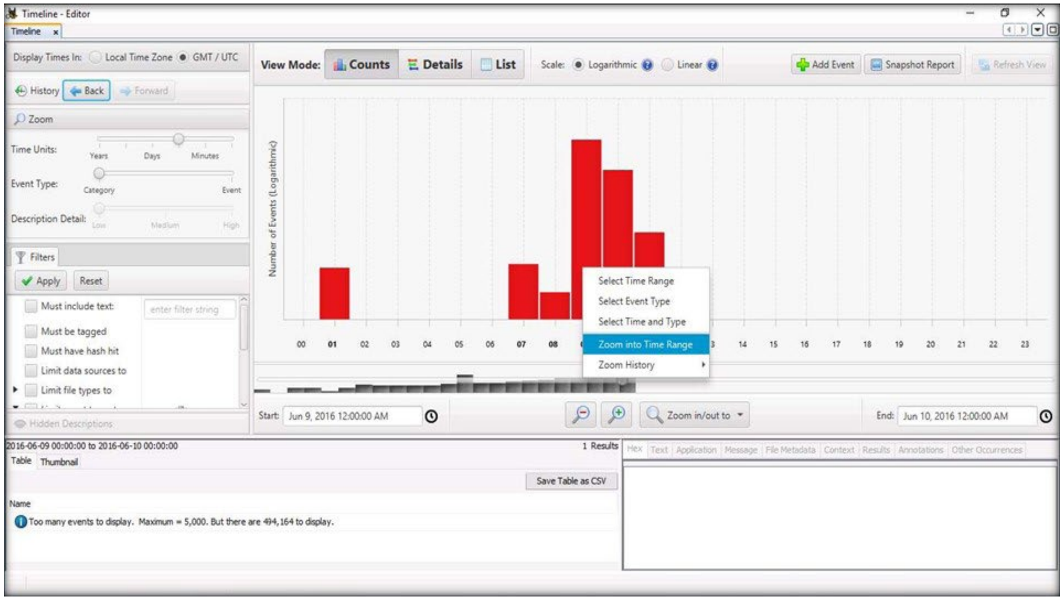
End: Jul 1, 2016 12:00:00 AM

2016-06-09 00:00:00 to 2016-06-10 00:00:00 1 Results

Name

Too many events to display. Maximum = 5,000. But there are 494,164 to display.

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY



Timeline - Editor

Display Times In: ○ Local Time Zone ● GMT / UTC

View Mode: Counts

Scale: ● Logarithmic ○ Linear

Start: Jun 9, 2016 12:00:00 AM

End: Jun 10, 2016 12:00:00 AM

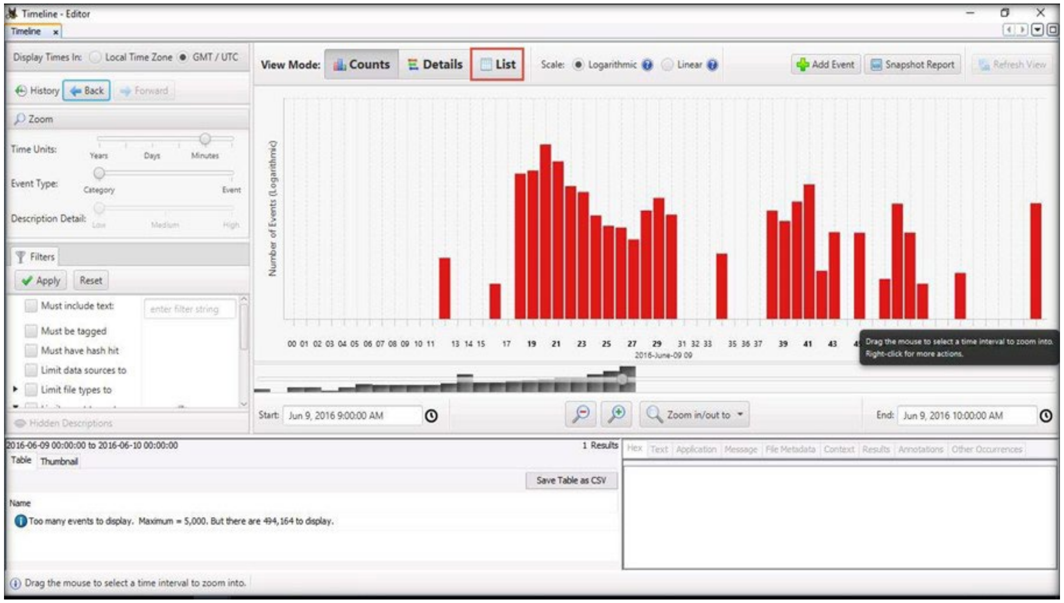
2016-06-09 00:00:00 to 2016-06-10 00:00:00

1 Results

Too many events to display. Maximum = 5,000. But there are 494,164 to display.

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY

36. Click on List from the View Mode options.



Display Times In: ○ Local Time Zone ● GMT / UTC

View Mode: Counts Details List

Scale: ● Logarithmic ○ Linear

Start: Jun 9, 2016 9:00:00 AM

End: Jun 9, 2016 10:00:00 AM

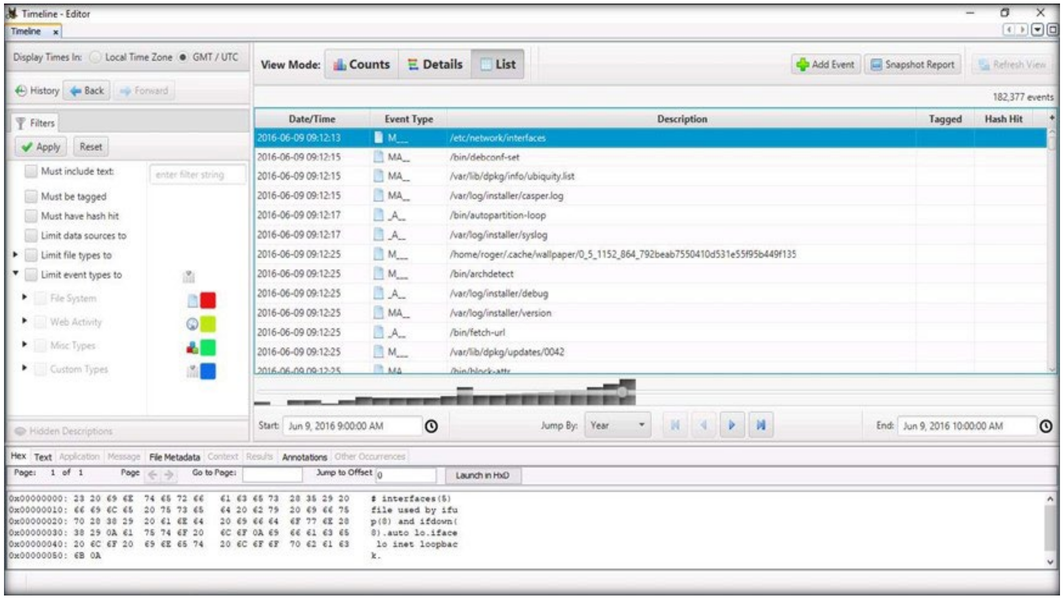
2016-06-09 00:00:00 to 2016-06-10 00:00:00 1 Results

Name

Too many events to display. Maximum = 5,000. But there are 494,164 to display.

Drag the mouse to select a time interval to zoom into.

37. The events will be listed in a time sequence; you can select any entry and click on Hex, Text, or File Metadata at the bottom of the window to view the Hex, Text or Metadata of the event.



Start: Jun 9, 2016 9:00:00 AM

Jump By: Year

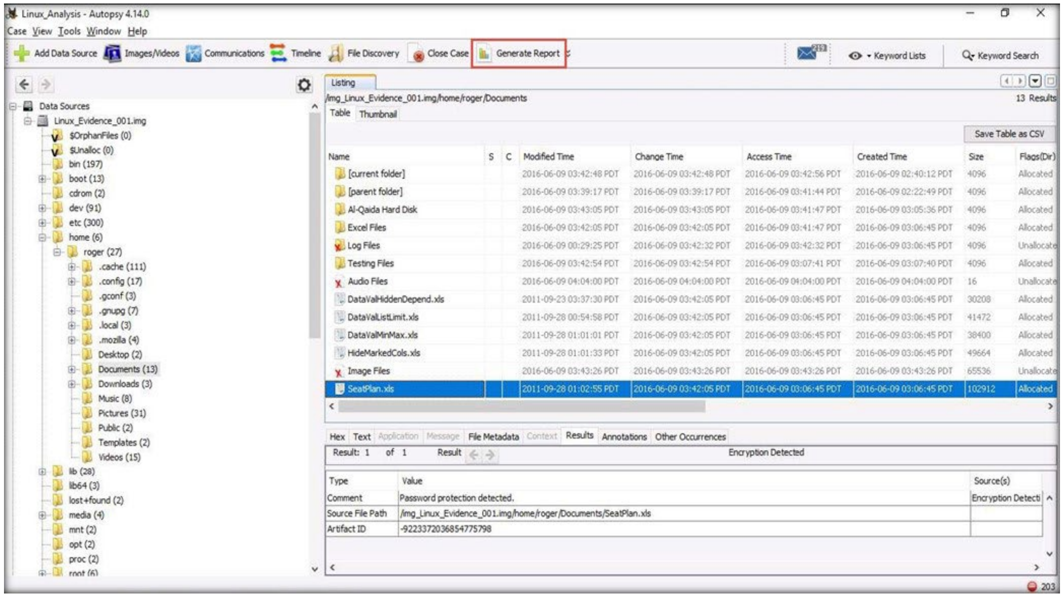
End: Jun 9, 2016 10:00:00 AM

Date/Time	Event Type	Description	Tagged	Hash Hit
2016-06-09 09:12:13	M___	/etc/network/interfaces		
2016-06-09 09:12:15	MA__	/bin/debconf-set		
2016-06-09 09:12:15	MA__	/var/lib/dpkg/info/ubiquity.list		
2016-06-09 09:12:15	MA__	/var/log/installer/casper.log		
2016-06-09 09:12:17	_A__	/bin/autopartition-loop		
2016-06-09 09:12:17	_A__	/var/log/installer/syslog		
2016-06-09 09:12:25	M___	/home/roger/.cache/wallpaper/0_5_1152_864_792beab7550410d531e55f95b449f135		
2016-06-09 09:12:25	M___	/bin/archdetect		
2016-06-09 09:12:25	_A__	/var/log/installer/debug		
2016-06-09 09:12:25	MA__	/var/log/installer/version		
2016-06-09 09:12:25	_A__	/bin/fetch-url		
2016-06-09 09:12:25	M___	/var/lib/dpkg/updates/0042		
2016-06-09 09:12:25	MA__	/bin/block-attr		

```
0x00000000: 23 20 69 6E  74 65 72 66  61 63 65 73  28 35 29 20   # interfaces(5)
0x00000010: 66 69 6C 65  20 75 73 65  64 20 62 79  20 69 66 75   file used by ifu
0x00000020: 70 28 38 29  20 61 6E 64  20 69 66 64  6F 77 6E 28   p(8) and ifdown(
0x00000030: 38 29 0A 61  75 74 6F 20  6C 6F 0A 69  66 61 63 65   8).auto lo.iface
0x00000040: 20 6C 6F 20  69 6E 65 74  20 6C 6F 6F  70 62 61 63    lo inet loopbac
0x00000050: 6B 0A                                                k.
```

38. Now close the Timeline-Editor window to navigate back to Autopsy main window. In the Autopsy window click on the Generate Report option from the menu bar.

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY



/img_Linux_Evidence_001.img/home/roger/Documents

13 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[current folder]			2016-06-09 03:42:48 PDT	2016-06-09 03:42:48 PDT	2016-06-09 03:42:56 PDT	2016-06-09 02:40:12 PDT	4096	Allocated
[parent folder]			2016-06-09 03:39:17 PDT	2016-06-09 03:39:17 PDT	2016-06-09 03:41:44 PDT	2016-06-09 02:22:49 PDT	4096	Allocated
Al-Qaida Hard Disk			2016-06-09 03:43:05 PDT	2016-06-09 03:43:05 PDT	2016-06-09 03:41:47 PDT	2016-06-09 03:05:36 PDT	4096	Allocated
Excel Files			2016-06-09 03:42:05 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:41:47 PDT	2016-06-09 03:06:45 PDT	4096	Allocated
Log Files			2016-06-09 00:29:25 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:42:32 PDT	2016-06-09 03:06:45 PDT	4096	Unallocate
Testing Files			2016-06-09 03:42:54 PDT	2016-06-09 03:42:54 PDT	2016-06-09 03:07:41 PDT	2016-06-09 03:07:40 PDT	4096	Allocated
Audio Files			2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	2016-06-09 04:04:00 PDT	16	Unallocate
DataValHiddenDepend.xls			2011-09-23 03:37:30 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	30208	Allocated
DataValListLimit.xls			2011-09-28 00:54:58 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	41472	Allocated
DataValMinMax.xls			2011-09-28 01:01:01 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	38400	Allocated
HideMarkedCols.xls			2011-09-28 01:01:33 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	49664	Allocated
Image Files			2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	2016-06-09 03:43:26 PDT	65536	Unallocate
SeatPlan.xls			2011-09-28 01:02:55 PDT	2016-06-09 03:42:05 PDT	2016-06-09 03:06:45 PDT	2016-06-09 03:06:45 PDT	102912	Allocated

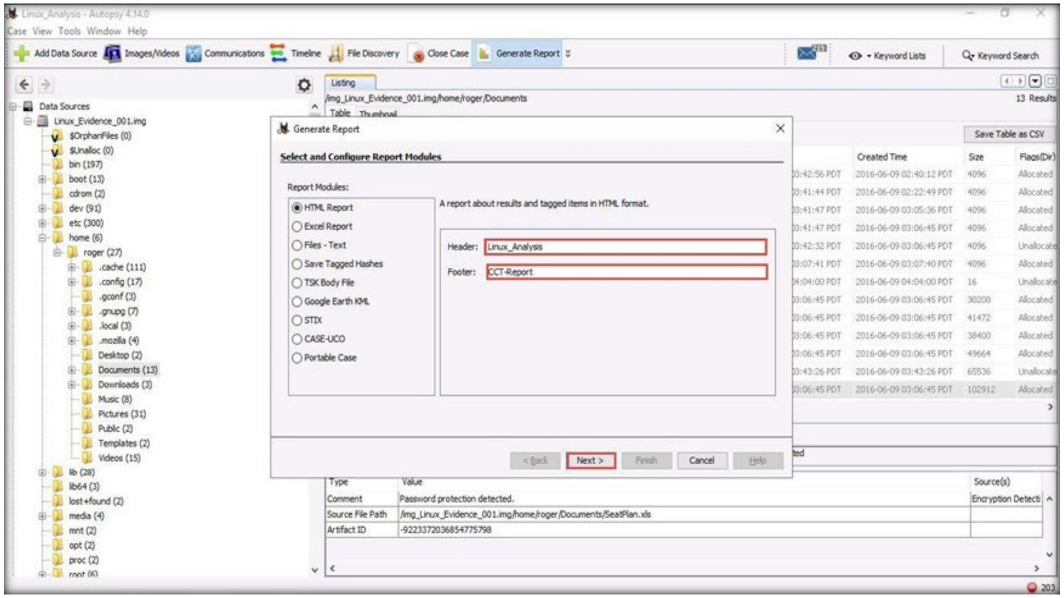
Result: 1 of 1 Result Encryption Detected

Type	Value	Source(s)
Comment	Password protection detected.	Encryption Detecti
Source File Path	/img_Linux_Evidence_001.img/home/roger/Documents/SeatPlan.xls	
Artifact ID	-9223372036854775798	

39. A Generate Report window appears. By default, HTML Report will be selected under Report Modules, enter Header and Footer details in the respective fields and click on Next.

Note: Here we are giving Linux_Analysis as the Header and CCT-Report as the footer.

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY



Generate Report

Select and Configure Report Modules

Report Modules:

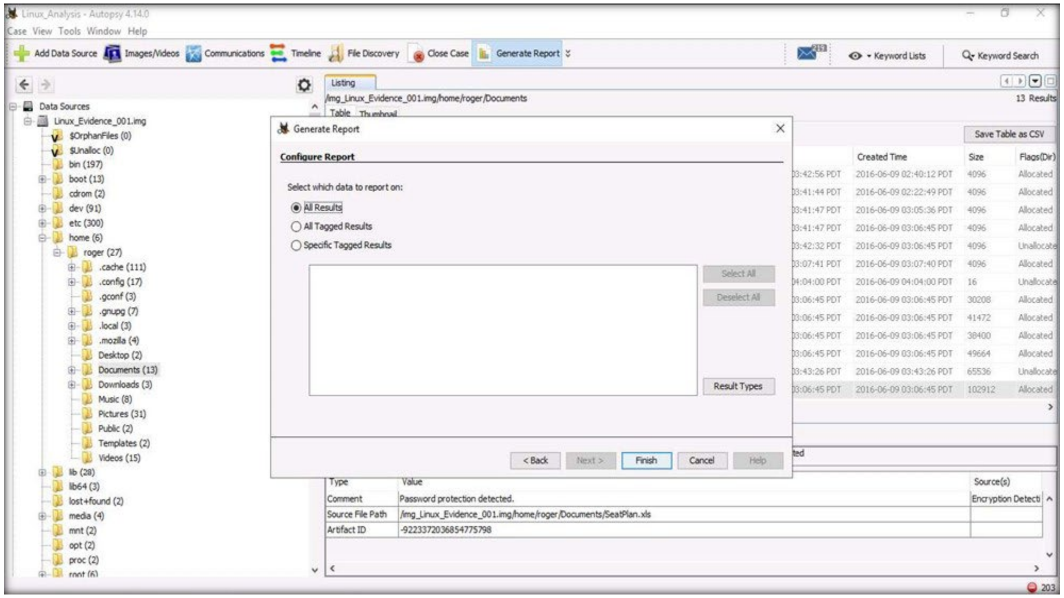
- ● HTML Report
- ○ Excel Report
- ○ Files - Text
- ○ Save Tagged Hashes
- ○ TSK Body File
- ○ Google Earth KML
- ○ STIX
- ○ CASE-UCO
- ○ Portable Case

A report about results and tagged items in HTML format.

Header: Linux_Analysis

Footer: CCT-Report

40. In the Configure Report window, select All Results radio button and click on Finish.



Generate Report

Configure Report

Select which data to report on:

● All Results

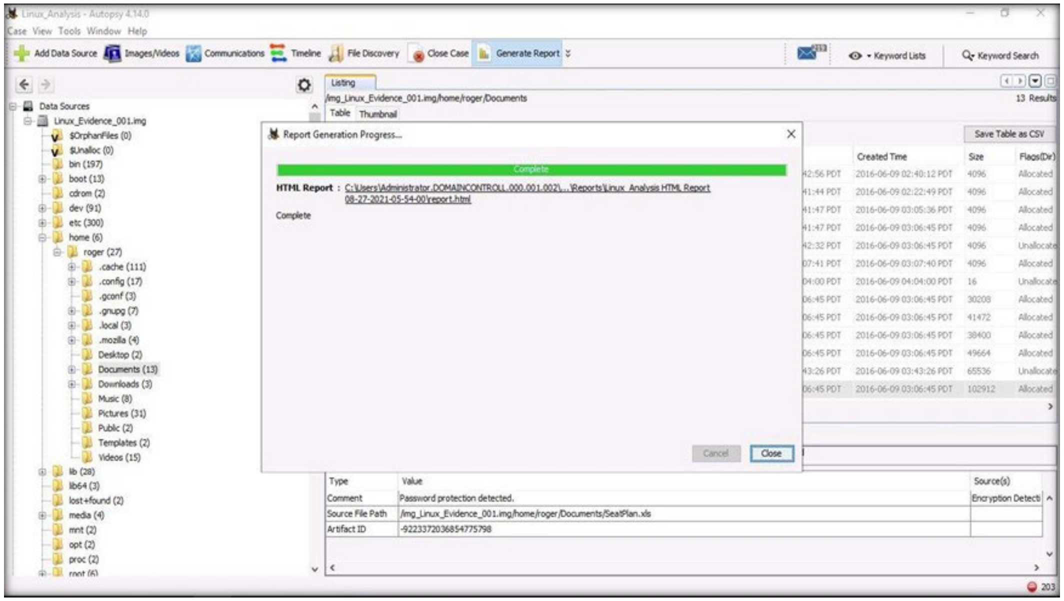
○ All Tagged Results

○ Specific Tagged Results

Type	Value	Source(s)
Comment	Password protection detected.	Encryption Detecti
Source File Path	/img_Linux_Evidence_001.img/home/roger/Documents/SeatPlan.xls	
Artifact ID	-9223372036854775798	

41. A Report Generation Progress... windows appear showing the progress, wait for it to complete.
42. After completion of report generation click on Close to close the window.

EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY



/img_Linux_Evidence_001.img/home/roger/Documents

Report Generation Progress...

Complete

HTML Report : C:\Users\Administrator.DOMAINCONTROLL.000.001.002\...\Reports\Linux_Analysis HTML Report 08-27-2021-05-54-00\report.html

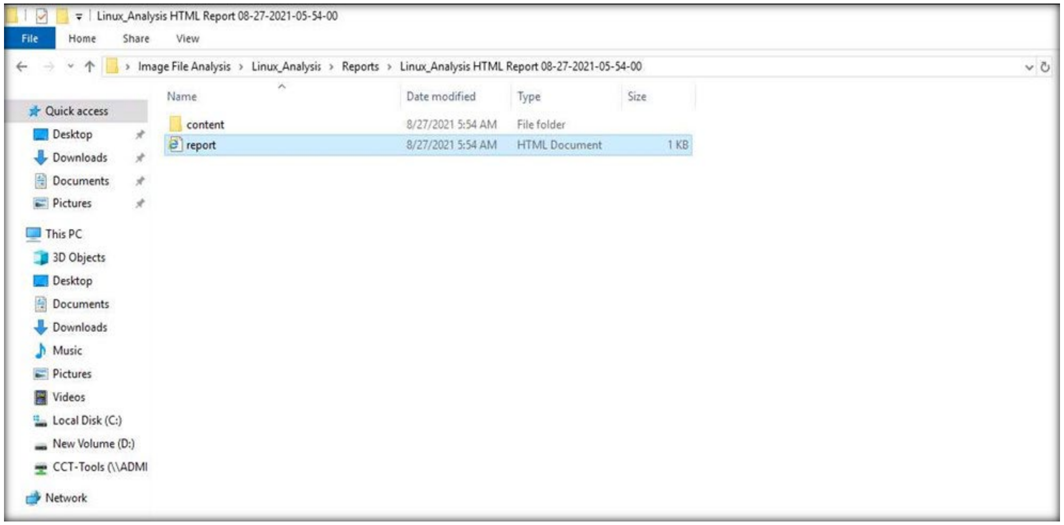
Complete

Type	Value	Source(s)
Comment	Password protection detected.	Encryption Detecti
Source File Path	/img_Linux_Evidence_001.img/home/roger/Documents/SeatPlan.xls	
Artifact ID	-9223372036854775798	

43. Minimize the Autopsy window, navigate to the Image File Analysis folder located on the Desktop. After this, navigate to Linux_Analysis/ Reports/Linux_Analysis HTML Report 08-27-2021-05-54-00 and double-click on report.

Note: The name of the HTML Report folder might vary in your lab environment.

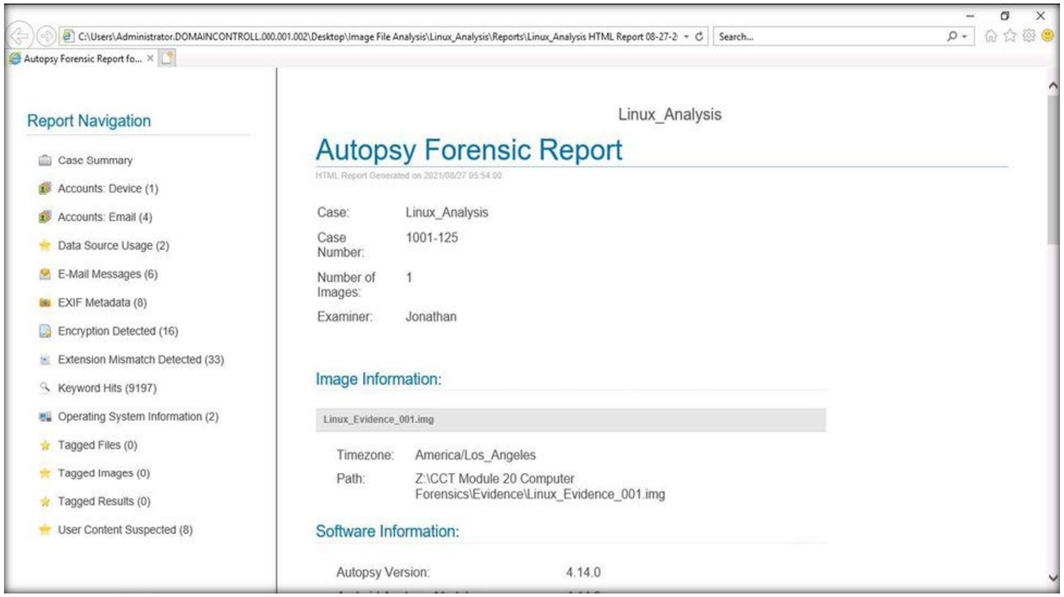
EXERCISE 4: ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY



Name	Date modified	Type	Size
content	8/27/2021 5:54 AM	File folder	
report	8/27/2021 5:54 AM	HTML Document	1 KB

Note: If a Set up Internet Explorer 11 window appears, click on Ask me later and close the opened Microsoft tab to navigate to Autopsy Forensic Report.

44. When the report opens in the default browser, you can explore the report by selecting the options under the Report Navigation menu.



C:\Users\Administrator.DOMAINCONTROLL.000.001.002\Desktop\Image File Analysis\Linux_Analysis\Reports\Linux_Analysis HTML Report 08-27-2
Search...
Autopsy Forensic Report fo...

Report Navigation

- Case Summary
- Accounts: Device (1)
- Accounts: Email (4)
- Data Source Usage (2)
- E-Mail Messages (6)
- EXIF Metadata (8)
- Encryption Detected (16)
- Extension Mismatch Detected (33)
- Keyword Hits (9197)
- Operating System Information (2)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- User Content Suspected (8)

Linux_Analysis

Autopsy Forensic Report

HTML Report Generated on 2021/08/27 05:54:00

Case:	Linux_Analysis
Case Number:	1001-125
Number of Images:	1
Examiner:	Jonathan

Image Information:

Linux_Evidence_001.img

Timezone:	America/Los_Angeles
Path:	Z:\CCT Module 20 Computer Forensics\Evidence\Linux_Evidence_001.img

Software Information:

Autopsy Version:	4.14.0

45. This concludes the demonstration showing how to analyze file system of a Linux image using Autopsy tool.

46. Close all open windows.

47. Turn off Admin Machine-1 and AD Domain Controller virtual machines.

EXERCISE 4:

ANALYZE FILE SYSTEM OF A LINUX IMAGE USING AUTOPSY

EXERCISE 5: CAPTURE AND ANALYSE MEMORY DUMP ON LINUX

Dump files are compressed versions of system log files that are recorded when system crashes or turned off unexpectedly.

LAB SCENARIO

Processes, profiles, other security events are logged in the dump file that allow security teams to identify the reasons for unexpected shutdowns or terminations, which are mostly caused by errors or bugs. Using these dump files, investigators can troubleshoot the software or OS issues. Hence a security professional, must be able to capture the memory dump on the system and further analyze it to test for any suspicious files or activities.

OBJECTIVE

This lab demonstrates how to capture and analyze memory dump on Linux system using various tools such as avml and volatility.

OVERVIEW OF THE LAB

This lab familiarized you with the procedures to capture memory dump using tools such as avml on a Linux system and then analyze the captured memory dump using volatility tool for any issues.
AVML is an X86_64 userland volatile memory acquisition tool which can be used to acquire memory without knowing the target OS distribution or kernel. Memory sources used by this tool are /dev/crash, /proc/kcore, /dev/mem.
The Volatility Framework is a completely open collection of tools, implemented in Python, for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer visibility into the runtime state of the system.

Note: For demonstration purpose, we are analyzing memory on the same machine from which it is acquired. But, in the real world, memory is collected from a different machine and further analyzed in a separate machine for issues.

Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on the Attacker Machine-2 virtual machine.
2. In the login page, the attacker username will be selected by default. Enter password as toor in the Password field and press Enter to log in to the machine.

Note: If a Parrot Updater pop-up appears at the top-right corner of Desktop, ignore and close it.

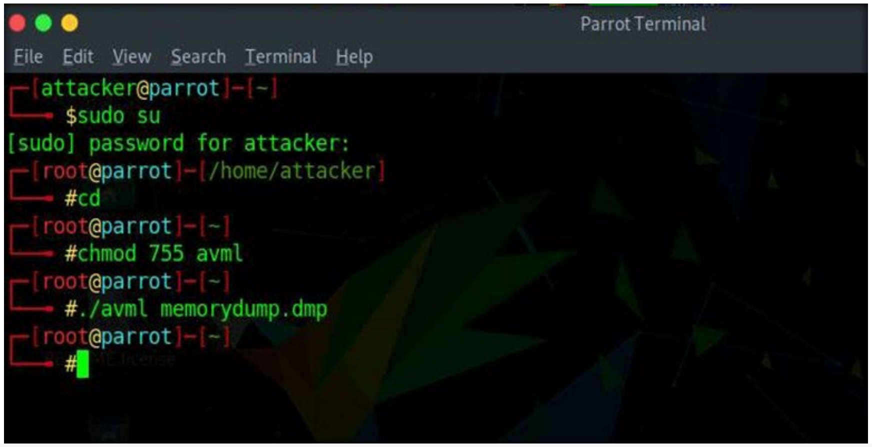
Note: If a Question pop-up window appears asking you to update the machine, click No to close the window.

3. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.
4. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.
5. In the [sudo] password for attacker field, type toor as a password and press Enter.

Note: The password that you type will not be visible.

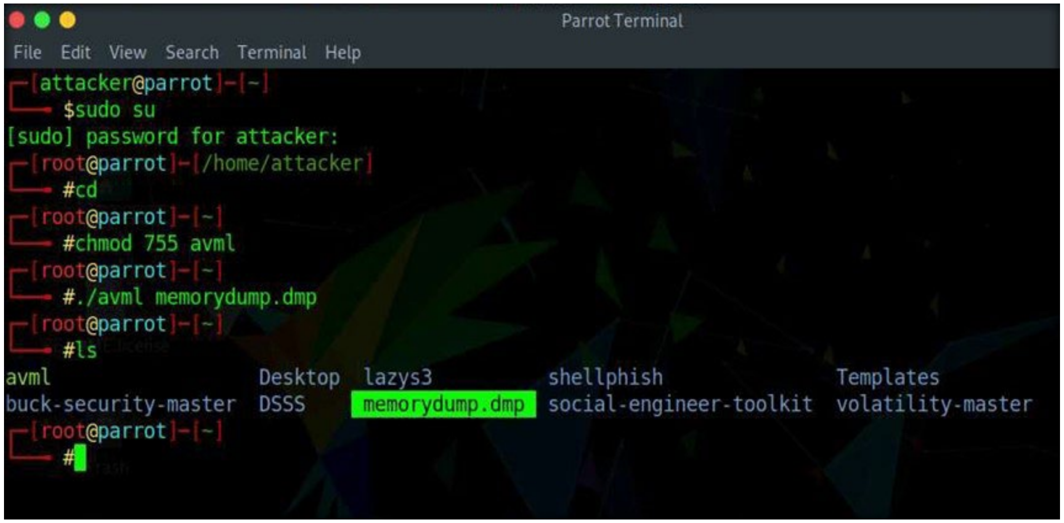
6. Now, type cd and press Enter to jump to the root directory.
7. Firstly, we will generate a memory dump of the system using avml tool.
8. Type chmod 755 avml and press Enter to change the file permissions.
9. Now, type ./avml memorydump.dmp and press Enter to dump system memory in a file named memorydump.dmp.

Note: It will take a while create a memory dump.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #chmod 755 avml
┌─[root@parrot]─[~]
└──╼ #./avml memorydump.dmp
┌─[root@parrot]─[~]
└──╼ #
```

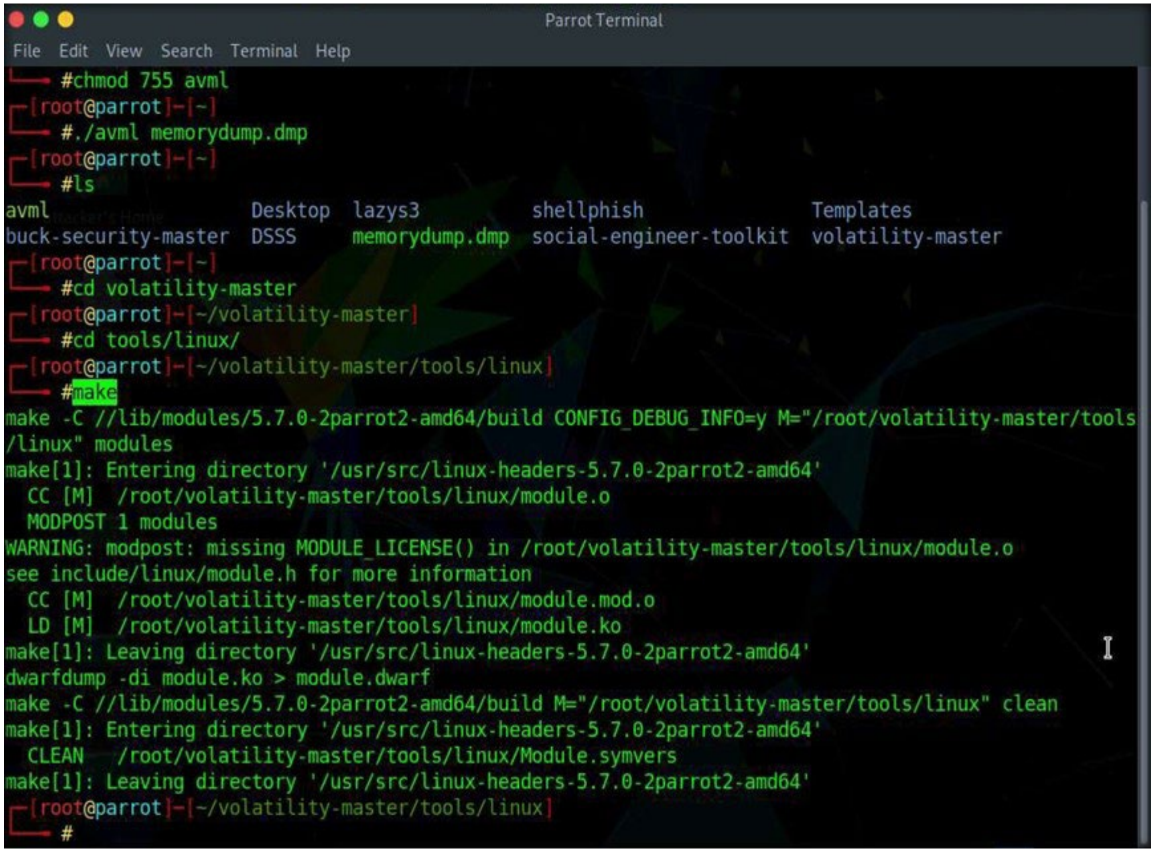
10. Type ls and press Enter to see the generated file memorydump.dmp in the /root directory.



```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #cd
┌─[root@parrot]─[~]
└──╼ #chmod 755 avml
┌─[root@parrot]─[~]
└──╼ #./avml memorydump.dmp
┌─[root@parrot]─[~]
└──╼ #ls
avml                  Desktop  lazys3          shellphish               Templates
buck-security-master  DSSS     memorydump.dmp  social-engineer-toolkit  volatility-master
┌─[root@parrot]─[~]
└──╼ #
```

11. Now, type cd volatility-master and press Enter to navigate to the Volatility tool repository.
12. Type cd tools/linux/ and press Enter.
13. Type make and press Enter to install the tool dependencies.

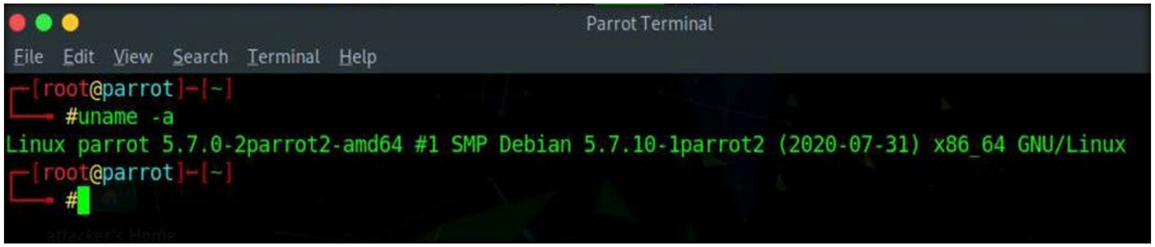
EXERCISE 5: CAPTURE AND ANALYSE MEMORY DUMP ON LINUX



```
└── #chmod 755 avml
┌[root@parrot]-[~]
└── #./avml memorydump.dmp
┌[root@parrot]-[~]
└── #ls
avml                   Desktop  lazys3          shellphish              Templates
buck-security-master   DSSS     memorydump.dmp  social-engineer-toolkit volatility-master
┌[root@parrot]-[~]
└── #cd volatility-master
┌[root@parrot]-[~/volatility-master]
└── #cd tools/linux/
┌[root@parrot]-[~/volatility-master/tools/linux]
└── #make
make -C //lib/modules/5.7.0-2parrot2-amd64/build CONFIG_DEBUG_INFO=y M="/root/volatility-master/tools
/linux" modules
make[1]: Entering directory '/usr/src/linux-headers-5.7.0-2parrot2-amd64'
  CC [M]  /root/volatility-master/tools/linux/module.o
  MODPOST 1 modules
WARNING: modpost: missing MODULE_LICENSE() in /root/volatility-master/tools/linux/module.o
see include/linux/module.h for more information
  CC [M]  /root/volatility-master/tools/linux/module.mod.o
  LD [M]  /root/volatility-master/tools/linux/module.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.7.0-2parrot2-amd64'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/5.7.0-2parrot2-amd64/build M="/root/volatility-master/tools/linux" clean
make[1]: Entering directory '/usr/src/linux-headers-5.7.0-2parrot2-amd64'
  CLEAN   /root/volatility-master/tools/linux/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-5.7.0-2parrot2-amd64'
┌[root@parrot]-[~/volatility-master/tools/linux]
└── #
```

14. Now, type cd and press Enter to navigate back to the /root directory.
15. Type uname -a press Enter to display the kernal version.

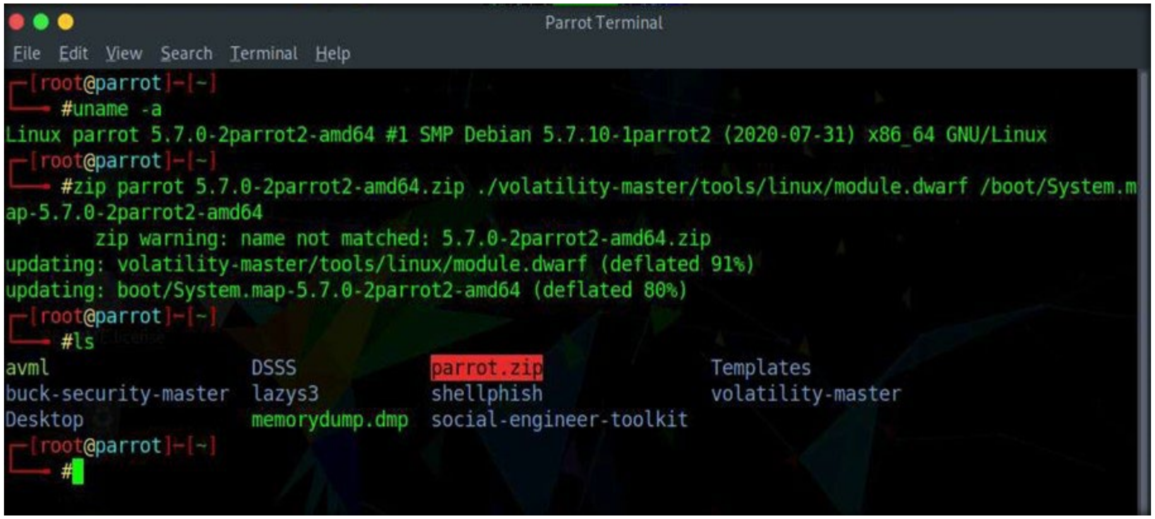
Note: The above command is used to display the details such as name of operating system, the system node name, operating system release, operating system version, hardware name, and processor type.



```
┌─[root@parrot]─[~]
└──╼ #uname -a
Linux parrot 5.7.0-2parrot2-amd64 #1 SMP Debian 5.7.10-1parrot2 (2020-07-31) x86_64 GNU/Linux
┌─[root@parrot]─[~]
└──╼ #
```

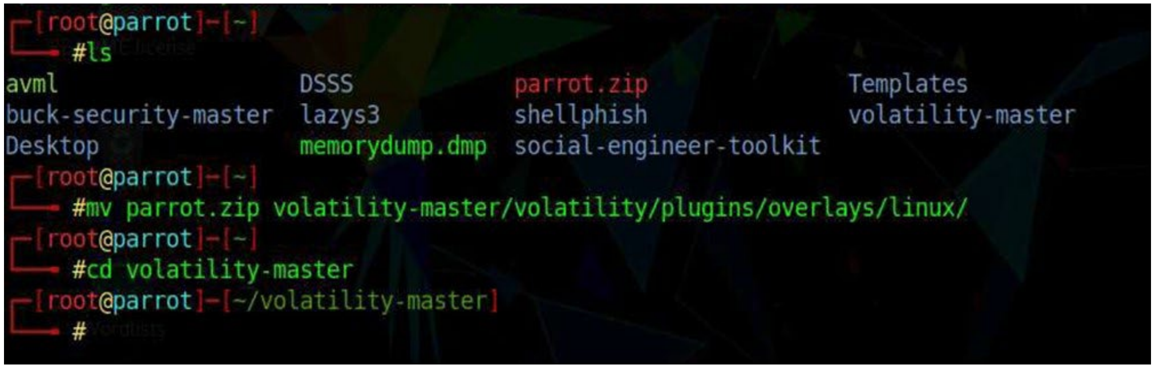
16. Now, type zip parrot 5.7.0-2parrot2-amd64.zip ./volatility-master/tools/linux/module.dwarf /boot/System.map-5.7.0-2parrot2-amd64 and press Enter to make a zip file and map with the system.
17. Type ls and press Enter to see the created zip file. Observe that a file named parrot.zip has been created, as shown in the screenshot below.

EXERCISE 5: CAPTURE AND ANALYSE MEMORY DUMP ON LINUX



```
┌─[root@parrot]─[~]
└──╼ #uname -a
Linux parrot 5.7.0-2parrot2-amd64 #1 SMP Debian 5.7.10-1parrot2 (2020-07-31) x86_64 GNU/Linux
┌─[root@parrot]─[~]
└──╼ #zip parrot 5.7.0-2parrot2-amd64.zip ./volatility-master/tools/linux/module.dwarf /boot/System.m
ap-5.7.0-2parrot2-amd64
        zip warning: name not matched: 5.7.0-2parrot2-amd64.zip
updating: volatility-master/tools/linux/module.dwarf (deflated 91%)
updating: boot/System.map-5.7.0-2parrot2-amd64 (deflated 80%)
┌─[root@parrot]─[~]
└──╼ #ls
avml                   DSSS            parrot.zip               Templates
buck-security-master   lazys3          shellphish               volatility-master
Desktop                memorydump.dmp  social-engineer-toolkit
┌─[root@parrot]─[~]
└──╼ #
```

18. Type mv parrot.zip volatility-master/volatility/plugins/overlays/linux/ and press Enter to move the zip file to the volatility tool folder.
19. Type cd volatility-master and press Enter to navigate to the tool repository.

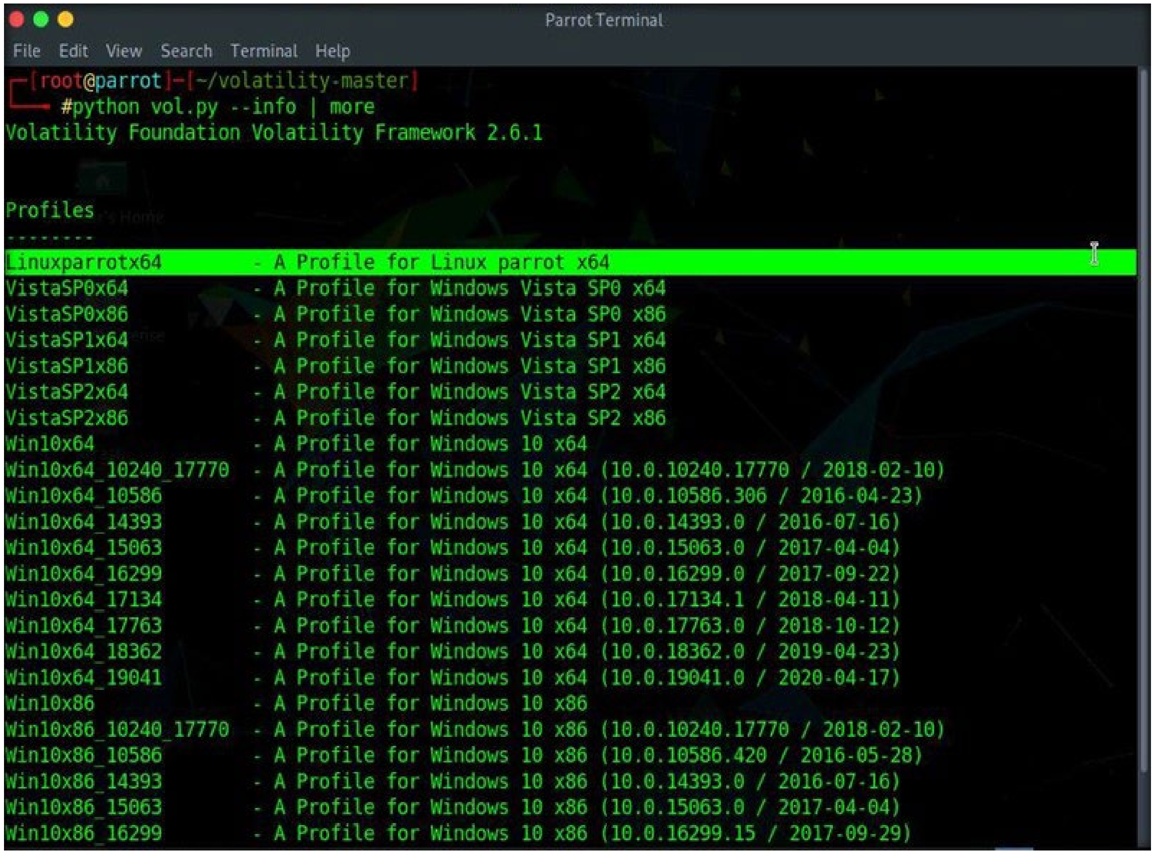


```
┌─[root@parrot]─[~]
└──╼ #ls
avml                  DSSS          parrot.zip             Templates
buck-security-master  lazys3        shellphish             volatility-master
Desktop               memorydump.dmp social-engineer-toolkit
┌─[root@parrot]─[~]
└──╼ #mv parrot.zip volatility-master/volatility/plugins/overlays/linux/
┌─[root@parrot]─[~]
└──╼ #cd volatility-master
┌─[root@parrot]─[~/volatility-master]
└──╼ #
```

20. Type python vol.py --info | more and press Enter to display all the profiles in the directory.

21. A list of Profiles appears, you can observe the first profile Linuxparrotx64, which was moved to this directory in the previous steps.

Note: After viewing the profile list, press Ctrl+C and press Enter to terminate the command.

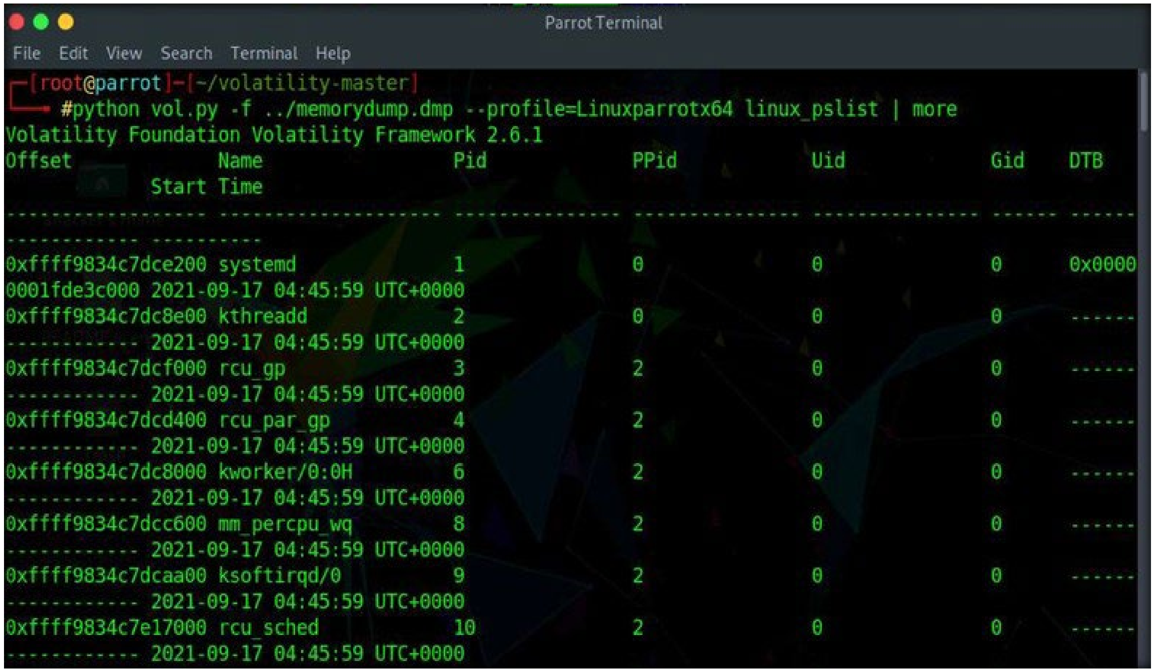


```
┌─[root@parrot]─[~/volatility-master]
└──╼ #python vol.py --info | more
Volatility Foundation Volatility Framework 2.6.1


Profiles
--------
Linuxparrotx64         - A Profile for Linux parrot x64
VistaSP0x64            - A Profile for Windows Vista SP0 x64
VistaSP0x86            - A Profile for Windows Vista SP0 x86
VistaSP1x64            - A Profile for Windows Vista SP1 x64
VistaSP1x86            - A Profile for Windows Vista SP1 x86
VistaSP2x64            - A Profile for Windows Vista SP2 x64
VistaSP2x86            - A Profile for Windows Vista SP2 x86
Win10x64               - A Profile for Windows 10 x64
Win10x64_10240_17770   - A Profile for Windows 10 x64 (10.0.10240.17770 / 2018-02-10)
Win10x64_10586         - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
Win10x64_14393         - A Profile for Windows 10 x64 (10.0.14393.0 / 2016-07-16)
Win10x64_15063         - A Profile for Windows 10 x64 (10.0.15063.0 / 2017-04-04)
Win10x64_16299         - A Profile for Windows 10 x64 (10.0.16299.0 / 2017-09-22)
Win10x64_17134         - A Profile for Windows 10 x64 (10.0.17134.1 / 2018-04-11)
Win10x64_17763         - A Profile for Windows 10 x64 (10.0.17763.0 / 2018-10-12)
Win10x64_18362         - A Profile for Windows 10 x64 (10.0.18362.0 / 2019-04-23)
Win10x64_19041         - A Profile for Windows 10 x64 (10.0.19041.0 / 2020-04-17)
Win10x86               - A Profile for Windows 10 x86
Win10x86_10240_17770   - A Profile for Windows 10 x86 (10.0.10240.17770 / 2018-02-10)
Win10x86_10586         - A Profile for Windows 10 x86 (10.0.10586.420 / 2016-05-28)
Win10x86_14393         - A Profile for Windows 10 x86 (10.0.14393.0 / 2016-07-16)
Win10x86_15063         - A Profile for Windows 10 x86 (10.0.15063.0 / 2017-04-04)
Win10x86_16299         - A Profile for Windows 10 x86 (10.0.16299.15 / 2017-09-29)
```

22. Now, we will analyze the captured memory dump using volatility tool.

23. Now, type python vol.py -f ../memorydump.dmp –-profile=Linuxparrotx64 linux_pslist | more and press Enter to list the process IDs.

Note: It will take a while to fetch the results.

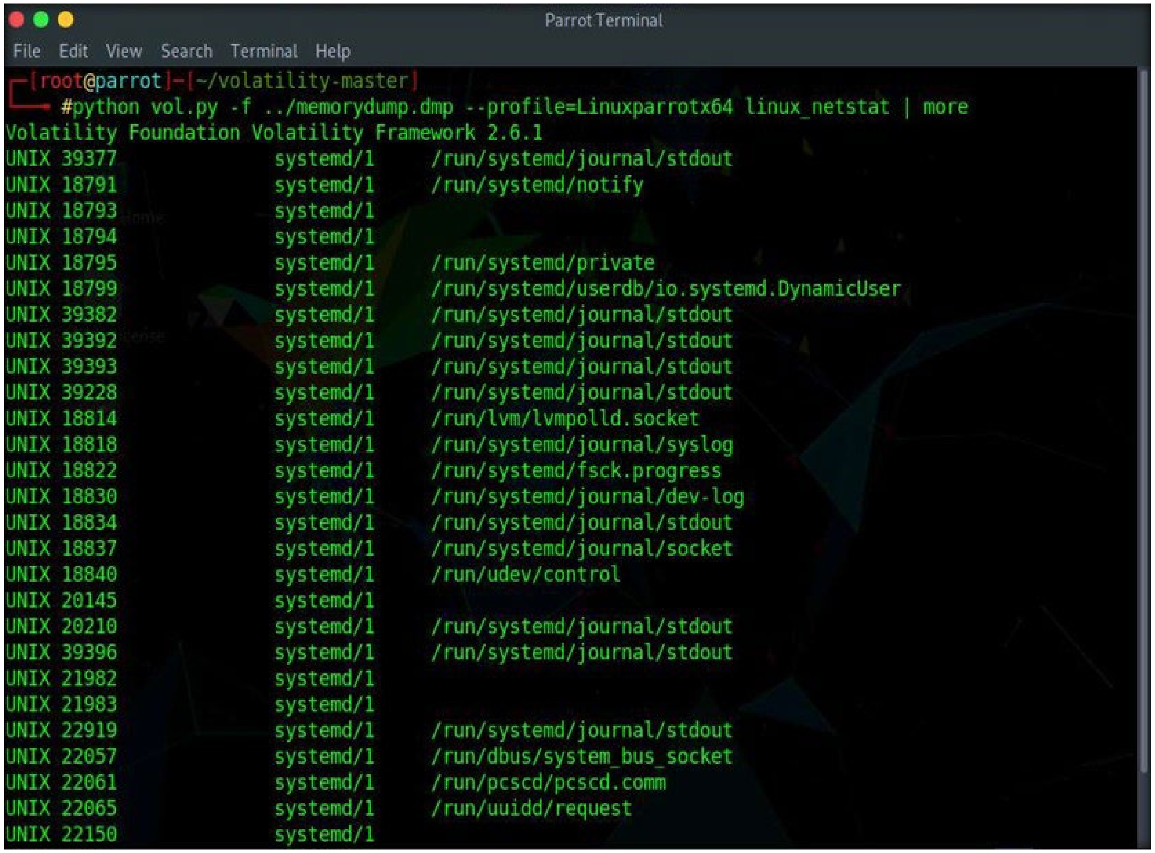


```
┌[root@parrot]─[~/volatility-master]
└──╼ #python vol.py -f ../memorydump.dmp --profile=Linuxparrotx64 linux_pslist | more
Volatility Foundation Volatility Framework 2.6.1
Offset             Name                 Pid             PPid            Uid             Gid    DTB
             Start Time
------------------ -------------------- --------------- --------------- --------------- ------ ------
------------ ----------
0xffff9834c7dce200 systemd              1               0               0               0      0x0000
0001fde3c000 2021-09-17 04:45:59 UTC+0000
0xffff9834c7dc8e00 kthreadd             2               0               0               0      ------
------------ 2021-09-17 04:45:59 UTC+0000
0xffff9834c7dcf000 rcu_gp               3               2               0               0      ------
------------ 2021-09-17 04:45:59 UTC+0000
0xffff9834c7dcd400 rcu_par_gp           4               2               0               0      ------
------------ 2021-09-17 04:45:59 UTC+0000
0xffff9834c7dc8000 kworker/0:0H         6               2               0               0      ------
------------ 2021-09-17 04:45:59 UTC+0000
0xffff9834c7dcc600 mm_percpu_wq         8               2               0               0      ------
------------ 2021-09-17 04:45:59 UTC+0000
0xffff9834c7dcaa00 ksoftirqd/0          9               2               0               0      ------
------------ 2021-09-17 04:45:59 UTC+0000
0xffff9834c7e17000 rcu_sched            10              2               0               0      ------
------------ 2021-09-17 04:45:59 UTC+0000
```

Note: After viewing the process list, press Ctrl+C and press Enter to terminate the command.

24. Type python vol.py -f ../memorydump.dmp –-profile=Linuxparrotx64 linux_netstat | more and press Enter to display the network connections, routing tables, and a number of network interface statistics.

Note: It will take a while to fetch the results.

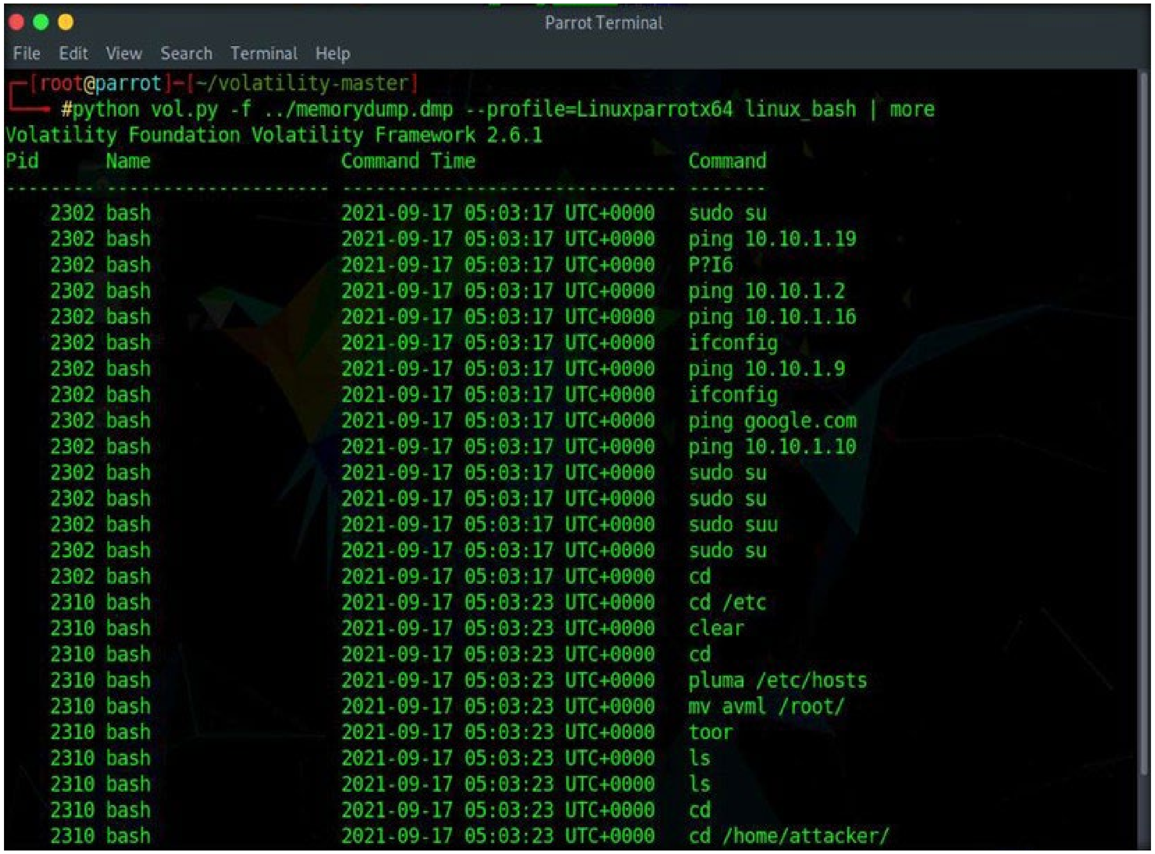


```
┌─[root@parrot]─[~/volatility-master]
└──╼ #python vol.py -f ../memorydump.dmp --profile=Linuxparrotx64 linux_netstat | more
Volatility Foundation Volatility Framework 2.6.1
UNIX 39377               systemd/1     /run/systemd/journal/stdout
UNIX 18791               systemd/1     /run/systemd/notify
UNIX 18793               systemd/1
UNIX 18794               systemd/1
UNIX 18795               systemd/1     /run/systemd/private
UNIX 18799               systemd/1     /run/systemd/userdb/io.systemd.DynamicUser
UNIX 39382               systemd/1     /run/systemd/journal/stdout
UNIX 39392               systemd/1     /run/systemd/journal/stdout
UNIX 39393               systemd/1     /run/systemd/journal/stdout
UNIX 39228               systemd/1     /run/systemd/journal/stdout
UNIX 18814               systemd/1     /run/lvm/lvmpolld.socket
UNIX 18818               systemd/1     /run/systemd/journal/syslog
UNIX 18822               systemd/1     /run/systemd/fsck.progress
UNIX 18830               systemd/1     /run/systemd/journal/dev-log
UNIX 18834               systemd/1     /run/systemd/journal/stdout
UNIX 18837               systemd/1     /run/systemd/journal/socket
UNIX 18840               systemd/1     /run/udev/control
UNIX 20145               systemd/1
UNIX 20210               systemd/1     /run/systemd/journal/stdout
UNIX 39396               systemd/1     /run/systemd/journal/stdout
UNIX 21982               systemd/1
UNIX 21983               systemd/1
UNIX 22919               systemd/1     /run/systemd/journal/stdout
UNIX 22057               systemd/1     /run/dbus/system_bus_socket
UNIX 22061               systemd/1     /run/pcscd/pcscd.comm
UNIX 22065               systemd/1     /run/uuidd/request
UNIX 22150               systemd/1
```

Note: After viewing the connection list, press Ctrl+C and press Enter to terminate the command.

25. Type python vol.py -f ../memorydump.dmp –-profile=Linuxparrotx64 linux_bash | more and press Enter to display the terminal history.

Note: It will take a while to fetch the results.



```
┌─[root@parrot]─[~/volatility-master]
└──╼ #python vol.py -f ../memorydump.dmp --profile=Linuxparrotx64 linux_bash | more
Volatility Foundation Volatility Framework 2.6.1
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
    2302 bash                 2021-09-17 05:03:17 UTC+0000   sudo su
    2302 bash                 2021-09-17 05:03:17 UTC+0000   ping 10.10.1.19
    2302 bash                 2021-09-17 05:03:17 UTC+0000   P?I6
    2302 bash                 2021-09-17 05:03:17 UTC+0000   ping 10.10.1.2
    2302 bash                 2021-09-17 05:03:17 UTC+0000   ping 10.10.1.16
    2302 bash                 2021-09-17 05:03:17 UTC+0000   ifconfig
    2302 bash                 2021-09-17 05:03:17 UTC+0000   ping 10.10.1.9
    2302 bash                 2021-09-17 05:03:17 UTC+0000   ifconfig
    2302 bash                 2021-09-17 05:03:17 UTC+0000   ping google.com
    2302 bash                 2021-09-17 05:03:17 UTC+0000   ping 10.10.1.10
    2302 bash                 2021-09-17 05:03:17 UTC+0000   sudo su
    2302 bash                 2021-09-17 05:03:17 UTC+0000   sudo su
    2302 bash                 2021-09-17 05:03:17 UTC+0000   sudo suu
    2302 bash                 2021-09-17 05:03:17 UTC+0000   sudo su
    2302 bash                 2021-09-17 05:03:17 UTC+0000   cd
    2310 bash                 2021-09-17 05:03:23 UTC+0000   cd /etc
    2310 bash                 2021-09-17 05:03:23 UTC+0000   clear
    2310 bash                 2021-09-17 05:03:23 UTC+0000   cd
    2310 bash                 2021-09-17 05:03:23 UTC+0000   pluma /etc/hosts
    2310 bash                 2021-09-17 05:03:23 UTC+0000   mv avml /root/
    2310 bash                 2021-09-17 05:03:23 UTC+0000   toor
    2310 bash                 2021-09-17 05:03:23 UTC+0000   ls
    2310 bash                 2021-09-17 05:03:23 UTC+0000   ls
    2310 bash                 2021-09-17 05:03:23 UTC+0000   cd
    2310 bash                 2021-09-17 05:03:23 UTC+0000   cd /home/attacker/
```

Note: After viewing the bash list, press Ctrl+C and press Enter to terminate the command.

26. Similarly, you can see other details such as a list of open files in the system by replacing the parameter with linux_lsof.
27. This concludes the demonstration showing how to capture and analyze memory dump on linux machine.
28. Close all open windows.
29. Turn off the Attacker Machine-2 virtual machine.

EXERCISE 6: **VIEW CONTENTS OF FORENSIC IMAGE FILE**

FTK Imager is a data preview and imaging tool that creates perfect copies (forensic images) of computer data without making changes to the original evidence.

LAB SCENARIO

As part of investigation in an information theft case, senior investigator Alex has concluded scanning all the systems using the AccessData FTK Imager tool to know if the deleted files on the systems contain any information of evidentiary value. The tool saves the investigator's time as it eliminates the hectic process of recovering every deleted file from the system.
An expert investigator must understand how to assess forensic images and collect the evidentiary data from those images.

OBJECTIVE

The objective of this lab is to learn how to use AccessData FTK Imager for viewing forensics images.

OVERVIEW OF THE LAB

This lab familiarizes you with the AccessData FTK Imager tool and helps you learn how to investigate forensic images of computer data without subjecting the original evidence to modification. It also helps you understand how to assess electronic evidence to determine whether further analysis of the evidence with a forensic tool is necessary.

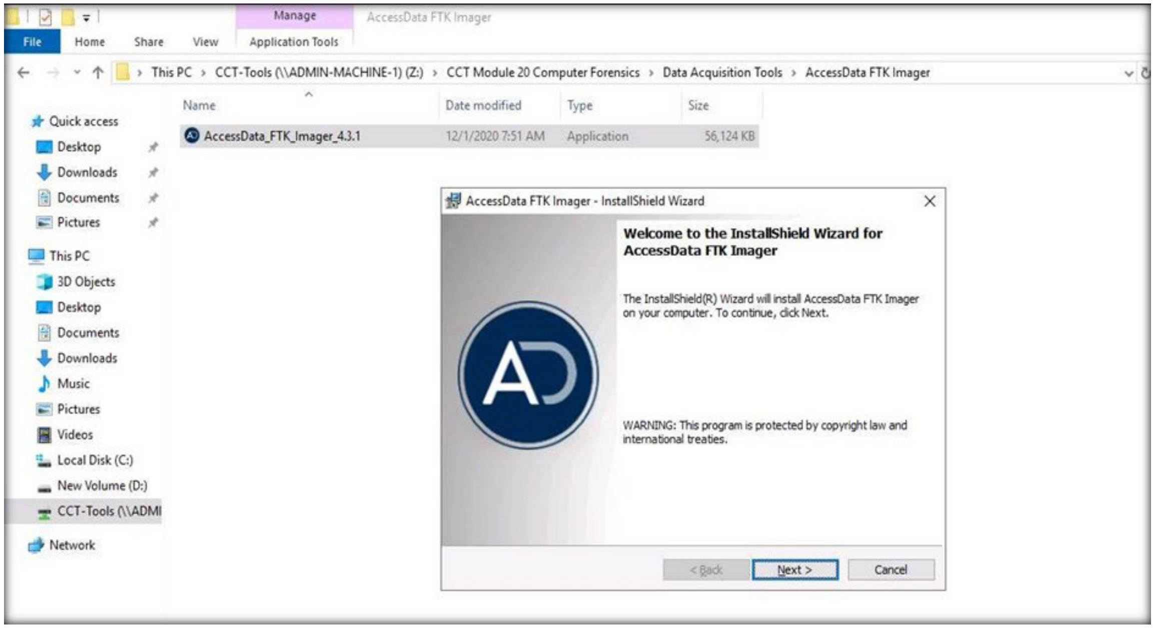
EXERCISE 6: VIEW CONTENTS OF FORENSIC IMAGE FILE

Note: Ensure that PfSense Firewall virtual machine is running.

1. Turn on Admin Machine-1 and AD Domain Controller virtual machine.
2. In the AD Domain Controller virtual machine, log in with the credentials CCT\Administrator and admin@123.

Note: If Networks pane appears, click Yes to allow your PC to discoverable by other PCs and Devices on this network.

3. Navigate to Z:\CCT Module 20 Computer Forensics\Data Acquisition Tools\AccessData FTK Imager, double-click AccessData_FTK_Imager_4.3.1.exe to launch the setup, and follow the wizard-driven installation instructions to install the application



This PC › CCT-Tools (\\ADMIN-MACHINE-1) (Z:) › CCT Module 20 Computer Forensics › Data Acquisition Tools › AccessData FTK Imager

Name	Date modified	Type	Size
AccessData_FTK_Imager_4.3.1	12/1/2020 7:51 AM	Application	56,124 KB

AccessData FTK Imager - InstallShield Wizard

Welcome to the InstallShield Wizard for AccessData FTK Imager

The InstallShield(R) Wizard will install AccessData FTK Imager on your computer. To continue, click Next.

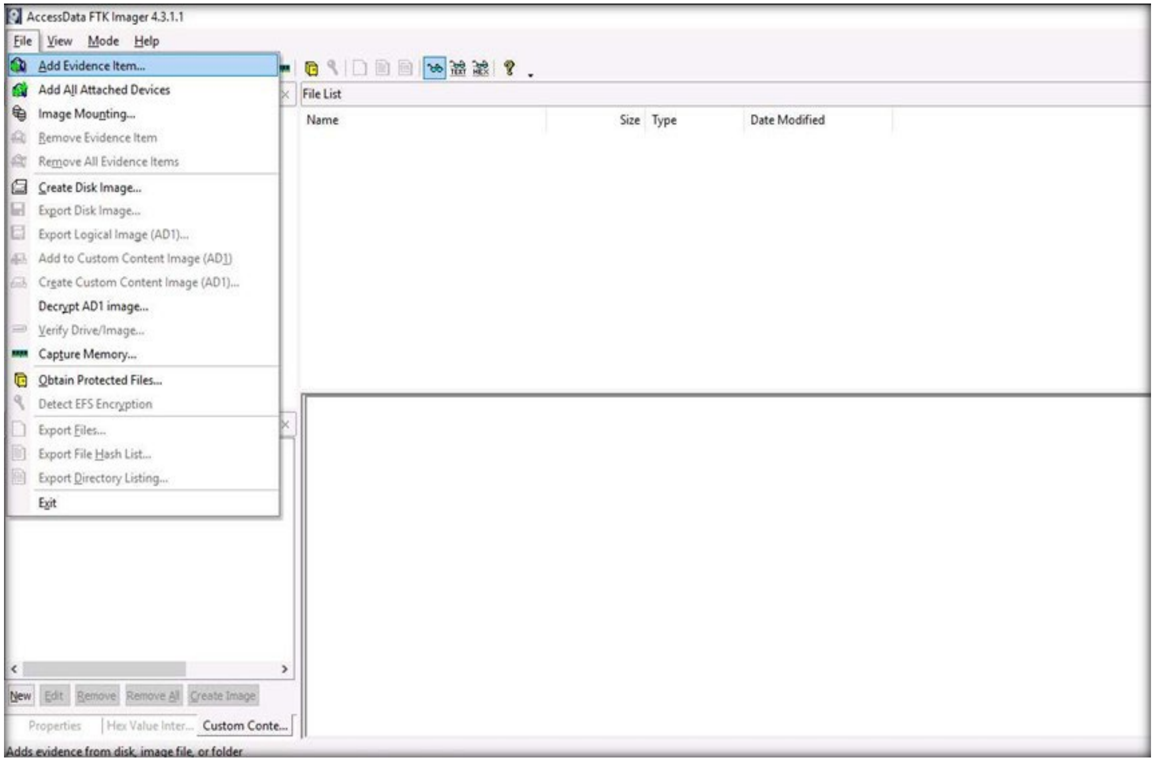
WARNING: This program is protected by copyright law and international treaties.

EXERCISE 6: VIEW CONTENTS OF FORENSIC IMAGE FILE

Note: At the end of the installation process, ensure that the Launch AccessData FTK Imager option is checked in the setup wizard and then click Finish.

4. The main window of AccessData FTK Imager appears, as shown in the following screenshot:

5. Click File → Add Evidence Item... to add evidence.

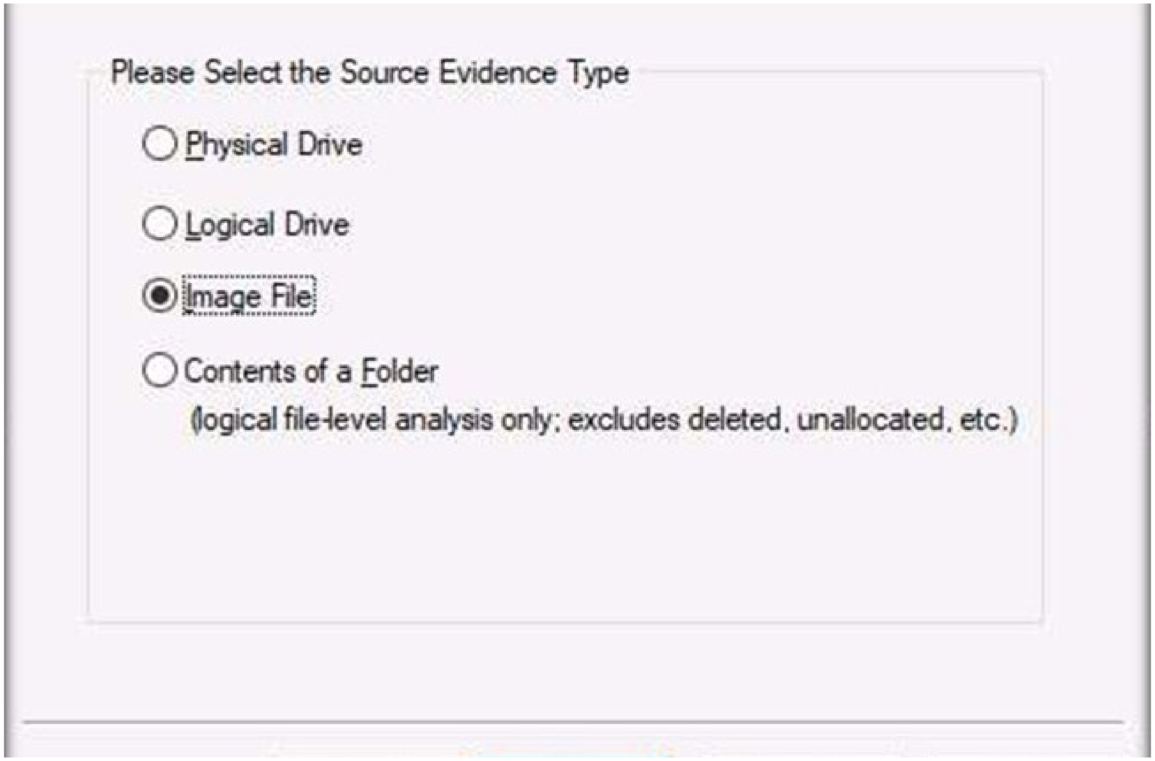


Adds evidence from disk, image file, or folder

Note: Alternatively, you may also click on the Add Evidence icon from the toolbar to add evidence.

6. A Select Source window opens. Select the Image File option and click Next.

Note: In this lab, we will be examining a dd image; therefore, select the Image File radio button.



Please Select the Source Evidence Type

○ Physical Drive

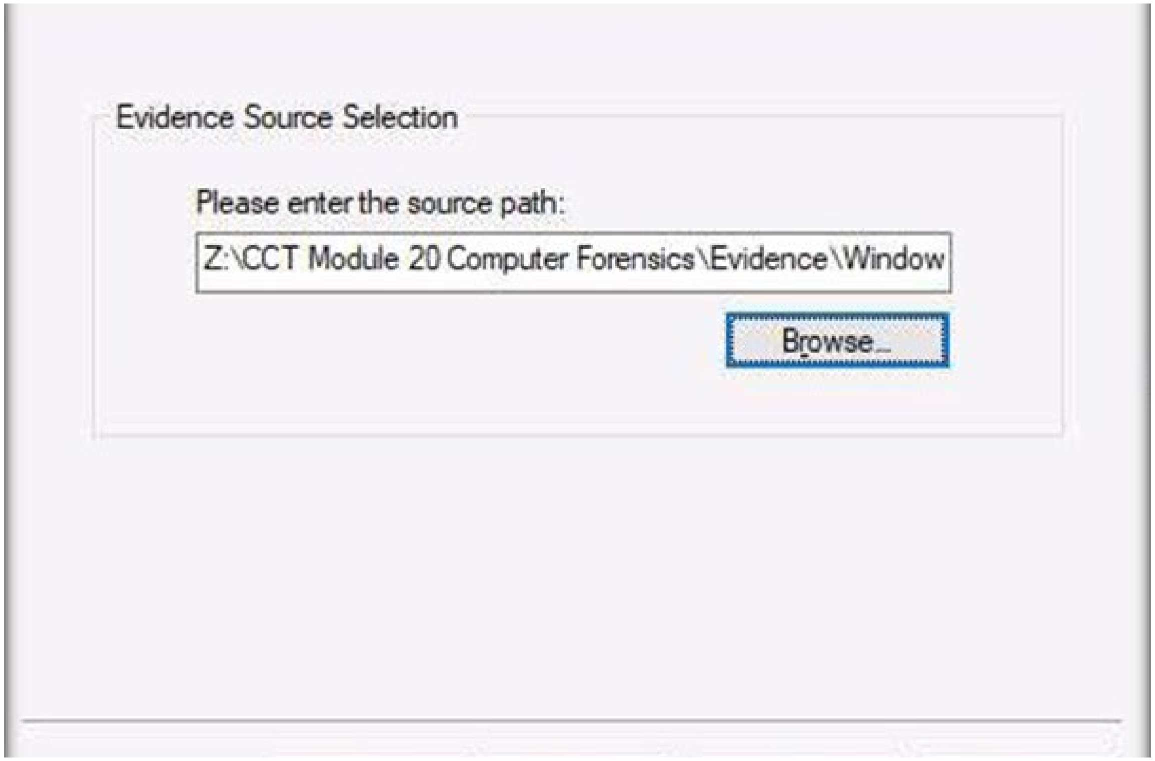
○ Logical Drive

● Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

EXERCISE 6: VIEW CONTENTS OF FORENSIC IMAGE FILE

7. Click the Browse button to specify the image file path (Z:\CCT Module 20 Computer Forensics\Evidence\Windows_Evidence_001.dd) and then click Finish.



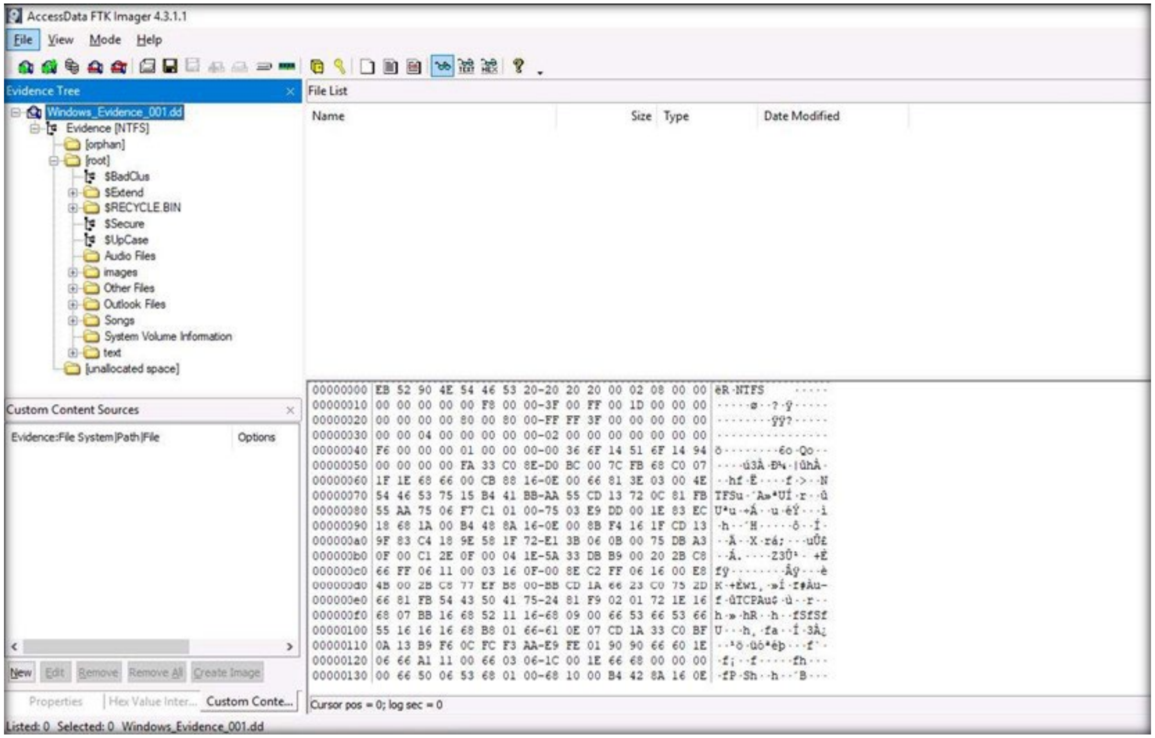
Evidence Source Selection

Please enter the source path:

Z:\CCT Module 20 Computer Forensics\Evidence\Window

8. The evidence file (Windows_Evidence_001.dd) appears in the left pane of the main window under the Evidence Tree section. Expand the evidence file and its contents so that it appears in the form of a tree, as shown in the following screenshot:

EXERCISE 6: VIEW CONTENTS OF FORENSIC IMAGE FILE



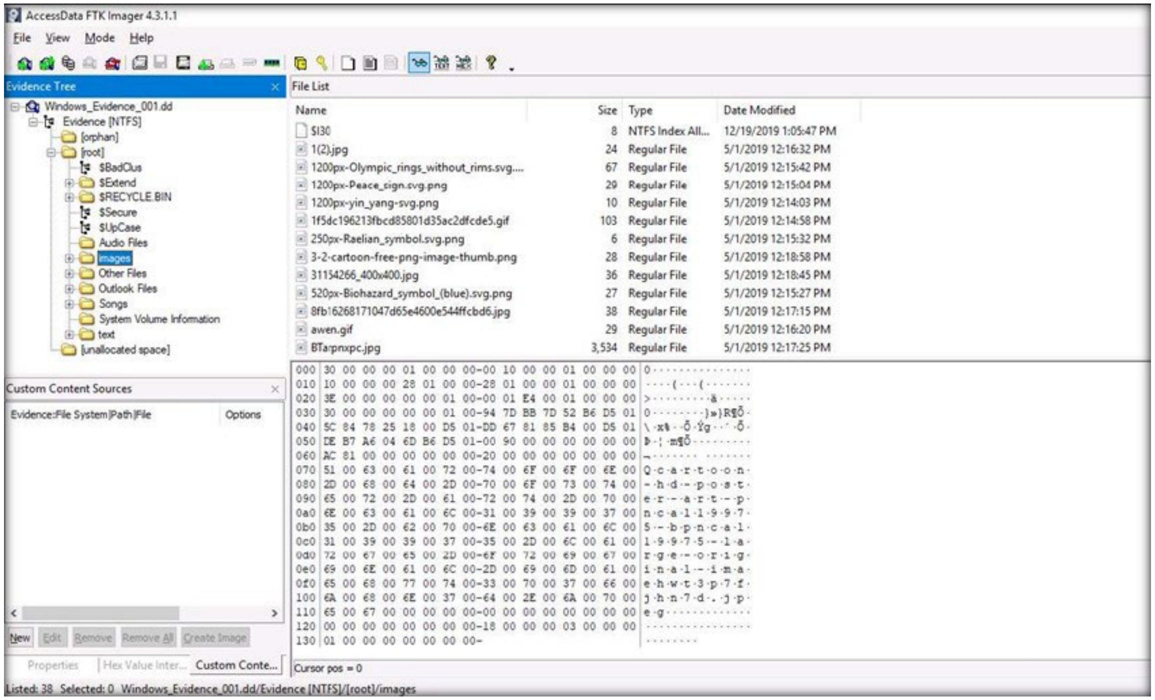
```
00000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00 ëR·NTFS     ·····
00000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 1D 00 00 00 ·····ø··?·ÿ·····
00000020 00 00 00 00 80 00 80 00-FF FF 3F 00 00 00 00 00 ········ÿÿ?·····
00000030 00 00 04 00 00 00 00 00-02 00 00 00 00 00 00 00 ················
00000040 F6 00 00 00 01 00 00 00-00 36 6F 14 51 6F 14 94 ö········6o·Qo··
00000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07 ····ú3À·Ð¼·|ûhÀ·
00000060 1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E ··hf·Ë····f·>··N
00000070 54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB TFSu·´A»ªUÍ·r··û
00000080 55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC Uªu·÷Á··u·éÝ···ì
00000090 18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13 ·h··´H·····ô··Í·
000000a0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3 ··Ä··X·rá;···uÛ£
000000b0 0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8 ··Á.····Z3Û¹· +È
000000c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8 fÿ·······Âÿ···è
000000d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D K·+Èwï¸·»Í·f#Àu-
000000e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f·ûTCPAu$·ù··r··
000000f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66 h·»·hR··h··fSfSf
00000100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U···h¸·fa··Í·3À¿
00000110 0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E ··¹ö·üóªéþ···f`·
00000120 06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00 ·f¡··f·····fh···
00000130 00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E ·fP·Sh··h··´B···
```

Cursor pos = 0; log sec = 0

Listed: 0 Selected: 0 Windows_Evidence_001.dd

EXERCISE 6: VIEW CONTENTS OF FORENSIC IMAGE FILE

9. Select any file or folder (here, we selected images folder) from the Evidence Tree to view the file list in the Right pane under File List.



Name	Size	Type	Date Modified
$I30	8	NTFS Index All...	12/19/2019 1:05:47 PM
1(2).jpg	24	Regular File	5/1/2019 12:16:32 PM
1200px-Olympic_rings_without_rims.svg....	67	Regular File	5/1/2019 12:15:42 PM
1200px-Peace_sign.svg.png	29	Regular File	5/1/2019 12:15:04 PM
1200px-yin_yang-svg.png	10	Regular File	5/1/2019 12:14:03 PM
1f5dc196213fbcd85801d35ac2dfcde5.gif	103	Regular File	5/1/2019 12:14:58 PM
250px-Raelian_symbol.svg.png	6	Regular File	5/1/2019 12:15:32 PM
3-2-cartoon-free-png-image-thumb.png	28	Regular File	5/1/2019 12:18:58 PM
31154266_400x400.jpg	36	Regular File	5/1/2019 12:18:45 PM
520px-Biohazard_symbol_(blue).svg.png	27	Regular File	5/1/2019 12:15:27 PM
8fb16268171047d65e4600e544ffcbd6.jpg	38	Regular File	5/1/2019 12:17:15 PM
awen.gif	29	Regular File	5/1/2019 12:16:20 PM
BTarpnxpc.jpg	3,534	Regular File	5/1/2019 12:17:25 PM

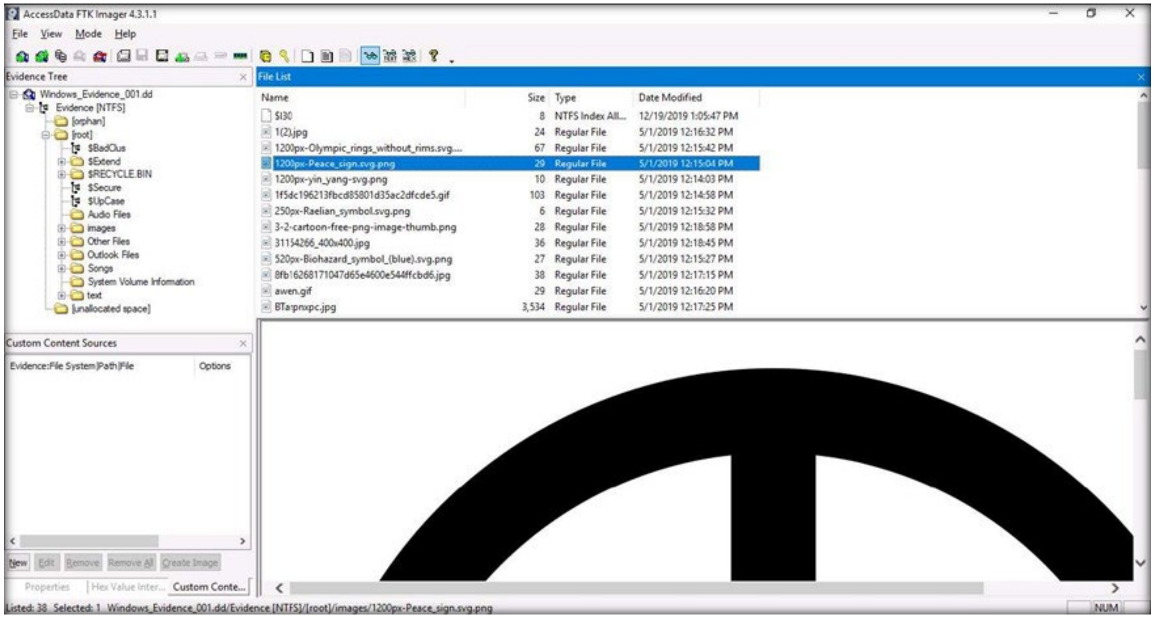
```
000  30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00  0...............
010  10 00 00 00 28 01 00 00-28 01 00 00 01 00 00 00  ....(...(.......
020  3E 00 00 00 00 00 01 00-00 01 E4 00 01 00 00 00  >..........ä....
030  30 00 00 00 00 00 01 00-94 7D BB 7D 52 B6 D5 01  0.......}»}R¶Õ.
040  5C 84 78 25 18 00 D5 01-DD 67 81 85 B4 00 D5 01  \.x%..Õ.Ýg..´.Õ.
050  DE B7 A6 04 6D B6 D5 01-00 90 00 00 00 00 00 00  Þ·¦.m¶Õ.........
060  AC 81 00 00 00 00 00 00-20 00 00 00 00 00 00 00  ¬....... .......
070  51 00 63 00 61 00 72 00-74 00 6F 00 6F 00 6E 00  Q.c.a.r.t.o.o.n.
080  2D 00 68 00 64 00 2D 00-70 00 6F 00 73 00 74 00  -.h.d.-.p.o.s.t.
090  65 00 72 00 2D 00 61 00-72 00 74 00 2D 00 70 00  e.r.-.a.r.t.-.p.
0a0  6E 00 63 00 61 00 6C 00-31 00 39 00 39 00 37 00  n.c.a.l.1.9.9.7.
0b0  35 00 2D 00 62 00 70 00-6E 00 63 00 61 00 6C 00  5.-.b.p.n.c.a.l.
0c0  31 00 39 00 39 00 37 00-35 00 2D 00 6C 00 61 00  1.9.9.7.5.-.l.a.
0d0  72 00 67 00 65 00 2D 00-6F 00 72 00 69 00 67 00  r.g.e.-.o.r.i.g.
0e0  69 00 6E 00 61 00 6C 00-2D 00 69 00 6D 00 61 00  i.n.a.l.-.i.m.a.
0f0  65 00 68 00 77 00 74 00-33 00 70 00 37 00 66 00  e.h.w.t.3.p.7.f.
100  6A 00 68 00 6E 00 37 00-64 00 2E 00 6A 00 70 00  j.h.n.7.d...j.p.
110  65 00 67 00 00 00 00 00-00 00 00 00 00 00 00 00  e.g.............
120  00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00  ................
130  01 00 00 00 00 00 00 00-                          ........
```

Cursor pos = 0

Listed: 38 Selected: 0 Windows_Evidence_001.dd/Evidence [NTFS]/[root]/images

10. Apart from viewing the contents of a file or folder, AccessData FTK Imager also lets you view the hex values of files. Hex values help determine the raw and exact contents of a file even if it has been deleted or overwritten. Hex values thus help you identify and retrieve information that normally cannot be accessed by the OS.
11. To view the Hex value of a file, select a file (here we selected 1200px-Peace_sign.svg.png) from the File List.

EXERCISE 6: VIEW CONTENTS OF FORENSIC IMAGE FILE

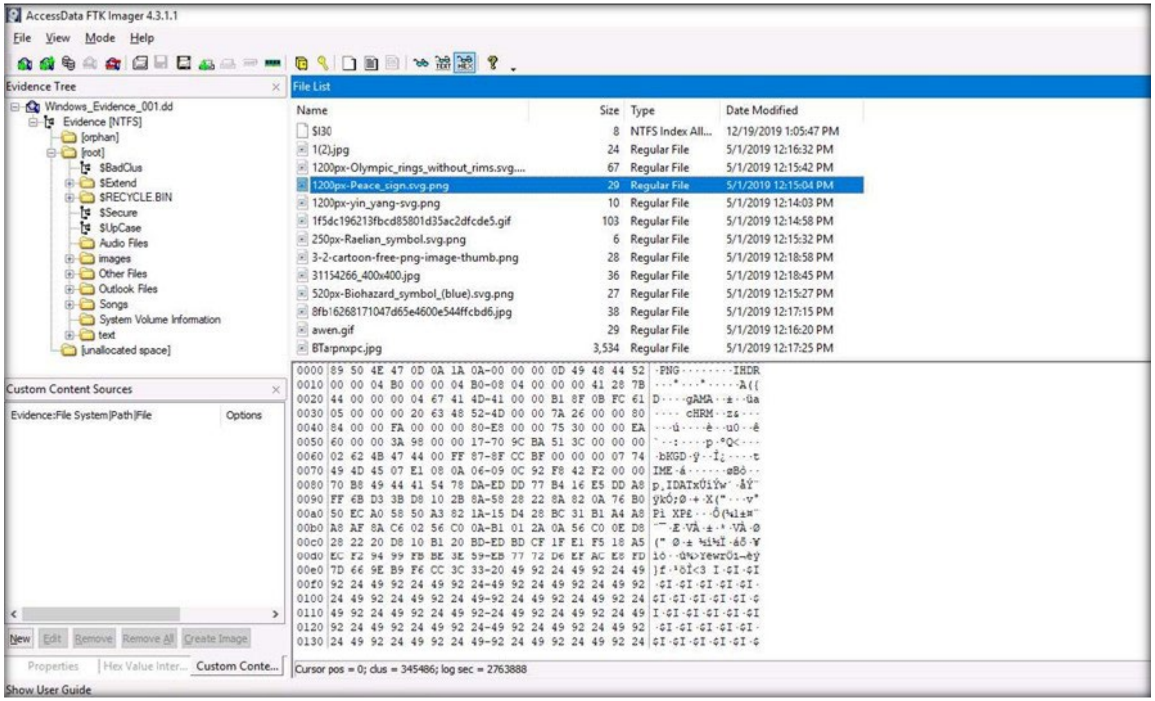


Name	Size	Type	Date Modified
$I30	8	NTFS Index All...	12/19/2019 1:05:47 PM
1(2).jpg	24	Regular File	5/1/2019 12:16:32 PM
1200px-Olympic_rings_without_rims.svg....	67	Regular File	5/1/2019 12:15:42 PM
1200px-Peace_sign.svg.png	29	Regular File	5/1/2019 12:15:04 PM
1200px-yin_yang-svg.png	10	Regular File	5/1/2019 12:14:03 PM
1f5dc196213fbcd85801d35ac2dfcde5.gif	103	Regular File	5/1/2019 12:14:58 PM
250px-Raelian_symbol.svg.png	6	Regular File	5/1/2019 12:15:32 PM
3-2-cartoon-free-png-image-thumb.png	28	Regular File	5/1/2019 12:18:58 PM
31154266_400x400.jpg	36	Regular File	5/1/2019 12:18:45 PM
520px-Biohazard_symbol_(blue).svg.png	27	Regular File	5/1/2019 12:15:27 PM
8fb16268171047d65e4600e544ffcbd6.jpg	38	Regular File	5/1/2019 12:17:15 PM
awen.gif	29	Regular File	5/1/2019 12:16:20 PM
BTa:pnxpc.jpg	3,534	Regular File	5/1/2019 12:17:25 PM

Listed: 38 Selected: 1 Windows_Evidence_001.dd/Evidence [NTFS]/[root]/images/1200px-Peace_sign.svg.png

EXERCISE 6: VIEW CONTENTS OF FORENSIC IMAGE FILE

12. Click the Hex icon on the toolbar and Hex values of the selected file will be displayed in the bottom-right pane.



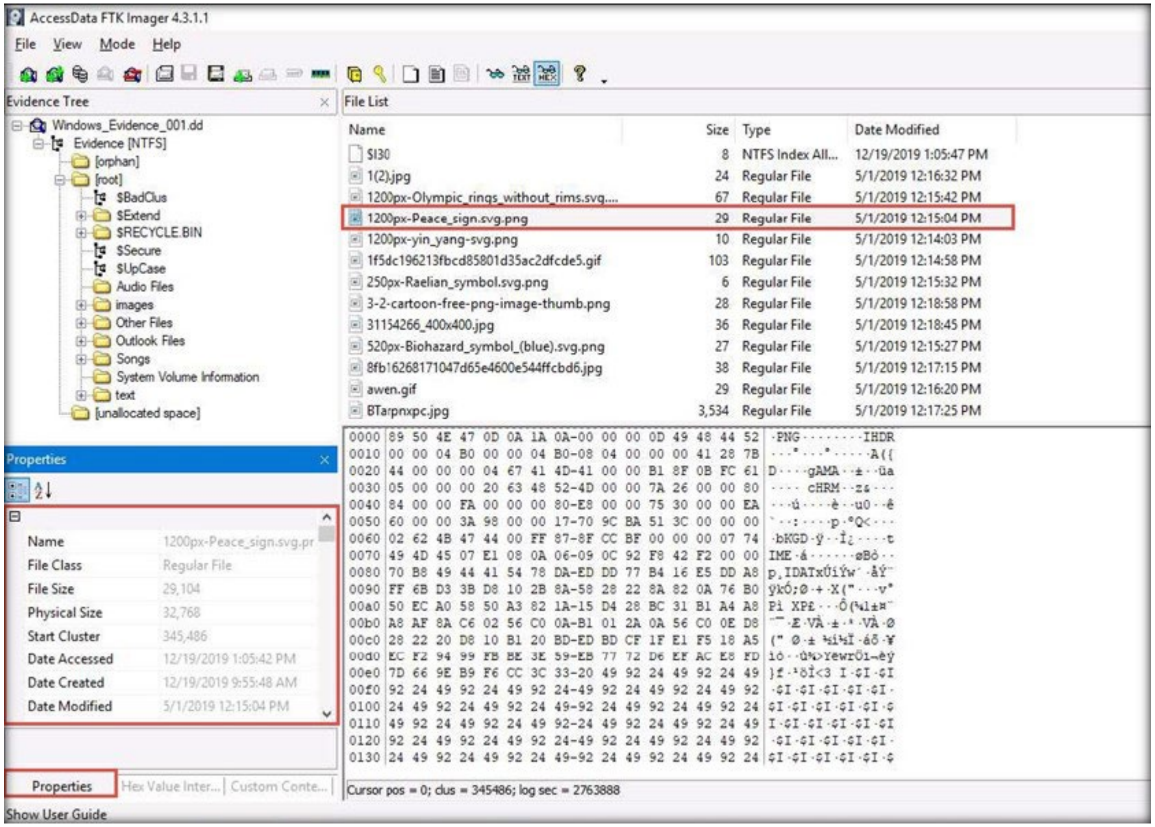
Name	Size	Type	Date Modified
$I30	8	NTFS Index All...	12/19/2019 1:05:47 PM
1(2).jpg	24	Regular File	5/1/2019 12:16:32 PM
1200px-Olympic_rings_without_rims.svg....	67	Regular File	5/1/2019 12:15:42 PM
1200px-Peace_sign.svg.png	29	Regular File	5/1/2019 12:15:04 PM
1200px-yin_yang-svg.png	10	Regular File	5/1/2019 12:14:03 PM
1f5dc196213fbcd85801d35ac2dfcde5.gif	103	Regular File	5/1/2019 12:14:58 PM
250px-Raelian_symbol.svg.png	6	Regular File	5/1/2019 12:15:32 PM
3-2-cartoon-free-png-image-thumb.png	28	Regular File	5/1/2019 12:18:58 PM
31154266_400x400.jpg	36	Regular File	5/1/2019 12:18:45 PM
520px-Biohazard_symbol_(blue).svg.png	27	Regular File	5/1/2019 12:15:27 PM
8fb16268171047d65e4600e544ffcbd6.jpg	38	Regular File	5/1/2019 12:17:15 PM
awen.gif	29	Regular File	5/1/2019 12:16:20 PM
BTarpnxpc.jpg	3,534	Regular File	5/1/2019 12:17:25 PM

```
0000 89 50 4E 47 0D 0A 1A 0A-00 00 00 0D 49 48 44 52  ·PNG········IHDR
0010 00 00 04 B0 00 00 04 B0-08 04 00 00 00 41 28 7B  ···°···°·····A({
0020 44 00 00 00 04 67 41 4D-41 00 00 B1 8F 0B FC 61  D····gAMA··±··üa
0030 05 00 00 00 20 63 48 52-4D 00 00 7A 26 00 00 80  ···· cHRM··z&···
0040 84 00 00 FA 00 00 00 80-E8 00 00 75 30 00 00 EA  ···ú····è··u0··ê
0050 60 00 00 3A 98 00 00 17-70 9C BA 51 3C 00 00 00  `··:····p·ºQ<···
0060 02 62 4B 47 44 00 FF 87-8F CC BF 00 00 00 07 74  ·bKGD·ÿ··Ì¿····t
0070 49 4D 45 07 E1 08 0A 06-09 0C 92 F8 42 F2 00 00  IME·á······øBò··
0080 70 B8 49 44 41 54 78 DA-ED DD 77 B4 16 E5 DD A8  p¸IDATxÚíÝw´·åÝ¨
0090 FF 6B D3 3B D8 10 2B 8A-58 28 22 8A 82 0A 76 B0  ÿkÓ;Ø·+·X("···v°
00a0 50 EC A0 58 50 A3 82 1A-15 D4 28 BC 31 B1 A4 A8  Pì XP£···Ô(¼1±¤¨
00b0 A8 AF 8A C6 02 56 C0 0A-B1 01 2A 0A 56 C0 0E D8  ¨¯·Æ·VÀ·±·*·VÀ·Ø
00c0 28 22 20 D8 10 B1 20 BD-ED BD CF 1F E1 F5 18 A5  (" Ø·± ½í½Ï·áõ·¥
00d0 EC F2 94 99 FB BE 3E 59-EB 77 72 D6 EF AC E8 FD  ìò··û¾>Yëwrÿï¬èý
00e0 7D 66 9E B9 F6 CC 3C 33-20 49 92 24 49 92 24 49  }f·¹öÌ<3 I·$I·$I
00f0 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92  ·$I·$I·$I·$I·$I·
0100 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24  $I·$I·$I·$I·$I·$
0110 49 92 24 49 92 24 49 92-24 49 92 24 49 92 24 49  I·$I·$I·$I·$I·$I
0120 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92  ·$I·$I·$I·$I·$I·
0130 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24  $I·$I·$I·$I·$I·$
```

Cursor pos = 0; clus = 345486; log sec = 2763888

13. Click the Properties tab in the lower-left pane to view the properties such as file class, size, date, start cluster, etc. of the selected file.

EXERCISE 6: VIEW CONTENTS OF FORENSIC IMAGE FILE



Windows_Evidence_001.dd
- Evidence [NTFS]
  - [orphan]
  - [root]
    - $BadClus
    - $Extend
    - $RECYCLE.BIN
    - $Secure
    - $UpCase
    - Audio Files
    - images
    - Other Files
    - Outlook Files
    - Songs
    - System Volume Information
    - text
  - [unallocated space]

Name	Size	Type	Date Modified
$I30	8	NTFS Index All...	12/19/2019 1:05:47 PM
1(2).jpg	24	Regular File	5/1/2019 12:16:32 PM
1200px-Olympic_rings_without_rims.svg....	67	Regular File	5/1/2019 12:15:42 PM
1200px-Peace_sign.svg.png	29	Regular File	5/1/2019 12:15:04 PM
1200px-yin_yang-svg.png	10	Regular File	5/1/2019 12:14:03 PM
1f5dc196213fbcd85801d35ac2dfcde5.gif	103	Regular File	5/1/2019 12:14:58 PM
250px-Raelian_symbol.svg.png	6	Regular File	5/1/2019 12:15:32 PM
3-2-cartoon-free-png-image-thumb.png	28	Regular File	5/1/2019 12:18:58 PM
31154266_400x400.jpg	36	Regular File	5/1/2019 12:18:45 PM
520px-Biohazard_symbol_(blue).svg.png	27	Regular File	5/1/2019 12:15:27 PM
8fb16268171047d65e4600e544ffcbd6.jpg	38	Regular File	5/1/2019 12:17:15 PM
awen.gif	29	Regular File	5/1/2019 12:16:20 PM
BTarpnxpc.jpg	3,534	Regular File	5/1/2019 12:17:25 PM

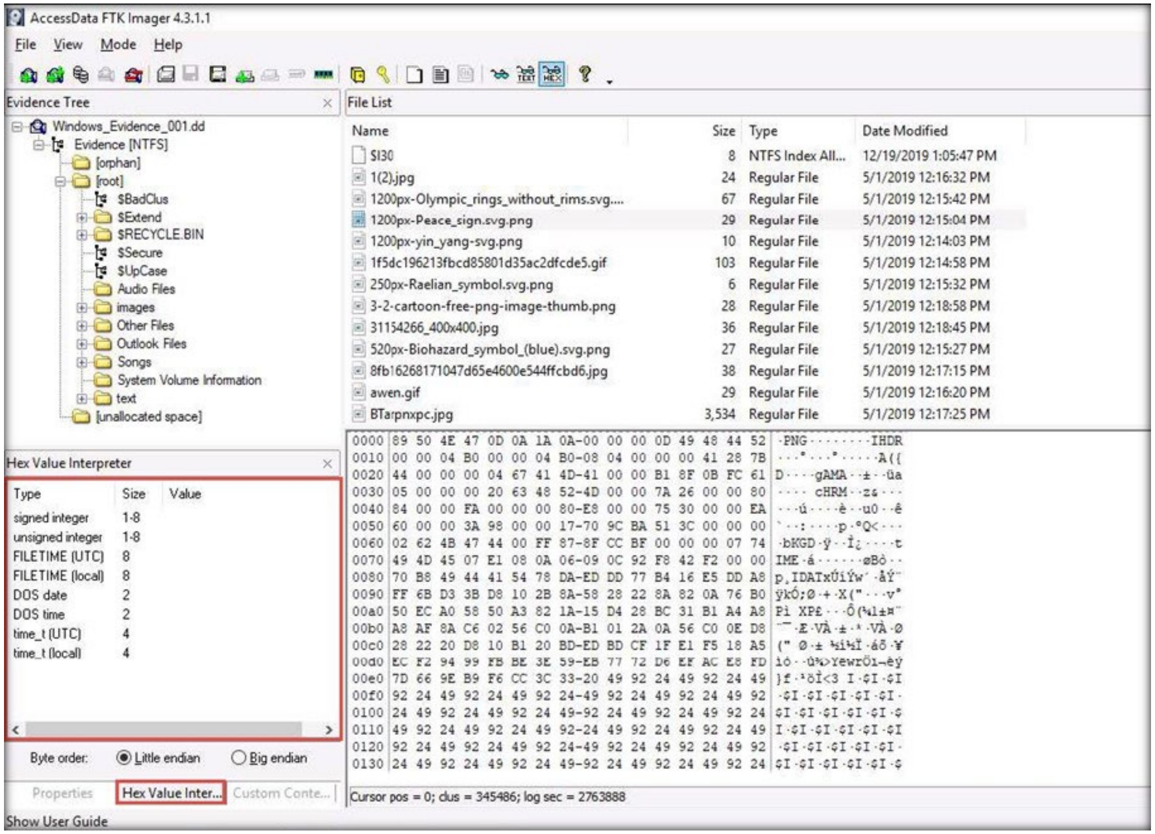
Name	1200px-Peace_sign.svg.pr
File Class	Regular File
File Size	29,104
Physical Size	32,768
Start Cluster	345,486
Date Accessed	12/19/2019 1:05:42 PM
Date Created	12/19/2019 9:55:48 AM
Date Modified	5/1/2019 12:15:04 PM

```
0000 89 50 4E 47 0D 0A 1A 0A-00 00 00 0D 49 48 44 52  ·PNG········IHDR
0010 00 00 04 B0 00 00 04 B0-08 04 00 00 00 41 28 7B  ···°···°·····A({
0020 44 00 00 00 04 67 41 4D-41 00 00 B1 8F 0B FC 61  D····gAMA··±··üa
0030 05 00 00 00 20 63 48 52-4D 00 00 7A 26 00 00 80  ···· cHRM··z&···
0040 84 00 00 FA 00 00 00 80-E8 00 00 75 30 00 00 EA  ···ú····è··u0··ê
0050 60 00 00 3A 98 00 00 17-70 9C BA 51 3C 00 00 00  `··:····p·ºQ<···
0060 02 62 4B 47 44 00 FF 87-8F CC BF 00 00 00 07 74  ·bKGD·ÿ··Ì¿····t
0070 49 4D 45 07 E1 08 0A 06-09 0C 92 F8 42 F2 00 00  IME·á·····øBò··
0080 70 B8 49 44 41 54 78 DA-ED DD 77 B4 16 E5 DD A8  p¸IDATxÚíÝw´·åÝ¨
0090 FF 6B D3 3B D8 10 2B 8A-58 28 22 8A 82 0A 76 B0  ÿkÓ;Ø·+·X("···v°
00a0 50 EC A0 58 50 A3 82 1A-15 D4 28 BC 31 B1 A4 A8  Pì XP£···Ô(¼1±¤¨
00b0 A8 AF 8A C6 02 56 C0 0A-B1 01 2A 0A 56 C0 0E D8  ¨¯·Æ·VÀ·±·*·VÀ·Ø
00c0 28 22 20 D8 10 B1 20 BD-ED BD CF 1F E1 F5 18 A5  (" Ø·± ½í½Ï·áõ·¥
00d0 EC F2 94 99 FB BE 3E 59-EB 77 72 D6 EF AC E8 FD  ìò··û¾>YëwrÖï¬èý
00e0 7D 66 9E B9 F6 CC 3C 33-20 49 92 24 49 92 24 49  }f·¹öÌ<3 I·$I·$I
00f0 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92  ·$I·$I·$I·$I·$I·
0100 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24  $I·$I·$I·$I·$I·$
0110 49 92 24 49 92 24 49 92-24 49 92 24 49 92 24 49  I·$I·$I·$I·$I·$I
0120 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92  ·$I·$I·$I·$I·$I·
0130 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24  $I·$I·$I·$I·$I·$
```

Cursor pos = 0; clus = 345486; log sec = 2763888

EXERCISE 6: VIEW CONTENTS OF FORENSIC IMAGE FILE

14. Click the Hex Value Interpreter tab in the lower-left pane to view the properties such as signed integer, DOS date, etc. of the selected file.



Name	Size	Type	Date Modified
$I30	8	NTFS Index All...	12/19/2019 1:05:47 PM
1(2).jpg	24	Regular File	5/1/2019 12:16:32 PM
1200px-Olympic_rings_without_rims.svg....	67	Regular File	5/1/2019 12:15:42 PM
1200px-Peace_sign.svg.png	29	Regular File	5/1/2019 12:15:04 PM
1200px-yin_yang-svg.png	10	Regular File	5/1/2019 12:14:03 PM
1f5dc196213fbcd85801d35ac2dfcde5.gif	103	Regular File	5/1/2019 12:14:58 PM
250px-Raelian_symbol.svg.png	6	Regular File	5/1/2019 12:15:32 PM
3-2-cartoon-free-png-image-thumb.png	28	Regular File	5/1/2019 12:18:58 PM
31154266_400x400.jpg	36	Regular File	5/1/2019 12:18:45 PM
520px-Biohazard_symbol_(blue).svg.png	27	Regular File	5/1/2019 12:15:27 PM
8fb16268171047d65e4600e544ffcbd6.jpg	38	Regular File	5/1/2019 12:17:15 PM
awen.gif	29	Regular File	5/1/2019 12:16:20 PM
BTarpnxpc.jpg	3,534	Regular File	5/1/2019 12:17:25 PM

```
0000 89 50 4E 47 0D 0A 1A 0A-00 00 00 0D 49 48 44 52 ·PNG········IHDR
0010 00 00 04 B0 00 00 04 B0-08 04 00 00 00 41 28 7B ···°···°·····A({
0020 44 00 00 00 04 67 41 4D-41 00 00 B1 8F 0B FC 61 D····gAMA··±··üa
0030 05 00 00 00 20 63 48 52-4D 00 00 7A 26 00 00 80 ···· cHRM··z&···
0040 84 00 00 FA 00 00 00 80-E8 00 00 75 30 00 00 EA ···ú····è··u0··ê
0050 60 00 00 3A 98 00 00 17-70 9C BA 51 3C 00 00 00 `··:····p·ºQ<···
0060 02 62 4B 47 44 00 FF 87-8F CC BF 00 00 00 07 74 ·bKGD·ÿ··Ì¿····t
0070 49 4D 45 07 E1 08 0A 06-09 0C 92 F8 42 F2 00 00 IME·á······øBò··
0080 70 B8 49 44 41 54 78 DA-ED DD 77 B4 16 E5 DD A8 p¸IDATxÚíÝw´·åÝ¨
0090 FF 6B D3 3B D8 10 2B 8A-58 28 22 8A 82 0A 76 B0 ÿkÓ;Ø·+·X("···v°
00a0 50 EC A0 58 50 A3 82 1A-15 D4 28 BC 31 B1 A4 A8 Pì XP£···Ô(¼1±¤¨
00b0 A8 AF 8A C6 02 56 C0 0A-B1 01 2A 0A 56 C0 0E D8 ¨¯·Æ·VÀ·±·*·VÀ·Ø
00c0 28 22 20 D8 10 B1 20 BD-ED BD CF 1F E1 F5 18 A5 (" Ø·± ½í½Ï·áõ·¥
00d0 EC F2 94 99 FB BE 3E 59-EB 77 72 D6 EF AC E8 FD ìò··û¾>YëwrÖï¬èý
00e0 7D 66 9E B9 F6 CC 3C 33-20 49 92 24 49 92 24 49 }f·¹öÌ<3 I·$I·$I
00f0 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92 ·$I·$I·$I·$I·$I·
0100 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24 $I·$I·$I·$I·$I·$
0110 49 92 24 49 92 24 49 92-24 49 92 24 49 92 24 49 I·$I·$I·$I·$I·$I
0120 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92 ·$I·$I·$I·$I·$I·
0130 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24 $I·$I·$I·$I·$I·$
```

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Byte order: ● Little endian ○ Big endian

Cursor pos = 0; clus = 345486; log sec = 2763888

15. In this manner, you can examine the contents of the forensic image file using AccessData FTK Imager tool.
16. This concludes the demonstration of showing how to view contents of forensic image file.
17. Close all open windows.
18. Turn off Admin Machine-1, AD Domain Controller and PfSense Firewall virtual machines.

EXERCISE 6:

VIEW CONTENTS OF FORENSIC IMAGE FILE

EC-Council