



LAB MANUAL
OF
“INCIDENT RESPONSE AND DIGITAL FORENSICS”

Submitted To

National Forensic Sciences University



In

CYBER SECURITY

Submitted By

Dhavalkumar Vijaykumar Patel

(032200300002034)

Under the Supervision of

Dr. Kashinath Chandelkar

**National Forensic Sciences University,
Goa Campus, Ponda, Goa - 403401.**

July, 2023

TABLE OF CONTENTS

Experiment No.	Name of Experience	Page
1	Analysis and monitor system log using event viewer	1
2	Installation and Demonstration of System Internal Tool (Process Explorer) for Data Classification by Process ID and Company Name	5
3	With the help of disk monitoring identify the read and write process having length>5.	8
4	Installation and demonstration of sawmill on windows OS. Generate a custom report.	17
5	Installation and Configuration of Snort for Network Security and Protection against Cyber Threats	22
6	Install and demonstrate Splunk for log analysis	29
7	Use Autopsy to recover file from the given data source. Present your details accordingly	32
8	Install cyber triage and collect the given system report. Analyse your data accordingly	41
9	Perform digital forensics to analyse RAM timeline using CAINE tool	45
10	Install Wireshark to analyse captured packet. Discuss your results obtained from the tool.	48
11	Examine files, folders on local hard disk and network drive using FTK Imager	51
12	Install Tally software and create a company. Add sufficient data. After modifications, analyze the windows registry to identify evidence related to the company.	55
13	Install fedora workstation using virtual environment to demonstrate working of open source-based platform	57
14	Use USB drive as data source and Belkasoft X to demonstrate data / file carving	60
15	Use PhotoRec to recover lost files, audio or video content from the HDD/USB Drive using file carving	62

Experiment: 1

Title: Analysis and monitor system log using event viewer

Requirement: Event Viewer

Procedure/experiment steps:

- Open Event Viewer : Start > event viewer
- In general we can see information in a middle Panel as
 - Summary of administrative event
 - Event type
 - Critical
 - Error
 - Warning
 - Information
 - Audit Success
 - Audit Failure
 - Event id
 - Source
 - Log
 - Last hour
 - 24 hour
 - 7days
 - Recently View Nods
 - Log summary
 - Log name
 - Size
 - Modified
 - Enable
 - Retention policy
- There is different log type in the left Panel
 - Custom
 - Windows Log
 - Application and Service logs
 - Subscription
- Select and view different logs
- Select any section and sub section and see the different logs and what this log contains

Result:

Event Viewer (Local)

File Action View Help

Event Viewer (Local)

Custom Views

Administrative Events

Summary page events

Windows Logs

- Application
- Security
- Setup
- System
- Forwarded Events

Applications and Services Logs

- Hardware Events
- HP Analytics
- Intel
- Internet Explorer
- Key Management Service
- Microsoft
- Microsoft Office Alerts
- OneApp_IGCC
- OpenSSH
- Windows PowerShell

Subscriptions

Event Viewer (Local)

Overview and Summary

Last refreshed: 04-05-2023 16:00:00

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

Overview

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	0	25	1
Error	-	-	-	6	25	266
Warning	-	-	-	11	135	766
Information	-	-	-	273	2,373	10,099
Audit Success	-	-	-	950	6,416	28,120
Audit Failure	-	-	-	0	2	5

Recently Viewed Nodes

Name	Description	Modified	Created
Windows Logs\Application	N/A	04-05-2023 16:15:53	01-05-2023 16:07:18
Windows Logs\Security	N/A	04-05-2023 16:10:41	01-05-2023 16:07:18
Windows Logs\Setup	N/A	03-05-2023 08:59:18	01-05-2023 16:07:18
Custom Views\Administrative	Critical, Err...	N/A	N/A
Applications and Services ..	N/A	04-05-2023 16:00:41	01-05-2023 16:07:18
Windows Logs\System	N/A	04-05-2023 16:01:32	01-05-2023 16:07:18

Log Summary

Log Name	Size (Current)	Modified	Enabled	Retention Policy
Windows PowerShell	1.07 MB/1...	04-05-2023 15:53:16	Enabled	Overwrite events as nece...
System	2.07 MB/2...	04-05-2023 15:53:18	Enabled	Overwrite events as nece...
Security	19.07 MB/...	04-05-2023 15:58:35	Enabled	Overwrite events as nece...
OneApp_IGCC	68 KB/100...	04-05-2023 15:38:02	Enabled	Overwrite events as nece...
Microsoft Office Alerts	68 KB/100...	04-05-2023 15:58:34	Enabled	Overwrite events as nece...
Key Management Service	68 KB/20 ...	01-05-2023 16:12:09	Enabled	Overwrite events as nece...

Event Viewer (Local)

Custom Views

Administrative Events

Summary page events

Windows Logs

- Application
- Security
- Setup
- System
- Forwarded Events

Applications and Services Logs

- Hardware Events
- HP Analytics
- Intel
- Internet Explorer
- Key Management Service
- Microsoft
- Microsoft Office Alerts
- OneApp_IGCC
- OpenSSH
- Windows PowerShell

Subscriptions

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event logs categorized by source: Custom Views, Windows Logs (Application, Security, Setup, System, Forwarded Events), Applications and Services Logs (Hardware Events, HP Analytics, Intel, Internet Explorer, Key Management Service, Microsoft, Microsoft Office Alerts, OneApp_JGCC, OpenSSH, Windows PowerShell), and Subscriptions. The right pane shows a detailed list of events from the Windows PowerShell log, with 668 total events. A specific event (Event ID 400) is selected, and its details are shown in a modal window.

Windows PowerShell Number of events: 668

Level	Date and Time	Source	Event ID	Task Category
Information	04-05-2023 15:52:48	PowerShell (PowerShell)	403	Engine Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	400	Engine Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	403	Engine Lifecycle
Information	04-05-2023 15:52:47	PowerShell (PowerShell)	400	Engine Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	400	Engine Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:52:46	PowerShell (PowerShell)	403	Engine Lifecycle
Information	04-05-2023 15:29:43	PowerShell (PowerShell)	400	Engine Lifecycle
Information	04-05-2023 15:29:43	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:29:43	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:29:43	PowerShell (PowerShell)	600	Provider Lifecycle
Information	04-05-2023 15:29:43	DnsServer (DnsServer)	600	Provider Lifecycle

Event 400, PowerShell (PowerShell)

General Details

Engine state is changed from None to Available.

Details:

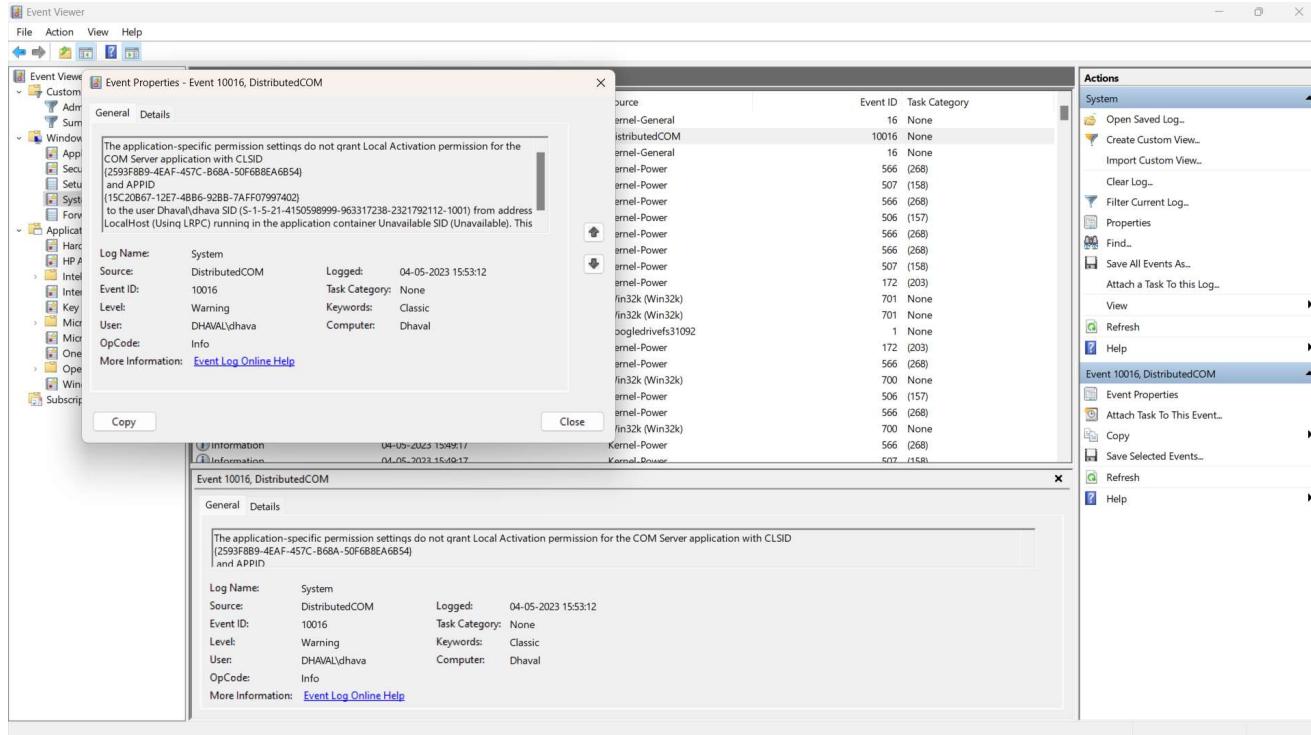
Log Name:	Windows PowerShell
Source:	PowerShell (PowerShell)
Event ID:	400
Level:	Information
User:	N/A
OpCode:	Info
More Information:	Event Log Online Help

Actions

- Open Saved Log...
- Create Custom View...
- Import Custom Log...
- Clear Log...
- Filter Current Log...
- Find...
- Save All Events As...
- Attach a Task To This Log...
- View
- Refresh
- Help

Event 400, PowerShell (PowerShell)

- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help



Result analysis:

Summary of Administrative Events				
Event Type	Last Hour	24 hour	7 days	
Critical	0	0	1	
Error	6	25	266	
Warning	11	135	766	
Information	273	2373	10099	
Audit Success	950	6416	28120	
Audit Failure	0	2	5	

Conclusion:

- With event view we can see different events that workers in our system. With the help of event view we can also see a different logs in the specific groups and specific filter work we can see what lock contains and the information which is passed through it.

Future scope:

- Even if you can use by your system administrator or by the security person To check what kind of event occur in the system to prevent if there is any suspicious event is there and protect the system. We can also see a warning and error the logs like bonding logs error logs informational logs then audit logs.

Experiment : 2

Title: Installation and Demonstration of System Internal Tool (Process Explorer) for Data Classification by Process ID and Company Name

Objective:

The objective of this experiment is to install and demonstrate the usage of the System Internal Tool called Process Explorer. Additionally, we aim to classify data using process ID and company name information obtained from Process Explorer.

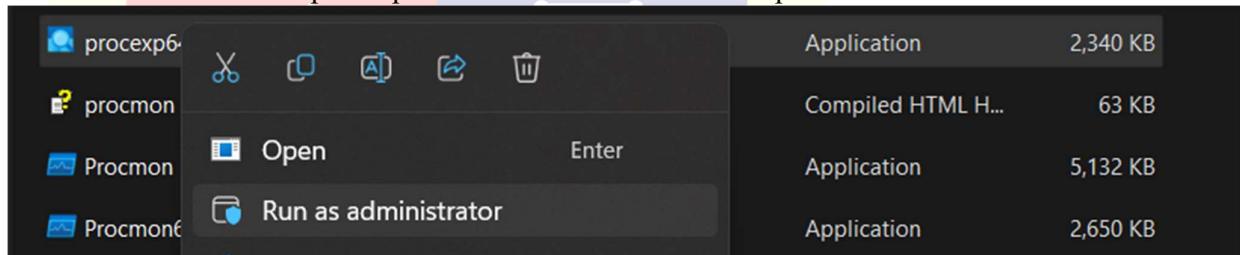
Requirements:

Sysinternal suite

Procedure/Experiment Steps:

1. Download Process Explorer:
 - a. Open a web browser.
 - b. Visit the official Microsoft website.
 - c. Search for "Process Explorer" or Sysinternal suite and navigate to the official download page.
 - d. Download the appropriate version that compatible with your Windows operating system.
 - e. Save the downloaded file.

2. Launch Process Explorer:
 - a. Navigate to the installation location of Process Explorer.
 - b. Double-click on the "procexp.exe" file to launch Process Explorer.



- c. It will ask for the installation for the first time only.

3. Explore Process Explorer Interface:
 - a. The Process Explorer interface, which provides a comprehensive view of running processes on your system.
 - b. Observe the various columns displayed, including process name, process ID, company name, CPU usage, memory usage, etc.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp.	188 K	30,828 K	108		
Registry		9,064 K	56,728 K	144		
System Idle Process	97.08	60 K	8 K	0		
System	0.37	60 K	124 K	4	n/a Hardware Interrupts and DPCs	
Interrupts	0.18	0 K	0 K			
mms.exe		1,116 K	1,040 K	552		
Memory Compression	< 0.01	1,396 K	1,03,632 K	4152		
cscs.exe		2,344 K	5,448 K	1004		
wireshark.exe		1,650 K	5,728 K	936		
services.exe	< 0.01	6,356 K	10,000 K	1008		
syshost.exe	< 0.01	19,264 K	68,824 K	1,248	Host Process for Windows S.	Microsoft Corporation
WmiPrvSE.exe		11,284 K	23,352 K	5216	WMI Provider Host	Microsoft Corporation
unscapp.exe		1,576 K	7,860 K	5,520	Sink to receive asynchronous.	Microsoft Corporation
SearchHost.exe	Susp...	1,90,004 K	11,952 K	10,620		
StartMenuExperienceHo...		51,964 K	86,308 K	10,564	Windows Start Experience H.	Microsoft Corporation
Widgets.exe		5,176 K	36,636 K	20996		
RuntimeBroker.exe		6,612 K	23,056 K	15,648	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		16,520 K	54,424 K	10,164	Runtime Broker	Microsoft Corporation
dhhost.exe		6,340 K	15,972 K	13,968	COM Surrogate	Microsoft Corporation
WidgetService.exe		4,620 K	22,728 K	7448		
TextinputHost.exe	< 0.01	3,60,980 K	3,59,528 K	20,888		
ShellExperienceHost.exe	Susp...	35,656 K	65,424 K	11,172	Windows Shell Experience H.	Microsoft Corporation
RuntimeBroker.exe		3,560 K	18,860 K	16,572	Runtime Broker	Microsoft Corporation
unscapp.exe		1,680 K	8,900 K	13,684	Sink to receive asynchronous.	Microsoft Corporation
SpotifyWidgetProvider.e...		10,816 K	29,372 K	17,196		
AcrobatNotificationClient...	Susp...	15,516 K	4,560 K	4,776		
RuntimeBroker.exe		1,304 K	7,616 K	18,792	Runtime Broker	Microsoft Corporation
SystemSettingsHost.exe	Susp...	59,920 K	3,952 K	15,344	Settings	Microsoft Corporation
ApplicationFrameHost.e...		17,980 K	39,520 K	13,868	Application Frame Host	Microsoft Corporation
UserOOBEBroker.exe		2,100 K	9,796 K	17,680	User OOBE Broker	Microsoft Corporation
SDXHelper.exe	< 0.01	11,512 K	22,984 K	16,636	Microsoft Office SDX Helper	Microsoft Corporation
WhatsApp.exe	< 0.01	1,40,516 K	2,01,604 K	20,056		
RuntimeBroker.exe		8,972 K	32,868 K	7,488	Runtime Broker	Microsoft Corporation
dhhost.exe		1,428 K	9,560 K	20,296	COM Surrogate	Microsoft Corporation
smartscreen.exe		5,056 K	21,120 K	19,012	Windows Defender SmartScr.	Microsoft Corporation
WmiPrvSE.exe		3,924 K	11,768 K	18,260	WMI Provider Host	Microsoft Corporation
WUDFHost.exe		14,680 K	24,536 K	1,232	Windows Driver Foundation	Microsoft Corporation
svchost.exe	< 0.01	13,812 K	25,200 K	1,424	Host Process for Windows S.	Microsoft Corporation
svchost.exe		3,864 K	10,388 K	4,76	Host Process for Windows S.	Microsoft Corporation
svchost.exe		1,880 K	5,252 K	657	Host Process for Windows S.	Microsoft Corporation
svchost.exe		3,467 K	8,648 K	1,932	Host Process for Windows S.	Microsoft Corporation
svchost.exe		6,128 K	11,088 K	1,654	Host Process for Windows S.	Microsoft Corporation
svchost.exe		3,936 K	14,784 K	1,824	Host Process for Windows S.	Microsoft Corporation
svchost.exe		3,690 K	15,404 K	1,828	Host Process for Windows S.	Microsoft Corporation
DropboxUpdate.exe		2,176 K	10,716 K	2,516	Dropbox Update	Dropbox Inc.
taskhost.exe		9,984 K	21,916 K	6,624	Host Process for Windows T.	Microsoft Corporation
SystemOptimizer.exe	< 0.01	43,580 K	25,276 K	16,872	HP Open SystemOptimizer	HP Inc.

4. Data Classification by Process ID:

- Identify the process ID (PID) column in Process Explorer.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Interrupts	0.19	0 K	0 K		n/a Hardware Interrupts and DPCs	
System Idle Process	94.74	60 K	8 K	0		
System	0.37	60 K	124 K	4		
Secure System	Susp...	188 K	30,828 K	108		

- Analyse the PID values associated with different processes.

- Classify or categorize the data based on the process IDs. For example, you can group processes by their PID ranges or assign specific actions based on PID values.

5. Data Classification by Company Name:

- Identify the company name column in Process Explorer.

Company Name
Adobe Systems Incorporated
Microsoft Corporation
Microsoft Corporation
HP Inc.
Microsoft Corporation
Adobe Inc.
Microsoft Corporation
Microsoft Corporation
Microsoft Corporation
BraveSoftware Inc.
BraveSoftware Inc.
Microsoft Corporation
Microsoft Corporation
Microsoft Corporation

- b. Analyse the company names associated with different processes.
- c. Classify or categorize the data based on the company names. For example, you can group processes by the company name or apply specific policies based on the company's reputation.

Result:

The obtained results from Process Explorer allow for efficient data classification based on process ID and company name. By grouping processes using process ID or company name, you can gain insights into system activity and make informed decisions regarding resource allocation, security policies, and more.

Conclusion:

In conclusion process Explorer is a powerful tool for monitoring and managing processes on a Windows system. The ability to classify data based on process ID and company name and other parameter enhances process analysis and decision-making capabilities, contributing to improved system performance and security.

Future Scope:

- 1. Further research and experimentation can explore additional criteria for data classification, such as process hierarchy, resource utilization, or network activity.
- 2. Integration of Process Explorer data with other security tools or automation scripts can enhance system monitoring and incident response capabilities.
- 3. Investigating process anomalies or suspicious behaviour abased on process ID and company name can lead to the development of advanced threat detection techniques.
- 4. Continual updates and enhancements to Process Explorer by Microsoft may introduce new features and functionalities for data classification and analysis.

Experiment : 3

Title: With the help of disk monitoring identify the read and write process having length>5.

Objective:

The objective of this project is to utilize disk monitoring software to identify read and write processes that have a length greater than 5. By analyzing the data collected through disk monitoring, we aim to identify processes with significant read and write operations on the disk.

Requirements:

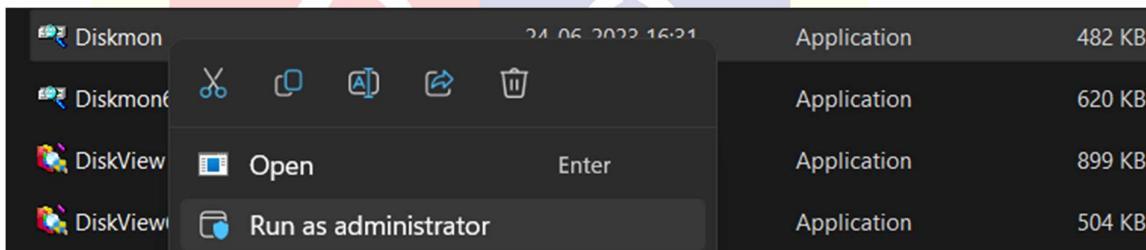
Sysinternal suite
Diskmon.exe

NFSU

Procedure/Experiment Steps:

1. Download Disk Monitor:
 - a. Open a web browser.
 - b. Visit the official Microsoft website.
 - c. Search for "Disk Monitor" or Sysinternal suite and navigate to the official download page.
 - d. Download the appropriate version that compatible with your Windows operating system.
 - e. Save the downloaded file.

2. Launch Disk Monitor:
 - a. Navigate to the installation location of Disk Monitor.
 - b. Double-click on the "Diskmon.exe" file to launch Disk Monitor.



- c. It will ask for the installation for the first time only.

3. Explore Disk Monitor Interface:

a. The Disk Monitor interface

Disk Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

#	Time	Duration (s)	Disk	Request	Sector	Length
6132	89.537536	0.0000000	1	Read	56028971	32
6133	89.537715	0.0000000	1	Read	56028959	32
6134	89.537714	0.0000000	1	Read	56028959	32
6135	89.536086	0.0000000	1	Read	56028257	32
6136	89.538854	0.0000000	1	Read	37744762	64
6137	89.540410	0.0000000	1	Read	30234308	128
6138	89.540928	0.0000000	1	Read	57114644	32
6139	89.541917	0.0000000	1	Read	20516428	48
6140	89.543763	0.0000000	1	Read	51200823	27
6141	89.543981	0.0000000	1	Read	51200763	32
6142	89.544230	0.0000000	1	Read	51200751	32
6143	89.544435	0.0000000	1	Read	51200687	32
6144	89.544595	0.0000000	1	Read	51200719	32
6145	89.544762	0.0000000	1	Read	51200447	32
6146	89.545045	0.0000000	1	Read	51200813	8
6147	89.545046	0.0000000	1	Read	51200843	32
6148	89.545216	0.0000000	1	Read	20517544	32
6149	89.545305	0.0000000	1	Read	51119952	64
6150	89.545875	0.0000000	1	Read	51119950	64
6151	89.546174	0.0000000	1	Read	57143560	64
6152	89.546400	0.0000000	1	Read	57143230	64
6153	89.546424	0.0000000	1	Read	20000144	64
6154	89.546474	0.0000000	1	Read	22603280	8
6155	89.546492	0.0000000	1	Read	50839544	8
6156	89.547799	0.0000000	1	Read	56741768	64
6157	89.547829	0.0000000	1	Read	23277152	64
6158	89.547749	0.0000000	1	Read	56741832	31
6159	89.548670	0.0000000	1	Read	23277162	8
6160	89.548694	0.0000000	1	Read	99314176	32
6161	89.550093	0.0000000	1	Read	99314144	32
6162	89.550285	0.0000000	1	Read	99314096	32
6163	89.555130	0.0000000	1	Read	20517646	24
6164	89.565338	0.0000000	1	Read	205159976	64
6165	89.565777	0.0000000	1	Read	205163744	64
6166	89.573747	0.0000000	1	Read	25049462	8
6167	89.588275	0.0000000	1	Read	51886856	56
6168	89.592518	0.0000000	1	Read	32482144	64
6169	89.597950	0.0000000	1	Read	95034216	56
6170	89.598033	0.0000000	1	Read	95034176	16
6171	90.317274	0.0000000	1	Write	62956444	8
6172	90.317312	0.0000000	1	Write	134750548	114
6173	90.317344	0.0000000	1	Write	918032	8
6174	90.658610	0.0000000	1	Read	55099448	64
6175	91.673331	0.0000000	1	Write	277346240	92
6176	91.673331	0.0000000	1	Write	134750560	96
6177	91.673338	0.0000000	1	Write	277346112	128
6178	91.673338	0.0000000	1	Write	567328	40
6179	91.673350	0.0000000	1	Write	62956444	9

- b. It automatic start capture the logs and data
- c. Go to file and click on capture Event or Press CTRL + E to stop

Disk Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

Save Ctrl+S

Save As...

Capture Events Ctrl+E

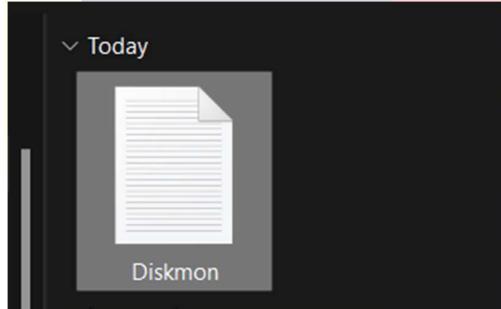
Exit

Disk	Request	Sector	Length
1	Write	5283352	16
1	Write	670200	32
1	Write	567336	40
1	Write	136438464	2
1	Write	950944	8
1	Write	3557064	128
1	Write	567496	8
1	Write	3557064	8
1	Write	567368	16
1	Write	22978608	8
1	Write	22978632	8

d. As we can see here all event in Read and write mode

#	Time	Durati...	Disk	Request	Sector	Length
182	16.836802	0.00000...	1	Write	53680296	7
183	18.196709	0.00000...	1	Write	53680296	11
184	19.552763	0.00000...	1	Write	53680472	2
185	19.552765	0.00000...	1	Write	567464	16
186	19.553026	0.00000...	1	Write	42435088	2
187	19.553061	0.00000...	1	Write	42233960	5
188	19.809072	0.00000...	1	Write	567344	16
189	19.811515	0.00000...	1	Write	51168072	8
190	20.922979	0.00000...	1	Write	53680304	4
191	21.389277	0.00000...	1	Read	3015256	24
192	22.286477	0.00000...	1	Write	62956512	5
193	22.286578	0.00000...	1	Write	53680472	4
194	23.653688	0.00000...	1	Write	5283304	48
195	23.653688	0.00000...	1	Write	567480	16
196	23.653840	0.00000...	1	Write	42233960	5
197	23.653878	0.00000...	1	Write	42435088	2
198	24.821141	0.00000...	1	Write	669144	144
199	24.821256	0.00000...	1	Write	567336	8
200	24.821278	0.00000...	1	Write	567328	8
201	25.006542	0.00000...	1	Write	53680472	6
202	25.006557	0.00000...	1	Write	68004986	2
203	25.006585	0.00000...	1	Write	65374658	67
204	25.682584	0.00000...	1	Read	203876802	40
205	25.683704	0.00000...	1	Read	209996563	32
206	26.373570	0.00000...	1	Write	53680304	6
207	27.733488	0.00000...	1	Write	567464	16
208	27.734502	0.00000...	1	Write	13557200	8
209	27.734512	0.00000...	1	Write	50775192	16
210	27.734656	0.00000...	1	Write	51083096	8
211	27.734736	0.00000...	1	Write	50775216	8
212	27.734762	0.00000...	1	Write	2452520	8
213	27.734781	0.00000...	1	Write	142430880	11
214	27.734816	0.00000...	1	Write	51083504	8
215	27.734835	0.00000...	1	Write	2452488	8
216	27.734848	0.00000...	1	Write	50775344	8
217	27.734909	0.00000...	1	Write	142430872	8
218	27.734941	0.00000...	1	Write	51083680	16
219	27.734963	0.00000...	1	Write	50775392	8
220	27.734979	0.00000...	1	Write	103287976	8
221	27.734989	0.00000...	1	Write	10886568	8
222	27.735011	0.00000...	1	Write	51084256	16
223	27.735027	0.00000...	1	Write	50775440	16
224	27.735046	0.00000...	1	Write	1084208	8
225	27.735059	0.00000...	1	Write	7673024	8
226	27.735107	0.00000...	1	Write	50775520	8
227	27.735114	0.00000...	1	Write	51084288	32
228	27.735114	0.00000...	1	Write	1645528	8
229	27.735130	0.00000...	1	Write	7673104	8

- e. We can see Time, Duration, Disk, Request, Sector, Length
f. Save the log file



- g. Locket the file copy the data

```

Diskmon
File Edit View
0 0.110624 0.00000000 1 Read 302102536 128
1 0.111160 0.00000000 1 Read 302102727 128
2 0.139893 0.00000000 1 Read 302359464 128
3 0.223553 0.00000000 1 Read 302479400 128
4 0.630641 0.00000000 0 Write 8198080 8
5 1.096052 0.00000000 1 Write 207524912 6
6 1.096052 0.00000000 1 Write 2444336 72
7 1.096070 0.00000000 1 Write 200589176 6
8 1.096120 0.00000000 1 Write 18187576 6
9 1.096155 0.00000000 1 Write 192641616 16
10 1.096432 0.00000000 1 Write 9451612 109
11 1.096512 0.00000000 1 Write 1185640 32
12 1.096584 0.00000000 1 Write 180850456 7
13 1.096650 0.00000000 1 Write 54396184 8
14 1.096688 0.00000000 1 Write 54572168 1
15 1.096761 0.00000000 1 Write 7820000 8
16 1.985192 0.00000000 0 Write 8198080 8
17 2.132952 0.00000000 1 Write 567504 24
18 2.134451 0.00000000 1 Write 567392 8
19 2.135656 0.00000000 1 Write 567520 8
20 2.398677 0.00000000 1 Write 567392 16
21 2.400535 0.00000000 1 Write 567528 16
22 2.401806 0.00000000 1 Write 567408 16
23 2.467212 0.00000000 1 Write 1118560 12
24 2.467216 0.00000000 1 Write 64804328 7
25 2.467222 0.00000000 1 Write 207524912 11
26 2.467235 0.00000000 1 Write 749456 13
27 2.552604 0.00000000 1 Write 567544 32
28 3.351000 0.00000000 0 Write 6102944 16
29 3.439904 0.00000000 0 Write 6298912 8
30 3.439904 0.00000000 0 Write 6335208 8
31 3.835428 0.00000000 1 Write 680850456 6
32 3.835428 0.00000000 1 Write 180850456 7
33 3.835448 0.00000000 1 Write 2465776 16
34 3.835456 0.00000000 1 Write 567440 16
35 3.835467 0.00000000 1 Write 4244564 17
36 4.206428 0.00000000 1 Write 142959648 32
37 4.206750 0.00000000 1 Write 567576 16
38 4.209224 0.00000000 1 Write 142959648 8
39 4.209417 0.00000000 1 Write 567456 8
40 4.210722 0.00000000 1 Write 22978608 8
41 4.210904 0.00000000 1 Write 277363880 8
42 4.211018 0.00000000 1 Write 21604674 8

```

h. open in excel

	A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	0	0.110624	0	1	Read	3.02E+08	128														
2	1	0.11116	0	1	Read	3.02E+08	128														
3	2	0.139893	0	1	Read	3.02E+08	128														
4	3	0.223553	0	1	Read	3.02E+08	128														
5	4	0.630641	0	0	Write	8198080	8														
6	5	1.096052	0	1	Write	2.08E+08	6														
7	6	1.096052	0	1	Write	2444336	72														
8	7	1.09607	0	1	Write	2.01E+08	6														
9	8	1.09612	0	1	Write	18187576	6														
10	9	1.096155	0	1	Write	1.92E+08	16														
11	10	1.096432	0	1	Write	9451612	109														
12	11	1.096512	0	1	Write	567352	32														
13	12	1.096584	0	1	Write	1.89E+08	7														
14	13	1.09665	0	1	Write	54396184	8														
15	14	1.096688	0	1	Write	54572168	1														
16	15	1.096761	0	1	Write	7820000	8														
17	16	1.985192	0	0	Write	8198080	8														
18	17	2.132952	0	1	Write	567504	24														
19	18	2.134451	0	1	Write	567392	8														
20	19	2.135656	0	1	Write	567520	8														
21	20	2.398677	0	1	Write	567392	16														
22	21	2.400535	0	1	Write	567528	16														
23	22	2.401806	0	1	Write	567408	16														
24	23	2.467212	0	1	Write	1118560	12														
25	24	2.467216	0	1	Write	64804328	7														
26	25	2.467222	0	1	Write	2.08E+08	11														
27	26	2.467235	0	1	Write	749456	13														
28	27	2.552604	0	1	Write	567544	32														
29	28	3.351	0	0	Write	6102944	16														
30	29	3.439094	0	0	Write	6298912	8														
31	30	3.439904	0	0	Write	6335200	8														

i. Analyze the result

Result:

- Read and Write Process with length >5.

#	Time	Duration	Disk	Request	Sector	Length
85	24.997138	0	1	Write	64804568	7
1	8.642404	0	1	Write	101392440	8
17	10.544672	0	1	Write	567392	8
20	10.545294	0	1	Write	47474184	8

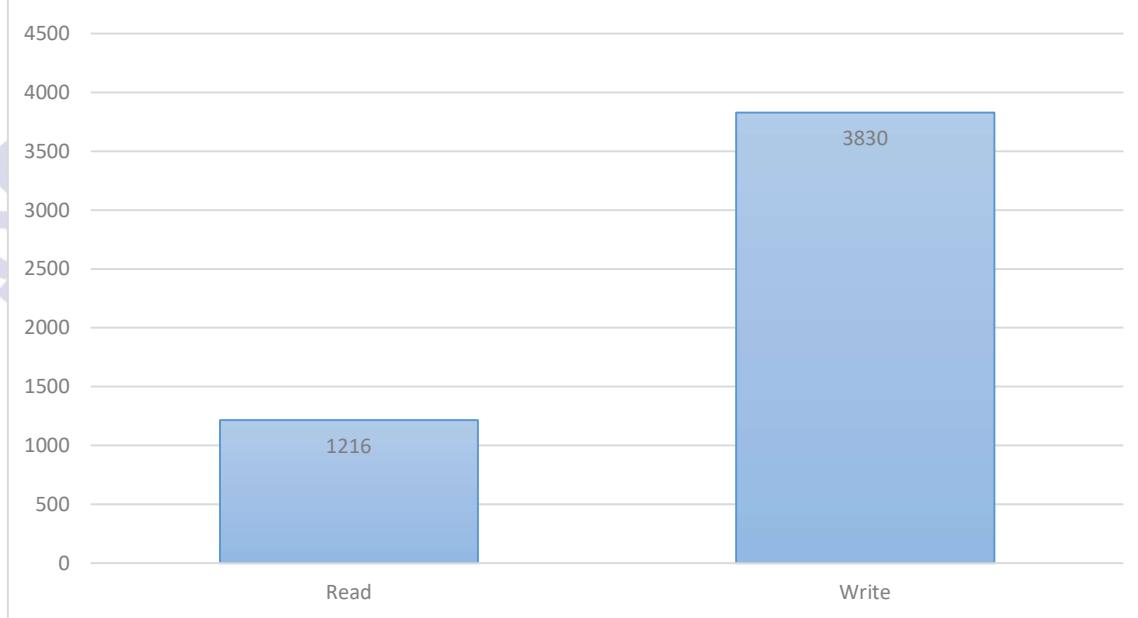
21	10.545326	0	1	Write	47474192	8
24	10.546761	0	1	Write	47474184	8
25	10.546978	0	1	Write	47474192	8
32	10.5489	0	1	Write	567520	8
33	10.549217	0	1	Write	567400	8
35	10.551006	0	1	Write	567528	8
37	10.551166	0	1	Write	567400	8
39	10.551573	0	1	Write	567528	8
40	10.551721	0	1	Write	80871376	8
41	10.551818	0	1	Write	80871384	8
42	10.552262	0	1	Write	567400	8
43	10.552373	0	1	Write	24583232	8
44	10.552491	0	1	Write	24583240	8
45	10.552678	0	1	Write	567528	8
47	10.55316	0	1	Write	24583232	8
48	10.553281	0	1	Write	24583240	8
49	10.553434	0	1	Write	567536	8
50	10.553618	0	1	Write	47474192	8
51	10.55377	0	1	Write	47474200	8
52	10.553827	0	1	Write	47474208	8
53	10.554253	0	1	Write	567408	8
54	10.554363	0	1	Write	24583232	8
55	10.554487	0	1	Write	24583240	8
56	10.554652	0	1	Write	567536	8
59	10.566633	0	1	Write	567544	8
70	18.891933	0	1	Write	567344	8
75	19.5396	0	1	Write	50971336	8
76	19.539738	0	1	Write	50971576	8
78	19.53999	0	1	Write	50971656	8
79	19.540114	0	1	Write	50974832	8
87	27.718742	0	1	Write	64804568	8
96	34.193014	0	1	Write	567424	8
104	35.889885	0	1	Write	567464	8
105	35.8928	0	1	Write	50984512	8
106	35.892826	0	1	Write	18045224	8
108	35.892883	0	1	Write	65642656	8
109	35.892938	0	1	Write	8168040	8
110	35.893005	0	1	Write	148436648	8
111	35.893094	0	1	Write	51008976	8
112	35.893142	0	1	Write	8167600	8
113	35.893181	0	1	Write	65655000	8
114	35.893187	0	1	Write	50775480	8
115	35.893206	0	1	Write	51009288	8
116	35.893242	0	1	Write	27761576	8
117	35.893254	0	1	Write	17904984	8
118	35.893274	0	1	Write	50775568	8
120	35.893322	0	1	Write	29124384	8
121	35.893325	0	1	Write	27761712	8

122	35.893357	0	1	Write	51009440	8
124	35.893379	0	1	Write	27761792	8
126	35.893414	0	1	Write	51009488	8
127	35.893462	0	1	Write	50775808	8
128	35.893488	0	1	Write	27761344	8
129	35.893507	0	1	Write	51009896	8
131	35.893536	0	1	Write	50776736	8
132	35.893568	0	1	Write	27761488	8
133	35.893658	0	1	Write	50776784	8
136	35.893722	0	1	Write	3683248	8
137	35.893734	0	1	Write	50776960	8
138	35.89377	0	1	Write	29124032	8
139	35.893789	0	1	Write	51010448	8
140	35.893805	0	1	Write	3683272	8
141	35.893821	0	1	Write	50777424	8
143	35.893853	0	1	Write	51074312	8
144	35.893872	0	1	Write	1814872	8
145	35.893885	0	1	Write	83221488	8
146	35.893904	0	1	Write	29124088	8
147	35.89392	0	1	Write	51078792	8
148	35.893939	0	1	Write	1645528	8
149	35.893958	0	1	Write	83226456	8
151	35.893994	0	1	Write	51085920	8
152	35.894019	0	1	Write	872208	8
153	35.894029	0	1	Write	50773824	8
156	35.894096	0	1	Write	5058712	8
157	35.894112	0	1	Write	50773840	8
159	35.894154	0	1	Write	51168072	8
160	35.894176	0	1	Write	16548600	8
163	35.894384	0	1	Write	103287976	8
164	35.894406	0	1	Write	200485976	8
167	35.894547	0	1	Write	1084208	8
168	35.894582	0	1	Write	200489400	8
169	35.894621	0	1	Write	50773984	8
171	35.894832	0	1	Write	280650632	8
173	35.89489	0	1	Write	50774064	8
175	35.895002	0	1	Write	279925152	8
176	35.895027	0	1	Write	43554632	8
177	35.89505	0	1	Write	50774168	8
178	35.895098	0	1	Write	80469344	8
179	35.895114	0	1	Write	24786184	8
180	35.89513	0	1	Write	50774232	8
181	35.895142	0	1	Write	21172040	8
182	35.895168	0	1	Write	80628872	8
183	35.895197	0	1	Write	50774272	8
184	35.895274	0	1	Write	7673024	8
185	35.895341	0	1	Write	50774304	8
186	35.895392	0	1	Write	10886568	8

64	16.813885	0	1	Write	64804560	9
90	31.815923	0	1	Write	64804568	10
5	9.998371	0	1	Write	72869200	12
26	10.54725	0	1	Write	24612512	16
27	10.54754	0	1	Write	24612528	16
28	10.547809	0	1	Write	24612512	16
29	10.547995	0	1	Write	24612512	16
36	10.551123	0	1	Write	24491056	16
38	10.551286	0	1	Write	2562160	16
46	10.553044	0	1	Write	567400	16
57	10.554891	0	1	Write	567408	16
63	16.8138	0	1	Write	14520456	16
68	18.891208	0	1	Write	567464	16
74	19.539421	0	1	Write	50971296	16
77	19.539867	0	1	Write	50971616	16
80	20.909389	0	1	Write	73912776	16
81	22.25939	0	1	Write	567384	16
86	27.718742	0	1	Write	567520	16
94	34.192336	0	1	Write	567544	16
119	35.893283	0	1	Write	51009400	16
123	35.893363	0	1	Write	50775784	16
142	35.893837	0	1	Write	29124064	16
155	35.894077	0	1	Write	51088632	16
158	35.89415	0	1	Write	29124248	16
161	35.894243	0	1	Write	29124272	16
165	35.894515	0	1	Write	29124304	16
174	35.89495	0	1	Write	80416888	16
91	33.165651	0	1	Write	567400	24
150	35.893978	0	1	Write	29124104	24
172	35.894867	0	1	Write	80416840	24
2	8.642429	0	1	Write	567496	32
10	10.539772	0	1	Read	27134568	32
11	10.540274	0	1	Read	27134536	32
12	10.540792	0	1	Read	27134224	32
13	10.541379	0	1	Read	54988880	32
14	10.54212	0	1	Read	54988752	32
15	10.542783	0	1	Read	54988720	32
130	35.893526	0	1	Write	29124472	32
162	35.894288	0	1	Write	50773872	32
166	35.894531	0	1	Write	50773912	32
107	35.892842	0	1	Write	148436656	40
154	35.894067	0	1	Write	29124144	40
8	10.53831	0	1	Read	54988040	48
16	10.5438	0	1	Read	27129584	48
72	19.538261	0	1	Write	567472	48
125	35.893402	0	1	Write	29124416	48
135	35.893699	0	1	Write	51010392	48
62	16.747099	0	1	Read	24129256	56

170	35.894784	0	1	Write	29124328	56
0	8.393994	0	1	Read	208032818	64
6	10.53689	0	1	Read	54987976	64
7	10.537573	0	1	Read	54988088	64
9	10.539061	0	1	Read	27130936	64
18	10.545037	0	1	Write	75053728	64
19	10.545158	0	1	Write	75053792	64
22	10.54593	0	1	Write	75060256	64
23	10.545934	0	1	Write	75060512	64
30	10.54828	0	1	Write	75051680	64
31	10.548511	0	1	Write	75051744	64
34	10.549894	0	1	Read	54987816	64
58	10.555232	0	1	Read	27129728	64
60	10.566827	0	1	Write	53299328	64
61	10.58215	0	1	Write	53298368	64
99	35.862893	0	1	Read	301720040	64
134	35.893686	0	1	Write	29124512	72
103	35.889744	0	1	Write	581920	128
65	18.170083	0	1	Write	581784	136
101	35.865245	0	1	Write	304010488	136
98	35.86288	0	1	Read	301720104	168
69	18.891597	0	1	Write	96081248	232
95	34.192707	0	1	Write	39353696	232
102	35.868669	0	1	Read	303151640	256
100	35.864877	0	1	Write	301779744	688

Sum of Length by Request



Result Analise:

After monitoring the disk activity and identifying the read and write processes with a length greater than 5, the following observations were made:

- The read processes listed above indicate the processes that performed data read operations with a length greater than 5.
- The write processes listed above indicate the processes that performed data write operations with a length greater than 5.
- By analysing these processes, further insights can be gained into potentially resource-intensive or suspicious activities on the system.

Conclusion:

- Disk monitoring can be a valuable technique to identify read and write processes with a length greater than 5. This information can be helpful in identifying potential performance bottlenecks, resource-intensive processes, or suspicious activities on the system.

Future scope:

- provide real-time alerts for processes with length > 5.
- Conducting a deeper analysis of the identified processes to understand their impact on system performance and security.
- Integrating the disk monitoring functionality with other security tools for comprehensive threat detection and prevention.

Experiment : 4

Title: Installation and demonstration of sawmill on windows OS. Generate a custom report.

Objective:

The objective of this experiment is to install and demonstrate the usage of Sawmill on a Windows operating system, specifically for generating a custom report.

Some information about “Sawmill”:

Sawmill software is used for log analysis and reporting, providing insights into website traffic and user behaviour. It processes log files and generates customizable reports, helping administrators and marketers understand website performance and security-related information.

Requirements:

Sawmill installer

Procedure/Experiment Steps:

1. Download the latest version of the Sawmill software from the official website.
2. Launch the installer and follow the on-screen instructions to install Sawmill on the Windows OS.
3. Once the installation is complete it ask for first time Configuration detail like Language, Licence agreement, username and password we need to set for the first time.

The screenshot shows a web-based setup interface for Sawmill. At the top, there's a browser header with the URL 127.0.0.1:8988. Below the header, the page title is "SAWMILL". A large, bold heading "Sawmill Setup" is centered at the top of the main content area. Underneath, the text "Root Administrator" is displayed. A message asks the user to choose a username and password for the Root Administrator, with a note that these credentials will be required for future access. There are three input fields for "Username", "Password", and "Reenter password". At the bottom of the form, there are two buttons: "< Back" and "Next >".

4. Configure the necessary settings, such as specifying the log file or data source for analysis.

Sawmill - Google Chrome

① 127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

Back Next Cancel

Log source

Please specify where you would like Sawmill to get your log data from.

Log source: Local disk or mapped/mounted disk ▾

Folder with optional file name, e.g.: C:\logs, C:\logs\access.log

Pathname: C:\logs [Add file mask](#)

Process subfolders

Best Practice Tip

Log files are your company's asset and irreplaceable. We strongly recommend that you retain your historical log files for as long as possible. Read more in [Log File Management](#).

Don't show again

5. Choose log file format to import the log data.

Sawmill - Google Chrome

① 127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

Back Next Cancel

Manual log format selection

Select a log format.

Filter log formats by ... (1146)

- Microsoft Windows Event Log (CSV)
- Microsoft Windows Event Log (dumpeventlogs.vbs export)
- Microsoft Windows Event Log (Tab Delimited)
- Microsoft Windows Event Log (XML)
- Microsoft Windows Event Logs (Powershell ETVX to CSV)
- Microsoft Windows Firewall**
- Microsoft Windows NT Scheduler
- Microsoft Windows NT Syslog
- Microsoft Windows NT4 Event (save as CSV)
- Microsoft Windows Performance Monitor
- Microsoft Windows Syslog
- Microsoft Windows XP Event Log (LogParser CSV Export)
- Microtech ImageMaker
- Microtech ImageMaker
- MikroTik Router
- MikroTik The Dude
- MikroTik Web Proxy
- Mirapoint Message Server

6. Set the appropriate log file parameters, including file location, log format, and any specific customization options.

Sawmill - Google Chrome
① 127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

Database [More Info](#)

Please choose the preferred database.
Note: for highest performance, and the smallest database, choose Internal.

Database server type:

Database folder: (optional) [i](#)

Back Next Cancel

Sawmill - Google Chrome
① 127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

Database performance options [More Info](#)

Please specify whether or not to turn on database field indices and cross reference groups.
Enabling all will result in fast report generation but increases the database build time and size.

Turn on database field indices
 Turn on cross reference groups

Back Next Cancel

Sawmill - Google Chrome
① 127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

Numerical field options [More Info](#)

Please select the numerical fields which you would like to have in the reports.

[Select All](#) | [Deselect All](#)

Packets
 Size
 Unique source IPs

Sawmill - Google Chrome
① 127.0.0.1:8988/?dp=new_profile_wizard.index

New Profile Wizard

Profile name

Please define a name for the new profile and click the Finish button.

Profile name:

Back Finish Cancel

The profile "Firewall" has been created

Please decide what to do next.

Process Data & View Reports
 Take this action if no additional customization is required. This action goes straight to the reports and automatically starts building the database by processing all log data in the log source.

View Profile in Config
 Take this action if you require additional customization prior to processing all log data in the log source, for example you wish to:

- Add or change log filters
- Turn on DNS lookup of IP addresses
- Add, delete or change database fields
- Other configuration options available in the Config pages

[Close Window](#)

7. Initiate the log data import process to populate the Sawmill database.
8. Once the data import is complete, navigate to the reporting section within Sawmill.
9. Select the desired report customization options, including specific data fields, filters, date ranges, and visualization preferences.

test - Reports

Date Picker Filters Macros Miscellaneous Printer Friendly Customize

Calendar Date and time Gateways Types Partners Originators Priorities Recipients Single-page Summary Log detail

Overview No date applied. The date filter "" is out of the available log date range.

Avg/day		
Messages	0	-
Length	0 B	-

Config Options Database / Tools Admin

- Log Source
- Log Parsing Filters
- Log Filters
- Log Fields
- Log Processing
- Database Server & Tuning
- Database Filters
- Database Fields
- Cross Reference Groups
- Reports Editor**
- Report Options
- Report Fields
- DNS Lookup, Support & Action Email
- New Field Wizard
- Snapshots

10. Generate the custom report based on the selected parameters.

The screenshot shows the Sawmill software interface. On the left, a sidebar titled 'Report Groups / Reports' lists various report categories with checkboxes. Under 'Date and time', the 'Months' checkbox is selected and highlighted in blue. In the main window, titled 'Report', there is a 'Report Elements' section with a single item labeled '1 Months'. At the top of the main window, there are buttons for 'Edit Report Properties' and 'New Report Element'.

11. Review and analyze the generated custom report for insights and information.

Result:

The custom report generated from Sawmill provides valuable insights and analysis based on the selected parameters. It allows for in-depth exploration and understanding of the log data, assisting in identifying patterns, anomalies, and trends.

Conclusion:

The installation and usage of Sawmill on the Windows operating system enable the generation of custom reports, offering an effective approach to analyse and interpret log data. The custom report assists in understanding the logged information, identifying important trends, and making informed decisions.

Future Scope:

1. Exploring advanced customization options within Sawmill to generate more specific and targeted reports.
2. Integrating Sawmill with other security tools or log sources to consolidate and analyze data from multiple sources.
3. Conducting further research on log analysis methodologies and techniques to enhance the effectiveness of Sawmill reports.

Experiment: 5

Title: Installation and Configuration of Snort for Network Security and Protection against Cyber Threats

Objective:

The objective of this experiment is to install and configure Snort, an open-source intrusion detection and prevention system, for enhancing network security and providing protection against cyber threats.

Requirements:

Snort installer

Procedure/Experiment Steps:

1. Download the latest version of Snort from the official website.
2. Launch the installer and follow instructions to install Snort.
3. Install Npcap because it's require for snort.
4. After installing Snort and Npcap. In command prompt open c:\ drive enter these commands in Command prompt to check snorts working
 - a. cd snort
 - b. cd bin
 - c. snort -v

```
C:\Users\dhava>cd ..  
C:\Users>cd ..  
C:\>cd Snort  
C:\Snort>cd bin  
C:\Snort\bin>snort  
Running in packet dump mode  
      === Initializing Snort ===  
Initializing Output Plugins!  
pcap DAQ configured to passive.  
The DAQ version does not support reload.  
Acquiring network traffic from "\Device\NPF_{AE347C8D-8D5E-4A4A-A887-CDE39C0AA904}".  
Decoding Ethernet  
      === Initialization Complete ===  
  
o'''~  -=> Snort! <--  
     By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
     Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.  
     Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
     Using PCRE version: 8.10 2010-06-25  
     Using ZLIB version: 1.2.11  
  
Commencing packet processing (pid=9352)  
|
```

- d. As we can see snort installed successfully
5. After installing Snort on Windows 10, Another important step to get started with Snort is configuring
 - a. Go to "<https://www.snort.org/downloads/#rule-downloads>" and download latest snort rule file

- b. Extract 3 folders from the downloaded snortrules-snapshot-29200.tar folder into the Snorts corresponding folders in C drive.

Name	Date modified	Type	Size
etc	22-06-2023 01:02	File folder	
preproc_rules	22-06-2023 01:02	File folder	
rules	22-06-2023 01:02	File folder	
so_rules	22-06-2023 01:17	File folder	
snortrules-snapshot-29200.tar	22-06-2023 01:20	TAR File	5,73,873 KB

- c. rules folder contains the rules files and the most important local.rules file. Which we will use to enter all our rules.
d. etc folder contains all configuration files and the most important file is snort.conf file which we will use for configuration
6. Now open the snort.conf file through the notepad++ editor or any other text editor to edit configurations of snort to make it work like we want it to.

- a. Setup the network addresses you are protecting

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.217.1
```

- b. define the directory for our rules and preproc rules folder

```
# other variables, these should not be modified
ipvar AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]
```

```
# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH C:\Snort\rules
var SO_RULE_PATH C:\Snort\so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

```
# If you are using reputation processor set these
var WHITE_LIST_PATH ../rules
var BLACK_LIST_PATH ../rules
```

- c. setup our white list and black list path it will be in our snorts' rule folder

```
# If you are using reputation processor set these
var WHITE_LIST_PATH C:\Snort\rules
var BLACK_LIST_PATH C:\Snort\rules
```

- d. enable log directory, so that we store logs in our log folder. Uncomment this line and set absolute path to log directory

```
# Configure default log directory for snort to log to. For more information see snort -h command line options (-l)
#
# config logdir: C:\Snort\log
```

- e. set the path to dynamic preprocessors and dynamic engine

```
# path to dynamic processor libraries
dynamicprocessor directory C:\Snort\lib\snort_dynamicprocessor
```

- f. do same thing for dynamic processor engine

```
# path to base processor engine
dynamicengine C:\Snort\lib\snort_dynamicengine
```

- g. Converted back slashes to forward slashes in this entire step

```
#####
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
#####

# site specific rules
include $RULE_PATH/local.rules

include $RULE_PATH\app-detect.rules
include $RULE_PATH\attack-responses.rules
include $RULE_PATH\backdoor.rules
include $RULE_PATH\bad-traffic.rules
include $RULE_PATH\blacklist.rules
include $RULE_PATH\botnet-cnc.rules
include $RULE_PATH\browser-chrome.rules
include $RULE_PATH\browser-firefox.rules
include $RULE_PATH\browser-ie.rules
include $RULE_PATH\browser-other.rules
```

- h. Again just convert forward slashes to backslashes and uncomment the lines below:

```
#####
# Step #8: Customize your processor and decoder alerts
# For more information, see README.decoder_proc_rules
#####

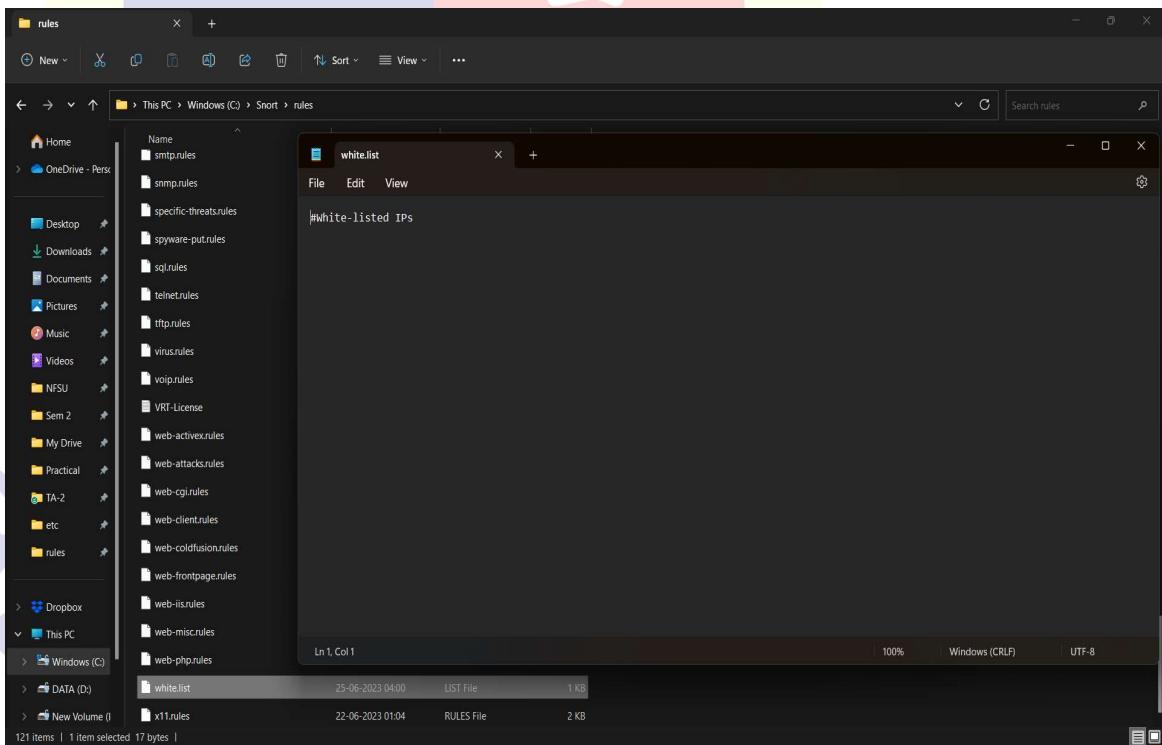
# decoder and processor event rules
# include $PREPROC_RULE_PATH\processor.rules
# include $PREPROC_RULE_PATH\decoder.rules
# include $PREPROC_RULE_PATH\sensitive-data.rules
```

- i. Now we just need to verify the presence of this command at the bottom of snort.conf file.

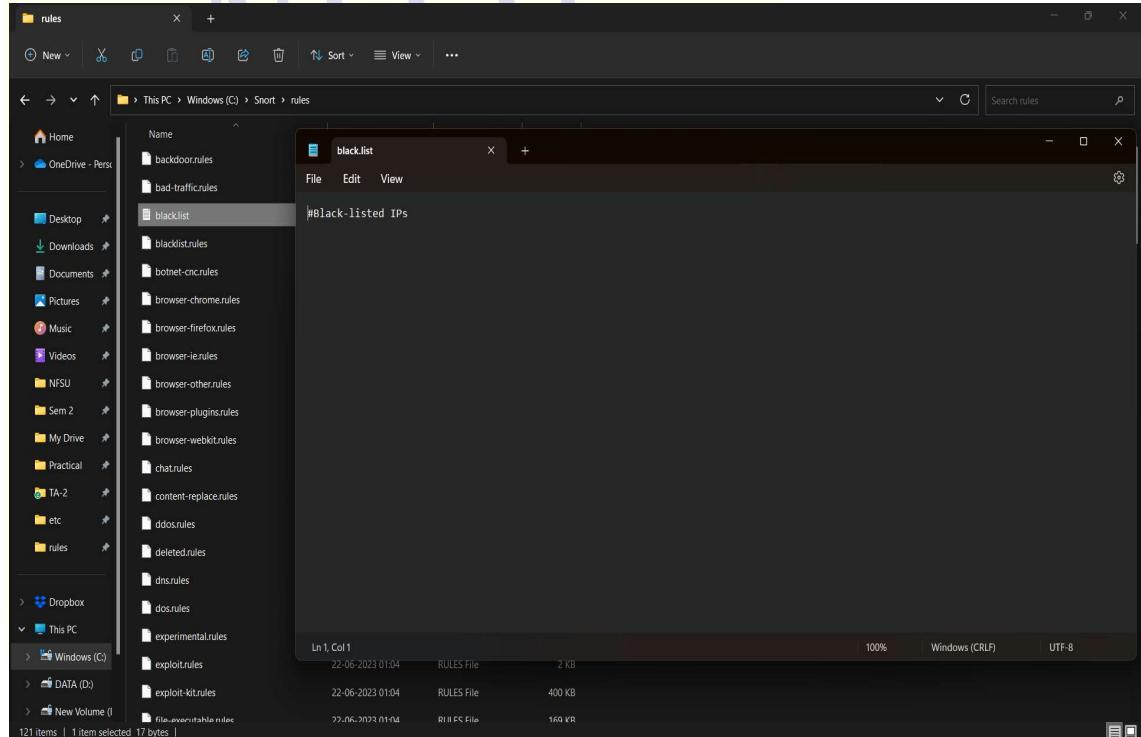
```
# include $SO_RULE_PATH/server-mysql.rules  
# include $SO_RULE_PATH/server-oracle.rules  
# include $SO_RULE_PATH/server-other.rules  
# include $SO_RULE_PATH/server-webapp.rules  
  
# Event thresholding or suppression commands. See threshold.conf  
include threshold.conf
```

J. Click on Save file and save all changes to save the configuration file (snort.conf).

7. Now recalling the Step 13 white list , black list are not rules they are just the list of IP addresses labelled as black or white right now these files don't exist in our rule path which is why we have to create them manually , save them in this folder C:\Snort\rules.
- White-List
 - Go to Notepad++ and create new file.
 - Comment it #White-listed IPs.
 - Name the file white.list and save the file.



- b. Black-List
- Create another new file.
 - Comment it #Black-listed IPs.
 - Name the file black.list and save the file.



8. Now we test snort again by running Command prompt as admin. To check if it's running fine after all the configurations.

```
C:\>cd Snort

C:\Snort>cdc bin
'cdc' is not recognized as an internal or external command,
operable program or batch file.

C:\Snort>cd bin

C:\Snort\bin>snort -v
Running in packet dump mode

      === Initializing Snort ===
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{AE347C8D-8D5E-4A4A-A887-CDE39C0AA904}".
Decoding Ethernet

      === Initialization Complete ===

      -*> Snort! <*-
      Version 2.9.20-WIN64 GRE (Build 82)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using PCRE version: 8.10 2010-06-25
      Using ZLIB version: 1.2.11

Commencing packet processing (pid=17656)
```

- We can also check the wireless interface cards from which we will be using snort by using the command below we can see the list of our wireless interface cards through entering this command in command prompt.

```
C:\Snort\bin>snort -W

      -*> Snort! <*-
      Version 2.9.20-WIN64 GRE (Build 82)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using PCRE version: 8.10 2010-06-25
      Using ZLIB version: 1.2.11

-----  

Index Physical Address      IP Address     Device Name      Description
-----  

  1  00:00:00:00:00:00      disabled       \Device\NPF_{AE347C8D-8D5E-4A4A-A887-CDE39C0AA904}      WAN Miniport (Network Monitor)
  2  00:00:00:00:00:00      disabled       \Device\NPF_{6E8B2BD4-3908-40D3-A5C8-50DF4CFAC847}    WAN Miniport (IPv6)
  3  00:00:00:00:00:00      disabled       \Device\NPF_{150FE8C-6343-483D-945B-7C5C2ED95E54}    WAN Miniport (IP)
  4  50:C2:E8:20:DD:39      192.168.1.2   \Device\NPF_{BE03E406-7418-4431-8F8A-959AD85F936F}  Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
  5  00:50:56:C0:00:08      192.168.152.1  \Device\NPF_{96F93BF6-2220-460D-AD9F-EBC5A2B5ABA}  VMware Virtual Ethernet Adapter for VMnet8
  6  00:50:56:C0:00:01      192.168.217.1  \Device\NPF_{F71D68F7-3FAB-4C49-B3B2-56C33477C45E}  VMware Virtual Ethernet Adapter for VMnet1
  7  D2:C2:E8:20:DD:39      169.254.174.88 \Device\NPF_{BC2BE74E-8290-4697-88A1-F99EB5D8C647}  Microsoft Wi-Fi Direct Virtual Adapter #2
  8  52:C2:E8:20:DD:39      169.254.137.113 \Device\NPF_{0A2DB3A4-4770-43DD-95E3-078E30CE8677}  Microsoft Wi-Fi Direct Virtual Adapter
  9  00:00:00:00:00:00      0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback Adapter for loopback traffic capture
  10 A8:B1:3B:AC:BF:B5      169.254.43.55   \Device\NPF_{0FC8D253-2281-426C-A916-A4C94CBED46E}  Realtek Gaming Gbe Family Controller
```

Result:

By monitoring the network traffic using Snort, the system can detect and analyse various types of cyber threats, including intrusion attempts, malware activity, and suspicious network behaviours. The Snort alerts and log files provide valuable information for security analysts to investigate and respond to potential security incidents.

Conclusion:

The installation and configuration of Snort as an intrusion detection and prevention system significantly enhance network security and provide protection against cyber threats. Snort's ability to monitor and analyse network traffic helps in identifying and mitigating potential security risks in real-time.

Future Scope:

1. Continuously update the Snort ruleset to keep up with the latest threats and attack techniques.
2. Integrate Snort with other security tools, such as SIEM (Security Information and Event Management) systems, for centralized security monitoring and incident response.
3. Explore advanced features of Snort, such as protocol analysis and anomaly detection, to enhance network security capabilities.
4. Conduct regular audits and assessments to ensure the effectiveness of Snort in protecting the network against emerging cyber threats.



Experiment: 6

Title: Install and demonstrate Splunk for log analysis

Objective:

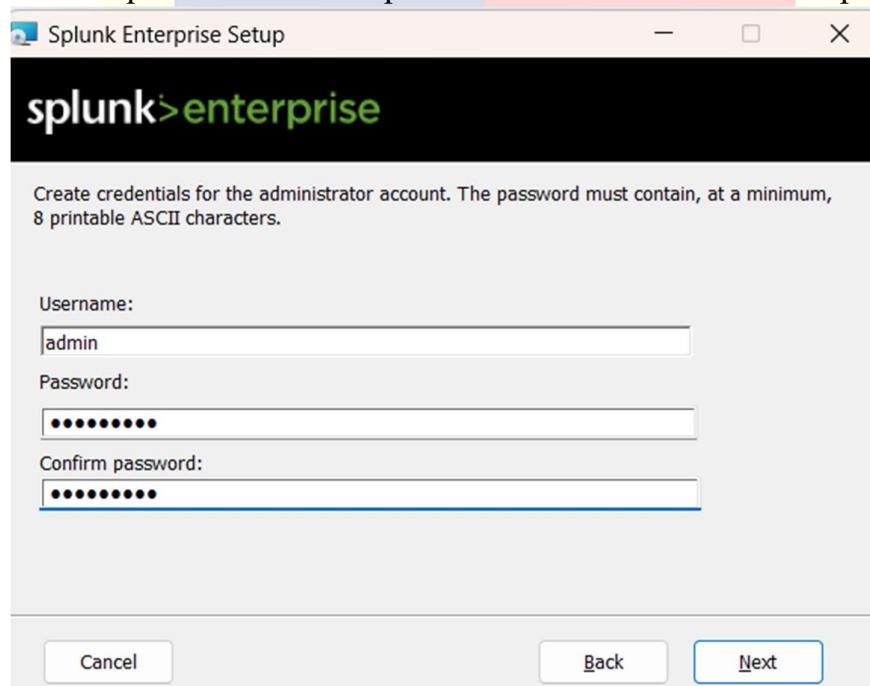
The objective of this experiment is to install and demonstrate the usage of Splunk, a log analysis and monitoring platform, for efficient log analysis and gaining insights from log data.

Requirements:

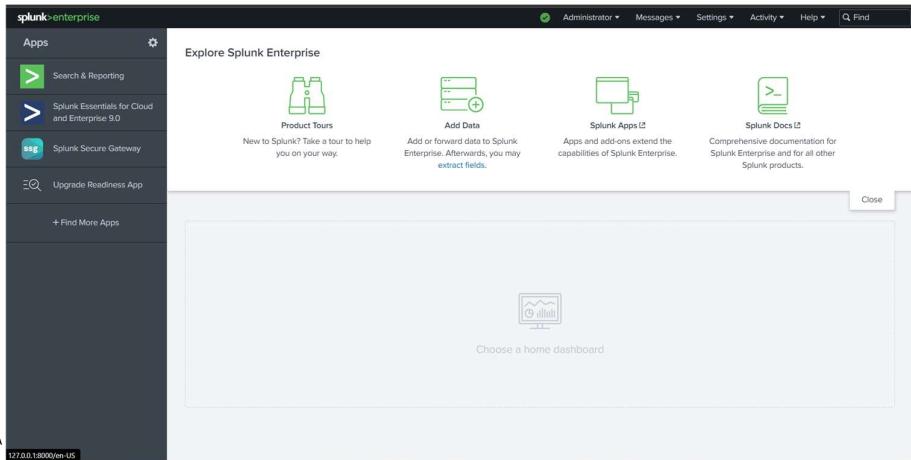
Splunk installer

Procedure/Experiment Steps:

1. Download Splunk: Visit the official Splunk website and download the appropriate installation package for your operating system.
2. Install Splunk: Follow the provided instructions to install Splunk on your computer.



3. Launch Splunk: After installation, launch Splunk from the installed location or desktop shortcut or just go to <http://localhost:8000>.
4. Set up Splunk: During the initial setup, create an administrator account and configure basic settings.



5. Configure data inputs: Set up data inputs to ingest log data from various sources such as log files, network devices, or cloud platforms.

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Next >

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: CertListDetail.1st

View Event Summary

Source type: default ▾

Save As

> Event Breaks

> Timestamp

> Advanced

List ▾ Format 20 Per Page ▾

	Time	Event	
		50 6E 87 5C 0B C5 D4 5E D8 1C 97 DB 06 00 4B BD 22 21 0F 3F D7 84 A7 SE 24 BF BB 14 06 3D C3 21 70 2D AA 81 DD 8B 7E 92 08 6D 0C 17 A8 6B 4F 0D	'Pn.\....^.....K.' "I.?.?...\$....=.!" 'p-....-.m...k0.'
		Show all 257 lines	
8	12/31/20 4:59:59.000 PM	CA A6 77 2F 3E F7 C2 C5 B3 BA FB 66 E2 16 22 52 70 5D AF BA 76 83 68 80 E3 9F EC 70 A3 B5 00 EE 91 96 9D 36 ED 87 85 BD 15 77 E2 C2 80 2E C6 51 5C AC 45 48 C2 20 94 23 F3 60 41 CB EC 7A AD 33 1F 18 C7 F1 73 F7 34 52 C8 5A 1A D1 30 A3 C0	'..w/>.....f..R' 'p]..v.h.....p...' '....6....w.....' '\Q.EH..#.'A..z..' '3...s.4R.Z..0...'
		Show all 118 lines	
9	12/31/20 4:59:59.000 PM	Fr1 Feb 27 14:00:12 2043 Aux PropId 124 (0x7c) :: C5 75 0B F8 5F 45 9F B7 0E 2B 6C 01 89 80 37 5E 92 D7 93 8E 47 A6 E0 34 CC E0 C1 2D 30 37 2C CD Aux PropId 25 (0x19) ::	'..u...E...+1...7*' '....G...4...-07...'
		Show all 110 lines	
10	12/31/20 4:59:59.000 PM	Tue May 13 09:12:59 1997 NotAfter:: Thu Dec 30 16:59:59 1999	

6. Index log data: Create and configure indexes to organize log data efficiently.
 7. Search and analyze logs: Utilize Splunk's Search Processing Language (SPL) to search and analyze log data, troubleshoot issues, and extract insights.
 8. Create visualizations and reports: Generate visualizations and reports to present log data in charts, graphs, and dashboards.
 9. Demonstrate log analysis: Use real or simulated log data to showcase the effectiveness of Splunk in log analysis, anomaly detection, and troubleshooting.

Result:

By following the installation and demonstration steps, Splunk was successfully installed and utilized for log analysis. Log data from various sources was ingested and indexed, allowing for efficient searching and analysis. Splunk's search capabilities and visualizations provided valuable insights into the log data, enabling effective troubleshooting and decision-making.

Conclusion:

Splunk is a powerful log analysis and monitoring tool that simplifies log management and analysis processes. Its features, including data ingestion, searching, and visualization, allow for efficient log analysis and troubleshooting. By utilizing Splunk, organizations can enhance their log management practices, improve operational efficiency, and gain valuable insights from log data.

Future Scope:

1. Integration with additional data sources such as cloud platforms, IoT devices, or specific application logs.
2. Exploring advanced analytics and machine learning capabilities within Splunk for deeper insights and automation of log analysis processes.
3. Utilizing Splunk's security features for robust security monitoring, threat detection, and compliance reporting.
4. Leveraging collaboration features to facilitate knowledge sharing, teamwork, and reporting among different stakeholders.
5. Optimizing Splunk deployment for scalability and performance as log data volume increases, including distributed architecture and performance tuning techniques.



Experiment : 7

Title: Use Autopsy to recover file from the given data source. Present your details accordingly

Objective:

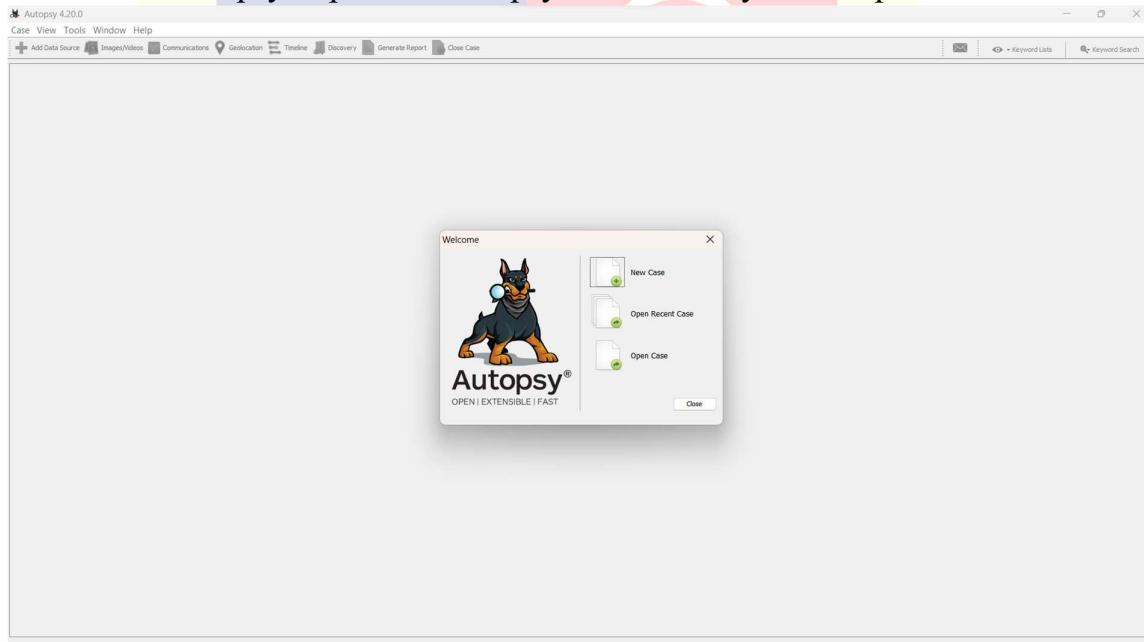
The objective of this experiment is to utilize Autopsy, a digital forensics tool, to recover a file from a specific data source.

Requirements:

- Autopsy software installed
- Data source containing the target file for recovery (e.g., a storage device, disk image, or forensic image)

Procedure/Experiment Steps:

1. Launch Autopsy: Open the Autopsy software on your computer.



2. Create a New Case: Create a new case within Autopsy to organize your investigation.

New Case Information

Steps

1. Case Information
2. Optional Information

Case Information

Case Name: Dhaval

Base Directory: E:\NFSU\Sem 2\P4 IRMDF\Practical\Autopsy_Case\

Case Type: Single-User Multi-User

Case data will be stored in the following directory:
E:\NFSU\Sem 2\P4 IRMDF\Practical\Autopsy_Case\DHaval

< Back **Next >** Finish Cancel Help

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 01

Examiner

Name: Dhaval

Phone: 70961556

Email: dhaval.patel70961@gmail.com

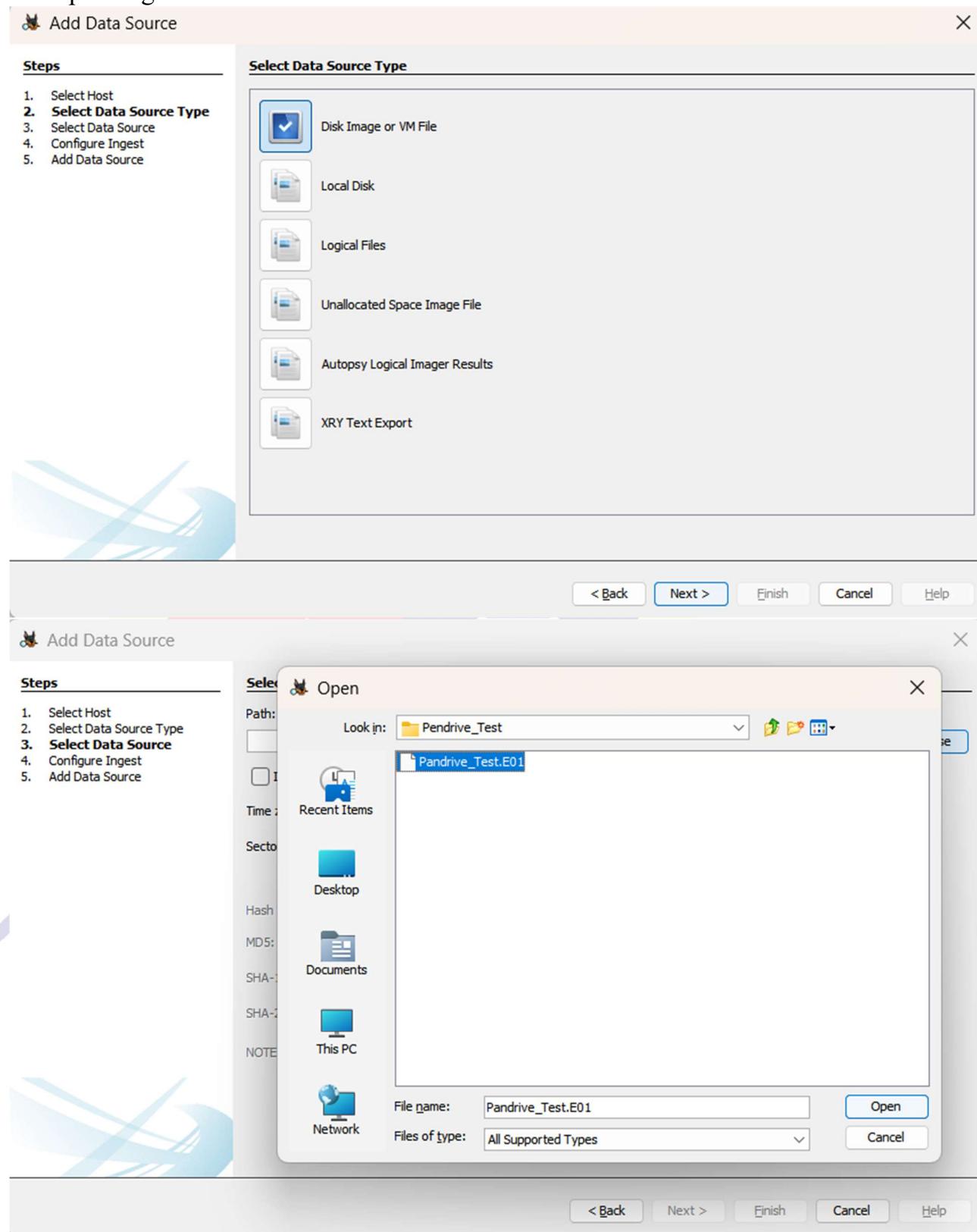
Notes: Test

Organization

Organization analysis is being done for: NFSU **Manage Organizations**

< Back **Next >** Finish Cancel Help

3. Add Data Source: Import the given data source, which contains the target file, into the Autopsy case. This can be done by selecting the "Add Image" or "Add Device" option, depending on the nature of the data source.



 Add Data Source X

Steps

1. Select Host
2. Select Data Source Type
- 3. Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\dhava\Downloads\Pendrive_Test\Pandrive_Test.E01

Ignore orphan files in FAT file systems

Time zone: (GMT+5:30) Asia/Calcutta

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.

4. Configure Data Source: Provide necessary information about the data source, such as the image file or device details, during the configuration process.

 Add Data Source X

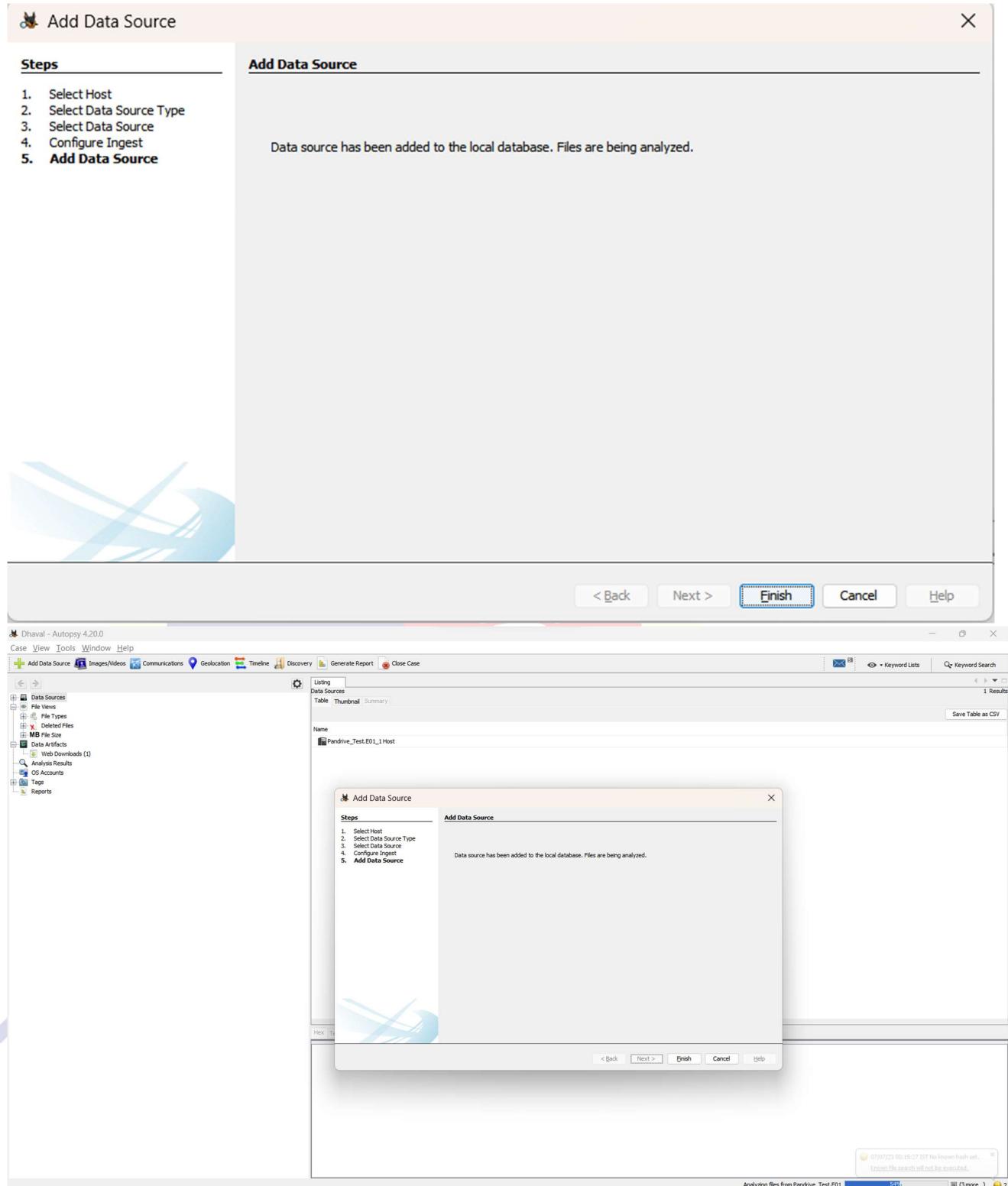
Steps

1. Select Host
2. Select Data Source Type
- 3. Select Data Source**
- 4. Configure Ingest**
5. Add Data Source

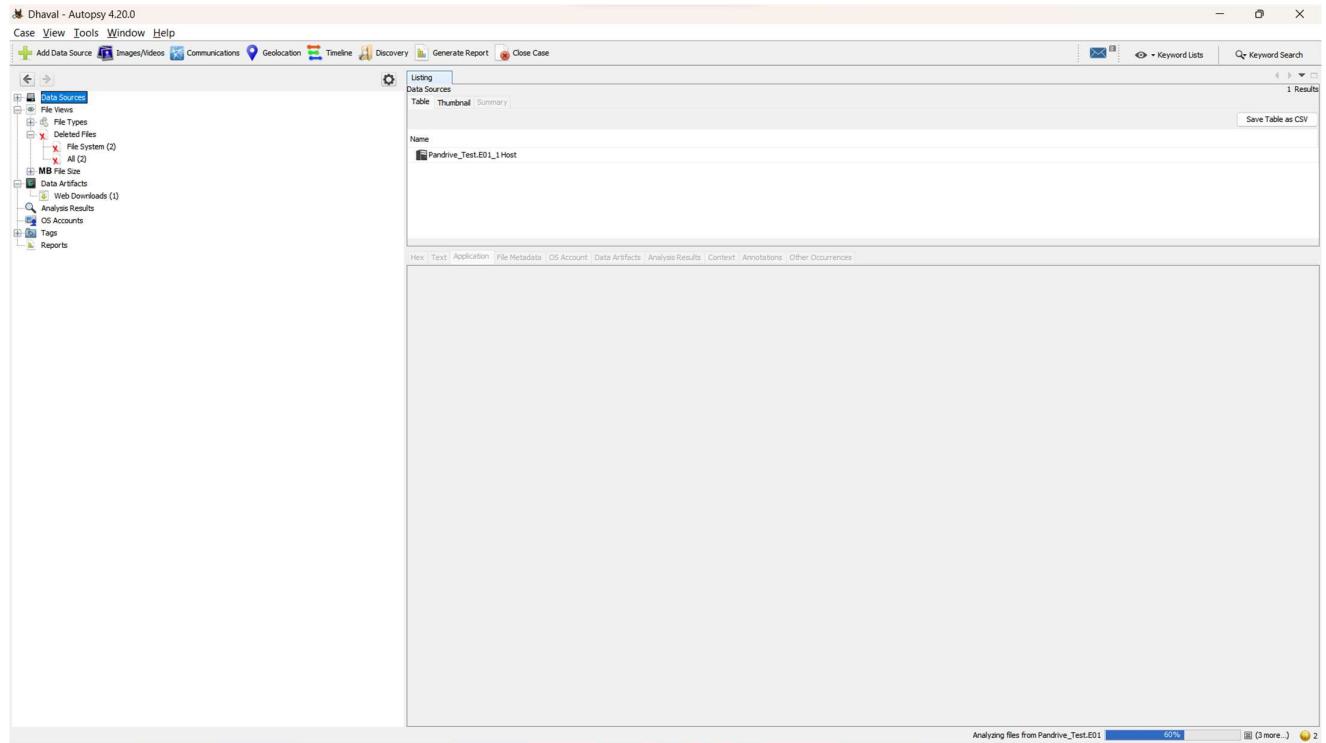
Configure Ingest

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

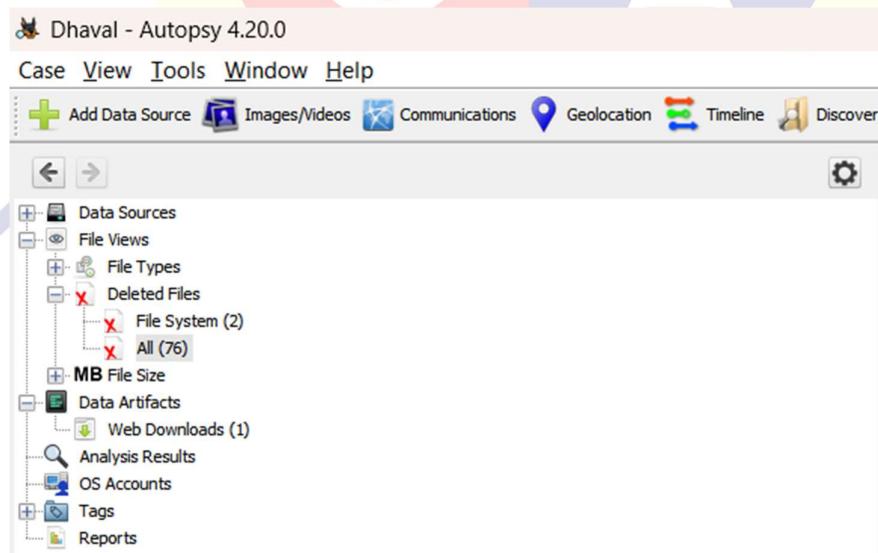
<input checked="" type="checkbox"/> Recent Activity <input checked="" type="checkbox"/> Hash Lookup <input checked="" type="checkbox"/> File Type Identification <input checked="" type="checkbox"/> Extension Mismatch Detector <input checked="" type="checkbox"/> Embedded File Extractor <input checked="" type="checkbox"/> Picture Analyzer <input checked="" type="checkbox"/> Keyword Search <input checked="" type="checkbox"/> Email Parser <input checked="" type="checkbox"/> Encryption Detection <input checked="" type="checkbox"/> Interesting Files Identifier <input checked="" type="checkbox"/> Central Repository <input checked="" type="checkbox"/> PhotoRec Carver <input checked="" type="checkbox"/> Virtual Machine Extractor <input checked="" type="checkbox"/> Data Source Integrity	The selected module has no per-run settings. Extracts recent user activity, such as Web browsing, recently us...
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------



5. Start Analysis: Once the data source is added and configured, initiate the analysis process within Autopsy.



6. Search for File: Utilize Autopsy's search functionality to locate the target file within the data source. You can specify the file name or use file metadata to narrow down the search results.

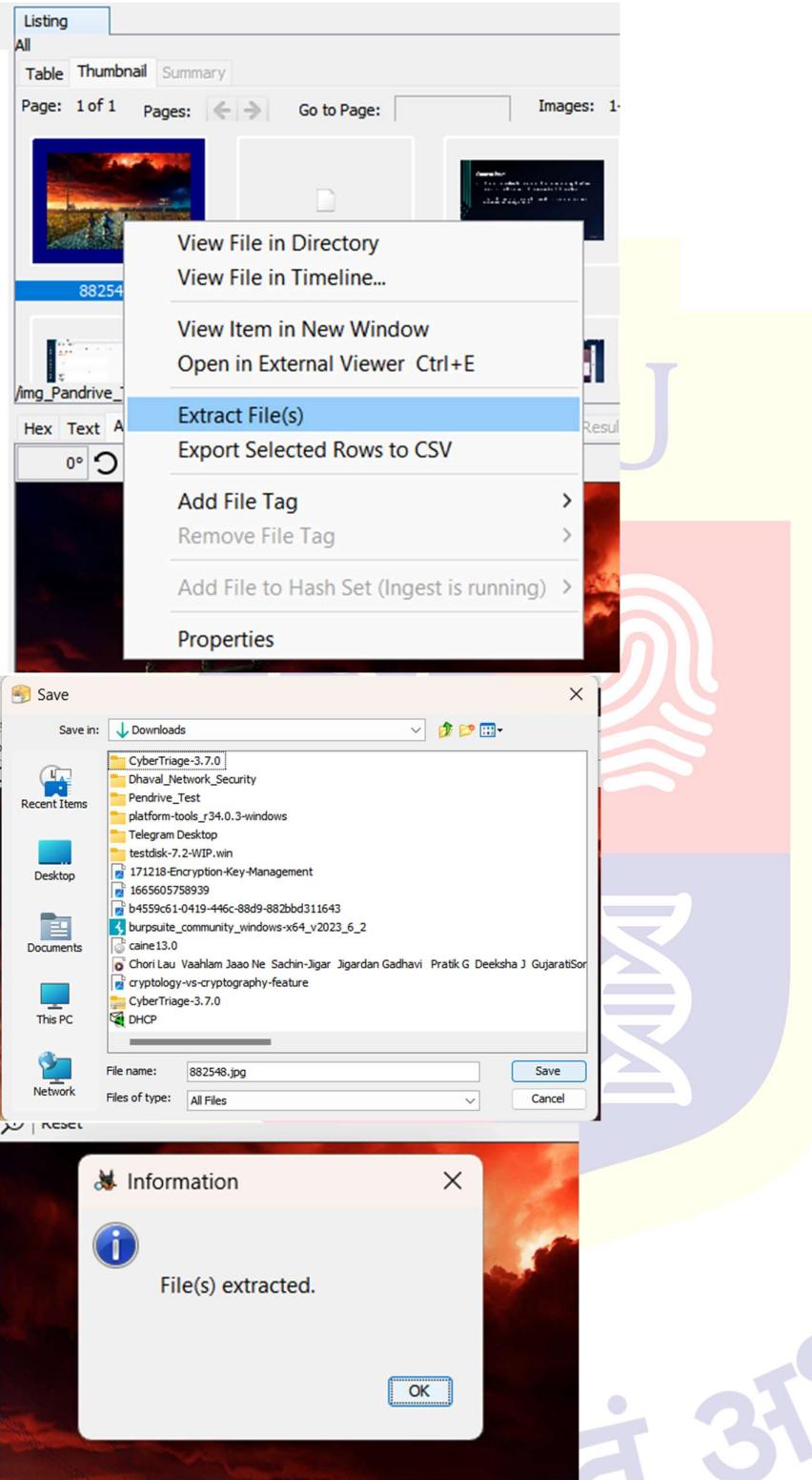


Listing												
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
882548.jpg				2023-04-12 15:40:39 IST	2023-04-12 15:50:41 IST	2023-07-06 20:41:29 IST	2023-07-06 20:41:29 IST	1875269	Unallocated	Unallocated	unknown	/img_Pandrv
882548.jpg:Zone.Identifier				2023-04-12 15:40:39 IST	2023-04-12 15:50:41 IST	2023-07-06 20:41:29 IST	2023-07-06 20:41:29 IST	50	Unallocated	Unallocated	unknown	/img_Pandrv
f0002304.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	54185764	Unallocated	Unallocated	unknown	/img_Pandrv
f0108160.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55175430	Unallocated	Unallocated	unknown	/img_Pandrv
f0215936.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	83205682	Unallocated	Unallocated	unknown	/img_Pandrv
f0378496.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	74447831	Unallocated	Unallocated	unknown	/img_Pandrv
f0523904.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	55114839	Unallocated	Unallocated	unknown	/img_Pandrv
f0631552.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	41164844	Unallocated	Unallocated	unknown	/img_Pandrv
f0712000.fat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	32768	Unallocated	Unallocated	unknown	/img_Pandrv
f0712064.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	29079640	Unallocated	Unallocated	unknown	/img_Pandrv
f0768896.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	31063557	Unallocated	Unallocated	unknown	/img_Pandrv
f0829568.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	32758229	Unallocated	Unallocated	unknown	/img_Pandrv
f0893568.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	46701562	Unallocated	Unallocated	unknown	/img_Pandrv
f0984832.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	39634331	Unallocated	Unallocated	unknown	/img_Pandrv
f1062272.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	61047629	Unallocated	Unallocated	unknown	/img_Pandrv
f1181568.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	43978714	Unallocated	Unallocated	unknown	/img_Pandrv
f1267520.fat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	32768	Unallocated	Unallocated	unknown	/img_Pandrv
f1267584.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	223782447	Unallocated	Unallocated	unknown	/img_Pandrv
f0000000.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1875269	Unallocated	Unallocated	unknown	/img_Pandrv
f0005688.txt				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	204	Unallocated	Unallocated	unknown	/img_Pandrv
f0017080.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	201394	Unallocated	Unallocated	unknown	/img_Pandrv
f0017528.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	789176	Unallocated	Unallocated	unknown	/img_Pandrv
f0019128.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	128519	Unallocated	Unallocated	unknown	/img_Pandrv
f0019384_Microsoft_Word_Document1.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2036374	Unallocated	Unallocated	unknown	/img_Pandrv
f0023416.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	467453	Unallocated	Unallocated	unknown	/img_Pandrv
f0032184.fat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_Pandrv
f0032248.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	425992	Unallocated	Unallocated	unknown	/img_Pandrv
f0033144.pdf				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	482307	Unallocated	Unallocated	unknown	/img_Pandrv
f0034104_A_Case_Study_on_Cyber_Crime_In_India_K				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	465252	Unallocated	Unallocated	unknown	/img_Pandrv
f0035064.fat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_Pandrv
f0035128.mp4				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	2575614	Unallocated	Unallocated	unknown	/img_Pandrv
f0040184.ai				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	860425	Unallocated	Unallocated	unknown	/img_Pandrv
f0041912.fat				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4096	Unallocated	Unallocated	unknown	/img_Pandrv

7. Recover File: Once the target file is located, select the file and choose the recovery option provided by Autopsy. Follow the prompts to specify the destination for the recovered file.

The screenshot shows the Autopsy 4.20 interface with the following details:

- Case:** Dhadav - Autopsy 4.20.0
- Tools:** Add Data Source, Images/Videos, Communications, Geolocation, Timeline, Discovery, Generate Report, Close Case
- Listing Table:**
 - Page: 1 of 1
 - Images: 1-55
 - Medium Thumbnails
 - Sort: Sorted by: ---
- Selected File:** 882548.jpg
- File Preview:** A large thumbnail image showing a sunset over a road with three people on bicycles. The image has a "WELCOME TO HAWKINS" sign visible on the right side.
- File Details:**
 - File Type: JPEG
 - File Size: 1.2 MB
 - MD5 Hash: 882548.jpg
 - SHA256 Hash: 882548.jpg
 - File Path: /img_Pandrive_Test.E01/vol_v02/882548.jpg
- Analysis Results:** Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences
- Annotations:** A note indicates "Analyzing files from Pandrive_Test.E01" and "100% (3 more...)"



8. Verify Recovery: After the recovery process is complete, verify the recovered file's integrity and accessibility to ensure a successful recovery.
9. Document Findings: Record the details of the recovery process, including the file name, location, and any additional observations or notes.

Result:

Using Autopsy, we successfully recovered the target file from the given data source. After adding and configuring the data source within the Autopsy case, we initiated the analysis and performed a search to locate the file. The file was successfully recovered, and its integrity and accessibility were verified. The details of the recovery, including the file name, location, and any relevant observations, were documented for further analysis.

Conclusion:

Autopsy proved to be an effective digital forensics tool for file recovery from the given data source. Its comprehensive search capabilities, combined with the recovery functionality, allowed us to successfully locate and recover the target file. Autopsy can be a valuable asset in forensic investigations, data recovery processes, and digital evidence analysis.

Future Scope:

1. Advanced file carving techniques: Explore Autopsy's advanced file carving capabilities to recover files even in fragmented or damaged states.
2. Timeline analysis: Utilize Autopsy's timeline feature to establish a chronological order of events related to the recovered file and other artifacts.
3. Metadata extraction and analysis: Extract and analyze file metadata using Autopsy to gain further insights into the recovered file's origin, timestamps, and associated attributes.
4. Hash analysis: Perform hash analysis on the recovered file to determine its integrity and check against known hash databases for potential matches.
5. Integration with other forensic tools: Explore integrating Autopsy with other digital forensics tools for a more comprehensive analysis and cross-validation of findings.

Experiment: 8

Title: Install cyber triage and collect the given system report. Analyse your data accordingly

Objective:

The objective of this experiment is to install Cyber Triage, a digital forensic tool, and collect a system report for analysis purposes.

Requirements:

- Cyber Triage system requirements
- Internet connectivity
- Cyber Triage installation package

Procedure/Experiment Steps:

1. Download Cyber Triage: Visit the official Cyber Triage website and download the appropriate installation package for your operating system.
2. Install Cyber Triage: Follow the provided instructions to install Cyber Triage on your computer.
3. Launch Cyber Triage: After installation, launch Cyber Triage from the installed location or desktop shortcut.

The screenshot shows the Cyber Triage Collection Summary interface. The left sidebar has a dark theme with various navigation options like Dashboard, Bad Items, Suspicious Items, Users, Accounts, Inbound Logons, Outbound Logons, Network Shares, Web Artifacts, Data Accessed, Malware, Startup Items (0), Triggered Tasks, Processes, Active Connections, Listening Ports, DNS Cache, System Configuration, OS Config Settings, Files, Timeline, Registry Entries, Search, and Collection Details. The main dashboard area has two cards: 'Bad Items' (0) and 'Suspicious Items' (1). Below these are sections for 'Status' (Targeted Analysis Started, Full Scan Not Started, Online File Reputation Not Started), 'Recent Messages' (listing log collection steps), 'Collection Information' (Incident: Evaluation Incident 2023-07-06, Hostname: evaluation - local host, Created Date: 2023-07-06 19:10:40 IST, Collection Date: 2023-07-06 19:10:51 IST, Collection Tool Version: 3.7.0), 'Host Information' (Local Host Name: Dhaval, Windows Product Name: Windows 10 Home Single Language, Windows Install Date: 2022-10-22 00:35:48 IST, Windows Version: 10.0 (Build 22621), Host IP: [redacted], BitLocker Encryption: System drive is encrypted with BitLocker, Mounted Drives: [redacted]), 'Background Tasks Status' (Processing Collection evaluation - local host | 2023-07-06 19:10:40 IST, Collecting Startup Items... (Step 5 of 14)), and 'Error Messages' (No Errors Occurred). A right-hand sidebar shows a 'Bad Items Timeline' with the message 'No Bad Items To Timeline'.

4. Configure Data Collection: Set up Cyber Triage to collect the system report by selecting the appropriate options or modules within the software.

5. Initiate System Report Collection: Start the system report collection process in Cyber Triage. Allow the software to scan and gather relevant system data.

6. Wait for Data Collection to Complete: Let Cyber Triage complete the system report collection process. The duration may vary depending on the size and complexity of the system being analyzed.

7. Analyze Collected Data: Once the system report collection is finished, access the collected data within Cyber Triage for analysis.

Executable	Arguments	Earliest Execution	Latest Execution	Exec Count
5319275a.whatsappdesktop_cvl1gvanjyjgmapp	Unknown	2023-07-06 19:09:02 IST	2023-07-06 19:09:02 IST	1
microsoft.office.winword.exe.15	Unknown	2023-07-06 19:06:07 IST	2023-07-06 19:06:07 IST	1
vmware-tray.exe	Unknown	2023-07-04 00:57:31 IST	2023-07-06 19:02:14 IST	13
adobeccollabsync.exe	Unknown	2023-07-04 00:57:29 IST	2023-07-06 19:02:13 IST	8
grammarly.desktop.exe	Unknown	2023-07-04 00:57:30 IST	2023-07-06 19:02:04 IST	13
lmc.exe	Unknown	2023-07-04 00:57:28 IST	2023-07-06 19:02:03 IST	13
googledrivefs.exe	--startup_mode	2023-07-04 00:57:26 IST	2023-07-06 19:02:02 IST	13
rtksaudioservice64.exe	-background	2023-07-04 00:57:25 IST	2023-07-06 19:01:56 IST	13
/users/public/desktop/autopy 4.20.0.lnk	Unknown	2023-07-06 19:01:37 IST	2023-07-06 19:01:37 IST	1
/windows/softwaredistribution/securityhealthsetup.exe	Unknown	2023-07-04 18:51:15 IST	2023-07-06 18:51:15 IST	2
ad2f1837-7psupportassistant_v10z@jaglk6e6	Unknown	2023-07-06 17:42:09 IST	2023-07-06 17:42:09 IST	1
microsoft.windows.startm_riencehost_cw5n1h2byewy	Unknown	2023-07-06 17:42:09 IST	2023-07-06 17:42:09 IST	1
microsoft.windows.shellx_riencehost_cw5n1h2byewy	Unknown	2023-07-06 17:42:09 IST	2023-07-06 17:42:09 IST	1

8. Interpret System Report: Review the collected system report to extract valuable insights, identify potential security issues, and gather relevant information for further analysis.
9. Document Findings: Record the details of the analysis, including any identified issues, notable observations, or suspicious artefacts.

Result:

Using Cyber Triage, we successfully installed the software and collected a system report from the given system. After configuring the data collection settings, we initiated the collection process and allowed Cyber Triage to scan and gather the relevant system data. Once the data collection was complete, we accessed and analyzed the collected data within Cyber Triage, identifying potential security issues and extracting valuable insights. The findings and observations from the analysis were documented for further examination and action.

Conclusion:

Cyber Triage proved to be a reliable digital forensic tool for system report collection and analysis. By installing and utilizing Cyber Triage, we were able to gather comprehensive system data and gain insights into potential security issues. The software provides a valuable resource for digital forensic investigations, incident response, and proactive system monitoring.

Future Scope:

1. Deeper analysis capabilities: Utilize advanced features within Cyber Triage to conduct more in-depth analysis, such as memory forensics, timeline analysis, or file carving.
2. Integration with other forensic tools: Explore the integration of Cyber Triage with other digital forensic tools for a more comprehensive and cross-validated analysis.
3. Automation and scripting: Investigate the automation capabilities of Cyber Triage, enabling the creation of custom workflows and scripts to streamline analysis processes.
4. Threat intelligence integration: Integrate Cyber Triage with threat intelligence platforms to enhance analysis by correlating system data with known indicators of compromise.
5. Reporting and visualization: Utilize Cyber Triage's reporting and visualization features to generate comprehensive reports, graphs, and charts for easier data interpretation and communication with stakeholders.



Experiment: 9

Title: Perform digital forensics to analyse RAM timeline using CAINE tool

Objective:

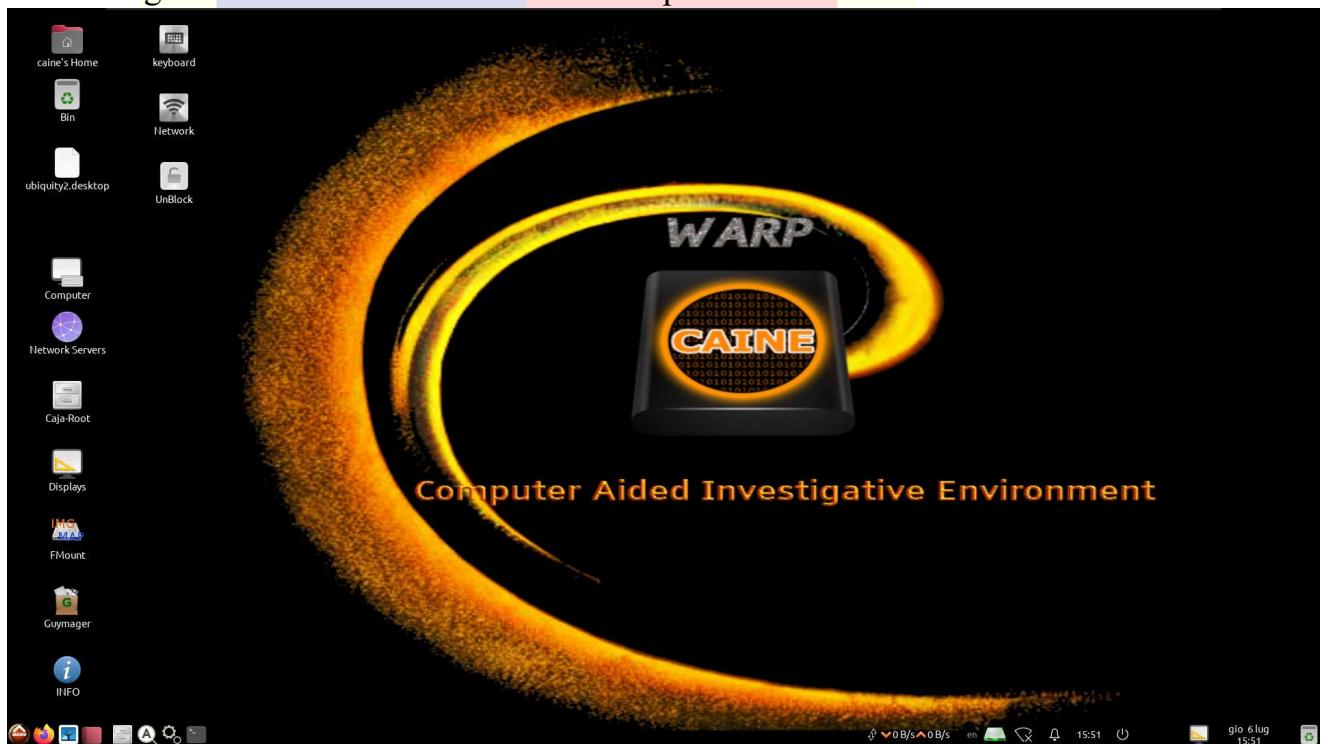
The objective of this experiment is to perform digital forensics analysis on the RAM timeline using the CAINE (Computer Aided Investigative Environment) tool.

Requirements:

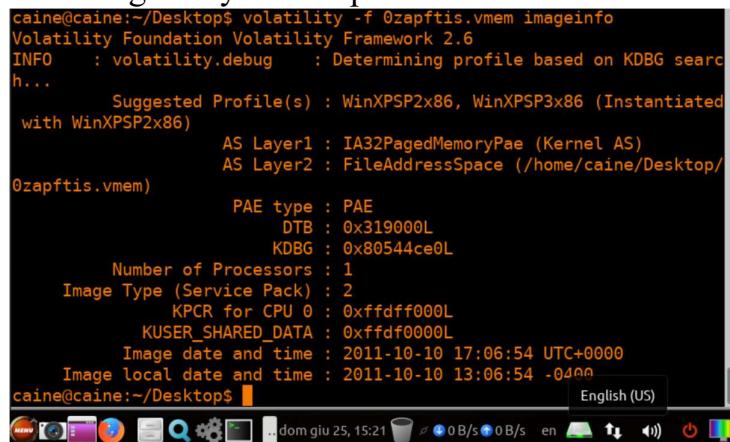
CAIN

Procedure/Experiment Steps:

1. Prepare the Environment: Ensure that the computer meets the system requirements for running CAINE. Install CAINE on the computer.

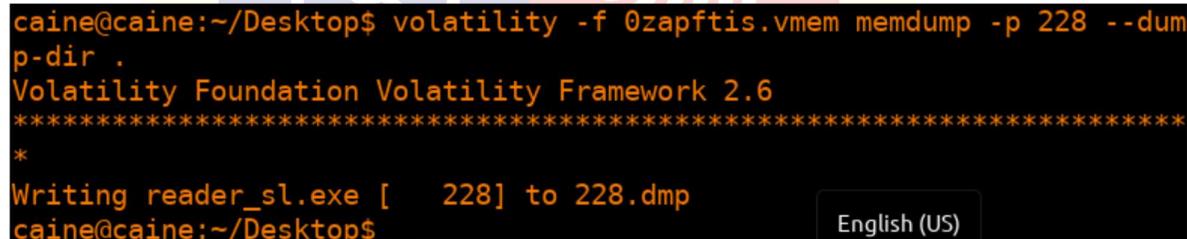


2. Analyze RAM Timeline: Use the CAINE tool to analyze the RAM timeline. This involves examining the timeline of events and activities that occurred in the RAM during the system's operation.



```
caine@caine:~/Desktop$ volatility -f 0zapftis.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/home/caine/Desktop/0zapftis.vmem)
PAE type : PAE
DTB : 0x319000L
KDBG : 0x80544ce0L
Number of Processors : 1
Image Type (Service Pack) : 2
KPCR for CPU 0 : 0xffffd0000L
KUSER_SHARED_DATA : 0xffffdf0000L
Image date and time : 2011-10-10 17:06:54 UTC+0000
Image local date and time : 2011-10-10 13:06:54 -0400
caine@caine:~/Desktop$
```

3. Extract Relevant Information: Identify and extract relevant information from the RAM timeline, such as processes, network connections, file accesses, or any other artifacts of interest.



```
caine@caine:~/Desktop$ volatility -f 0zapftis.vmem memdump -p 228 --dump-dir .
Volatility Foundation Volatility Framework 2.6
*****
*
Writing reader_sl.exe [ 228] to 228.dmp
caine@caine:~/Desktop$
```

4. Interpret the Timeline: Interpret the extracted information to reconstruct the sequence of events and identify any suspicious or malicious activities that may have occurred.
5. Document Findings: Record the details of the analysis, including notable events, timestamps, processes, and any other relevant findings or observations.

Result:

Using the CAINE tool, we successfully analyzed the RAM timeline to investigate the events and activities that occurred during the system's operation. By importing the RAM image into CAINE, we were able to examine the timeline and extract relevant information. Through the analysis, we reconstructed the sequence of events and identified any suspicious or malicious activities. The findings, including notable events, timestamps, processes, and other relevant details, were documented for further investigation and action.

Conclusion:

The CAINE tool proved to be an effective resource for performing digital forensics analysis on the RAM timeline. By leveraging CAINE's capabilities, we were able to explore the timeline of events and activities stored in the RAM image. This analysis plays a crucial role in identifying potential security breaches, investigating incidents, and understanding the system's behavior during a specific timeframe.

Future Scope:

1. Advanced artifact analysis: Dive deeper into the RAM data to extract and analyze specific artifacts, such as volatile data, cryptographic keys, or memory-resident malware.
2. Memory carving techniques: Explore CAINE's memory carving capabilities to recover deleted or obscured data from the RAM image.
3. Memory forensics automation: Investigate the automation capabilities of CAINE for memory forensics analysis, allowing for the creation of custom workflows and scripts to streamline the analysis process.
4. Integration with other forensic tools: Explore the integration of CAINE with other digital forensic tools to enhance the analysis and cross-validation of findings.
5. Research and development: Stay updated with the latest research and developments in RAM analysis techniques, tools, and methodologies to continually enhance the capabilities of CAINE in this area of digital forensics.

NFSU



विद्या अमृतं अङ्गुले

Experiment: 10

Title: Install Wireshark to analyse captured packet. Discuss your results obtained from the tool.

Objective:

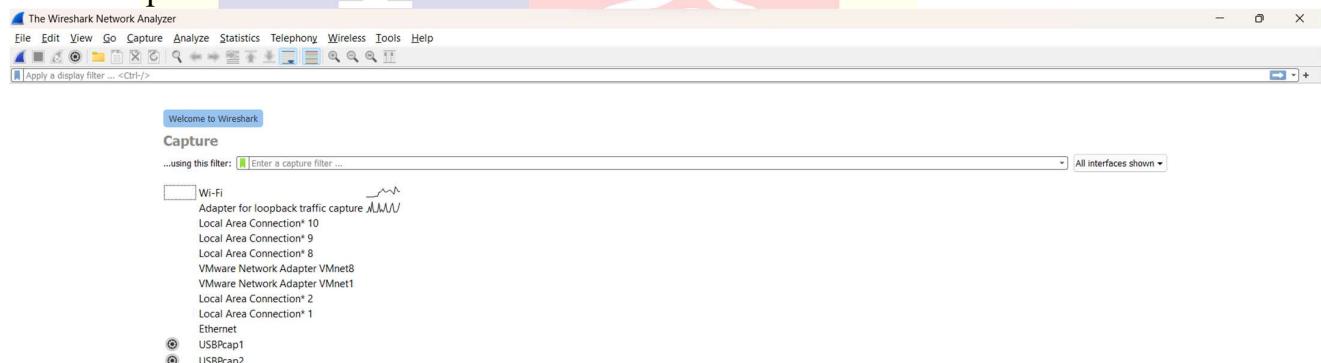
The objective of this experiment is to install Wireshark, a network protocol analyzer, and analyze captured packets using the tool.

Requirements:

Wireshark

Procedure/Experiment Steps:

1. Download Wireshark: Visit the official Wireshark website and download the appropriate installation package for your operating system.
2. Install Wireshark: Follow the provided instructions to install Wireshark on your computer.
3. Launch Wireshark: After installation, launch Wireshark from the installed location or desktop shortcut.

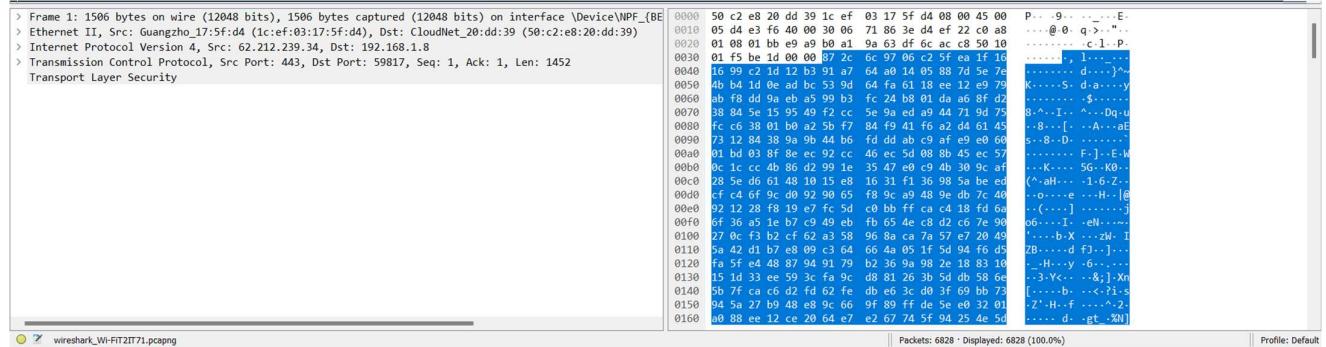


4. Capture Packets: Start capturing packets by selecting the appropriate network interface within Wireshark. Choose the desired capture filters, such as specific protocols or IP addresses, to focus on relevant traffic.

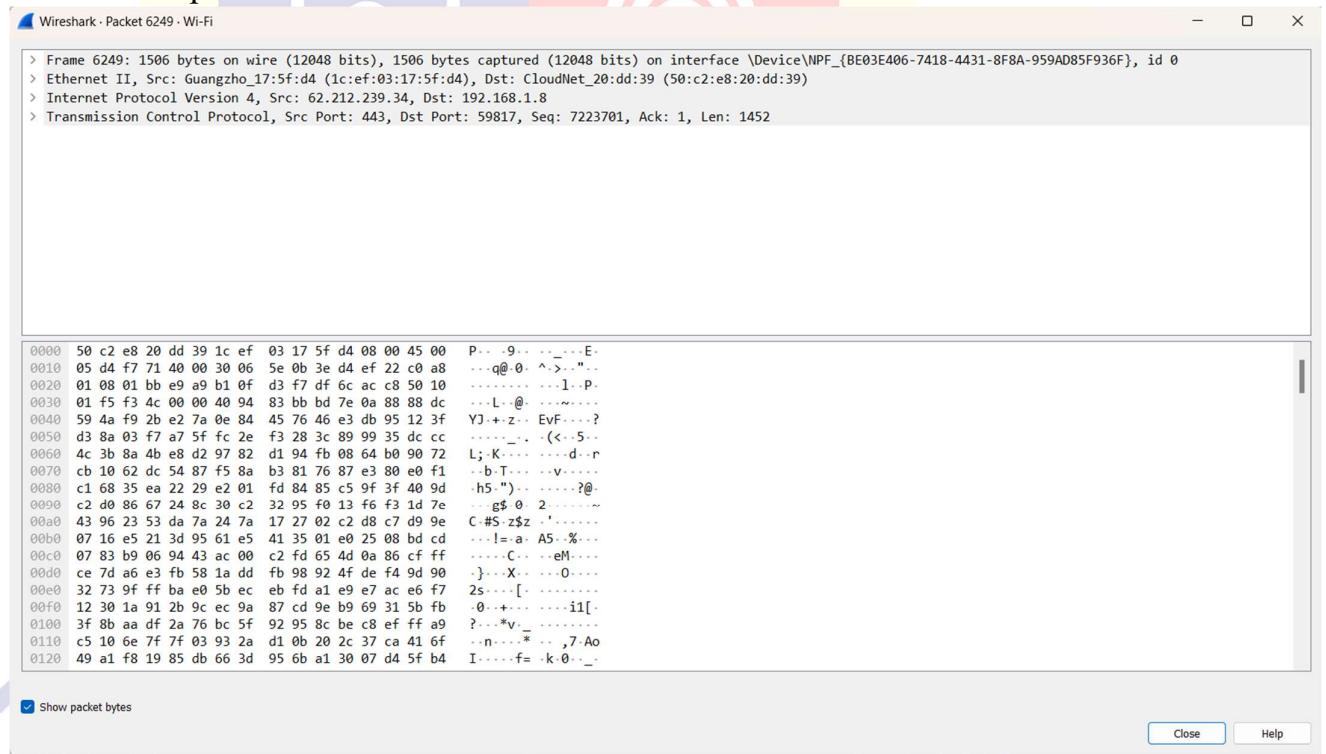
No.	Time	Source	Destination	Protocol	Length	Info
6284 4.840151	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7264357 Ack<1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6285 4.840151	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7265809 Ack<1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6286 4.840151	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7267261 Ack<1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6287 4.840151	62.212.239.34	192.168.1.8	SSLv2	1506	Encrypted Data	
6288 4.841160	192.168.1.8	62.212.239.34	TCP	74	[TCP Dup ACK 629451] 59817 → 443 [ACK] Seq=1 Ack=6979765 Win=16516 Len=0 SLE=7181593 SRE=7270165 SLE=6981217 SRE=7177237	
6289 4.844299	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7270165 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6290 4.844299	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7271617 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6291 4.844299	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7273069 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6292 4.844299	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7274521 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6293 4.845395	192.168.1.8	62.212.239.34	TCP	74	[TCP Dup ACK 629452] 59817 → 443 [ACK] Seq=1 Ack=6979765 Win=16516 Len=0 SLE=7181593 SRE=7275973 SLE=6981217 SRE=7177237	
6294 4.846372	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7275973 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6295 4.846372	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7277425 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6296 4.846372	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7278877 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6297 4.846372	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7289329 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6298 4.847386	192.168.1.8	62.212.239.34	TCP	74	[TCP Dup ACK 629453] 59817 → 443 [ACK] Seq=1 Ack=6979765 Win=16516 Len=0 SLE=7181593 SRE=7281781 SLE=6981217 SRE=7177237	
6299 4.848456	62.212.239.34	192.168.1.8	SSLv2	1506	Encrypted Data	
6300 4.848456	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7283233 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6301 4.848456	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7284685 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6302 4.848456	62.212.239.34	192.168.1.8	TCP	1506	443	→ 59817 [ACK] Seq=7286137 Ack=1 Win=501 Len=1452 [TCP segment of a reassembled PDU]
6303 4.849484	192.168.1.8	62.212.239.34	TCP	74	[TCP Dup ACK 629454] 59817 → 443 [ACK] Seq=1 Ack=6979765 Win=16516 Len=0 SLE=7181593 SRE=7287589 SLE=6981217 SRE=7177237	

5. Monitor Packet Capture: Let Wireshark capture packets for a specific duration or until you have gathered sufficient data for analysis.

6. Stop Packet Capture: Stop the packet capture process in Wireshark once you have captured enough packets.
7. Analyze Captured Packets: Explore the captured packets within Wireshark to analyze network traffic, dissect protocols, and identify any anomalies or security issues.



8. Interpret Results: Interpret the results obtained from Wireshark analysis, paying attention to packet details, protocols used, source and destination addresses, and any observed patterns or abnormalities.



9. Document Findings: Record the details of the analysis, including notable findings, suspicious activities, or any other relevant observations.

Result:

By installing and utilizing Wireshark, we successfully captured and analyzed packets from the network traffic. After launching Wireshark, we captured packets using the specified capture filters. Once the capture was complete, we analyzed the captured packets within Wireshark, dissecting protocols, and examining packet details. The analysis yielded notable findings, including unusual network behaviors, suspicious traffic patterns, or security issues, which were documented for further investigation and action.

Conclusion:

Wireshark is a powerful network protocol analyzer that allows for the detailed analysis of captured packets. Through its intuitive interface and robust features, we were able to capture and examine network traffic, dissect protocols, and identify potential security issues. Wireshark proves to be a valuable tool for network troubleshooting, performance analysis, and security monitoring.

Future Scope:

1. Deep packet inspection: Utilize Wireshark's advanced features to perform deep packet inspection, including extracting and analyzing application-layer data, payloads, and specific protocol behaviors.
2. Network forensics analysis: Apply Wireshark's capabilities for network forensics investigations, including identifying attack patterns, malicious activities, or evidence of data breaches.
3. Statistical analysis: Leverage Wireshark's statistical tools and plugins to perform statistical analysis on captured packets, such as traffic patterns, packet sizes, or network latency.
4. Integration with other tools: Explore the integration of Wireshark with complementary tools, such as intrusion detection systems (IDS), security information and event management (SIEM) platforms, or traffic visualization tools, for enhanced network analysis and correlation of events.
5. Stay updated with Wireshark: Regularly update Wireshark to benefit from the latest features, protocol dissectors, and security enhancements, ensuring efficient and accurate packet analysis.

विद्या अमृतं अङ्गु

Experiment: 11

Title: Examine files, folders on local hard disk and network drive using FTK Imager

Objective:

The objective of this experiment is to utilize FTK Imager, a digital forensic tool, to examine files and folders on both a local hard disk and a network drive.

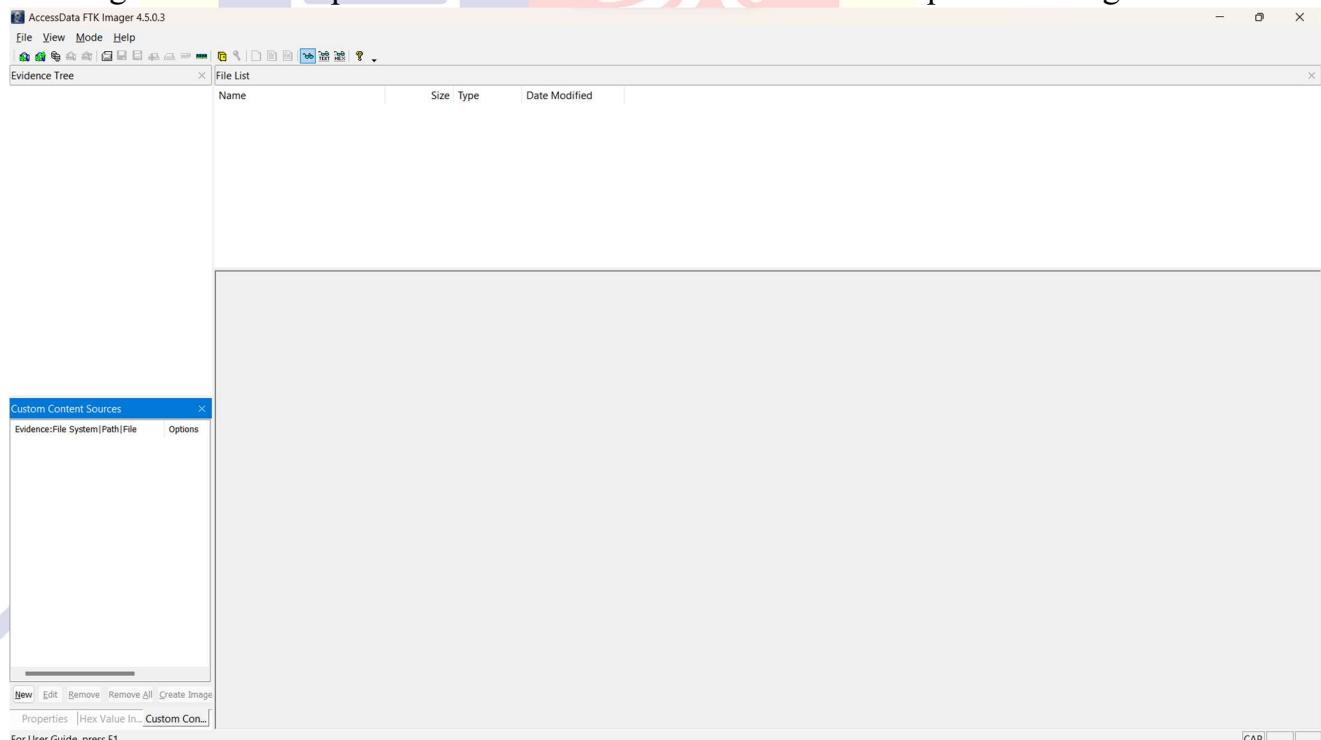
Requirements:

FTK Imager

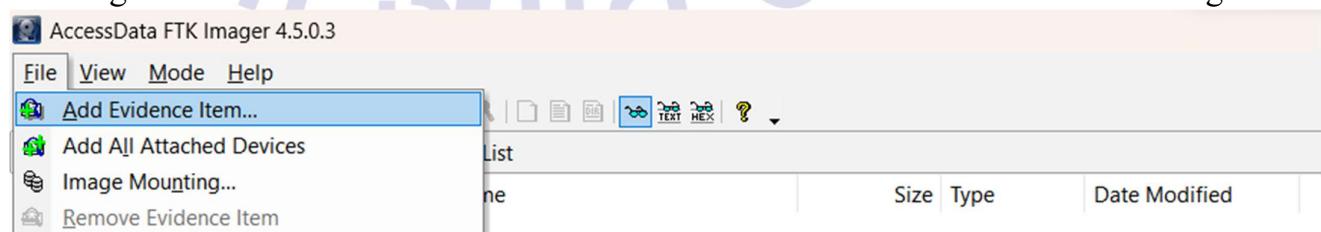
Disk or drive for make image

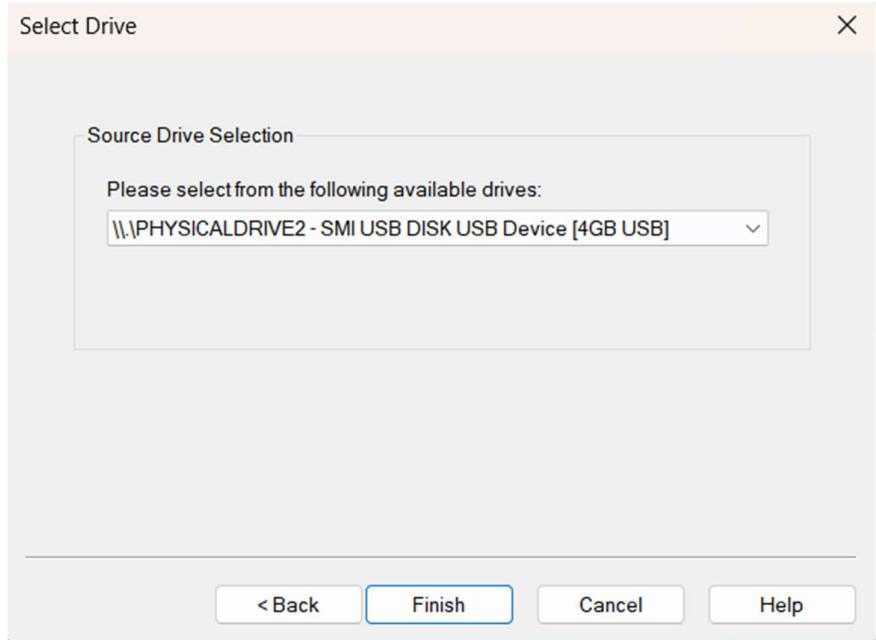
Procedure/Experiment Steps:

1. Prepare the Environment: Ensure that the computer meets the system requirements for running FTK Imager. Install FTK Imager on the computer.
2. Launch FTK Imager: Start FTK Imager from the installed location or desktop shortcut.
3. Acquire Local Hard Disk Image: Create an image of the local hard disk using FTK Imager. Follow the provided instructions within the tool to acquire the image.

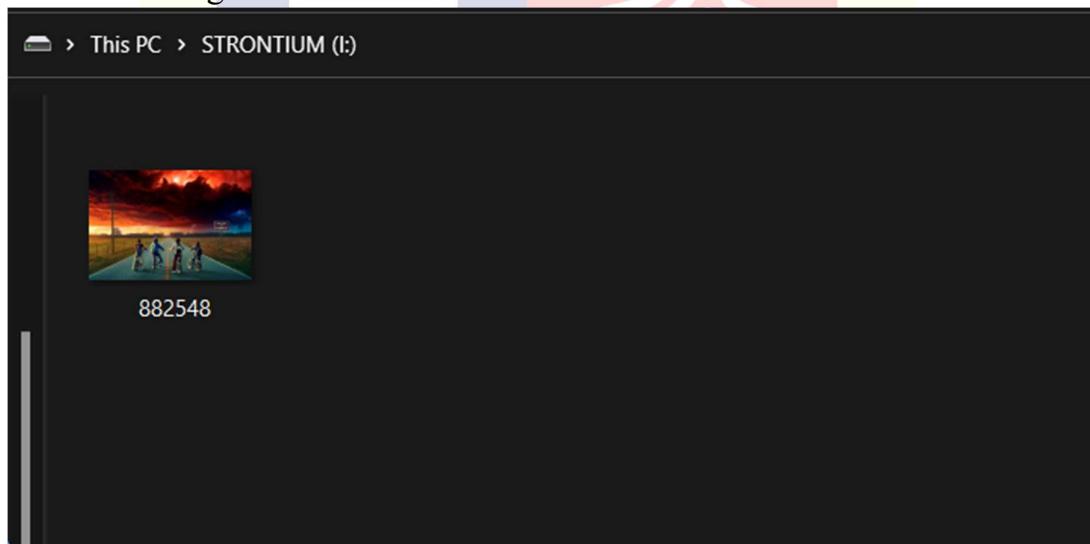


4. Add Local Hard Disk Image: Import the acquired local hard disk image into FTK Imager. This will allow examination of the file and folder structure within the image.



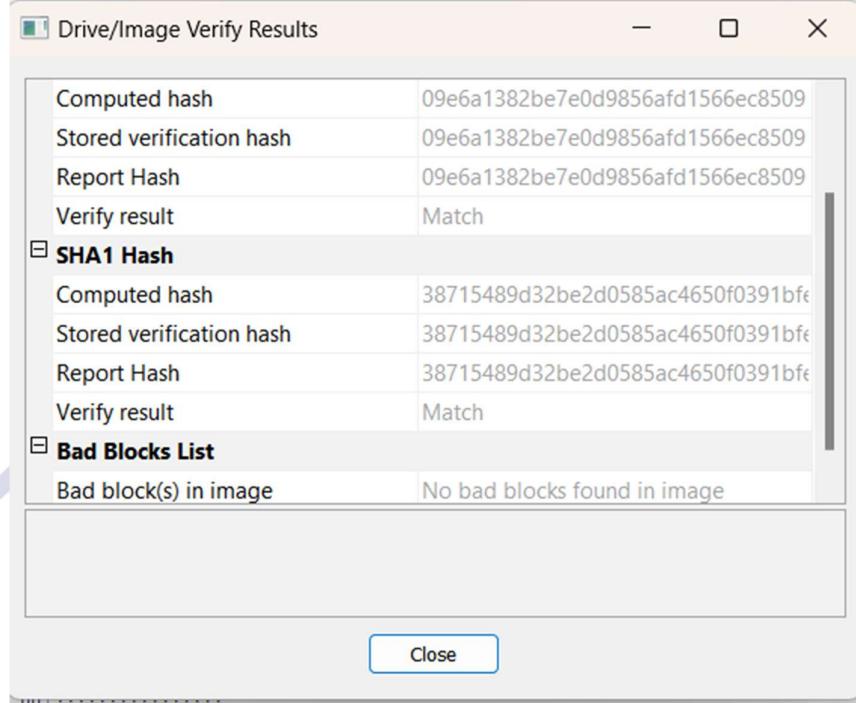
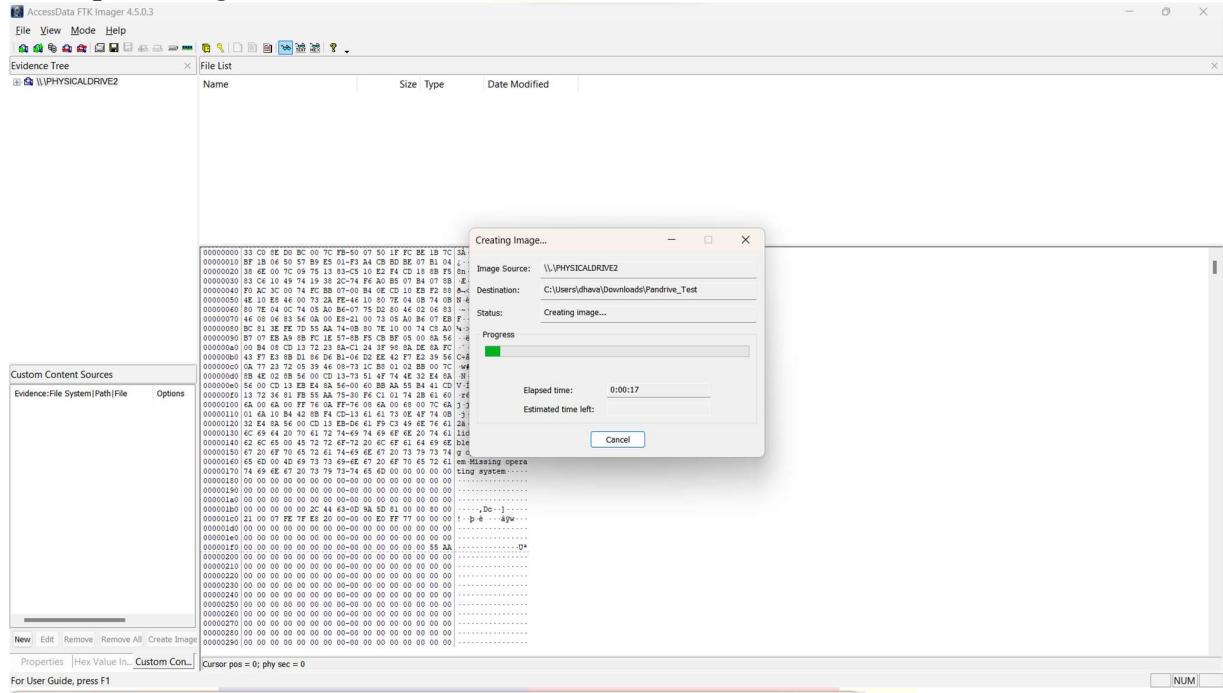


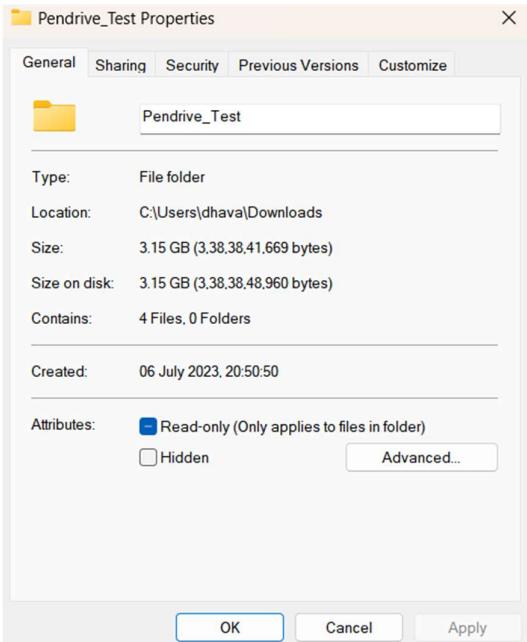
5. File or image in the drive



6. Explore Local Hard Disk: Use FTK Imager to navigate through the file and folder structure of the local hard disk image. Examine the files, folders, metadata, and any other relevant information.

7. Export Image file





8. Document Findings: Record the details of the examination, including notable files, folders, timestamps, or any other relevant findings or observations.

Result:

By utilizing FTK Imager, we successfully examined files and folders on both a local hard disk and a network drive. We acquired images of the local hard disk and network drive, and then imported them into FTK Imager for analysis. Using the tool, we explored the file and folder structures, examined metadata, and documented relevant findings. Notable files, folders, timestamps, and other observed details were recorded for further analysis and reporting.

Conclusion:

FTK Imager is an effective digital forensic tool for examining files and folders on local and network drives. Through its image acquisition and analysis capabilities, we were able to navigate and explore the file systems of both the local hard disk and the network drive. FTK Imager proves to be a valuable asset in digital forensic investigations, data recovery processes, and file system analysis.

Future Scope:

1. Advanced metadata analysis: Utilize FTK Imager's metadata extraction capabilities to gather and analyze extended file attributes, timestamps, file permissions, and other relevant information.
2. Carving and recovery techniques: Explore FTK Imager's file carving and recovery features to extract deleted or hidden files from acquired images.
3. Timeline analysis: Perform timeline analysis using FTK Imager to establish a chronological order of file creation, modification, or access events.
4. Integration with other forensic tools: Explore the integration of FTK Imager with other digital forensic tools to enhance analysis and cross-validation of findings.
5. Stay updated with FTK Imager: Regularly update FTK Imager to benefit from the latest features, improvements, and support for new file system formats, ensuring efficient and accurate file and folder examination.

Experiment: 12

Title: Install Tally software and create a company. Add sufficient data. After modifications, analyze the windows registry to identify evidence related to the company.

Objective:

The objective of this experiment is to install Tally software, create a company, add sufficient data, and then analyze the Windows registry to identify evidence related to the company.

Requirements:

Tally Software

Procedure/Experiment Steps:

1. Prepare the Environment: Ensure that the computer meets the system requirements for running Tally software. Install Tally software on the computer.
2. Launch Tally Software: Start Tally software from the installed location or desktop shortcut.
3. Create a Company: Follow the provided instructions within Tally software to create a new company. Provide the necessary details, such as company name, address, and financial year.
4. Add Sufficient Data: Populate the created company with sufficient data, including ledger entries, vouchers, and transactions. This will ensure a realistic representation for analysis purposes.
5. Modify Company Data: Make modifications to the company data, such as altering ledger entries, updating voucher details, or changing transaction information. Document the modifications made for future reference.
6. Analyze Windows Registry: Launch the Windows Registry Editor on the computer.
7. Navigate to Tally Entries: Within the Windows Registry Editor, navigate to the registry entries related to Tally software. These entries can typically be found under "HKEY_CURRENT_USER" or "HKEY_LOCAL_MACHINE" in the "Software" or "Programs" section.
8. Examine Registry Keys and Values: Analyze the registry keys and values associated with Tally software. Look for evidence of the created company, modified data, or any other relevant information related to Tally usage.
9. Document Findings: Record the details of the analysis, including notable registry keys, values, timestamps, or any other evidence discovered.

Result:

By installing Tally software and creating a company, we successfully populated the company with sufficient data. Modifications were made to the company data, and the Windows Registry was analyzed to identify evidence related to the company. Registry keys, values, and other relevant information were examined, and notable findings were documented for further analysis and reporting.

Conclusion:

Tally software provides an efficient accounting solution, and its usage leaves traces in the Windows Registry. By installing Tally, creating a company, and modifying company data, we were able to examine the Windows Registry to identify evidence related to the company. Analyzing the registry provides insights into Tally software usage, company data modifications, and other relevant information for forensic investigations.

Future Scope:

1. Advanced registry analysis: Dive deeper into the Windows Registry to identify additional evidence related to Tally software usage, user activities, or specific data modifications.
2. Timeline analysis: Conduct timeline analysis by correlating registry entries with other artifacts to establish a chronological sequence of events related to Tally software usage and company data modifications.
3. Registry forensics: Explore other forensic tools and techniques dedicated to Windows Registry analysis to extract and interpret more detailed information from the registry.
4. Integration with other forensic tools: Investigate the integration of Tally software and Windows Registry analysis with other digital forensic tools to enhance analysis and cross-validation of findings.
5. Stay updated with Tally software: Regularly update Tally software to benefit from the latest features, improvements, and security enhancements, ensuring efficient and accurate accounting data management and analysis.

Experiment: 13

Title: Install fedora workstation using virtual environment to demonstrate working of open source-based platform

Objective:

The objective of this experiment is to install Fedora Workstation, an open-source-based platform, using a virtual environment and demonstrate its functionalities and features.

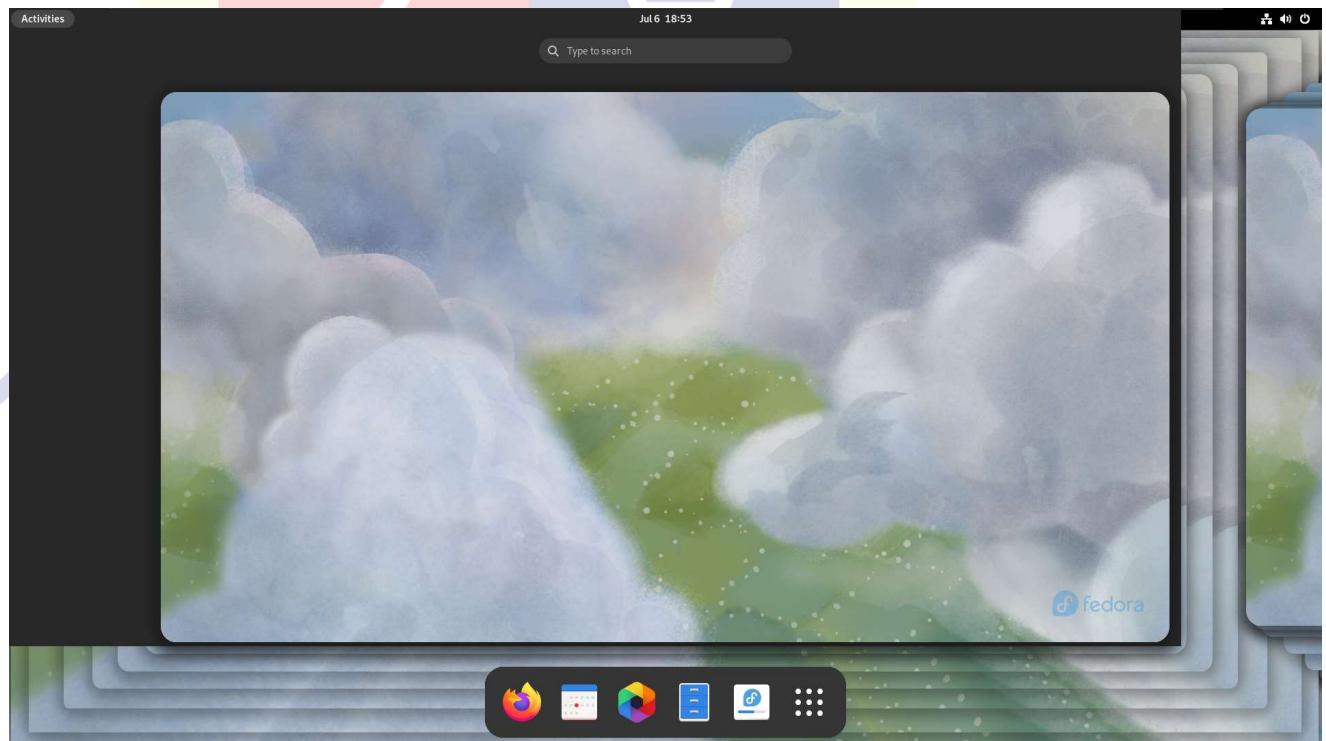
Requirements:

Virtualization tool

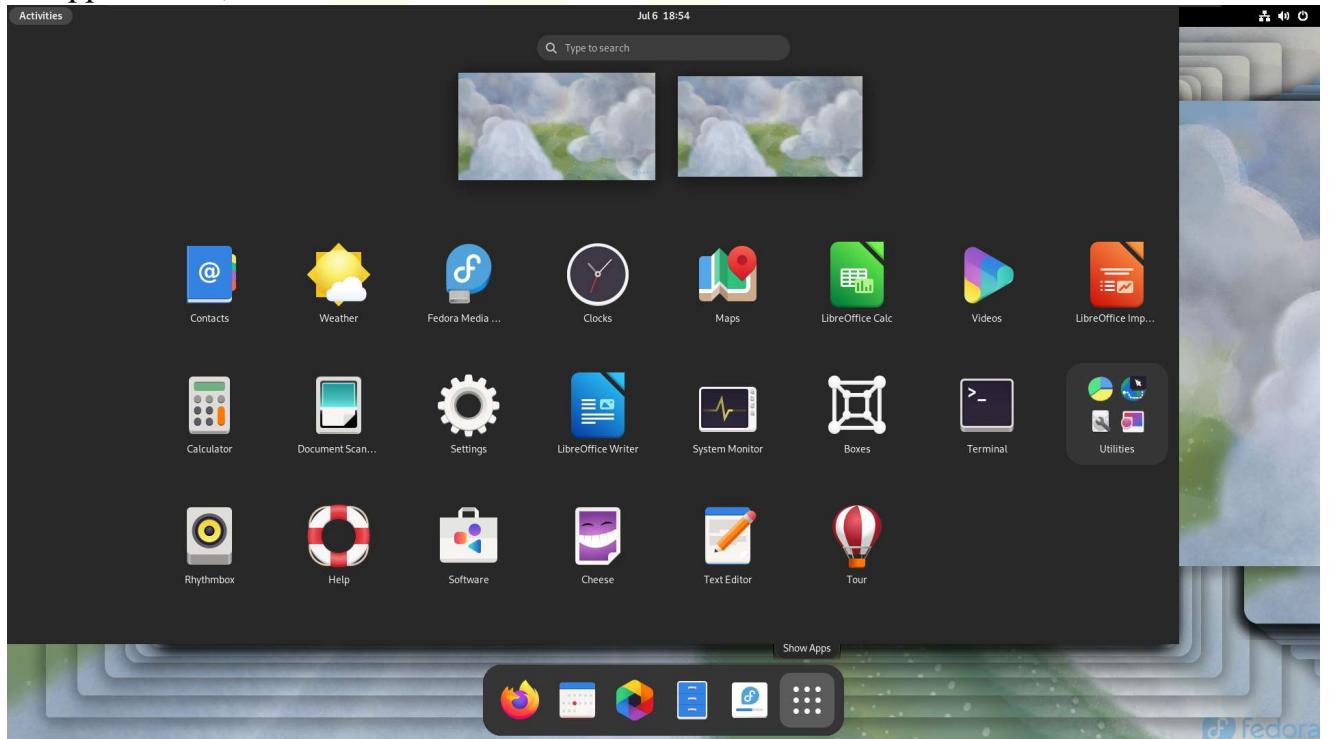
Fedora iso

Procedure/Experiment Steps:

1. Set Up Virtual Environment: Install virtualization software (e.g., Oracle VM VirtualBox) on your computer, ensuring that it meets the system requirements.
2. Download Fedora Workstation: Obtain the Fedora Workstation ISO image from the official Fedora website (<https://getfedora.org>).
3. Create a Virtual Machine: Open the virtualization software and create a new virtual machine. Configure the virtual machine settings, including the name, memory size, hard disk, and network settings.
4. Install Fedora Workstation: Attach the Fedora Workstation ISO image to the virtual machine's optical drive. Start the virtual machine and follow the on-screen instructions to install Fedora Workstation.



- Configure Fedora Workstation: Set up Fedora Workstation by providing necessary information during the installation process, such as the language, time zone, user account, and network settings.
- Explore Fedora Workstation: Once the installation is complete, launch Fedora Workstation within the virtual machine and familiarize yourself with its interface, applications, and functionalities.



- Document Observations: Record your observations and experiences while working with Fedora Workstation, highlighting notable features, performance, and user-friendliness.

Result:

By setting up a virtual environment and installing Fedora Workstation, we successfully demonstrated the functionalities and features of this open-source-based platform. After configuring the necessary settings during installation, we explored the GNOME desktop environment, utilized software management tools, and performed tasks such as web browsing, document editing, and file management. Throughout the demonstration, we documented our observations, noting key features, performance, and overall user experience.

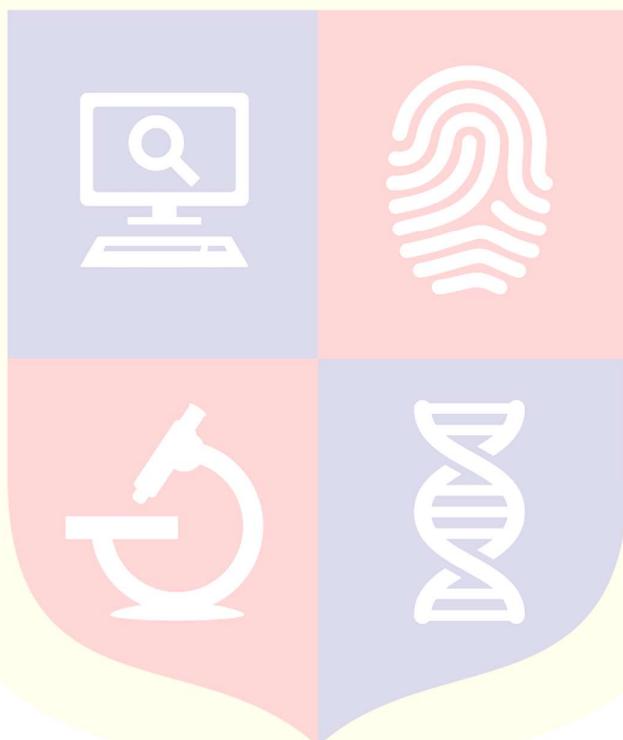
Conclusion:

Fedora Workstation, as an open-source-based platform, provides a robust and user-friendly environment for productivity and various computing tasks. By installing Fedora Workstation in a virtual environment, we showcased its key features, including the GNOME desktop environment, software management, and customization options. Fedora Workstation proves to be a viable open-source choice for individuals and organizations seeking a reliable and feature-rich operating system.

Future Scope:

1. Advanced customization: Explore advanced customization options within Fedora Workstation, such as desktop theming, extensions, and application integration.
2. Software development environment: Utilize Fedora Workstation for software development purposes, leveraging its tools, libraries, and package management system.
3. Security features: Investigate the security features and tools available in Fedora Workstation, such as SELinux (Security-Enhanced Linux) and firewall configuration.
4. Integration with enterprise solutions: Explore the integration of Fedora Workstation with enterprise solutions and services, such as cloud platforms or centralized user management systems.
5. Stay updated with Fedora: Regularly update Fedora Workstation to benefit from the latest software updates, security patches, and new features, ensuring a stable and secure computing environment.

NFSU



विद्या अमृतं अङ्गु

Experiment: 14

Title: Use USB drive as data source and Belkasoft X to demonstrate data / file carving

Objective:

The objective of this experiment is to utilize Belkasoft X, a digital forensics tool, to demonstrate data/file carving from a USB drive.

Requirements:

Belkasoft installer

Procedure/Experiment Steps:

1. Prepare the Environment: Ensure that the computer meets the system requirements for running Belkasoft X. Install Belkasoft X on the computer.
2. Connect USB Drive: Connect the USB drive containing the data for carving to the computer.
3. Launch Belkasoft X: Start Belkasoft X from the installed location or desktop shortcut.
4. Add USB Drive as Evidence Source: Within Belkasoft X, add the connected USB drive as an evidence source. Follow the provided instructions in the software to add and mount the USB drive.
5. Start Carving Process: Initiate the carving process within Belkasoft X to search for and recover deleted or hidden files from the USB drive. Configure the carving settings according to your requirements.
6. Monitor Carving Progress: Let Belkasoft X perform the carving process on the USB drive. Monitor the progress of the carving operation within the software.
7. Examine Carved Files: Once the carving process is complete, explore the carved files within Belkasoft X. Review the recovered files and metadata, such as file types, timestamps, and file paths.
8. Recover Selected Files: Select the desired carved files within Belkasoft X and recover them to a designated location on the computer's storage.
9. Document Findings: Record the details of the carving process, including notable findings, recovered files, timestamps, or any other relevant observations.

Result:

By using Belkasoft X, we successfully demonstrated data/file carving from a USB drive. The USB drive containing the data was added as an evidence source within Belkasoft X. The carving process was initiated, and deleted or hidden files were recovered from the USB drive. The carved files were examined within Belkasoft X, and selected files were successfully recovered to a designated location for further analysis.

Conclusion:

Belkasoft X proved to be an effective digital forensic tool for data/file carving from a USB drive. Through its intuitive interface and carving capabilities, we were able to search for and extract recoverable files from the USB drive. Carving can be a valuable technique in forensic investigations, data recovery processes, and extracting valuable artifacts from various data sources.

Future Scope:

1. Advanced carving techniques: Explore Belkasoft X's advanced carving features, such as custom file signatures, data pattern analysis, or deep carving for fragmented files.
2. File system-specific carving: Investigate Belkasoft X's support for specific file systems (e.g., FAT, NTFS, HFS+) and perform carving based on file system-specific structures.
3. Carving from other data sources: Extend carving capabilities to other data sources, such as disk images, memory dumps, or network captures, using Belkasoft X.
4. Integration with other forensic tools: Explore the integration of Belkasoft X with other digital forensic tools to enhance analysis and cross-validation of carved files.
5. Stay updated with Belkasoft X: Regularly update Belkasoft X to benefit from the latest features, improvements, and support for new file formats or carving techniques, ensuring efficient and accurate file carving.



विद्या अमृतं अङ्गोऽन्तः

Experiment: 15

Title: Use PhotoRec to recover lost files, audio or video content from the HDD/USB Drive using file carving

Objective:

The objective of this experiment is to utilize PhotoRec, a file recovery tool, to recover lost files, including audio and video content, from an HDD or USB drive using file carving techniques.

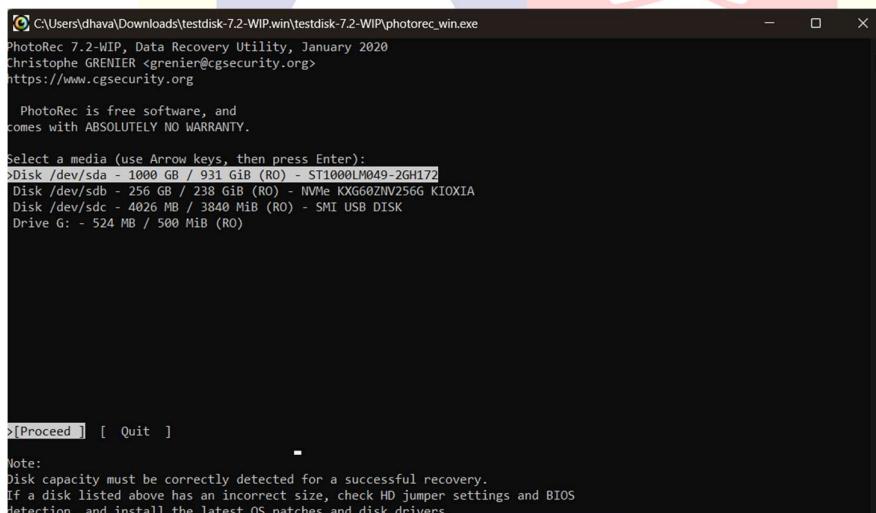
Requirements:

PhotoRec

Disk or drive contain lost file for recovery

Procedure/Experiment Steps:

1. Prepare the Environment: Ensure that the computer meets the system requirements for running PhotoRec. Install PhotoRec on the computer.
2. Connect HDD/USB Drive: Connect the HDD or USB drive containing the lost files to be recovered to the computer.
3. Launch PhotoRec: Start PhotoRec from the installed location or command-line interface.



4. Select Target Drive: Choose the target drive (HDD or USB drive) from which the lost files need to be recovered using PhotoRec.

```
C:\Users\dhava\Downloads\testdisk-7.2-WIP.win\testdisk-7.2-WIP\photorec_win.exe
PhotoRec 7.2-WIP, Data Recovery Utility, January 2020
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdc - 4026 MB / 3840 MiB (RO) - SMI USB DISK

Partition      Start      End  Size in sectors
  No partition    0     0 1   489 135 30  7864320 [Whole disk]
> 1 * HPFS - NTFS    0     0 33 489 135 30  7864288 [STRONTIUM]

>[ Search ] [Options ] [File Opt] [ Quit ]
          Start file recovery
```

5. Configure File Carving Settings: Configure the file carving settings within PhotoRec, such as the file types to recover (e.g., audio, video), block size, and other advanced options as needed.

```
C:\Users\dhava\Downloads\testdisk-7.2-WIP.win\testdisk-7.2-WIP\photorec_win.exe
PhotoRec 7.2-WIP, Data Recovery Utility, January 2020
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

1 * HPFS - NTFS          0     0 33 489 135 30  7864288 [STRONTIUM]

Please choose if all space needs to be analysed:
>[ Free ] Scan for file from NTFS unallocated space only
[ Whole ] Extract files from whole partition
```

6. Start Recovery Process: Initiate the file recovery process in PhotoRec to scan the target drive for lost files and employ file carving techniques to recover them.

```
C:\Users\dhava\Downloads\testdisk-7.2-WIP.win\testdisk-7.2-WIP\photorec_win.exe
PhotoRec 7.2-WIP, Data Recovery Utility, January 2020
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

isk /dev/sdc - 4026 MB / 3840 MiB (RO) - SMI USB DISK
Partition Start End Size in sectors
1 * HPFS - NTFS 0 33 489 135 30 7864288 [STRONTIUM]

estination /cygdrive/i/System Volume Information/recup_dir

ass 1 - Reading sector 2121168/7864288, 0 files found
lapsed time 0h00m03s - Estimated time to completion 0h00m08

Stop
```

7. Monitor Recovery Progress: Monitor the recovery progress within PhotoRec, allowing the tool to scan and analyze the target drive for recoverable files.
8. Review Recovered Files: Once the recovery process is complete, review the recovered files within PhotoRec. Verify the integrity of the recovered files and organize them accordingly.

```
C:\Users\dhava\Downloads\testdisk-7.2-WIP.win\testdisk-7.2-WIP\photorec_win.exe
PhotoRec 7.2-WIP, Data Recovery Utility, January 2020
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk /dev/sdc - 4026 MB / 3840 MiB (RO) - SMI USB DISK
Partition Start End Size in sectors
No partition 0 0 1 489 135 30 7864320 [Whole disk]

99 files saved in /cygdrive/i/System Volume Information/recup_dir directory.
Recovery completed.

You are welcome to donate to support and encourage further development
https://www.cgsecurity.org/wiki/Donation

[ Quit ]
```

9. Document Findings: Record the details of the recovery process, including notable recovered files, their original locations (if available), and any other relevant observations.

Result:

Using PhotoRec, we successfully recovered lost files, including audio and video content, from the HDD/USB drive. By selecting the target drive and configuring the file carving settings, we initiated the recovery process in PhotoRec. Upon completion, we reviewed the recovered files, verified their integrity, and organized them for further analysis. Notable findings, including recovered files and relevant observations, were documented for future reference.

Conclusion:

PhotoRec proved to be an effective file recovery tool for retrieving lost files, including audio and video content, from an HDD or USB drive using file carving techniques. Through its usage, we were able to scan and recover files that were no longer accessible through conventional means. File carving plays a crucial role in forensic investigations, data recovery processes, and restoring important data from various storage devices.

Future Scope:

1. Advanced file carving techniques: Explore PhotoRec's advanced options and techniques for specific file types, fragmented files, or customized file signatures.
2. Disk imaging integration: Integrate PhotoRec with disk imaging tools to recover files from disk images, improving the efficiency and flexibility of file recovery processes.
3. Automated recovery workflows: Investigate the automation capabilities of PhotoRec, enabling the creation of custom recovery workflows and scripts to streamline the recovery process.
4. Integration with other forensic tools: Explore the integration of PhotoRec with other digital forensic tools to enhance analysis, cross-validation of findings, and a more comprehensive recovery process.
5. Stay updated with PhotoRec: Regularly update PhotoRec to benefit from the latest features, improvements, and support for new file formats or carving techniques, ensuring efficient and accurate file recovery.