LAB MANUAL (IRM)

Exp. No: 1 **Date: 15-6-2023**

Title: Analyze and monitor system logs using the event viewer

Requirements: A computer having windows-based operating system. An event viewer tool installed on this system

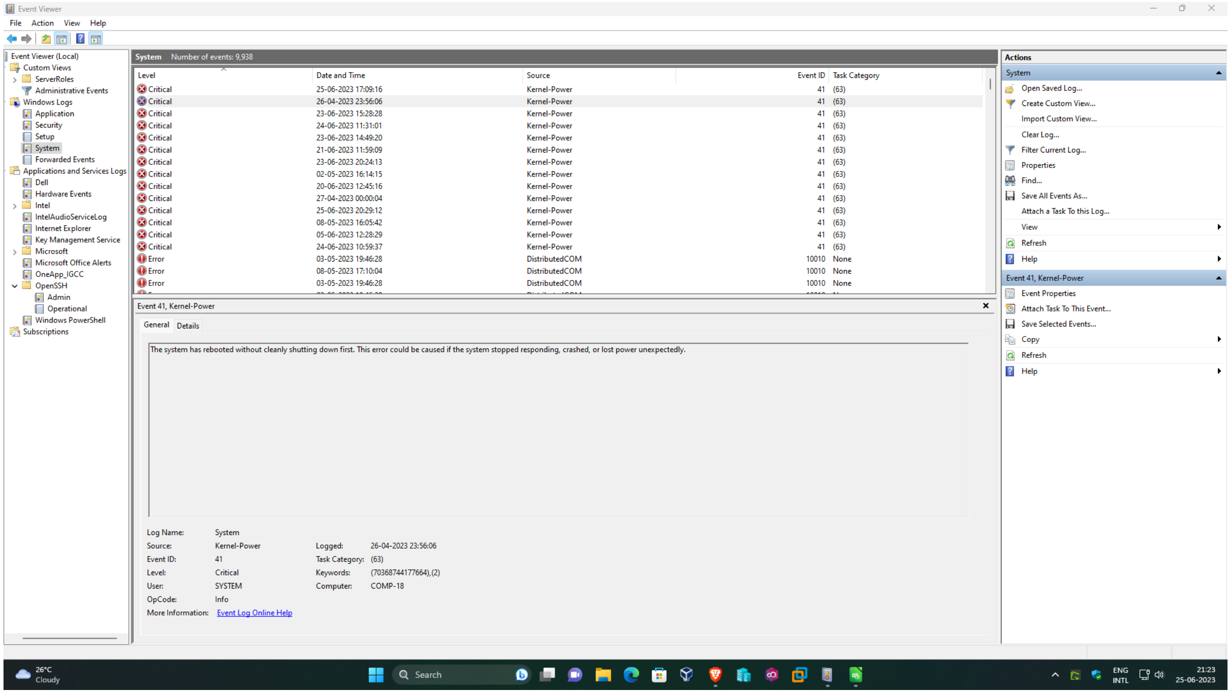
Objectives:

Monitor system for performance and security, using event viewer.

Procedure:

Install the event viewer tool. run the tool to collect system logs. In an ideal condition, it is expected to run the tool 24×7 to identify incidents related to system security. Performance issues, if any, are identified based on the collected dataset. The system performance related to applications, security and system is used to perform analysis. The obtained results are shown below.

Results & Observations:



System Number of events: 9,938

Level	Date and Time	Source	Event ID	Task Category
Critical	25-06-2023 17:09:16	Kernel-Power	41	(63)
Critical	26-04-2023 23:56:06	Kernel-Power	41	(63)
Critical	23-06-2023 15:28:28	Kernel-Power	41	(63)
Critical	24-06-2023 11:31:01	Kernel-Power	41	(63)
Critical	23-06-2023 14:49:20	Kernel-Power	41	(63)
Critical	21-06-2023 11:59:09	Kernel-Power	41	(63)
Critical	23-06-2023 20:24:13	Kernel-Power	41	(63)
Critical	02-05-2023 16:14:15	Kernel-Power	41	(63)
Critical	20-06-2023 12:45:16	Kernel-Power	41	(63)
Critical	27-04-2023 00:00:04	Kernel-Power	41	(63)
Critical	25-06-2023 20:29:12	Kernel-Power	41	(63)
Critical	08-05-2023 16:05:42	Kernel-Power	41	(63)
Critical	05-06-2023 12:28:29	Kernel-Power	41	(63)
Critical	24-06-2023 10:59:37	Kernel-Power	41	(63)
Error	03-05-2023 19:46:28	DistributedCOM	10010	None
Error	08-05-2023 17:10:04	DistributedCOM	10010	None
Error	03-05-2023 19:46:28	DistributedCOM	10010	None

Event 41, Kernel-Power

The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.

Log Name:	System		
Source:	Kernel-Power	Logged:	26-04-2023 23:56:06
Event ID:	41	Task Category:	(63)
Level:	Critical	Keywords:	(70368744177664),(2)
User:	SYSTEM	Computer:	COMP-18
OpCode:	Info		
More Information:	Event Log Online Help		

Fig 1: Dashboard of event viewer

Level	Date & Time	Source	Event ID	Task Category
Critical	14-06-2023 3.15.36 PM	Kernel-Power	41	(63)
Critical	12-06-2023 2.52.20 PM	Kernel-Power	41	(63)
Critical	13-05-2023 5.14.24 PM	Kernel-Power	41	(63)
Critical	10-05-2023 4.03.12 PM	Kernel-Power	41	(63)
Critical	11-05-2023 3.03.12 PM	Kernel-Power	41	(63)

Table 1: Critical System events in 30 days

Result analysis and discussion:

To check the system performance and security, an event viewer was used. The system was evaluated based on events and logs related to system, security and applications. From table-1 it is observed that in last 30 days, four critical events were generated by the kernel having event ID 41 and Task category 63. No critical events were observed regarding system security and application

Future Scope:

In the above experiment the event viewer was used from the specified system. This limits the usability to a single node. In actual scenario, multiple computers which are connected in some topology are available. High end tool that collectively collects real-time logs may be used in future.

Exp. No: 2 **Date: 16-6-2023**

Title: Install and demonstrate system internal tools (Process Explorer). Classify data with process ID and company name

Requirements: A computer having at least 4GB RAM and installed windows-based operating system. Install process explorer to obtain results.

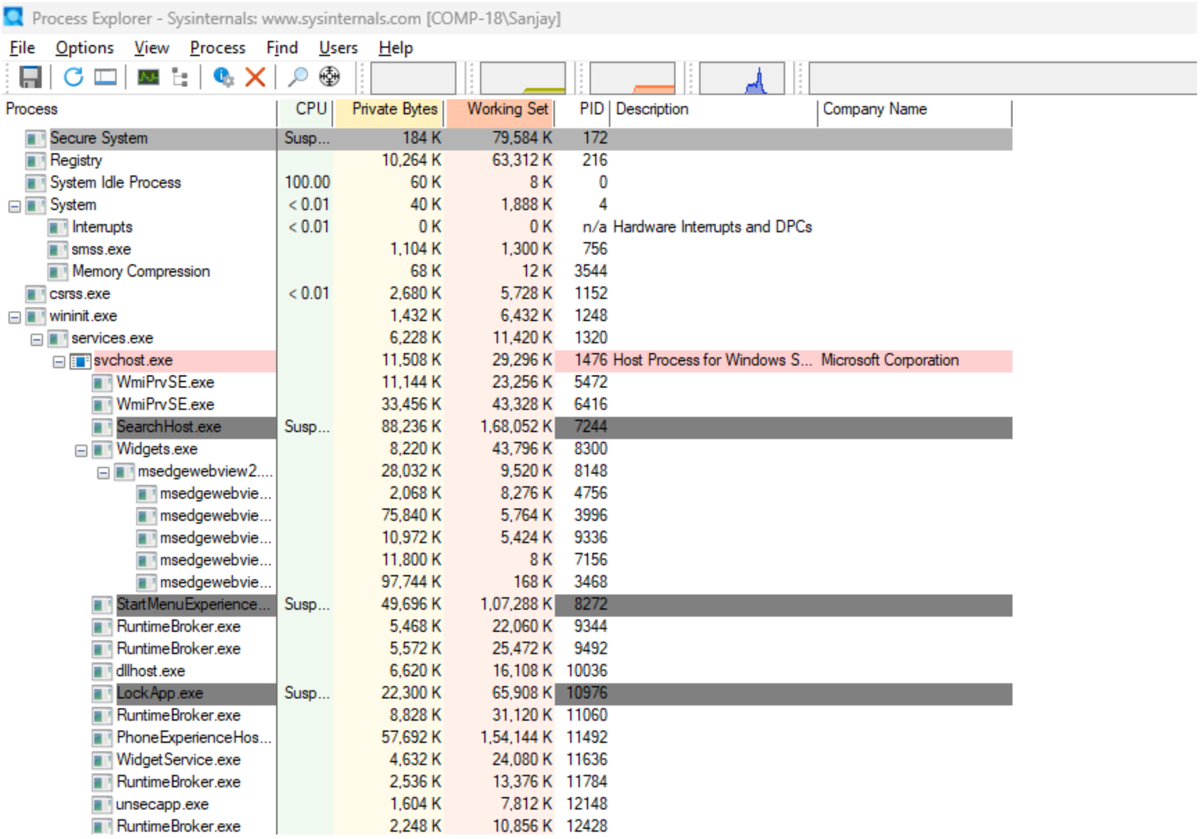
Objectives:

- Installing process explorer in windows machine.
- Classify data using data analysis techniques.

Procedure:

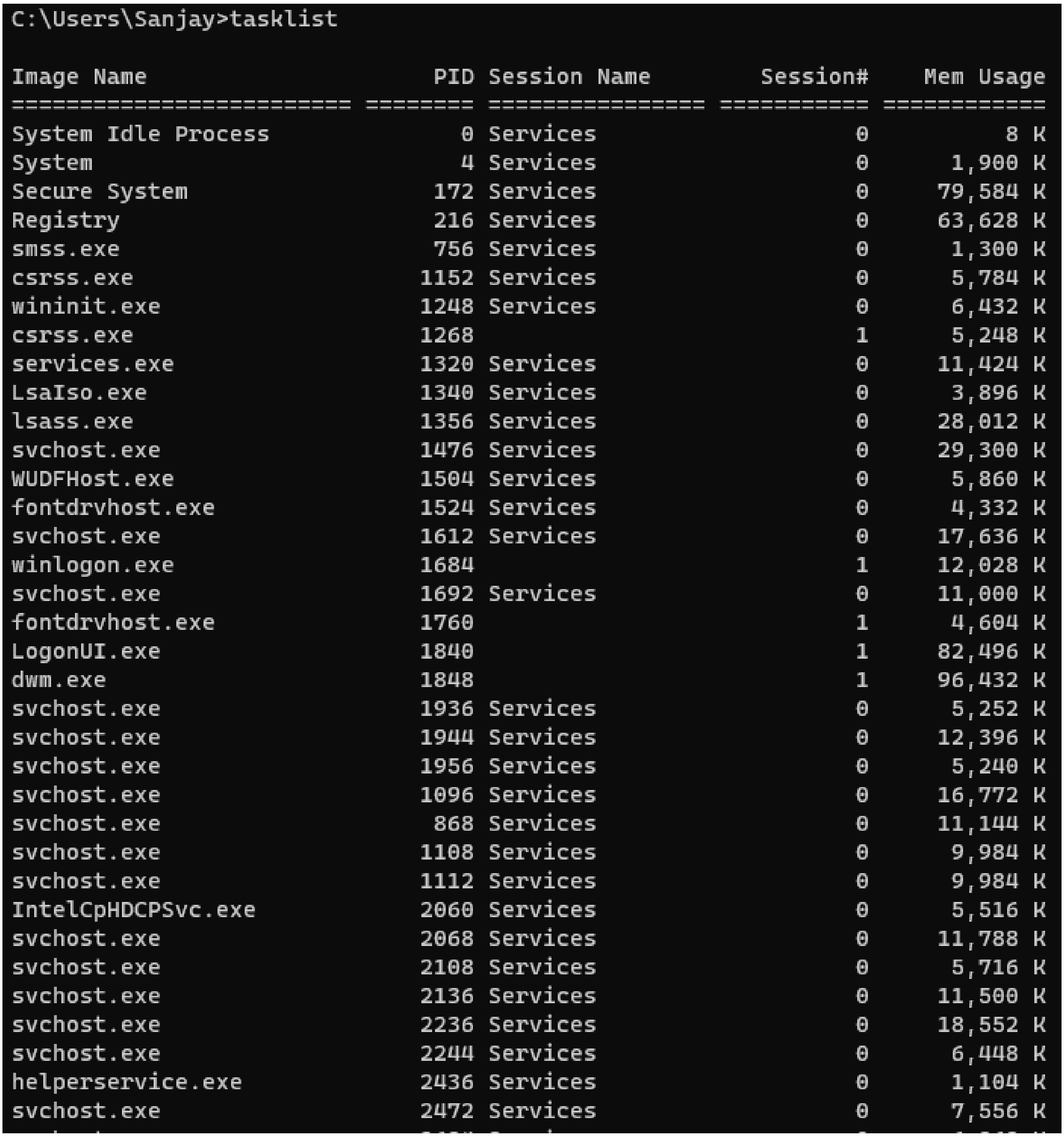
Install the process explorer utility in a windows-based operating system having minimum 4gb ram. Use data classification techniques to group process ID and name of the company from which the application or tool belongs.

Results & Observations:



Process Explorer - Sysinternals: www.sysinternals.com [COMP-18\Sanjay]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System	Susp...	184 K	79,584 K	172		
Registry		10,264 K	63,312 K	216		
System Idle Process	100.00	60 K	8 K	0		
System	< 0.01	40 K	1,888 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,104 K	1,300 K	756		
Memory Compression		68 K	12 K	3544		
csrss.exe	< 0.01	2,680 K	5,728 K	1152		
wininit.exe		1,432 K	6,432 K	1248		
services.exe		6,228 K	11,420 K	1320		
svchost.exe		11,508 K	29,296 K	1476	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		11,144 K	23,256 K	5472		
WmiPrvSE.exe		33,456 K	43,328 K	6416		
SearchHost.exe	Susp...	88,236 K	1,68,052 K	7244		
Widgets.exe		8,220 K	43,796 K	8300		
msedgewebview2....		28,032 K	9,520 K	8148		
msedgewebvie...		2,068 K	8,276 K	4756		
msedgewebvie...		75,840 K	5,764 K	3996		
msedgewebvie...		10,972 K	5,424 K	9336		
msedgewebvie...		11,800 K	8 K	7156		
msedgewebvie...		97,744 K	168 K	3468		
StartMenuExperience...	Susp...	49,696 K	1,07,288 K	8272		
RuntimeBroker.exe		5,468 K	22,060 K	9344		
RuntimeBroker.exe		5,572 K	25,472 K	9492		
dllhost.exe		6,620 K	16,108 K	10036		
LockApp.exe	Susp...	22,300 K	65,908 K	10976		
RuntimeBroker.exe		8,828 K	31,120 K	11060		
PhoneExperienceHos...		57,692 K	1,54,144 K	11492		
WidgetService.exe		4,632 K	24,080 K	11636		
RuntimeBroker.exe		2,536 K	13,376 K	11784		
unsecapp.exe		1,604 K	7,812 K	12148		
RuntimeBroker.exe		2,248 K	10,856 K	12428		



```
C:\Users\Sanjay>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      1,900 K
Secure System                  172 Services                   0     79,584 K
Registry                       216 Services                   0     63,628 K
smss.exe                       756 Services                   0      1,300 K
csrss.exe                     1152 Services                   0      5,784 K
wininit.exe                   1248 Services                   0      6,432 K
csrss.exe                     1268                            1      5,248 K
services.exe                  1320 Services                   0     11,424 K
LsaIso.exe                    1340 Services                   0      3,896 K
lsass.exe                     1356 Services                   0     28,012 K
svchost.exe                   1476 Services                   0     29,300 K
WUDFHost.exe                  1504 Services                   0      5,860 K
fontdrvhost.exe               1524 Services                   0      4,332 K
svchost.exe                   1612 Services                   0     17,636 K
winlogon.exe                  1684                            1     12,028 K
svchost.exe                   1692 Services                   0     11,000 K
fontdrvhost.exe               1760                            1      4,604 K
LogonUI.exe                   1840                            1     82,496 K
dwm.exe                       1848                            1     96,432 K
svchost.exe                   1936 Services                   0      5,252 K
svchost.exe                   1944 Services                   0     12,396 K
svchost.exe                   1956 Services                   0      5,240 K
svchost.exe                   1096 Services                   0     16,772 K
svchost.exe                    868 Services                   0     11,144 K
svchost.exe                   1108 Services                   0      9,984 K
svchost.exe                   1112 Services                   0      9,984 K
IntelCpHDCPSvc.exe            2060 Services                   0      5,516 K
svchost.exe                   2068 Services                   0     11,788 K
svchost.exe                   2108 Services                   0      5,716 K
svchost.exe                   2136 Services                   0     11,500 K
svchost.exe                   2236 Services                   0     18,552 K
svchost.exe                   2244 Services                   0      6,448 K
helperservice.exe             2436 Services                   0      1,104 K
svchost.exe                   2472 Services                   0      7,556 K
```

Fig 2. List of tasks using tasklist command

Working sets / process ID/ Company
762K 3920 Brave Browser
109K 2992 Intel Corporation
128K 2000 VMware
176 K 1632 Microsoft Corporation
788 K 1660 Microsoft Corporation
216 K 1724 Microsoft Corporation

548 K 1776 Microsoft Corporation
291 K 1476 Microsoft Corporation
872 K 2005 Dell Inc.

Table 1: process Id with company name

Result analysis and discussion:

Process explorer is installed on the given system. The process explorer displays results which is classified. Based on the obtained results it is shown that different system tools and applications are running different processes. In table 1 the list of some of the processes are given with their process Id and Company name. It is also observed that some tools don't have company name. Such processes should be put on priority to confirm that they are system tools and not any random application running in background.

Future Scope:

Process explorer is an internal tool running in stand-alone system. Similar types of tools can be used to perform network related process.

LAB MANUAL (IRM)

Exp. No: 3 **Date: 17-6-2023**

Title: Identification of Read and Write Processes with Disk Monitoring System

Requirements: A computer with a disk monitoring system installed. Disk monitoring software capable of capturing read and write process information.

Objectives:

1. Utilize a disk monitoring system to identify read and write processes on the system.
2. Determine the length of read and write operations performed by these processes.

Procedure:

Launch the disk monitoring system on the pc. Configure the disk monitoring utiltiy to capture read and write processes. Use data filtering techniques to filter out the process which have read and write length more than 5.

Results & Observations:

Table 1: Results from disk monitoring tool

Sr. No	Time	Duration	Disk	Request	Sector	Length
0	0.099725	0	1	Read	55763248	40
1	0.134826	0	1	Read	55763104	64
2	0.351603	0	1	Read	745585920	64
3	0.351743	0	1	Write	996436032	64
4	0.351868	0	1	Write	996247872	32
5	0.351965	0	1	Write	745585904	56
6	0.352077	0	1	Write	6978144	48
7	1.026035	0	1	Write	526381304	8
8	1.057489	0	1	Write	96198208	96
9	1.05749	0	1	Write	562608744	16
10	1.057528	0	1	Write	526376584	8
11	1.057574	0	1	Write	1002976	8
12	1.057611	0	1	Write	330319936	8
13	1.057689	0	1	Write	834252072	8
14	1.057727	0	1	Write	965762936	72
15	2.113554	0	1	Read	15714384	16
16	2.122262	0	1	Read	15720656	16
17	2.12755	0	1	Read	15758192	16
18	2.14382	0	1	Read	15720736	16
19	2.144131	0	1	Read	15720640	16
20	2.144316	0	1	Read	15744144	16
21	2.151015	0	1	Read	15720320	16

22	2.157255	0	1	Read	15712656	16
23	2.175385	0	1	Read	10614304	16
24	2.176222	0	1	Read	10614240	16
25	2.176368	0	1	Read	15757856	16
26	2.176488	0	1	Read	15760128	16
27	2.176642	0	1	Read	15758144	16
28	2.176789	0	1	Read	15758240	16
29	2.17695	0	1	Read	15758112	16
30	2.177159	0	1	Read	15758080	16
31	2.177279	0	1	Read	15760208	16
32	2.177411	0	1	Read	15757920	16
33	2.177543	0	1	Read	15760048	16
34	2.177684	0	1	Read	15760144	16
35	2.177819	0	1	Read	15758352	16
36	2.177931	0	1	Read	15760304	16
37	2.178068	0	1	Read	15757952	16
38	2.178186	0	1	Read	15759648	16
39	2.178362	0	1	Read	15760080	16
40	2.178528	0	1	Read	15758368	16
41	2.178659	0	1	Read	15760192	16
42	2.178875	0	1	Read	15759968	16
43	2.179076	0	1	Read	15760176	16
44	2.179209	0	1	Read	15758000	16
45	2.179332	0	1	Read	15760240	16
46	2.179495	0	1	Read	15760416	16
47	2.179684	0	1	Read	15746192	16
48	2.179871	0	1	Read	15758128	14
49	2.180079	0	1	Read	15733264	15
50	2.180194	0	1	Read	15760016	16

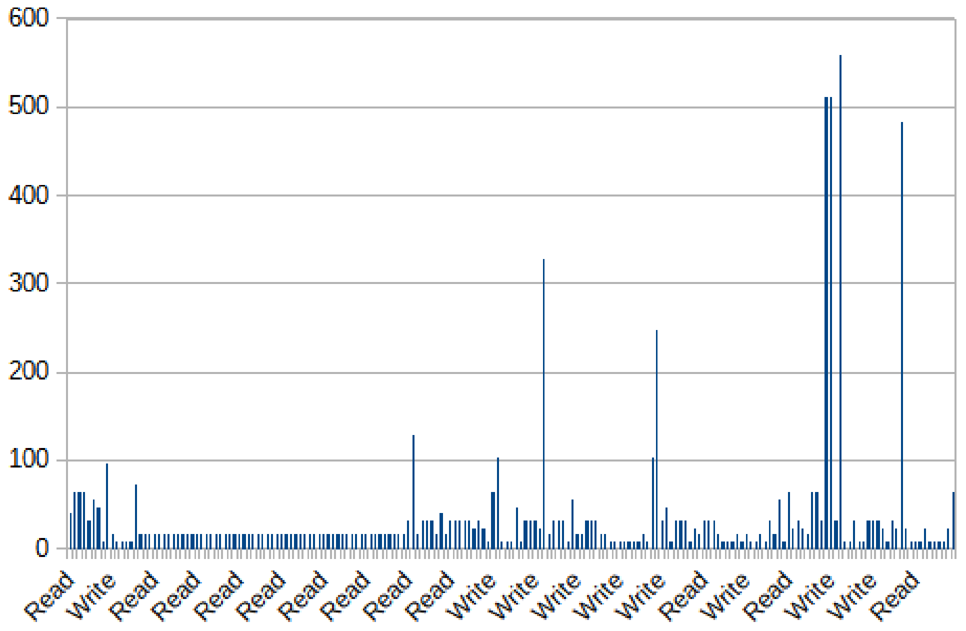


Fig 1 Chart of read and write processes

Result analysis and discussion:

Based on the above results it is observed that the given system has one disk in which . Multiple read and write operations are performed for the said session. Fig-1 shows that in the given duration, more read operations were made compared to write operations having duration or length more than five.

Future Scope:

The above experimental setup was created to understand how the disk is utilized for multiple requests from the system and user. This scenario and commercialized tools shall be used to setup data server which required continues monitoring of the disk

Exp. No: 4 **Date:16-6-2023**

Title: Installation and Demonstration of Sawmill on Windows OS, and Generating a Custom Report

Requirements: A computer running a Windows operating system. Sawmill software installer.

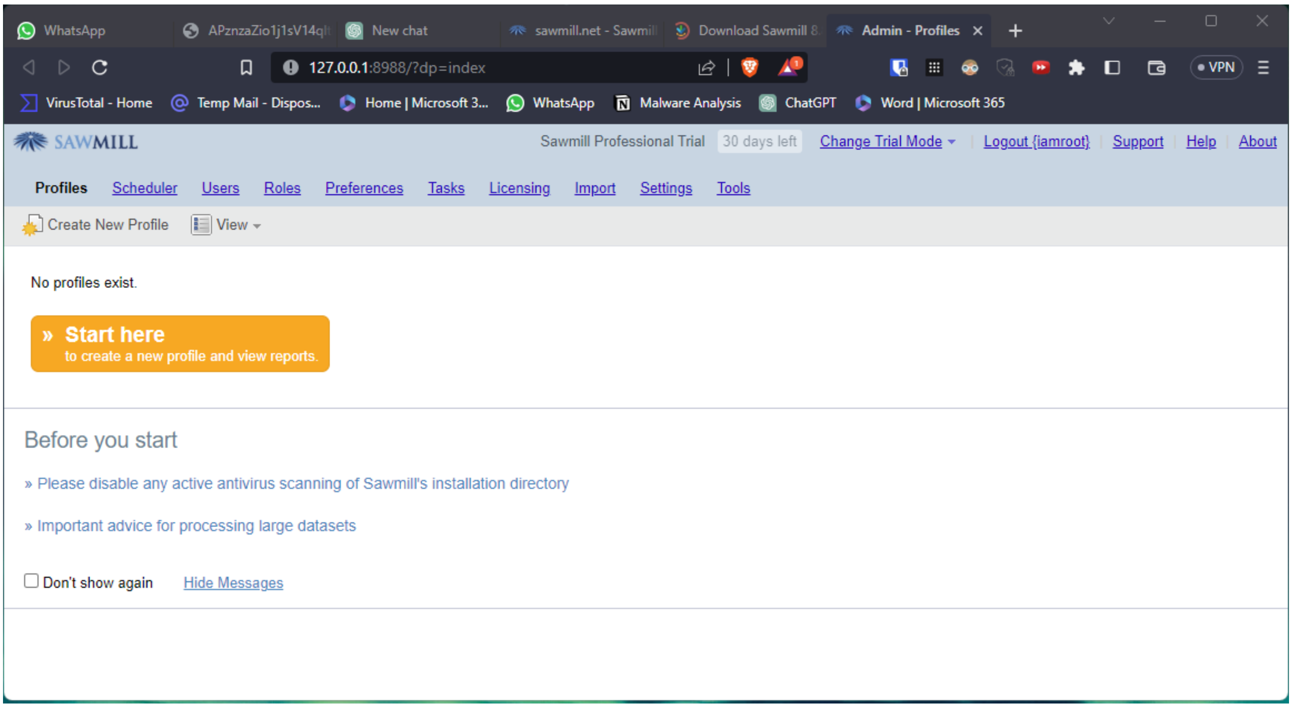
Objectives:

1. Install the Sawmill software on a Windows OS.
2. Demonstrate the usage of Sawmill for log analysis and reporting.
3. Generate a custom report using Sawmill.

Procedure:

Install the sawmill software using sawmill installer. Once the installation is done run the sawmill application. Sawmill will show you the logs related to your machine. Once enough logs are generated then you can easily create custom report by using filters.

Results & Observations:



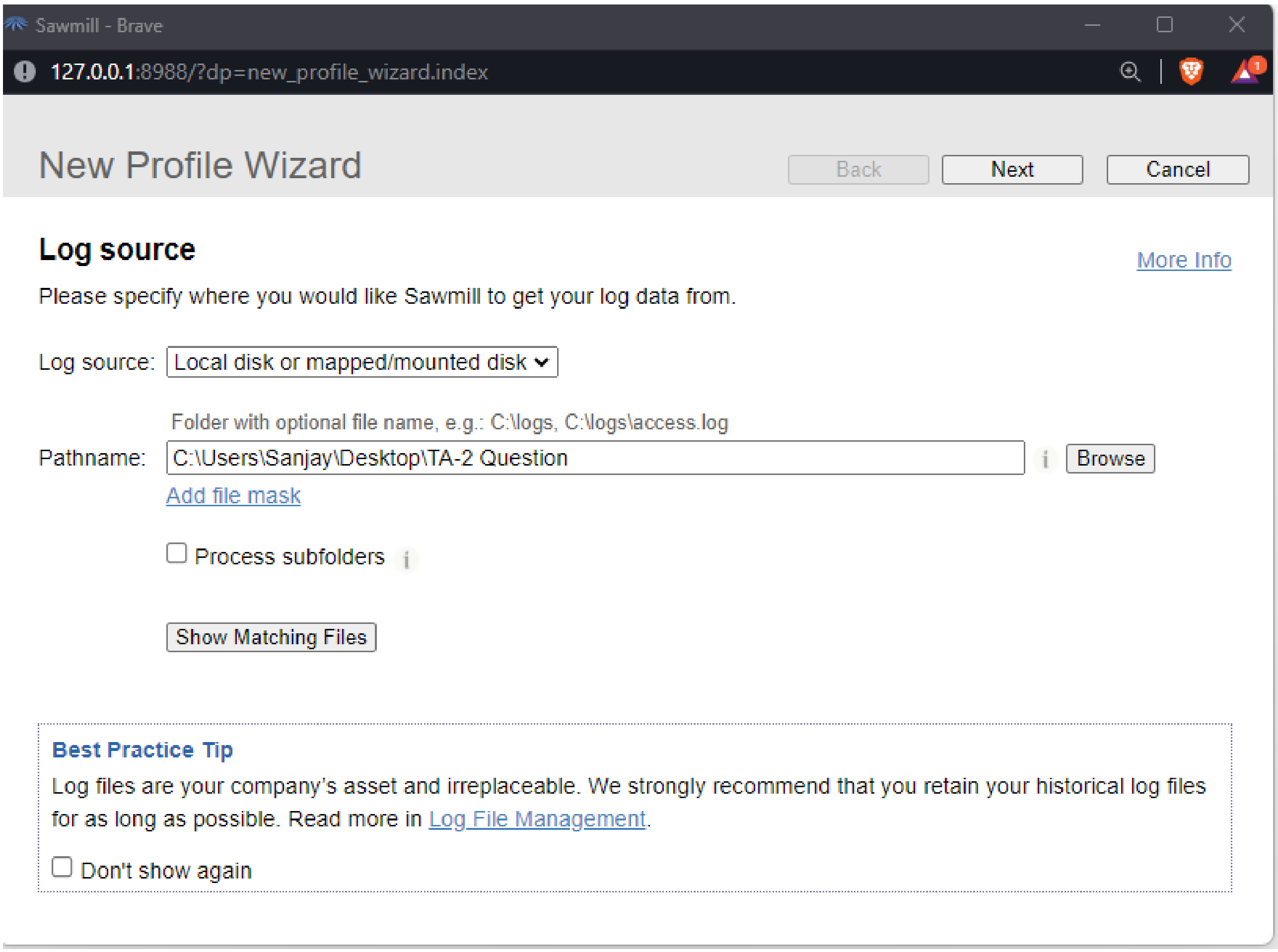
No profiles exist.

Before you start

» Please disable any active antivirus scanning of Sawmill's installation directory

» Important advice for processing large datasets

Fig 1. Dashboard of sawmill software



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:\Users\Sanjay\Desktop\TA-2 Question

□ 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

Fig 2: Sawmill Option to import log files

Result analysis and discussion:

The demonstration showcased the log analysis and reporting capabilities of Sawmill. Currently the system that is used to install the sawmill don't have any log files that can be imported into the sawmill. For that reason, only dashboard is presented.

Future Scope:

Sawmill is a great tool for log analysis but in future it can be integrated with other tools and formats. It will enhance the capabilities of the sawmill software.

LAB MANUAL (IRM)

Exp. No: 5 **Date: 20-6-2023**

Title: Install and configure snort for network security and protection against cyber threats.

Requirements: A computer or server running a supported operating system (e.g., Windows, Linux). Snort software installer. A working internet connection.

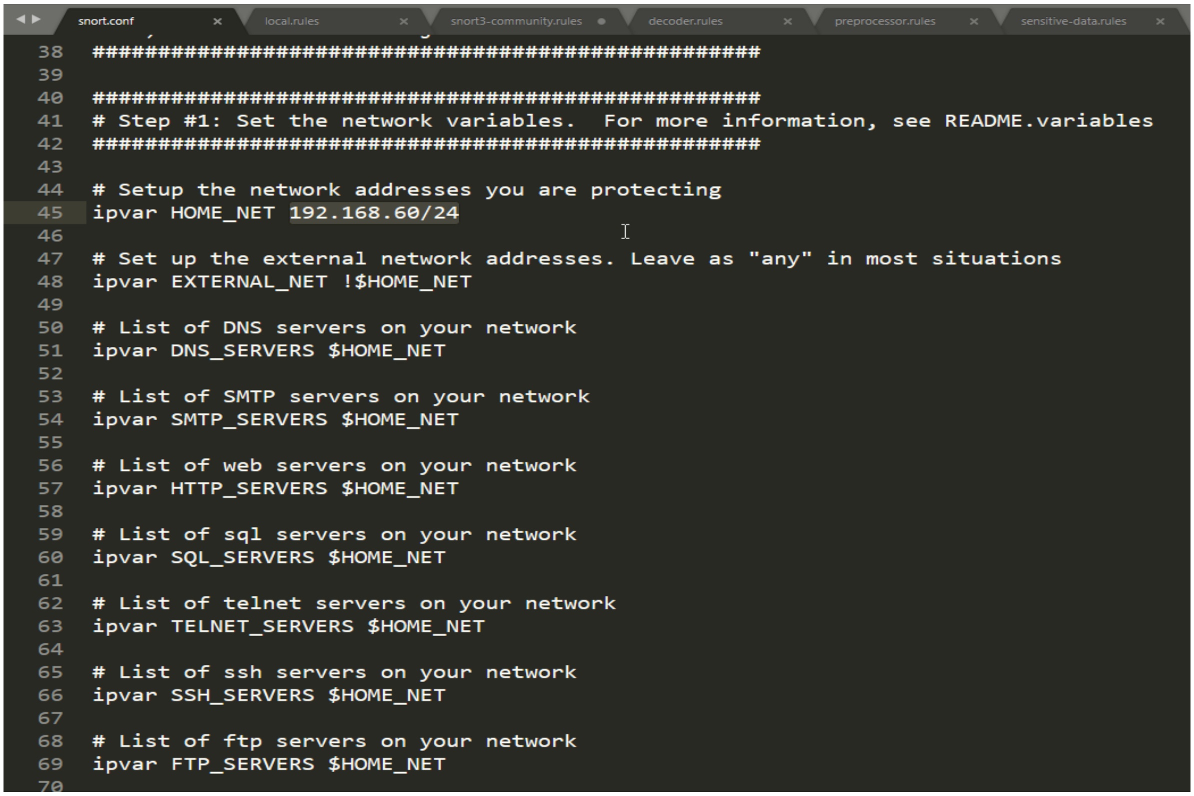
Objectives:

- Install Snort on the designated computer or server.
- Collecting a detailed network report using Snort to analyze network security.
- Installing snort rules

Procedure:

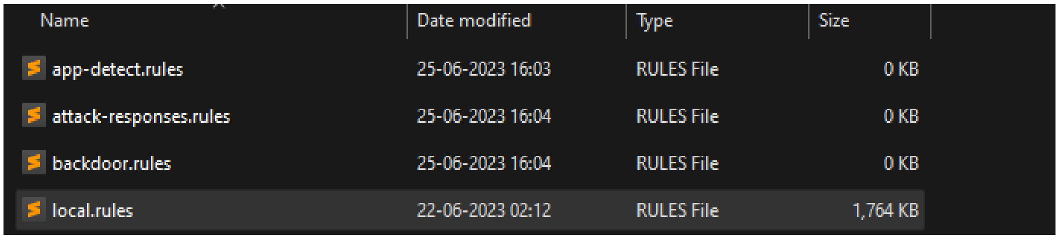
Install the snort software using Snort installer. After installing the Snort, Configure Snort to collect the network logs. Allow Snort to log and analyze the network files. Installing the snort rules and creating custom rules also.

Results & Observations:



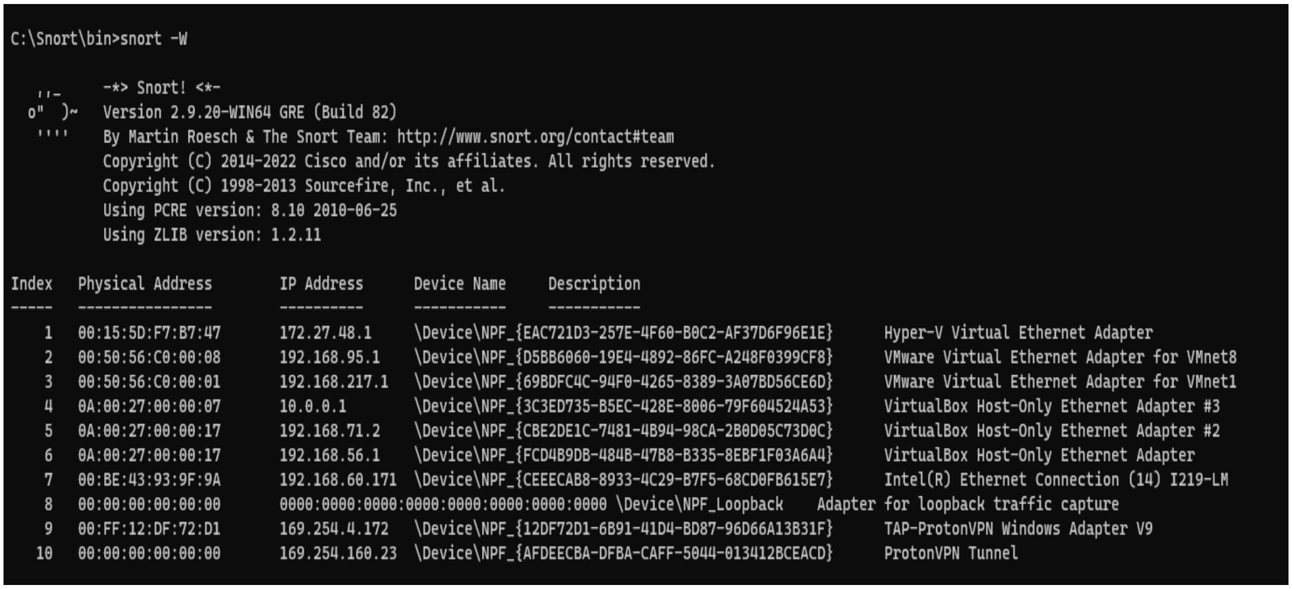
```
##################################################

##################################################
# Step #1: Set the network variables.  For more information, see README.variables
##################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.60/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET
```

Fig 1. Snort conf file settings



Name	Date modified	Type	Size
app-detect.rules	25-06-2023 16:03	RULES File	0 KB
attack-responses.rules	25-06-2023 16:04	RULES File	0 KB
backdoor.rules	25-06-2023 16:04	RULES File	0 KB
local.rules	22-06-2023 02:12	RULES File	1,764 KB

Fig 2. Snort rules files



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

   ,,_     -*> Snort! <*-
  o"  )~   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   00:15:5D:F7:B7:47       172.27.48.1     \Device\NPF_{EAC721D3-257E-4F60-B0C2-AF37D6F96E1E}      Hyper-V Virtual Ethernet Adapter
    2   00:50:56:C0:00:08       192.168.95.1    \Device\NPF_{D5BB6060-19E4-4892-86FC-A248F0399CF8}      VMware Virtual Ethernet Adapter for VMnet8
    3   00:50:56:C0:00:01       192.168.217.1   \Device\NPF_{69BDFC4C-94F0-4265-8389-3A07BD56CE6D}      VMware Virtual Ethernet Adapter for VMnet1
    4   0A:00:27:00:00:07       10.0.0.1        \Device\NPF_{3C3ED735-B5EC-428E-8006-79F604524A53}      VirtualBox Host-Only Ethernet Adapter #3
    5   0A:00:27:00:00:17       192.168.71.2    \Device\NPF_{CBE2DE1C-7481-4B94-98CA-2B0D05C73D0C}      VirtualBox Host-Only Ethernet Adapter #2
    6   0A:00:27:00:00:17       192.168.56.1    \Device\NPF_{FCD4B9DB-484B-47B8-B335-8EBF1F03A6A4}      VirtualBox Host-Only Ethernet Adapter
    7   00:BE:43:93:9F:9A       192.168.60.171  \Device\NPF_{CEEECAB8-8933-4C29-B7F5-68CD0FB615E7}      Intel(R) Ethernet Connection (14) I219-LM
    8   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
    9   00:FF:12:DF:72:D1       169.254.4.172   \Device\NPF_{12DF72D1-6B91-41D4-BD87-96D66A13B31F}      TAP-ProtonVPN Windows Adapter V9
   10   00:00:00:00:00:00       169.254.160.23  \Device\NPF_{AFDEECBA-DFBA-CAFF-5044-013412BCEACD}      ProtonVPN Tunnel
```

Fig2. Checking the no. of interface snort can be run on

Result analysis and discussion:

The installation of snort was successfully completed. After installing the snort many options needed to be configured. After that interface is selected on which the Snort run. After all this packet capturing was started .

Future Scope:

Snort is a great tool for network security and it work as an IDS(Intrusion detection system) . In future it can be integrated with ai and it can provide more robust output.

LAB MANUAL (IRM)

Exp. No: 6 **Date: 16-6-2023**

Title: Installation and Demonstration of Splunk for Log Analysis

Requirements: A computer or server running a supported operating system (e.g., Windows, Linux). Splunk software installer.

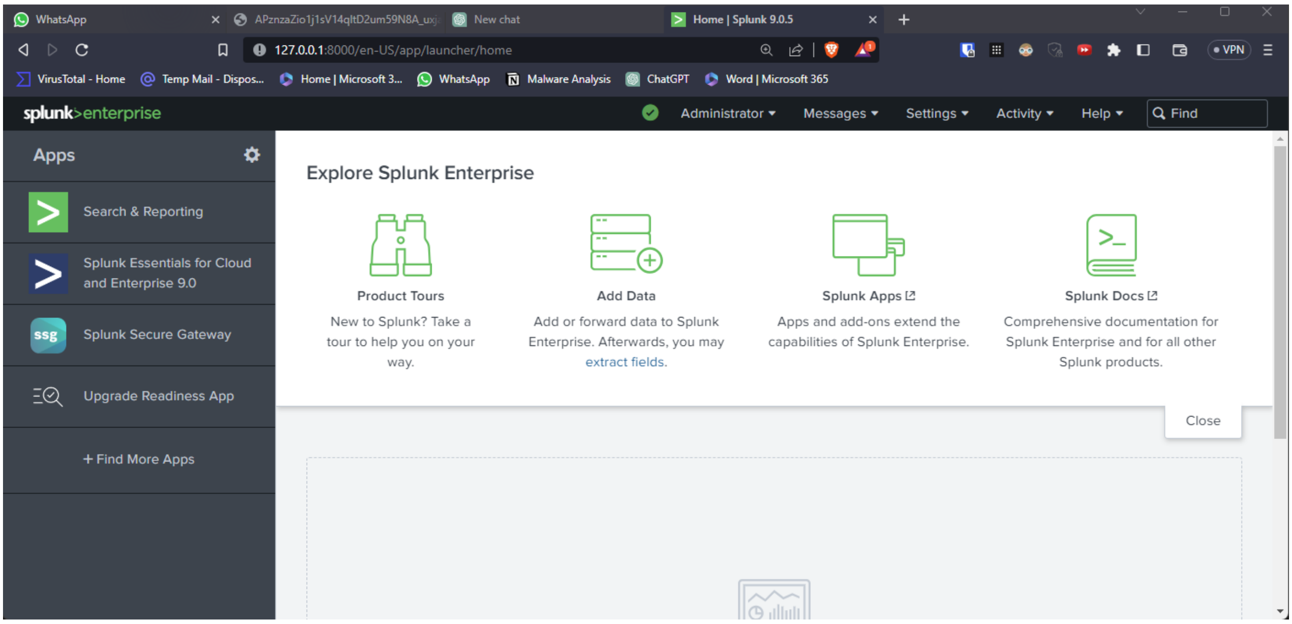
Objectives:

- Install Splunk on the designated computer or server.
- Use the Splunk for log analysis
- Checking the critical log for any harm done on the computer or not.

Procedure:

Install the Splunk software using Splunk installer. After installing the Splunk, Configure Splunk to save the logs of the local system. Use search method for search the logs using custom parameters. Search for the activities that can be harmful for the system.

Results & Observations:



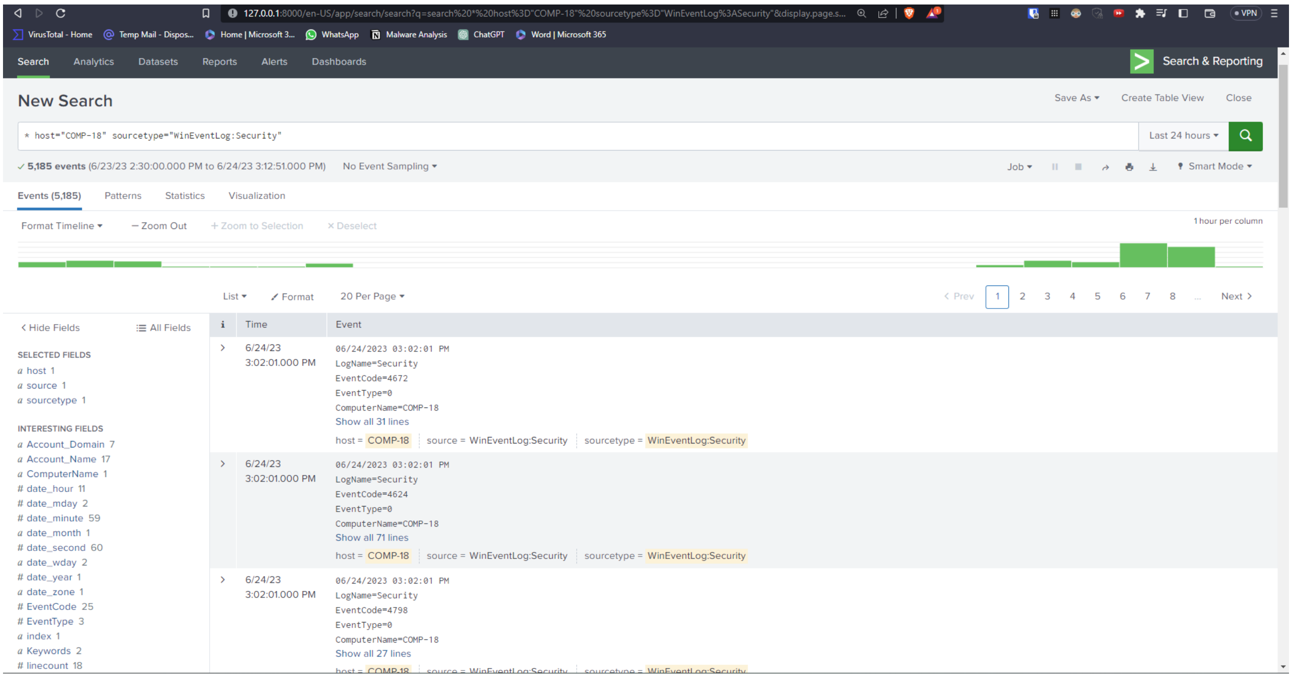
New to Splunk? Take a tour to help you on your way.

Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk Enterprise.

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

Fig 1: Splunk dashboard



```
* host="COMP-18" sourcetype="WinEventLog:Security"
```

Last 24 hours

✓ 5,185 events (6/23/23 2:30:00.000 PM to 6/24/23 3:12:51.000 PM)   No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 7
a Account_Name 17
a ComputerName 1
# date_hour 11
# date_mday 2
# date_minute 59
a date_month 1
# date_second 60
a date_wday 2
# date_year 1
a date_zone 1
EventCode 25
EventType 3
a index 1
a Keywords 2
# linecount 18

```
6/24/23 3:02:01.000 PM
06/24/2023 03:02:01 PM
LogName=Security
EventCode=4672
EventType=0
ComputerName=COMP-18
Show all 31 lines
host = COMP-18   source = WinEventLog:Security   sourcetype = WinEventLog:Security

6/24/23 3:02:01.000 PM
06/24/2023 03:02:01 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=COMP-18
Show all 71 lines
host = COMP-18   source = WinEventLog:Security   sourcetype = WinEventLog:Security

6/24/23 3:02:01.000 PM
06/24/2023 03:02:01 PM
LogName=Security
EventCode=4798
EventType=0
ComputerName=COMP-18
Show all 27 lines
host = COMP-18   source = WinEventLog:Security   sourcetype = WinEventLog:Security
```

Fig 2: Splunk search dashboard for viewing the logs

Result analysis and discussion:

Figure 1 is the default dashboard of the Splunk tool. There are many filters that we can use in Splunk. In the above figures system, security logs are created of the local system and then analysed using Splunk's scan & reporting feature. In the search query option “host and source type” parameter are selected to view only logs related to these parameters. The Splunk logs are stored for 15 minutes and then analysed. During analysis nothing critical found

Future Scope:

Splunk is a great tool for system monitoring. Custom rule sets can also be used to enhance the security of the infrastructure. Splunk can also be integrated with other cyber security tools. Continuous learning and exploration of Splunk's capabilities will enable you to maximize its potential for comprehensive log analysis in various scenarios.

LAB MANUAL (IRM)

Exp. No: 7 **Date: 18-6-2023**

Title: File Recovery Using Autopsy

Requirements: A computer or forensic workstation capable of running Autopsy software. Data source containing files for recovery.

Objectives:

Utilize Autopsy, a digital forensics tool, to recover files from a given data source.

Present the details of the file recovery process using Autopsy.

Procedure:

Install Autopsy software on the designated system following the provided instructions.

Prepare the data source containing files for recovery, such as a hard drive, USB drive, or disk image..

Results & Observations:

Result analysis and discussion:

Autopsy software was successfully installed and utilized to recover files from the given data source.

Future Scope:

In future experiments, explore additional features and functionalities of Autopsy to enhance file recovery capabilities. Experiment with different settings and configurations to optimize the recovery process for specific file types or scenarios.

LAB MANUAL (IRM)

Exp. No: 8 **Date: 20-6-2023**

Title: Install Cyber triage and collect the given system report

Requirements: A computer or server running a supported operating system (e.g., Windows, Linux). Cyber Triage software installer.

Objectives:

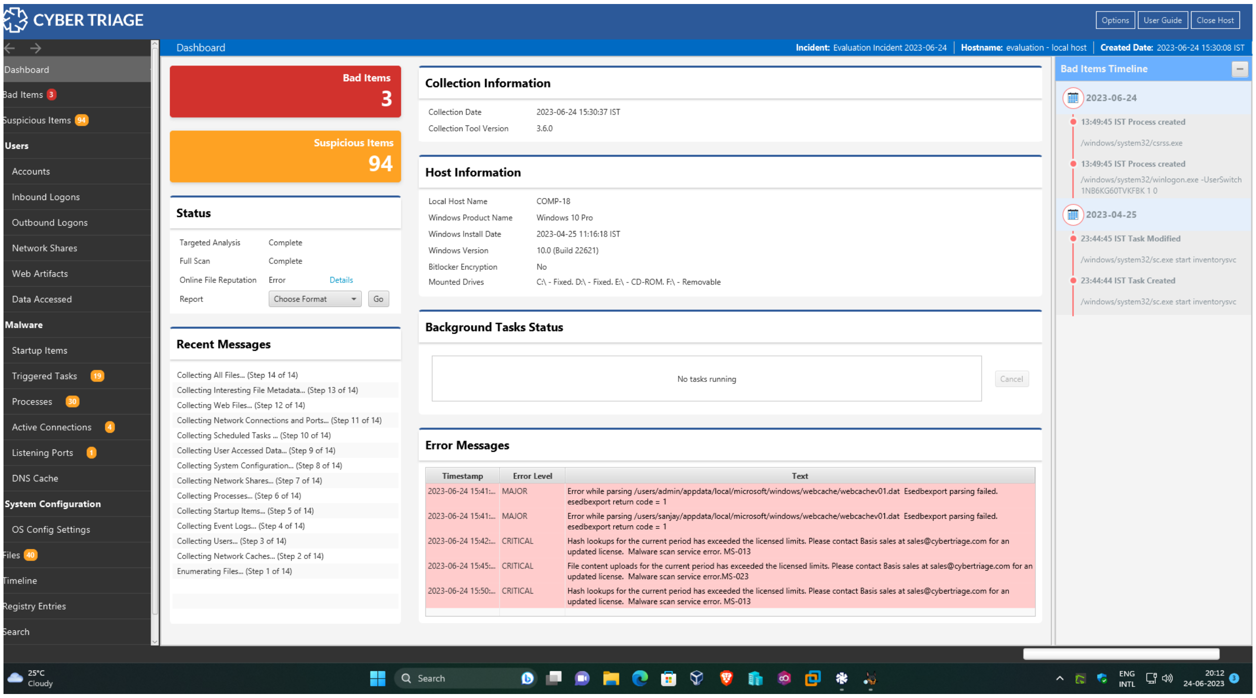
- Install Cyber Triage on the designated computer or server.
- Collecting a detailed system report using Cyber Triage to analyze system information.

Procedure:

Install the Cyber Triage software using Cyber Triage installer. After installing the Cyber Triage, Configure Cyber Triage to collect the desired system information. Allow cyber triage to scan and analyze the system.

Results & Observations:

Fig 1: Report of cyber triage



Incident: Evaluation Incident 2023-06-24 | **Hostname:** evaluation - local host | **Created Date:** 2023-06-24 15:30:08 IST

Bad Items 3

Suspicious Items 94

Status

Targeted Analysis	Complete	
Full Scan	Complete	
Online File Reputation	Error	Details
Report	Choose Format	Go

Recent Messages

Collecting All Files... (Step 14 of 14)
Collecting Interesting File Metadata... (Step 13 of 14)
Collecting Web Files... (Step 12 of 14)
Collecting Network Connections and Ports... (Step 11 of 14)
Collecting Scheduled Tasks ... (Step 10 of 14)
Collecting User Accessed Data... (Step 9 of 14)
Collecting System Configuration... (Step 8 of 14)
Collecting Network Shares... (Step 7 of 14)
Collecting Processes... (Step 6 of 14)
Collecting Startup Items... (Step 5 of 14)
Collecting Event Logs... (Step 4 of 14)
Collecting Users... (Step 3 of 14)
Collecting Network Caches... (Step 2 of 14)
Enumerating Files... (Step 1 of 14)

Collection Information

Collection Date	2023-06-24 15:30:37 IST
Collection Tool Version	3.6.0

Host Information

Local Host Name	COMP-18
Windows Product Name	Windows 10 Pro
Windows Install Date	2023-04-25 11:16:18 IST
Windows Version	10.0 (Build 22621)
Bitlocker Encryption	No
Mounted Drives	C:\ - Fixed. D:\ - Fixed. E:\ - CD-ROM. F:\ - Removable

Background Tasks Status

No tasks running

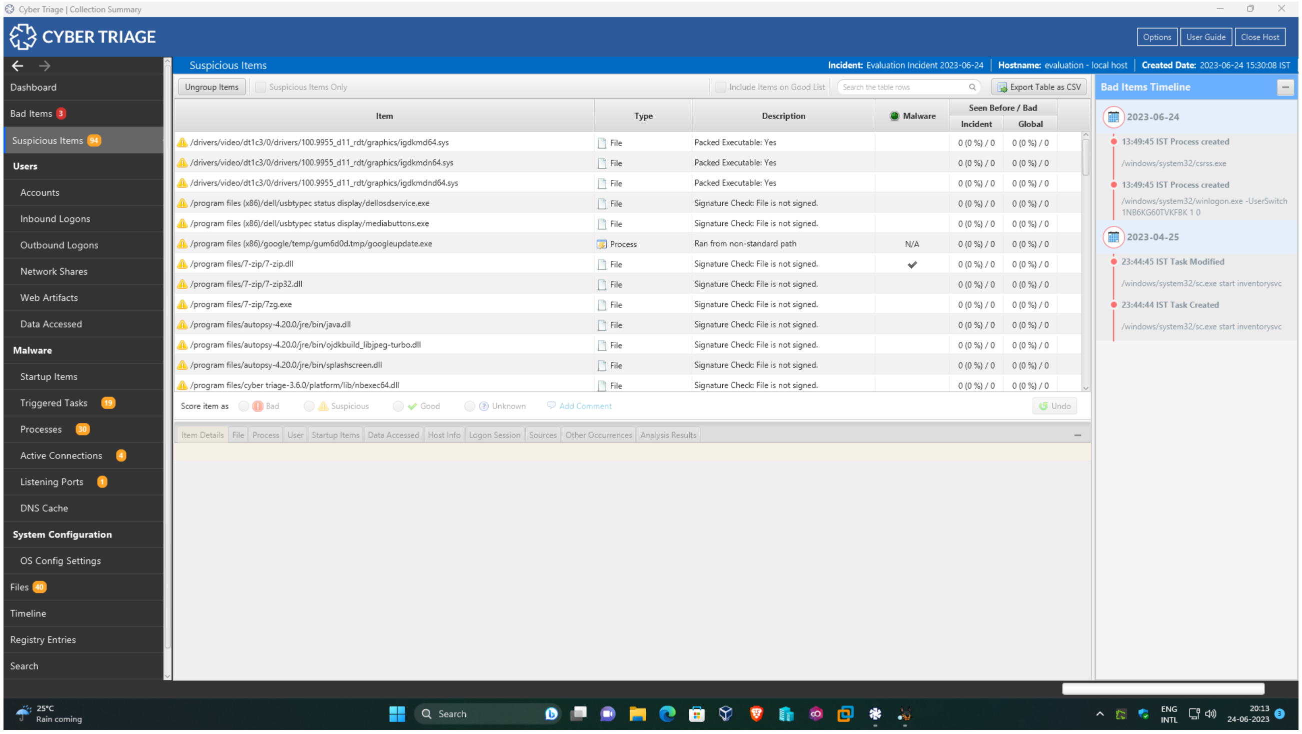
Error Messages

Timestamp	Error Level	Text
2023-06-24 15:41:...	MAJOR	Error while parsing /users/admin/appdata/local/microsoft/windows/webcache/webcachev01.dat Esedbexport parsing failed. esedbexport return code = 1
2023-06-24 15:41:...	MAJOR	Error while parsing /users/sanjay/appdata/local/microsoft/windows/webcache/webcachev01.dat Esedbexport parsing failed. esedbexport return code = 1
2023-06-24 15:42:...	CRITICAL	Hash lookups for the current period has exceeded the licensed limits. Please contact Basis sales at sales@cybertriage.com for an updated license. Malware scan service error. MS-013
2023-06-24 15:45:...	CRITICAL	File content uploads for the current period has exceeded the licensed limits. Please contact Basis sales at sales@cybertriage.com for an updated license. Malware scan service error.MS-023
2023-06-24 15:50:...	CRITICAL	Hash lookups for the current period has exceeded the licensed limits. Please contact Basis sales at sales@cybertriage.com for an updated license. Malware scan service error. MS-013

Bad Items Timeline

2023-06-24
13:49:45 IST Process created
/windows/system32/csrss.exe
13:49:45 IST Process created
/windows/system32/winlogon.exe -UserSwitch 1NB6KG60TVKFBK 1 0

2023-04-25
23:44:45 IST Task Modified
/windows/system32/sc.exe start inventorysvc
23:44:44 IST Task Created
/windows/system32/sc.exe start inventorysvc



Suspicious Items

Incident: Evaluation Incident 2023-06-24 | **Hostname:** evaluation - local host | **Created Date:** 2023-06-24 15:30:08 IST

Item	Type	Description	Malware	Seen Before / Bad	
				Incident	Global
/drivers/video/dt1c3/0/drivers/100.9955_d11_rdt/graphics/igdkmd64.sys	File	Packed Executable: Yes		0 (0 %) / 0	0 (0 %) / 0
/drivers/video/dt1c3/0/drivers/100.9955_d11_rdt/graphics/igdkmdn64.sys	File	Packed Executable: Yes		0 (0 %) / 0	0 (0 %) / 0
/drivers/video/dt1c3/0/drivers/100.9955_d11_rdt/graphics/igdkmdnd64.sys	File	Packed Executable: Yes		0 (0 %) / 0	0 (0 %) / 0
/program files (x86)/dell/usbtypec status display/dellosdservice.exe	File	Signature Check: File is not signed.		0 (0 %) / 0	0 (0 %) / 0
/program files (x86)/dell/usbtypec status display/mediabuttons.exe	File	Signature Check: File is not signed.		0 (0 %) / 0	0 (0 %) / 0
/program files (x86)/google/temp/gum6d0d.tmp/googleupdate.exe	Process	Ran from non-standard path	N/A	0 (0 %) / 0	0 (0 %) / 0
/program files/7-zip/7-zip.dll	File	Signature Check: File is not signed.	✓	0 (0 %) / 0	0 (0 %) / 0
/program files/7-zip/7-zip32.dll	File	Signature Check: File is not signed.		0 (0 %) / 0	0 (0 %) / 0
/program files/7-zip/7zg.exe	File	Signature Check: File is not signed.		0 (0 %) / 0	0 (0 %) / 0
/program files/autopsy-4.20.0/jre/bin/java.dll	File	Signature Check: File is not signed.		0 (0 %) / 0	0 (0 %) / 0
/program files/autopsy-4.20.0/jre/bin/ojdkbuild_libjpeg-turbo.dll	File	Signature Check: File is not signed.		0 (0 %) / 0	0 (0 %) / 0
/program files/autopsy-4.20.0/jre/bin/splashscreen.dll	File	Signature Check: File is not signed.		0 (0 %) / 0	0 (0 %) / 0
/program files/cyber triage-3.6.0/platform/lib/nbexec64.dll	File	Signature Check: File is not signed.		0 (0 %) / 0	0 (0 %) / 0

Bad Items Timeline

2023-06-24

13:49:45 IST Process created
/windows/system32/csrss.exe

13:49:45 IST Process created
/windows/system32/winlogon.exe -UserSwitch 1NB6KG60TVKFBK 1 0

2023-04-25

23:44:45 IST Task Modified
/windows/system32/sc.exe start inventorysvc

23:44:44 IST Task Created
/windows/system32/sc.exe start inventorysvc

Fig2. Scanning of Suspicious file

Result analysis and discussion:

The installation of Cyber Triage was successfully completed, and the system report collection process was carried out to gather detailed information about the system. In the report of Cyber Triage many suspicious items and files were found. Many of the files and processes are not malicious but they are just system or another software files but some files were malicious.

Future Scope:

In future advanced features of the cyber triage can be explored. Cyber triage's advanced reporting functionalities can be used to generate comprehensive reports the present the system information in an organized way.

LAB MANUAL (IRM)

Exp. No: 9 **Date: 20-6-2023**

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

Requirements: A computer or forensic workstation capable of running the CAINE (Computer Aided Investigative Environment) tool. Ram on which we want to perform analysis.

Objectives:

- Perform digital forensics analysis on the RAM timeline using the CAINE tool.
- Using the tools available in CAINE O.S to Analyze RAM. Ex Volatility, Autopsy

Procedure:

Installing the CAINE in Virtual Box. Exploring the tools available in CAINE for doing ram timeline analysis. Best tool for ram analysis is volatility, Autopsy.

Results & Observations:

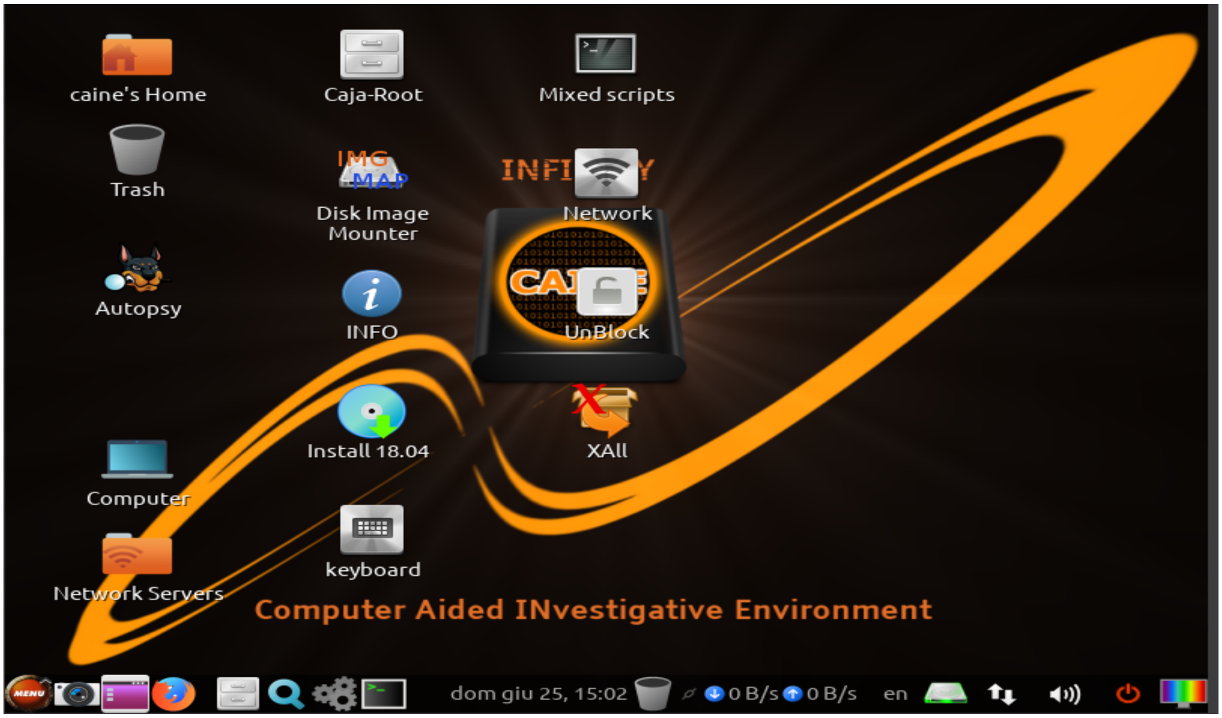
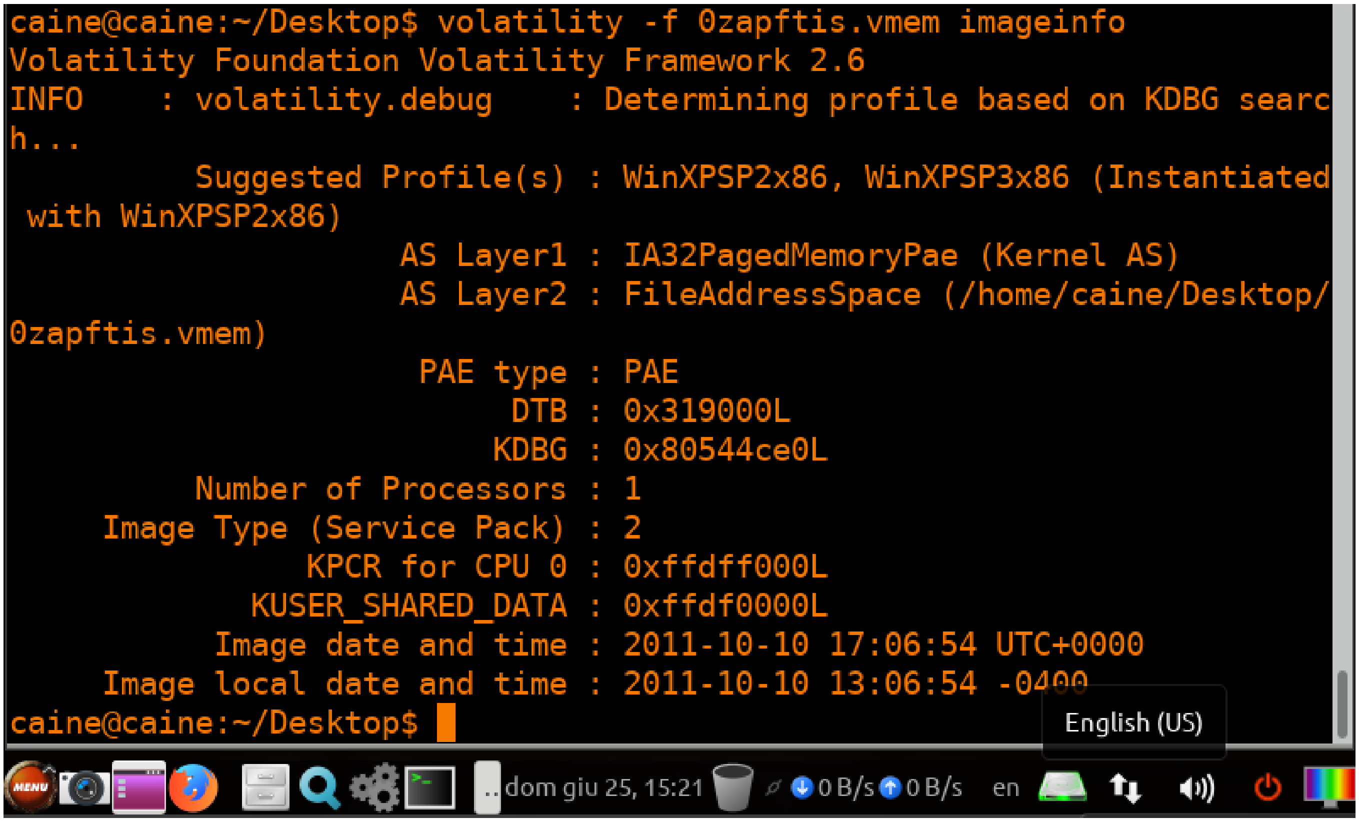
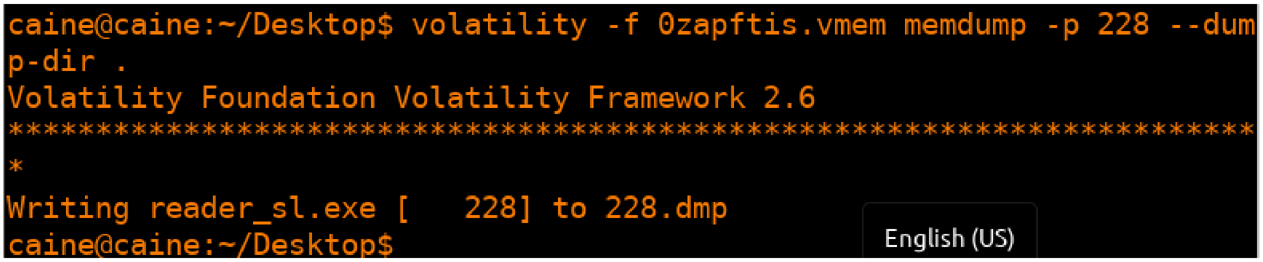


Fig 1: CAINE default dashboard



```
caine@caine:~/Desktop$ volatility -f 0zapftis.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG searc
h...
          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 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           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$ 
```

Fig 2. Analysis a ram file using volatility in CAINE



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

Fig 3. Dumping the data of a process using volatility

Result analysis and discussion:

CAINE is a tool that is specifically designed for forensic purpose. In CAINE many tools are available to do memory forensic. In the above figures volatility is used for ram analysis.

Future Scope:

CAINE is a great tool for forensic experts. In future many more tools can be created to efficiently doing forensic.

LAB MANUAL (IRM)

Exp. No: 10 **Date: 21-6-2023**

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

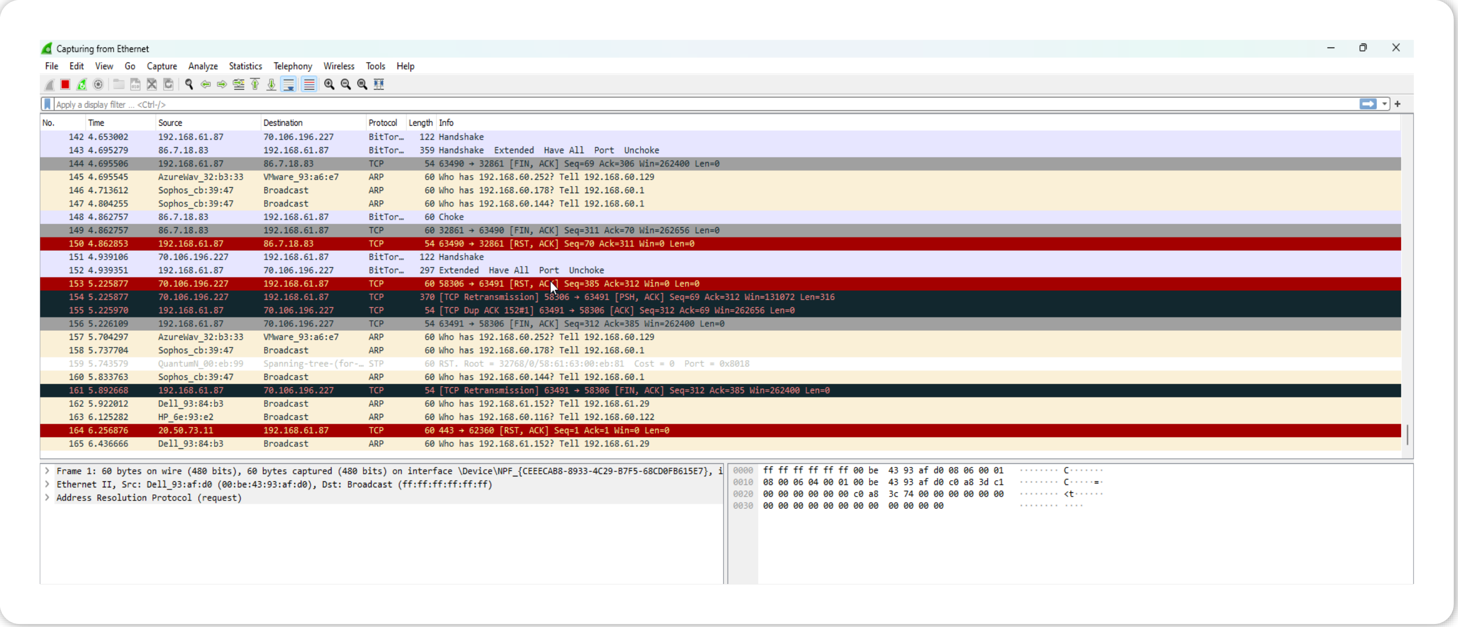
Requirements: A computer or forensic workstation capable of running the Wireshark tool. Wireshark installation file. A working internet connection

Objectives:

- Installing the Wireshark in the computer.
- Analyzing the captured packets using Wireshark

Procedure:

Install the Wireshark in the computer. Use Wireshark to capture network traffic. Analyze it using filters & options available in Wireshark.



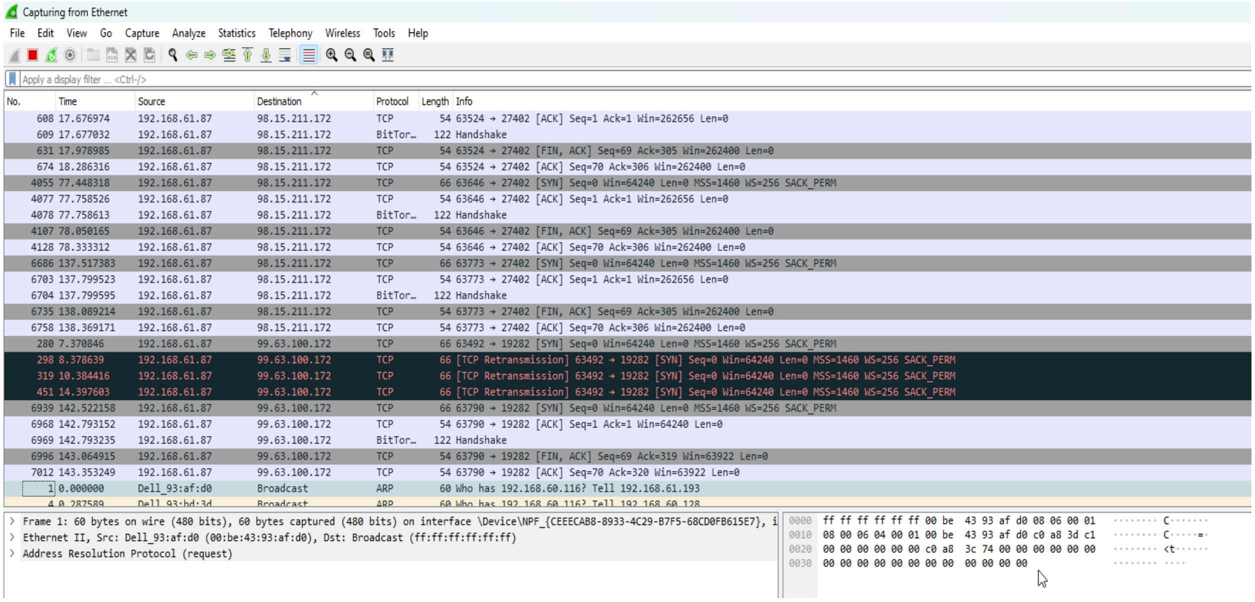
```
No.  Time      Source             Destination          Protocol Length Info
 142 4.653002  192.168.61.87      70.106.196.227       BitTor…   122 Handshake
 143 4.695279  86.7.18.83         192.168.61.87        BitTor…   359 Handshake  Extended  Have All  Port  Unchoke
 144 4.695506  192.168.61.87      86.7.18.83           TCP        54 63490 → 32861 [FIN, ACK] Seq=69 Ack=306 Win=262400 Len=0
 145 4.695545  AzureWav_32:b3:33  VMware_93:a6:e7      ARP        60 Who has 192.168.60.252? Tell 192.168.60.129
 146 4.713612  Sophos_cb:39:47    Broadcast            ARP        60 Who has 192.168.60.178? Tell 192.168.60.1
 147 4.804255  Sophos_cb:39:47    Broadcast            ARP        60 Who has 192.168.60.144? Tell 192.168.60.1
 148 4.862757  86.7.18.83         192.168.61.87        BitTor…    60 Choke
 149 4.862757  86.7.18.83         192.168.61.87        TCP        60 32861 → 63490 [FIN, ACK] Seq=311 Ack=70 Win=262656 Len=0
 150 4.862853  192.168.61.87      86.7.18.83           TCP        54 63490 → 32861 [RST, ACK] Seq=70 Ack=311 Win=0 Len=0
 151 4.939106  70.106.196.227     192.168.61.87        BitTor…   122 Handshake
 152 4.939351  192.168.61.87      70.106.196.227       BitTor…   297 Extended  Have All  Port  Unchoke
 153 5.225877  70.106.196.227     192.168.61.87        TCP        60 58306 → 63491 [RST, ACK] Seq=385 Ack=312 Win=0 Len=0
 154 5.225877  70.106.196.227     192.168.61.87        TCP       370 [TCP Retransmission] 58306 → 63491 [PSH, ACK] Seq=69 Ack=312 Win=131072 Len=316
 155 5.225970  192.168.61.87      70.106.196.227       TCP        54 [TCP Dup ACK 152#1] 63491 → 58306 [ACK] Seq=312 Ack=69 Win=262656 Len=0
 156 5.226109  192.168.61.87      70.106.196.227       TCP        54 63491 → 58306 [FIN, ACK] Seq=312 Ack=385 Win=262400 Len=0
 157 5.704297  AzureWav_32:b3:33  VMware_93:a6:e7      ARP        60 Who has 192.168.60.252? Tell 192.168.60.129
 158 5.737704  Sophos_cb:39:47    Broadcast            ARP        60 Who has 192.168.60.178? Tell 192.168.60.1
 159 5.743579  QuantumN_00:eb:99  Spanning-tree-(for-… STP        60 RST. Root = 32768/0/58:61:63:00:eb:81  Cost = 0  Port = 0x8018
 160 5.833763  Sophos_cb:39:47    Broadcast            ARP        60 Who has 192.168.60.144? Tell 192.168.60.1
 161 5.892668  192.168.61.87      70.106.196.227       TCP        54 [TCP Retransmission] 63491 → 58306 [FIN, ACK] Seq=312 Ack=385 Win=262400 Len=0
 162 5.922012  Dell_93:84:b3      Broadcast            ARP        60 Who has 192.168.61.152? Tell 192.168.61.29
 163 6.125282  HP_6e:93:e2        Broadcast            ARP        60 Who has 192.168.60.116? Tell 192.168.60.122
 164 6.256876  20.50.73.11        192.168.61.87        TCP        60 443 → 62360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 165 6.436666  Dell_93:84:b3      Broadcast            ARP        60 Who has 192.168.61.152? Tell 192.168.61.29
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{CEEECAB8-8933-4C29-B7F5-68CD0FB615E7}, i
> Ethernet II, Src: Dell_93:af:d0 (00:be:43:93:af:d0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 be  43 93 af d0 08 06 00 01   ········ C·······
0010  08 00 06 04 00 01 00 be  43 93 af d0 c0 a8 3d c1   ········ C·····=·
0020  00 00 00 00 00 00 c0 a8  3c 74 00 00 00 00 00 00   ········ <t······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Results & observations:

Fig 1: Wireshark dashboard for capturing packets



```
No.     Time         Source          Destination     Protocol  Length Info
    608 17.676974    192.168.61.87   98.15.211.172   TCP         54 63524 → 27402 [ACK] Seq=1 Ack=1 Win=262656 Len=0
    609 17.677032    192.168.61.87   98.15.211.172   BitTor…    122 Handshake
    631 17.978985    192.168.61.87   98.15.211.172   TCP         54 63524 → 27402 [FIN, ACK] Seq=69 Ack=305 Win=262400 Len=0
    674 18.286316    192.168.61.87   98.15.211.172   TCP         54 63524 → 27402 [ACK] Seq=70 Ack=306 Win=262400 Len=0
   4055 77.448318    192.168.61.87   98.15.211.172   TCP         66 63646 → 27402 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   4077 77.758526    192.168.61.87   98.15.211.172   TCP         54 63646 → 27402 [ACK] Seq=1 Ack=1 Win=262656 Len=0
   4078 77.758613    192.168.61.87   98.15.211.172   BitTor…    122 Handshake
   4107 78.050165    192.168.61.87   98.15.211.172   TCP         54 63646 → 27402 [FIN, ACK] Seq=69 Ack=305 Win=262400 Len=0
   4128 78.333312    192.168.61.87   98.15.211.172   TCP         54 63646 → 27402 [ACK] Seq=70 Ack=306 Win=262400 Len=0
   6686 137.517383   192.168.61.87   98.15.211.172   TCP         66 63773 → 27402 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   6703 137.799523   192.168.61.87   98.15.211.172   TCP         54 63773 → 27402 [ACK] Seq=1 Ack=1 Win=262656 Len=0
   6704 137.799595   192.168.61.87   98.15.211.172   BitTor…    122 Handshake
   6735 138.089214   192.168.61.87   98.15.211.172   TCP         54 63773 → 27402 [FIN, ACK] Seq=69 Ack=305 Win=262400 Len=0
   6758 138.369171   192.168.61.87   98.15.211.172   TCP         54 63773 → 27402 [ACK] Seq=70 Ack=306 Win=262400 Len=0
    280 7.370846     192.168.61.87   99.63.100.172   TCP         66 63492 → 19282 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    298 8.378639     192.168.61.87   99.63.100.172   TCP         66 [TCP Retransmission] 63492 → 19282 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    319 10.384416    192.168.61.87   99.63.100.172   TCP         66 [TCP Retransmission] 63492 → 19282 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    451 14.397603    192.168.61.87   99.63.100.172   TCP         66 [TCP Retransmission] 63492 → 19282 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   6939 142.522158   192.168.61.87   99.63.100.172   TCP         66 63790 → 19282 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   6968 142.793152   192.168.61.87   99.63.100.172   TCP         54 63790 → 19282 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   6969 142.793235   192.168.61.87   99.63.100.172   BitTor…    122 Handshake
   6996 143.064915   192.168.61.87   99.63.100.172   TCP         54 63790 → 19282 [FIN, ACK] Seq=69 Ack=319 Win=63922 Len=0
   7012 143.353249   192.168.61.87   99.63.100.172   TCP         54 63790 → 19282 [ACK] Seq=70 Ack=320 Win=63922 Len=0
      1 0.000000     Dell_93:af:d0   Broadcast       ARP         60 Who has 192.168.60.116? Tell 192.168.61.193
      4 0.287589     Dell_93:bd:3d   Broadcast       ARP         60 Who has 192.168.60.116? Tell 192.168.60.128
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{CEEECAB8-8933-4C29-B7F5-68CD0FB615E7}, i
> Ethernet II, Src: Dell_93:af:d0 (00:be:43:93:af:d0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 be  43 93 af d0 08 06 00 01   ········ C·······
0010  08 00 06 04 00 01 00 be  43 93 af d0 c0 a8 3d c1   ········ C·····=·
0020  00 00 00 00 00 00 c0 a8  3c 74 00 00 00 00 00 00   ········ <t······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Result analysis and discussion:

In Fig 1. the Wireshark is started and then it used to capture the network traffic. After capturing the network traffic about 5 minutes and then analyzing it, I found that no malicious activity is going in the pc.

Future Scope:

Wireshark can be integrated with other tools to automatically find the malicious network traffic. Filters can be utilized to find out more specific data.

Exp. No: 11 **Date: 21-6-2023**

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

Requirements: A computer or forensic workstation capable of running the FTK Imager tool. Hard disk on which operations will be performed.

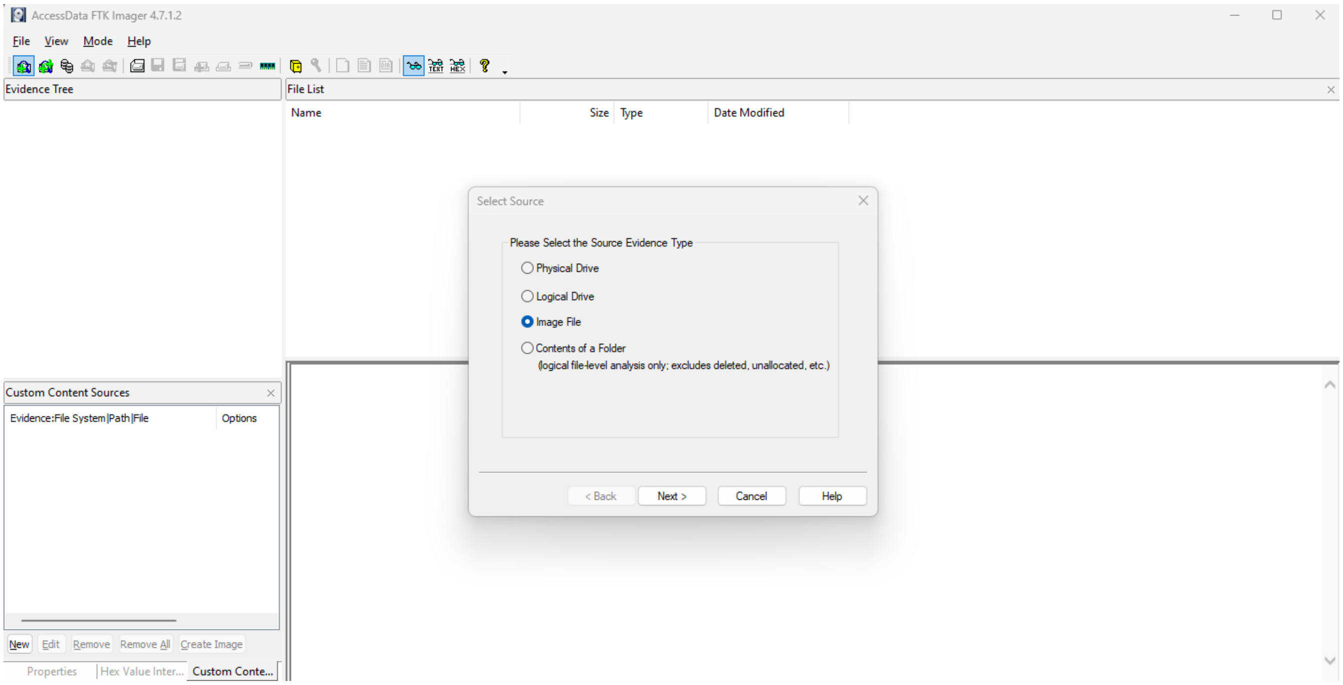
Objectives:

Installing FTK Imager in windows operating system. Using FTK Imager to analyze Hard disk's files and folder's structure.

Procedure:

Installing the FTK Imager in windows operating system. Using FTK Imager to analyze hard disk structure.

Results & Observations:



Select Source

Please Select the Source Evidence Type

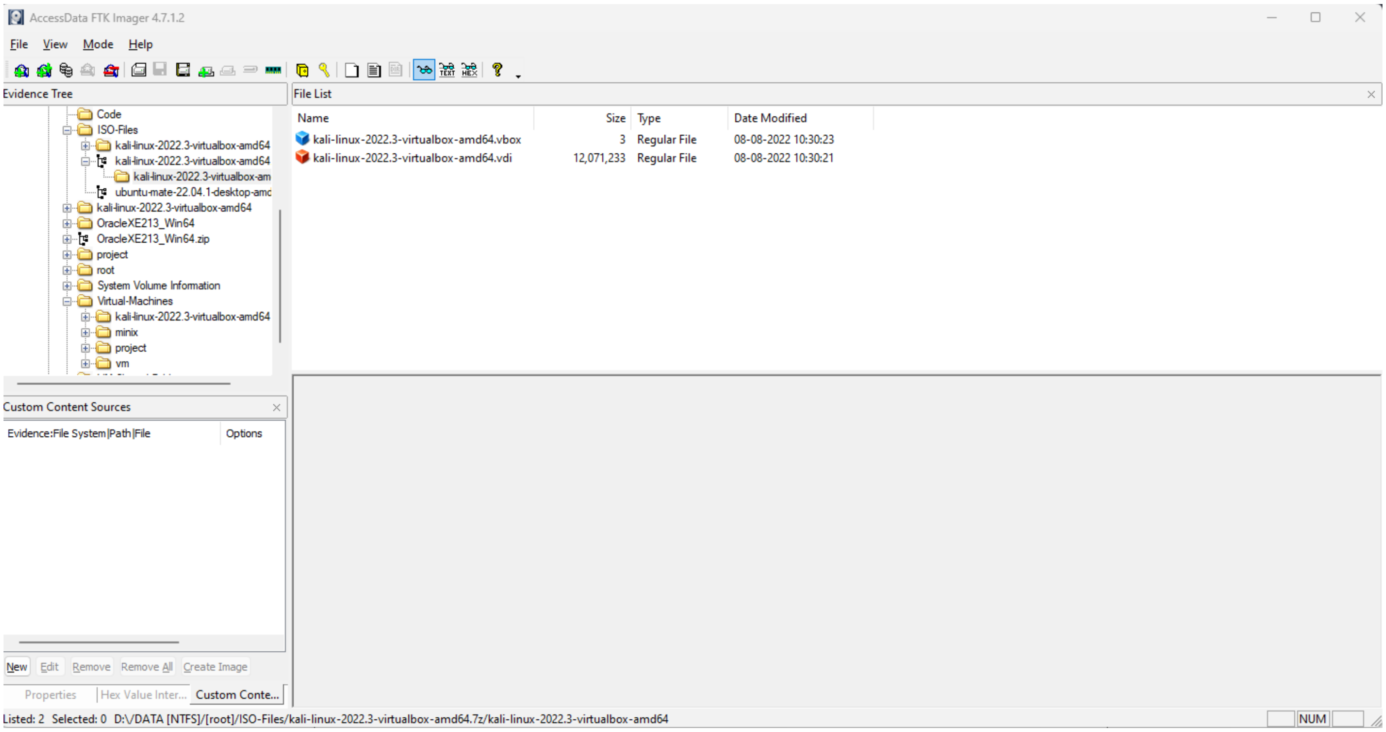
○ Physical Drive

○ Logical Drive

● Image File

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

Fig 1. FTK Imager's default dashboard to select disk for input



```
Code
ISO-Files
    kali-linux-2022.3-virtualbox-amd64
    kali-linux-2022.3-virtualbox-amd64
        kali-linux-2022.3-virtualbox-am
    ubuntu-mate-22.04.1-desktop-amc
kali-linux-2022.3-virtualbox-amd64
OracleXE213_Win64
OracleXE213_Win64.zip
project
root
System Volume Information
Virtual-Machines
    kali-linux-2022.3-virtualbox-amd64
    minix
    project
    vm
```

Name	Size	Type	Date Modified
kali-linux-2022.3-virtualbox-amd64.vbox	3	Regular File	08-08-2022 10:30:23
kali-linux-2022.3-virtualbox-amd64.vdi	12,071,233	Regular File	08-08-2022 10:30:21

```
Listed: 2  Selected: 0  D:\/DATA [NTFS]/[root]/ISO-Files/kali-linux-2022.3-virtualbox-amd64.7z/kali-linux-2022.3-virtualbox-amd64
```

Fig 2. Analyzing system's hard disk

Result analysis and discussion:

In Fig2 hard disk is analyzed that is present in the system. How many files are present and what type of contents it store is analyzed.

Future Scope:

FTK Imager is a tool for cloning the memory device. It can also be used to analyze file structure of memory device. In future A.I can be implemented with FTK to find out the malicious files in memory.

LAB MANUAL (IRM)

Exp. No: 12 **Date: 22-6-2023**

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

Requirements: A computer with Windows operating system. Tally software installation files. Sufficient data for creating and modifying a company in Tally. Windows registry analysis tool (e.g., Registry Editor, third-party registry analysis software).

Objectives:

Install Tally software and set up a company. Add sufficient data to the company and perform modifications. Analyze the Windows registry to identify evidence related to the created company.

Procedure:

Install the Tally Software in the computer. Add sufficient data to the company, including accounting entries, transactions, inventory details, and any other relevant data. Perform modifications in the company, such as making changes to existing entries, adding or deleting accounts, and updating financial information.

Results & Observations:

Result analysis and discussion:

Upon installation and setup of Tally software, a company was created and sufficient data was added. Modifications were made within the company to reflect changes in financial information and other relevant data.

Future Scope:

In future experiments, consider expanding the analysis to other areas of the Windows registry, exploring additional registry keys, values, or data that may provide further insights into Tally software and its interaction with the system.

LAB MANUAL (IRM)

Exp. No: 13 **Date: 25-6-2023**

Title: Installation and Demonstration of Fedora Workstation in a Virtual Environment.

Requirements: A computer with virtualization support. Virtualization software (e.g., VirtualBox, VMware) installed on the computer. Fedora Workstation ISO image. Sufficient system resources (CPU, RAM, storage) for running the virtual environment.

Objectives:

Install Fedora Workstation, an open-source-based platform, in a virtual environment.

Demonstrate the working and features of Fedora Workstation within the virtual environment**.**

Procedure:

Ensure that the computer meets the system requirements for running the virtualization software and creating a virtual environment. Install the virtualization software (e.g., VirtualBox, VMware). Download fedora iso and install it in virtual software.

Results & Observations:

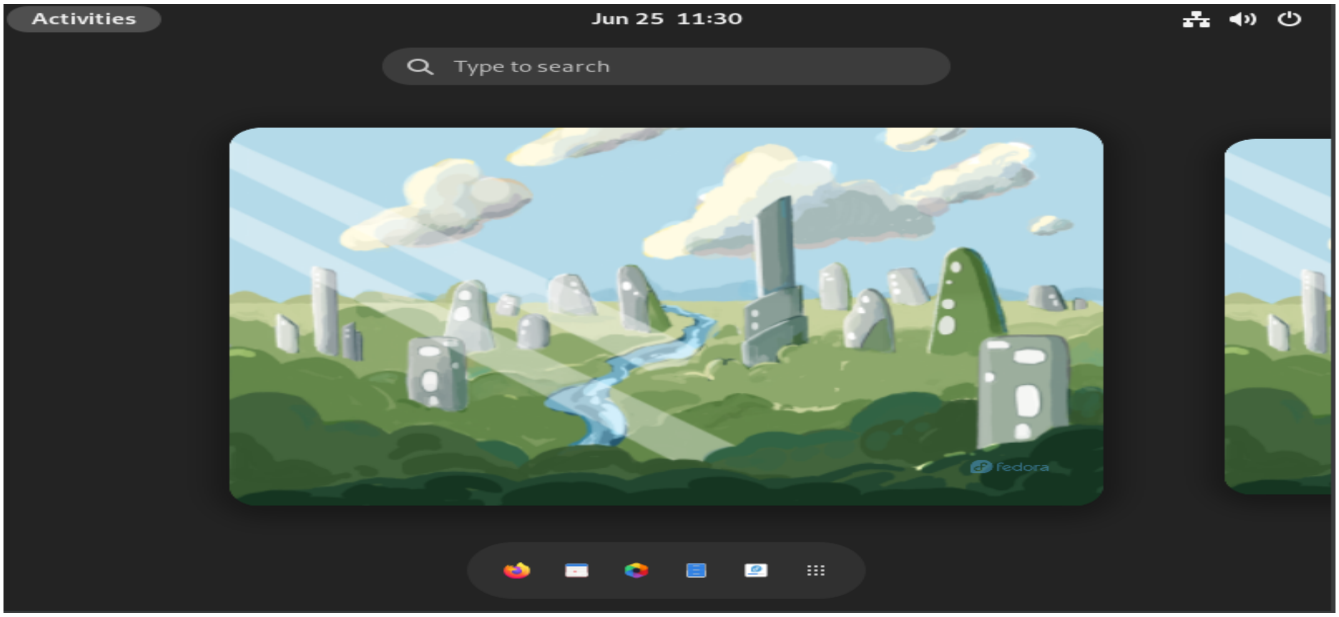


Fig 1: Default screen of fedora OS

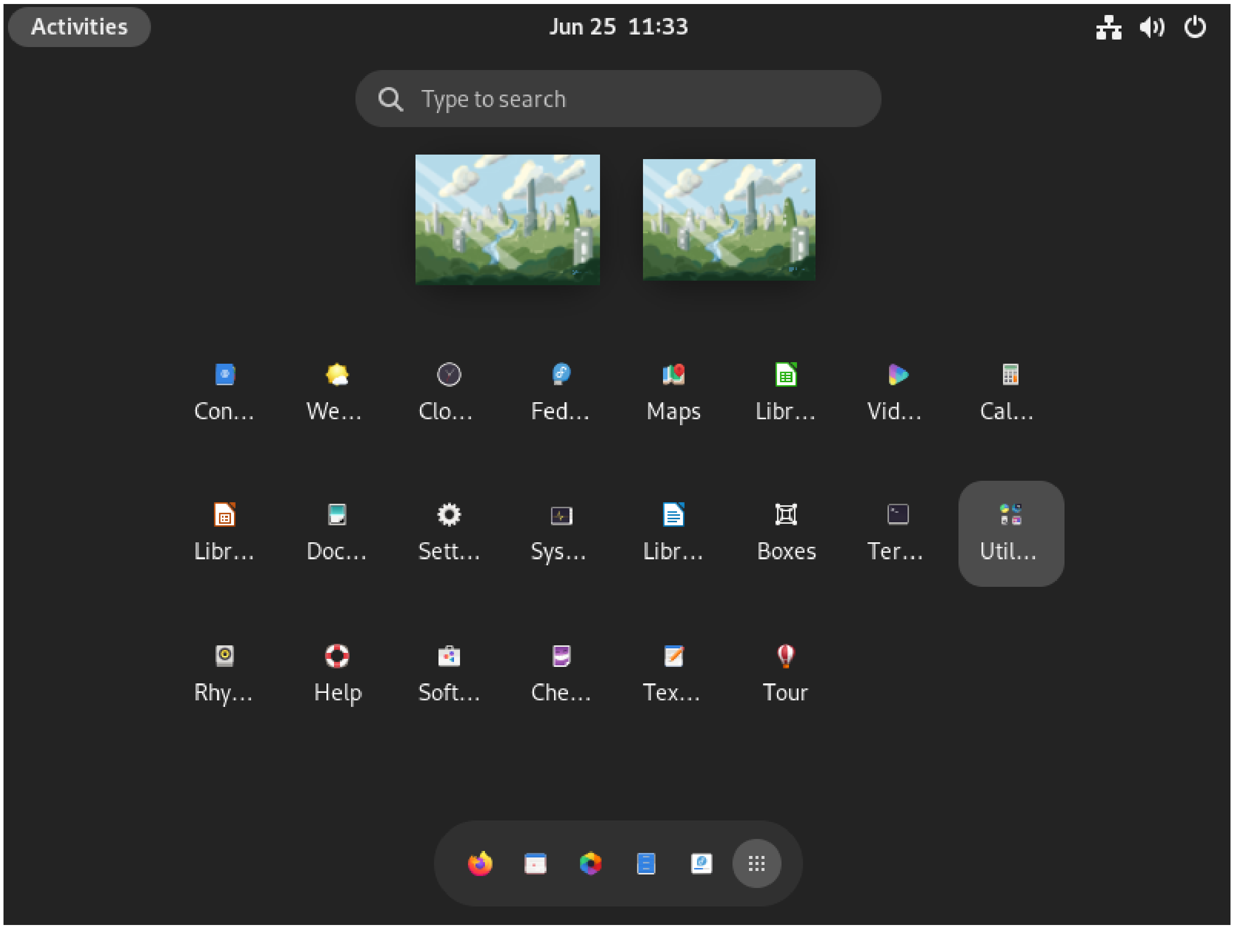


Fig 2: Software comes preinstalled in fedora OS

Result analysis and discussion:

Fedora Workstation was successfully installed within the virtual environment, showcasing the working and features of this open-source-based platform. The desktop environment provided a user-friendly interface, allowing easy navigation and access to essential applications and tools. The demonstration highlighted the availability of a vast range of open-source software, emphasizing the flexibility and security offered by the Fedora ecosystem.

Future Scope:

In future experiments, explore advanced features and customization options available within Fedora Workstation. Experiment with different software packages and extensions to personalize the desktop environment and optimize workflow. Continual exploration and utilization of open-source-based platforms like Fedora Workstation will enhance your understanding of the open-source community and contribute to leveraging the power of open-source software in various computing environments.

LAB MANUAL (IRM)

Exp. No: 14 **Date: 23-6-2023**

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

Requirements: A computer or forensic workstation capable of running Belkasoft X software. USB drive containing data/files for carving. Belkasoft X software installation files.

Objectives:

Utilize Belkasoft X, a powerful digital forensic tool, to perform data/file carving. Demonstrate the process of data/file carving using a USB drive as the data source.

Procedure:

Ensure that the computer or forensic workstation meets the system requirements for running Belkasoft X. Install the Belkasoft X software on the designated system following the provided instructions. Connect the USB drive containing the data/files to the computer or forensic workstation.

Results & Observations:

Result analysis and discussion:

Belkasoft X software was successfully installed and utilized to perform data/file carving using a USB drive as the data source.

Future Scope:

In future experiments, explore additional features and functionalities of Belkasoft X to enhance data/file carving capabilities.

LAB MANUAL (IRM)

Exp. No: 15 **Date: 25-6-2023**

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

Requirements: A computer or forensic workstation capable of running the PhotoRec. USB drive containing lost files.

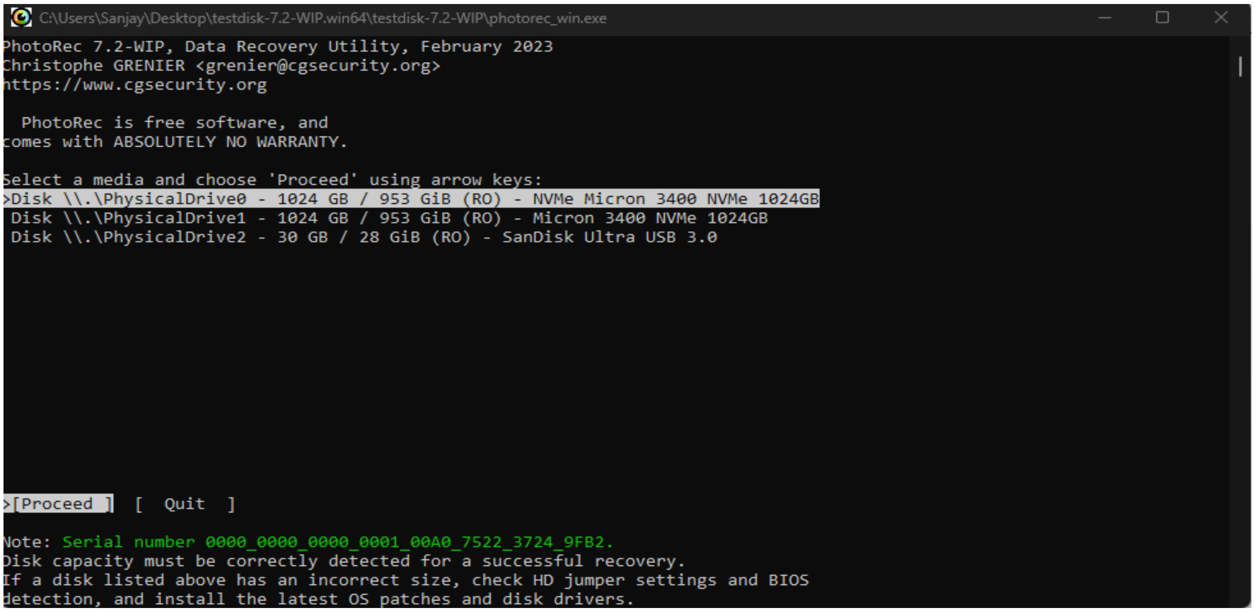
Objectives:

Utilize PhotoRec, a powerful file recovery tool, to recover lost files, audio, or video content. Using file carving techniques to extract fragmented data and recover files from the HDD/USB Drive.

Procedure:

Install the PhotoRec software on the designated system following the provided instructions. Connect the HDD/USB Drive containing the lost files to the computer or forensic workstation.

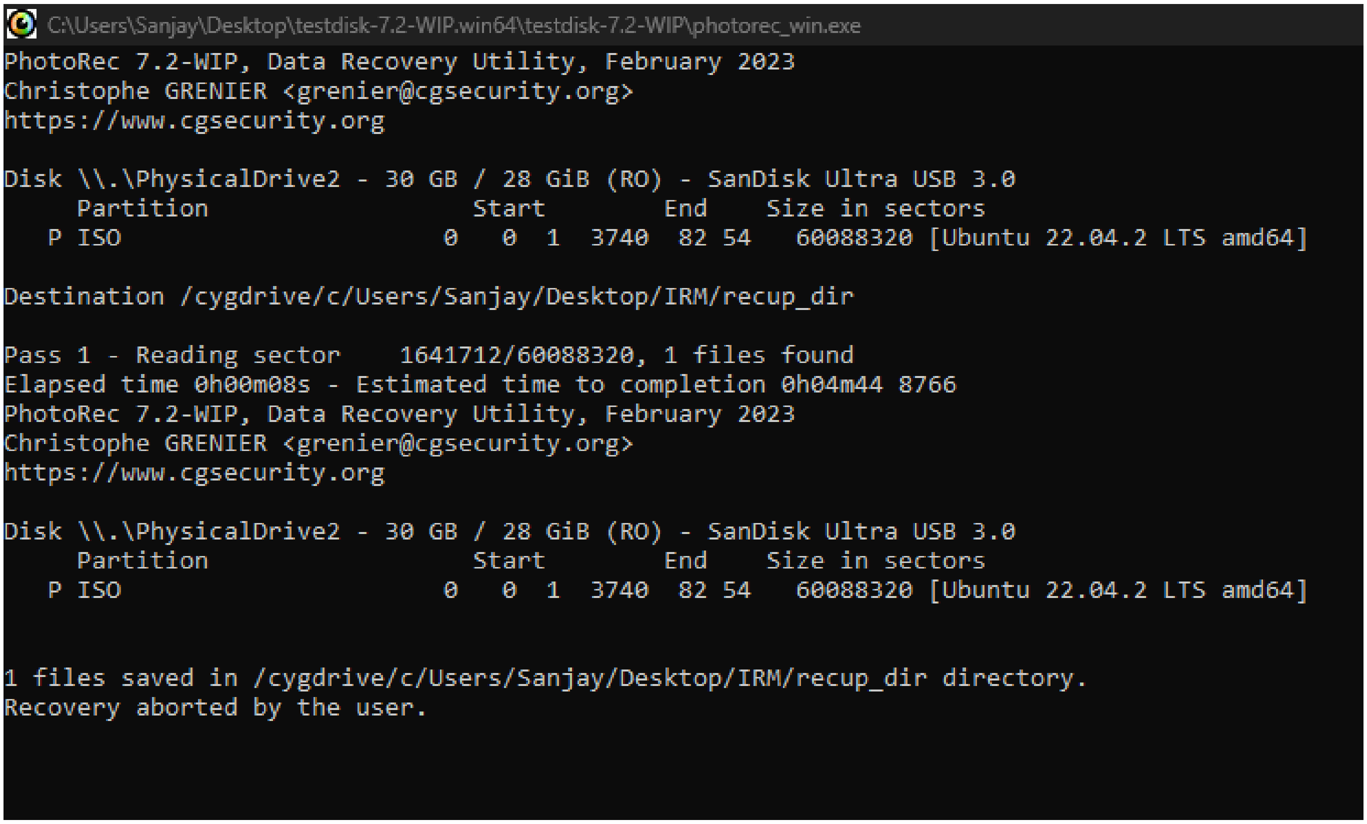
Results & Observations:



C:\Users\Sanjay\Desktop\testdisk-7.2-WIP.win64\testdisk-7.2-WIP\photorec_win.exe

```
PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

  PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media and choose 'Proceed' using arrow keys:
>Disk \\.\PhysicalDrive0 - 1024 GB / 953 GiB (RO) - NVMe Micron 3400 NVMe 1024GB
 Disk \\.\PhysicalDrive1 - 1024 GB / 953 GiB (RO) - Micron 3400 NVMe 1024GB
 Disk \\.\PhysicalDrive2 - 30 GB / 28 GiB (RO) - SanDisk Ultra USB 3.0

>[Proceed ]  [  Quit  ]

Note: Serial number 0000_0000_0000_0001_00A0_7522_3724_9FB2.
Disk capacity must be correctly detected for a successful recovery.
If a disk listed above has an incorrect size, check HD jumper settings and BIOS
detection, and install the latest OS patches and disk drivers.
```

Fig 1: PhotoRec cmd dashboard



C:\Users\Sanjay\Desktop\testdisk-7.2-WIP.win64\testdisk-7.2-WIP\photorec_win.exe

```
PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive2 - 30 GB / 28 GiB (RO) - SanDisk Ultra USB 3.0
     Partition                  Start        End    Size in sectors
   P ISO                      0   0  1  3740  82 54   60088320 [Ubuntu 22.04.2 LTS amd64]

Destination /cygdrive/c/Users/Sanjay/Desktop/IRM/recup_dir

Pass 1 - Reading sector    1641712/60088320, 1 files found
Elapsed time 0h00m08s - Estimated time to completion 0h04m44 8766
PhotoRec 7.2-WIP, Data Recovery Utility, February 2023
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk \\.\PhysicalDrive2 - 30 GB / 28 GiB (RO) - SanDisk Ultra USB 3.0
     Partition                  Start        End    Size in sectors
   P ISO                      0   0  1  3740  82 54   60088320 [Ubuntu 22.04.2 LTS amd64]


1 files saved in /cygdrive/c/Users/Sanjay/Desktop/IRM/recup_dir directory.
Recovery aborted by the user.
```

Fig 2. PhotoRec able to recover image file

Result analysis and discussion:

In Fig2 PhotoRec was able to recover the jpg file that was deleted from the USB media storage.

Future Scope:

PhotoRec is a advanced tool to recover the deleted files. In future a GUI based tool can be implemented of the PhotoRec for easy understanding of users. The CLI version is hard to use