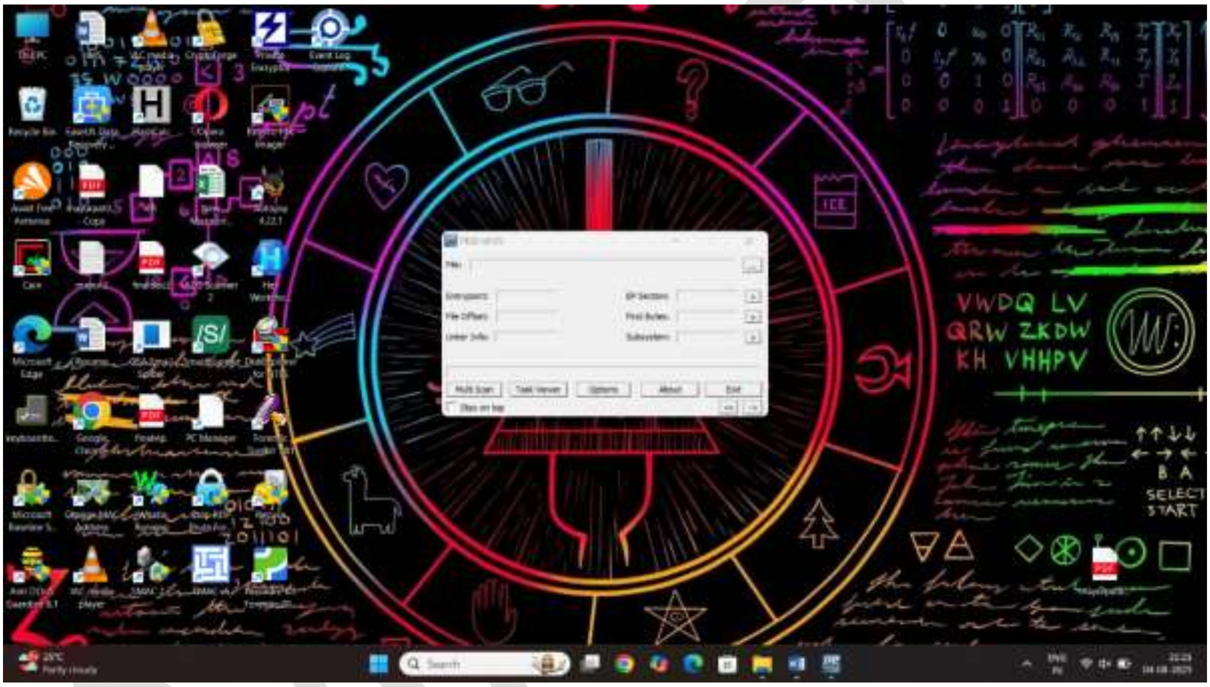
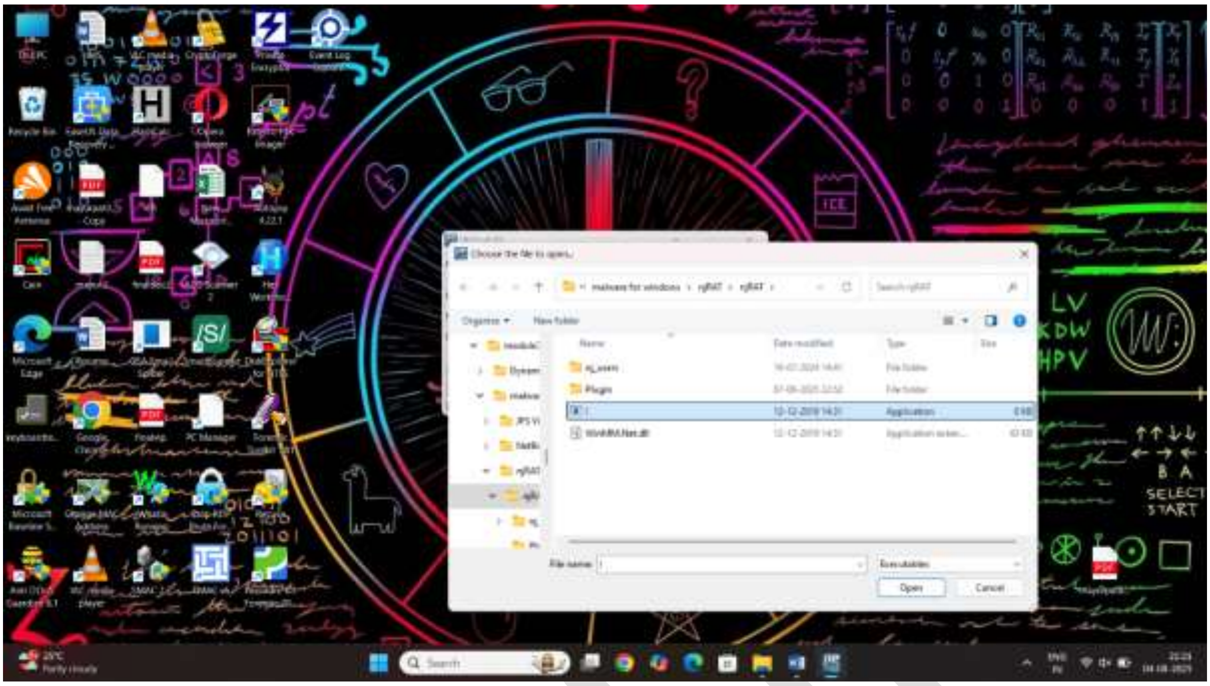
Module 9 malware forensic

Lab 1 Perfrom static analysis on a suspicious file using Peid tool

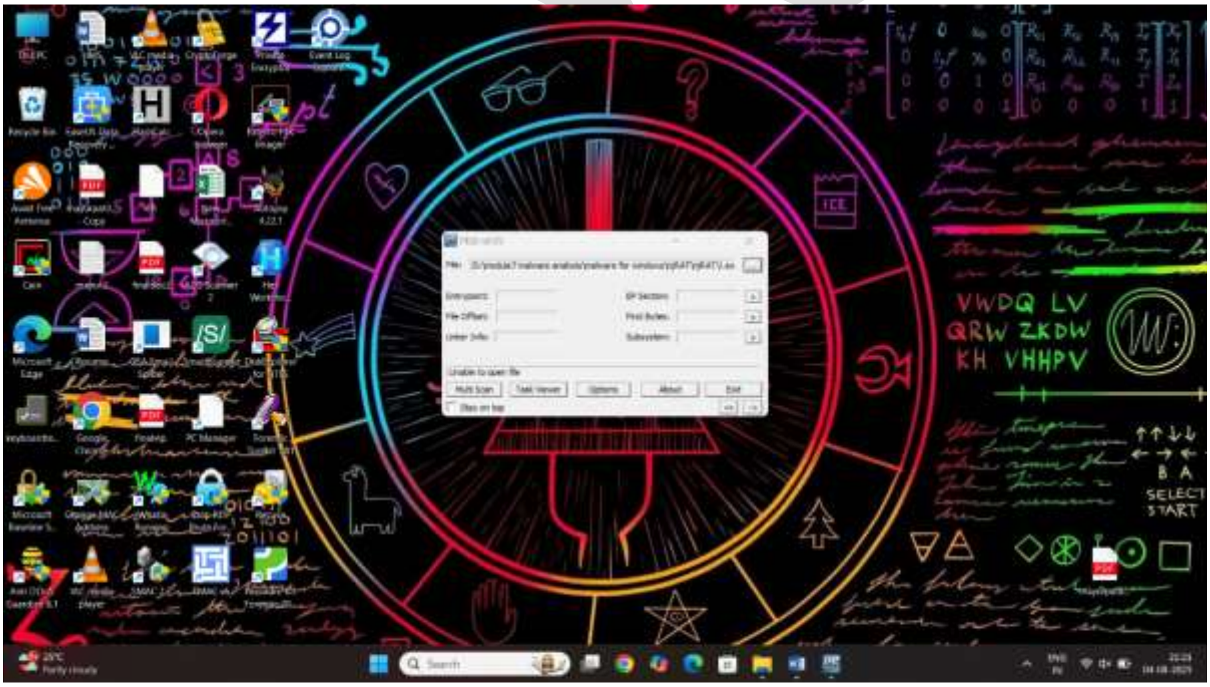
Step1 start the peid application



Step2 select the file option



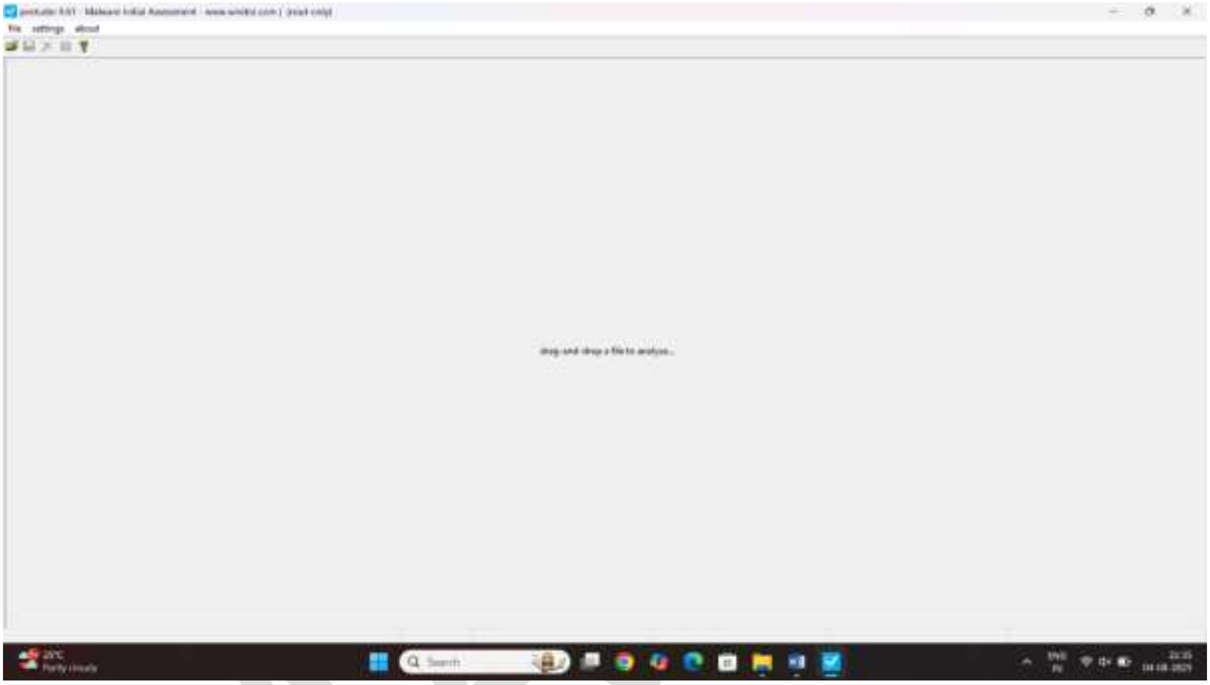
Step3 select the malware file click on next



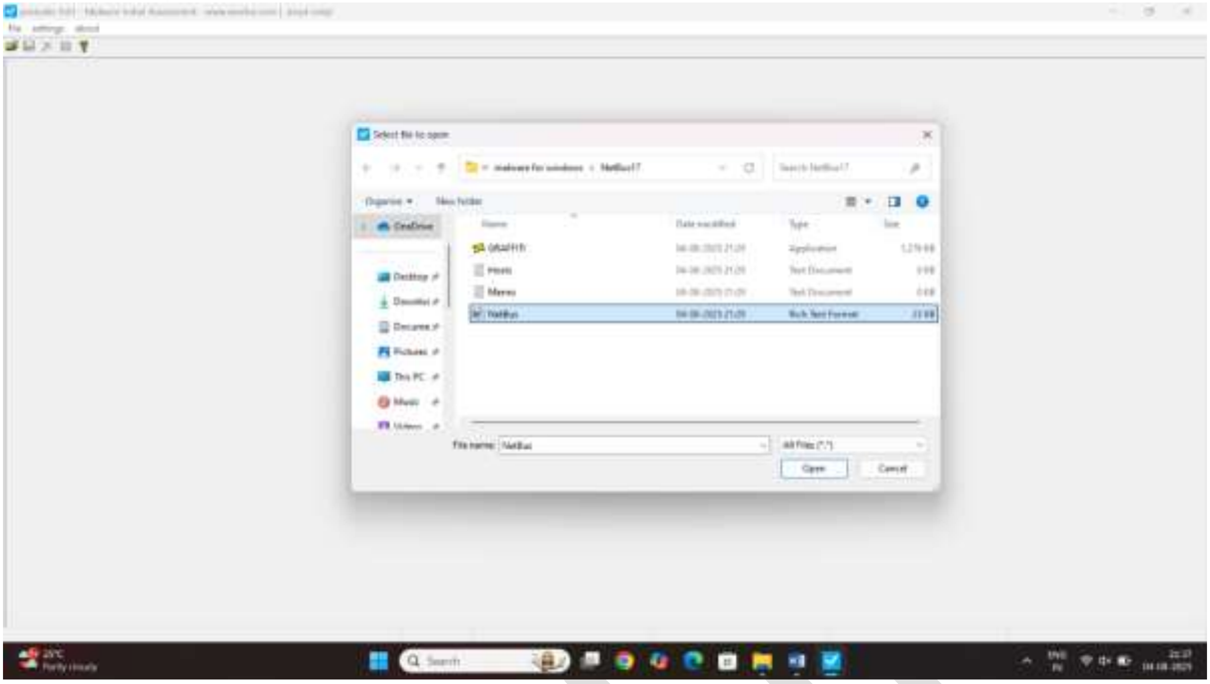
Unable to open file

Method 2d static analysis on a suspicious file using pestudio

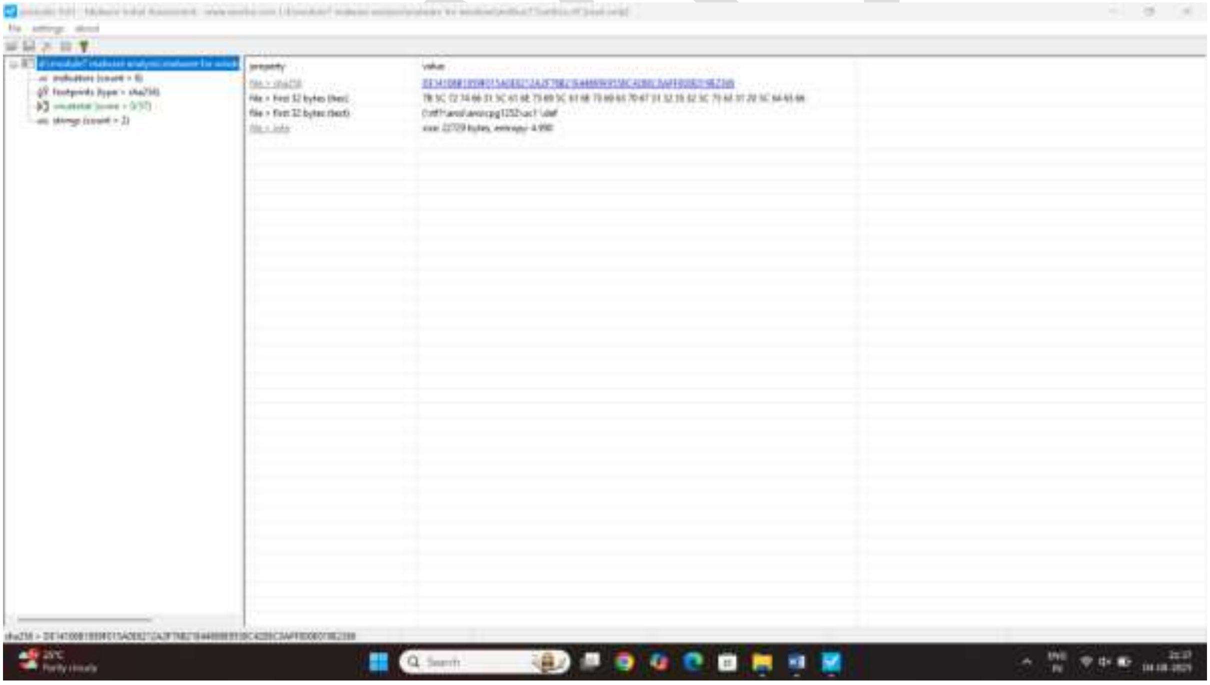
Step1 start the tool


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | (read-only)
file settings about
drag and drop a file to analyze...
Search

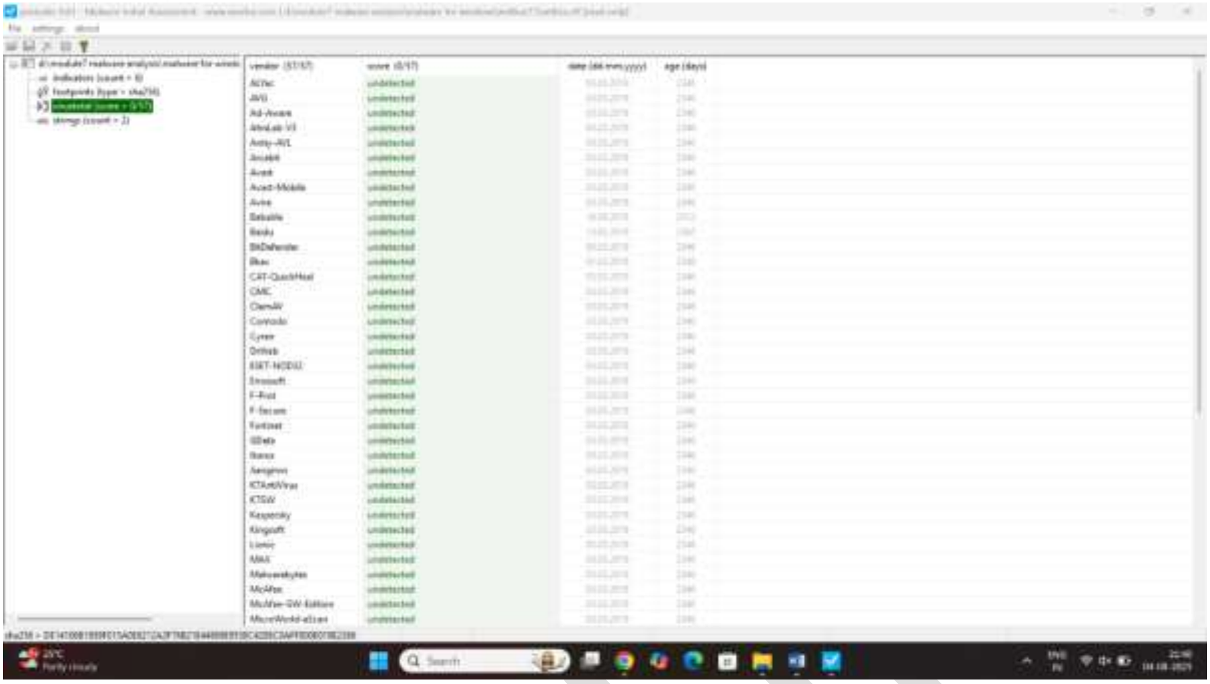
Step2 select the suspicious file



Name	Date modified	Type	Size
[illegible]	04-08-2023 21:29	Application	[illegible]
Hosts	04-08-2023 21:29	Text Document	0 KB
Memo	04-08-2023 21:29	Text Document	0 KB
NetBus	04-08-2023 21:29	Rich Text Format	[illegible]



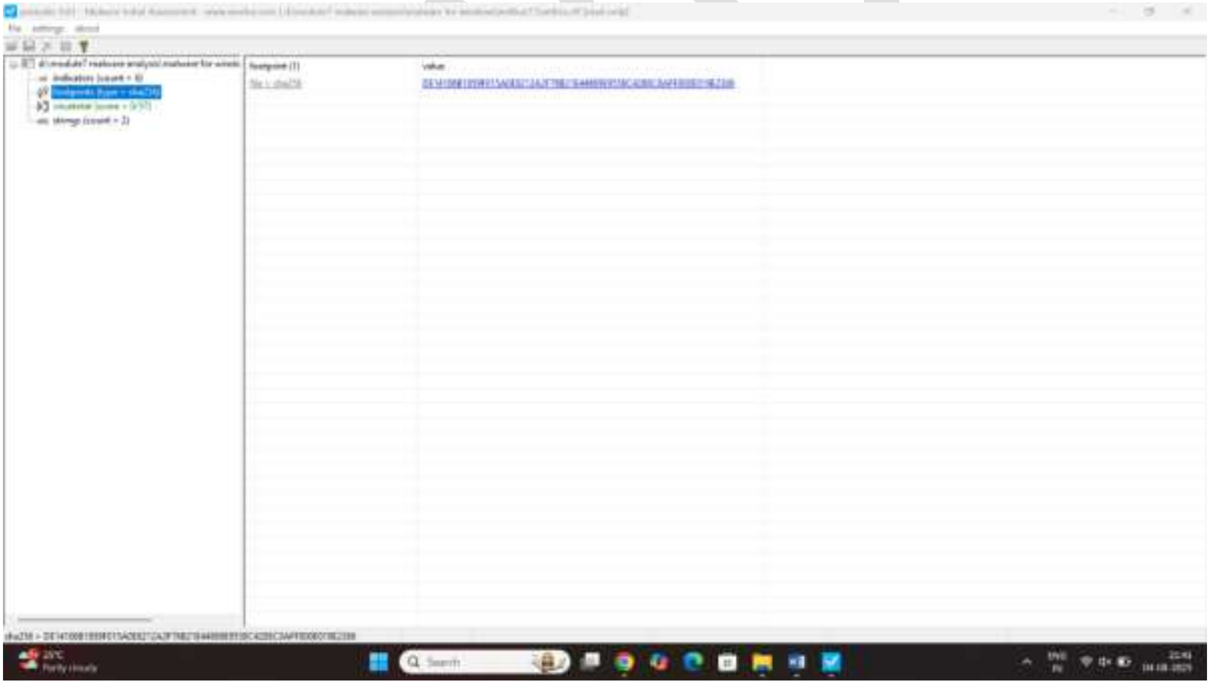
property	value
file > sha256	[illegible]
file > first 32 bytes (hex)	[illegible]
file > first 32 bytes (text)	{\rtf1\ansi\ansicpg1252\uc1 \deff
file > info	size: 22709 bytes, entropy: 4.990



d:\module7 malware analysis\malware for windo
- indicators (count = 0)
- footprints (type = sha256)
- virustotal (score = 0/57)
- strings (count = 2)

vendor (57/57)	score (0/57)	date (dd.mm.yyyy)	age (days)
ALYac	undetected	[illegible]	[illegible]
AVG	undetected	[illegible]	[illegible]
Ad-Aware	undetected	[illegible]	[illegible]
AhnLab-V3	undetected	[illegible]	[illegible]
Antiy-AVL	undetected	[illegible]	[illegible]
Arcabit	undetected	[illegible]	[illegible]
Avast	undetected	[illegible]	[illegible]
Avast-Mobile	undetected	[illegible]	[illegible]
Avira	undetected	[illegible]	[illegible]
Babable	undetected	[illegible]	[illegible]
Baidu	undetected	[illegible]	[illegible]
BitDefender	undetected	[illegible]	[illegible]
Bkav	undetected	[illegible]	[illegible]
CAT-QuickHeal	undetected	[illegible]	[illegible]
CMC	undetected	[illegible]	[illegible]
ClamAV	undetected	[illegible]	[illegible]
Comodo	undetected	[illegible]	[illegible]
Cyren	undetected	[illegible]	[illegible]
DrWeb	undetected	[illegible]	[illegible]
ESET-NOD32	undetected	[illegible]	[illegible]
Emsisoft	undetected	[illegible]	[illegible]
F-Prot	undetected	[illegible]	[illegible]
F-Secure	undetected	[illegible]	[illegible]
Fortinet	undetected	[illegible]	[illegible]
GData	undetected	[illegible]	[illegible]
Ikarus	undetected	[illegible]	[illegible]
Jiangmin	undetected	[illegible]	[illegible]
K7AntiVirus	undetected	[illegible]	[illegible]
K7GW	undetected	[illegible]	[illegible]
Kaspersky	undetected	[illegible]	[illegible]
Kingsoft	undetected	[illegible]	[illegible]
Lionic	undetected	[illegible]	[illegible]
MAX	undetected	[illegible]	[illegible]
Malwarebytes	undetected	[illegible]	[illegible]
McAfee	undetected	[illegible]	[illegible]
McAfee-GW-Edition	undetected	[illegible]	[illegible]
MicroWorld-eScan	undetected	[illegible]	[illegible]

sha256 > [illegible]



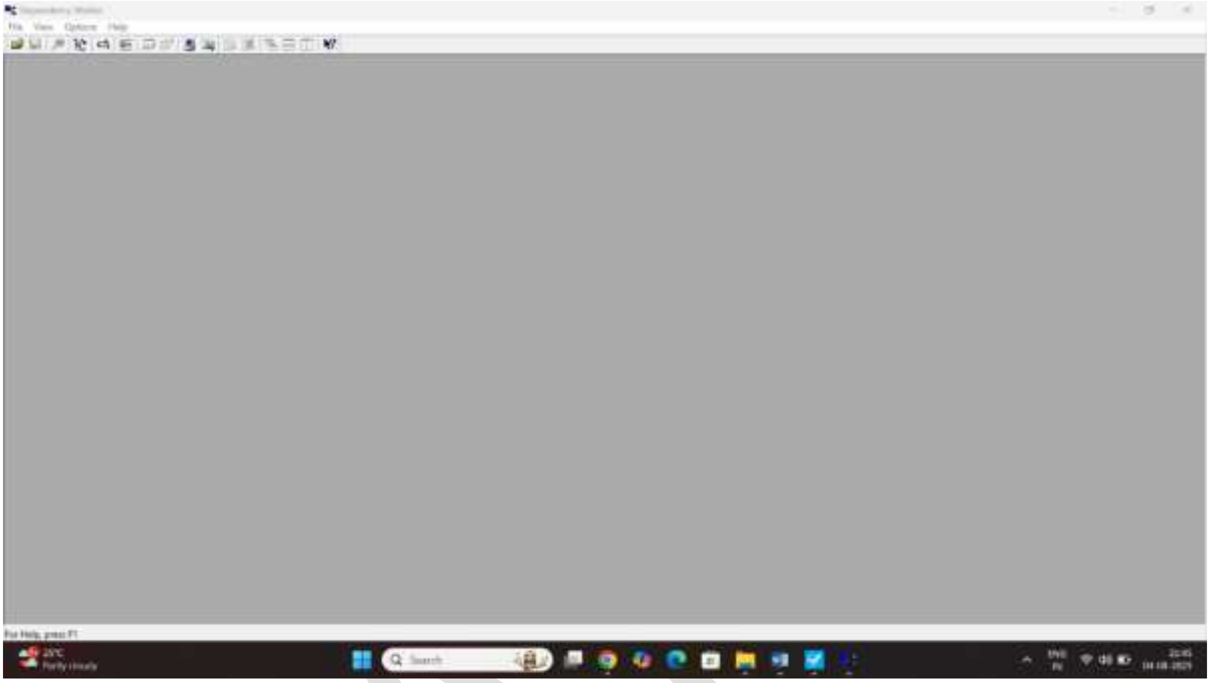
d:\module7 malware analysis\malware for windo
- indicators (count = 0)
- footprints (type = sha256)
- virustotal (score = 0/57)
- strings (count = 2)

footprint (1)	value
file > sha256	[illegible]

sha256 > [illegible]

Method 3d static analysis on a suspicious file using depency walker

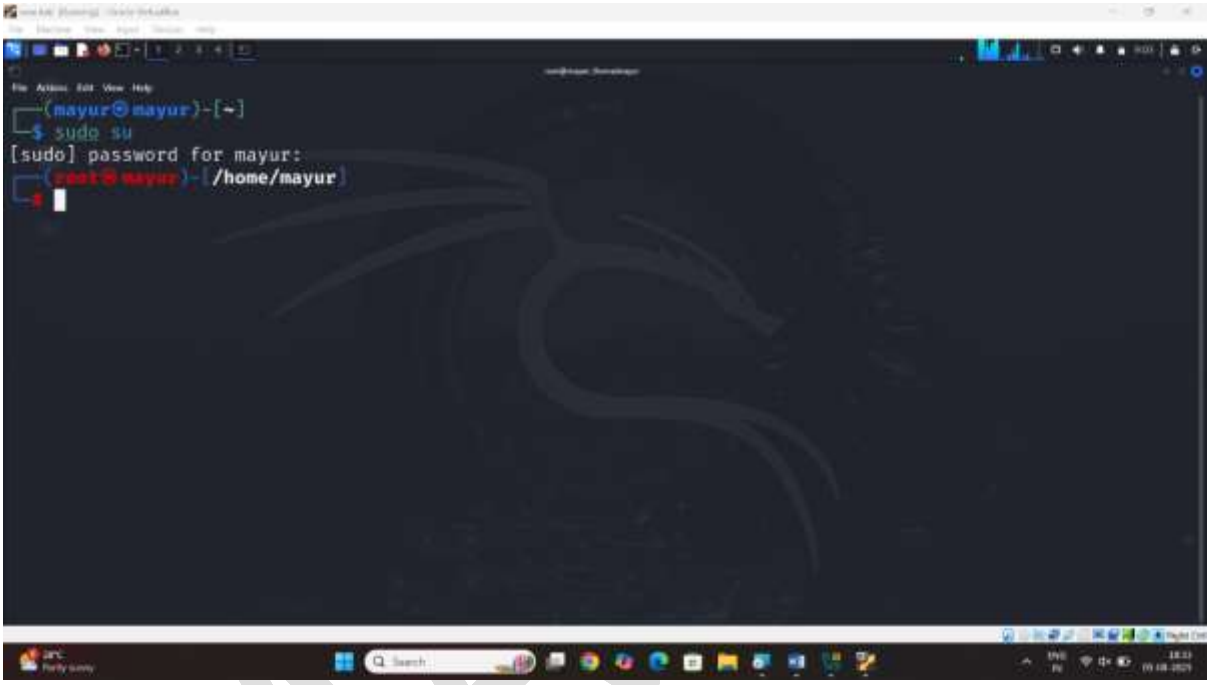
Step1 start the application



Lab3 forensic examination of a suspicious pdf file using Didier staven suite

Step1 start the kali linux machine

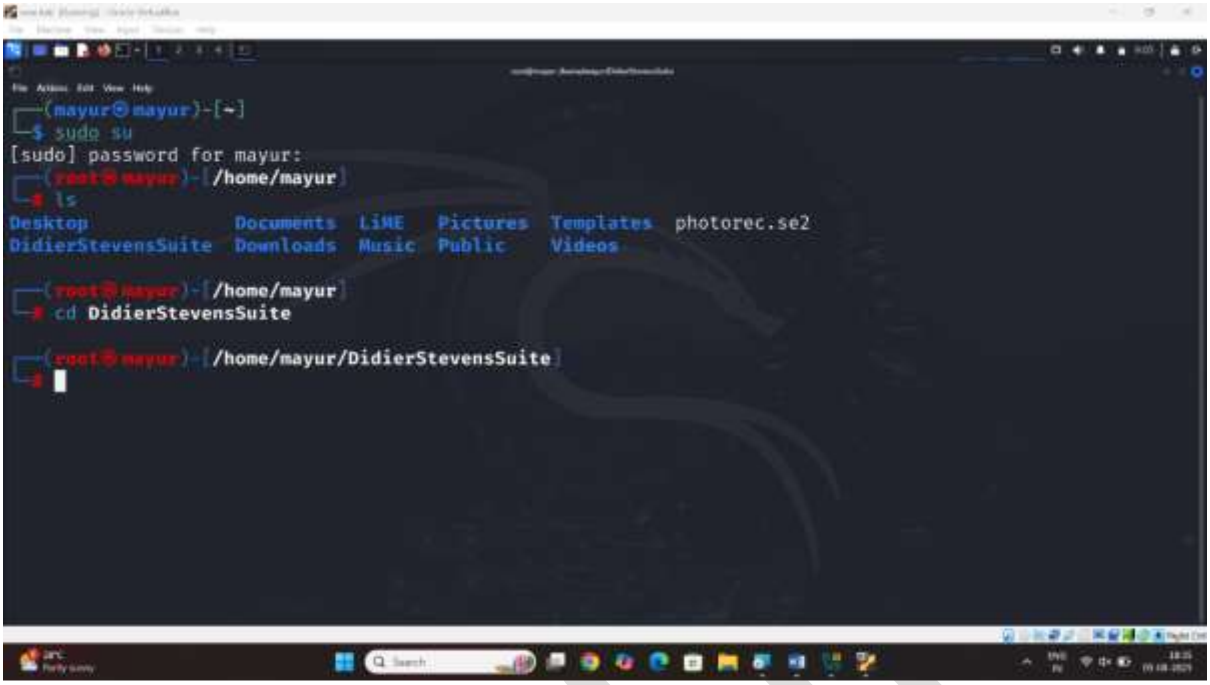
Step2 download the tool in github



```
┌──(mayur㉿mayur)-[~]
└─$ sudo su
[sudo] password for mayur:
┌──(root㉿mayur)-[/home/mayur]
└─#
```

Go to didierstavensuite tool

Command cd Didierstavensuite

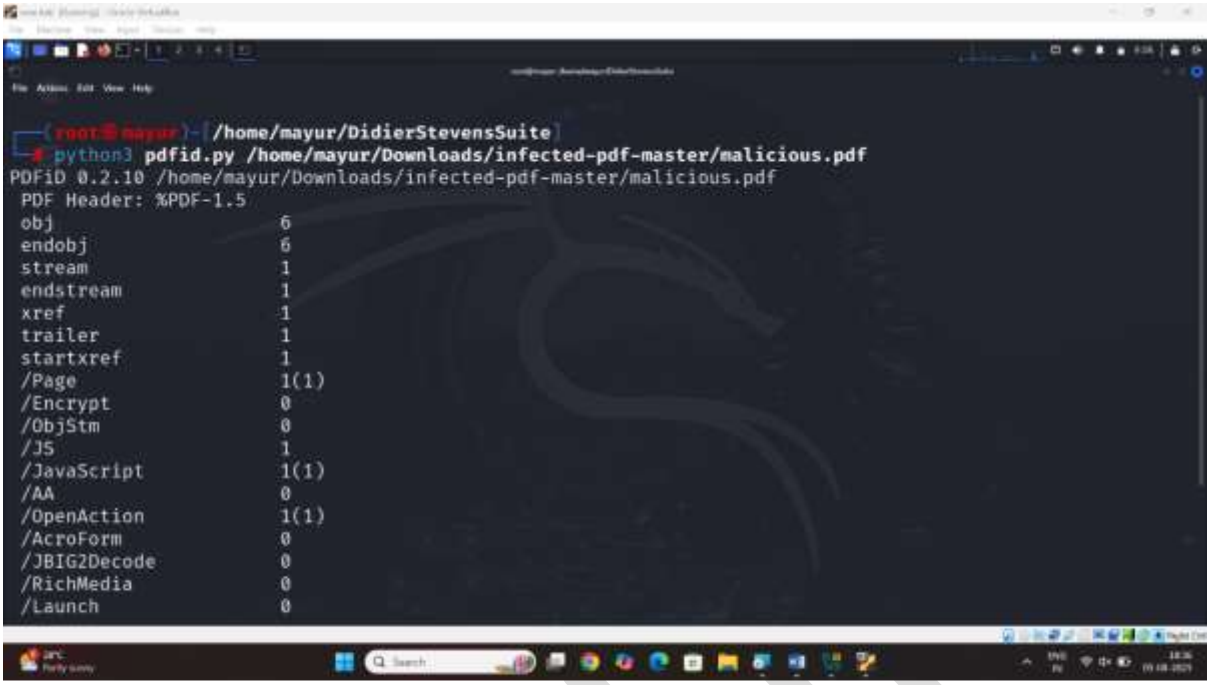


```
┌──(mayur㉿mayur)-[~]
└─$ sudo su
[sudo] password for mayur:
┌──(root㉿mayur)-[/home/mayur]
└─# ls
Desktop             Documents  LiME   Pictures  Templates  photorec.se2
DidierStevensSuite  Downloads  Music  Public    Videos

┌──(root㉿mayur)-[/home/mayur]
└─# cd DidierStevensSuite

┌──(root㉿mayur)-[/home/mayur/DidierStevensSuite]
└─# █
```

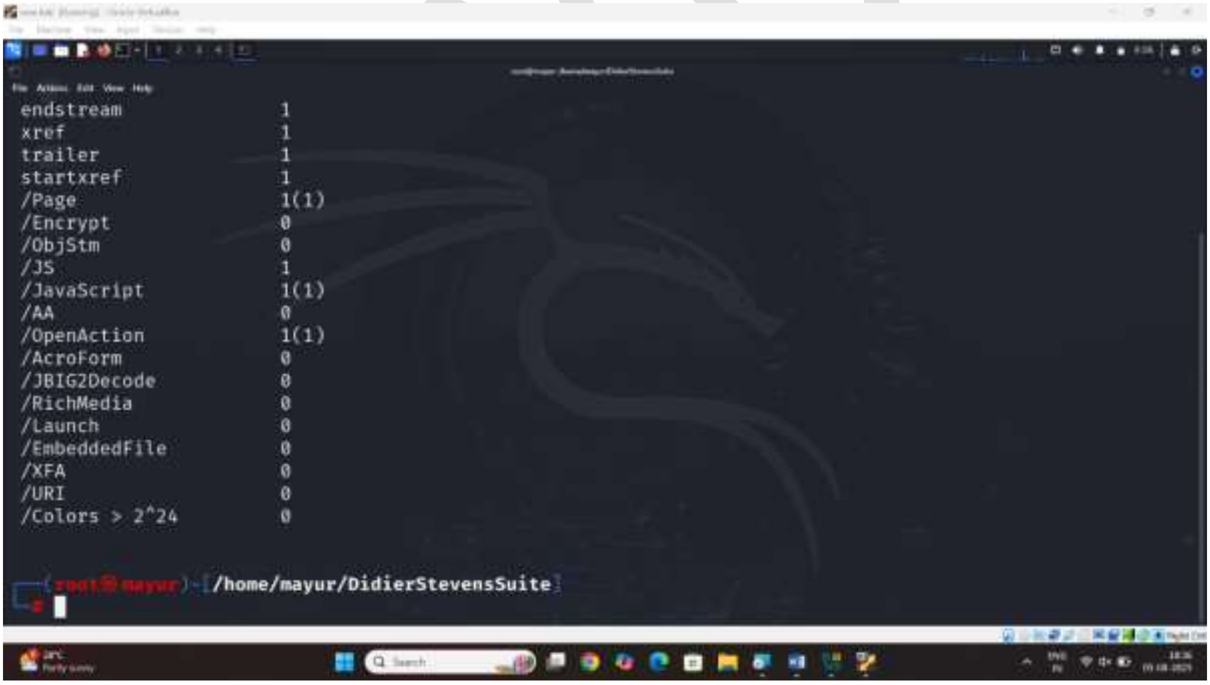
Step3 analysis malicious pdf file

Command python3 pdfid.py /home/mayur/kali/downloads/infected-pdf-master/malicious.pdf

Result:



```
┌──(root㉿mayur)-[/home/mayur/DidierStevensSuite]
└─# python3 pdfid.py /home/mayur/Downloads/infected-pdf-master/malicious.pdf
PDFiD 0.2.10 /home/mayur/Downloads/infected-pdf-master/malicious.pdf
 PDF Header: %PDF-1.5
 obj                    6
 endobj                 6
 stream                 1
 endstream              1
 xref                   1
 trailer                1
 startxref              1
 /Page                  1(1)
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1(1)
 /AA                    0
 /OpenAction            1(1)
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
```

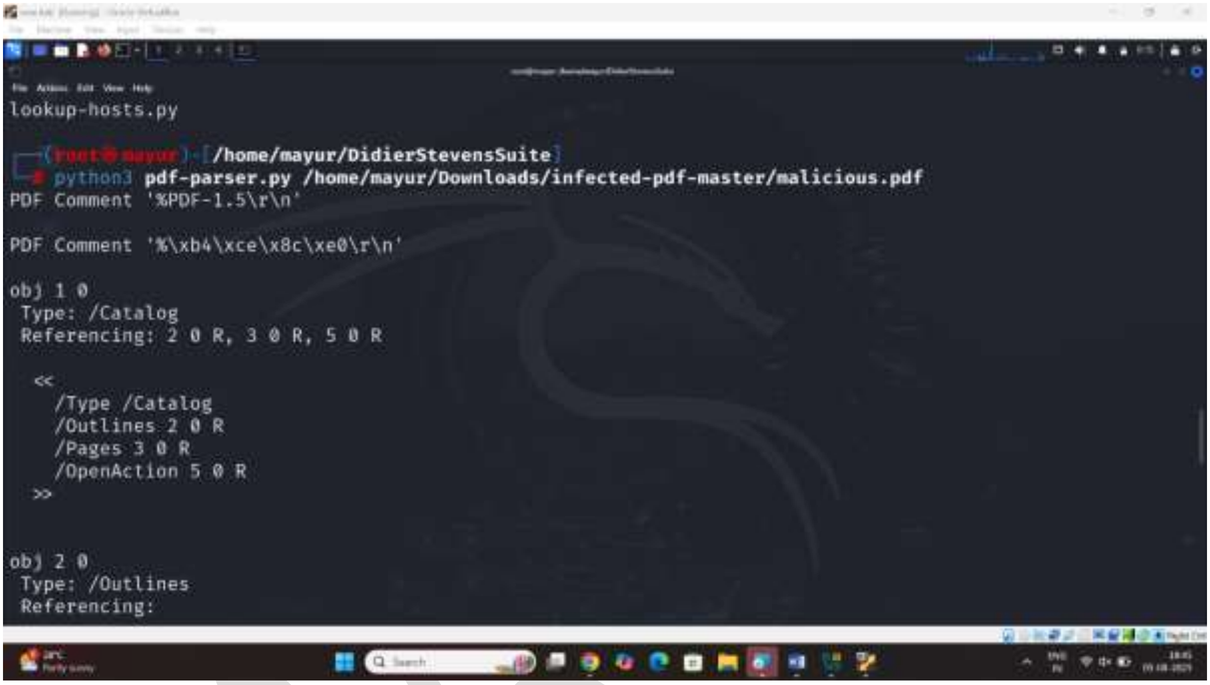


```
 endstream              1
 xref                   1
 trailer                1
 startxref              1
 /Page                  1(1)
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            1(1)
 /AA                    0
 /OpenAction            1(1)
 /AcroForm              0
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /URI                   0
 /Colors > 2^24         0

┌──(root㉿mayur)-[/home/mayur/DidierStevensSuite]
└─# 
```

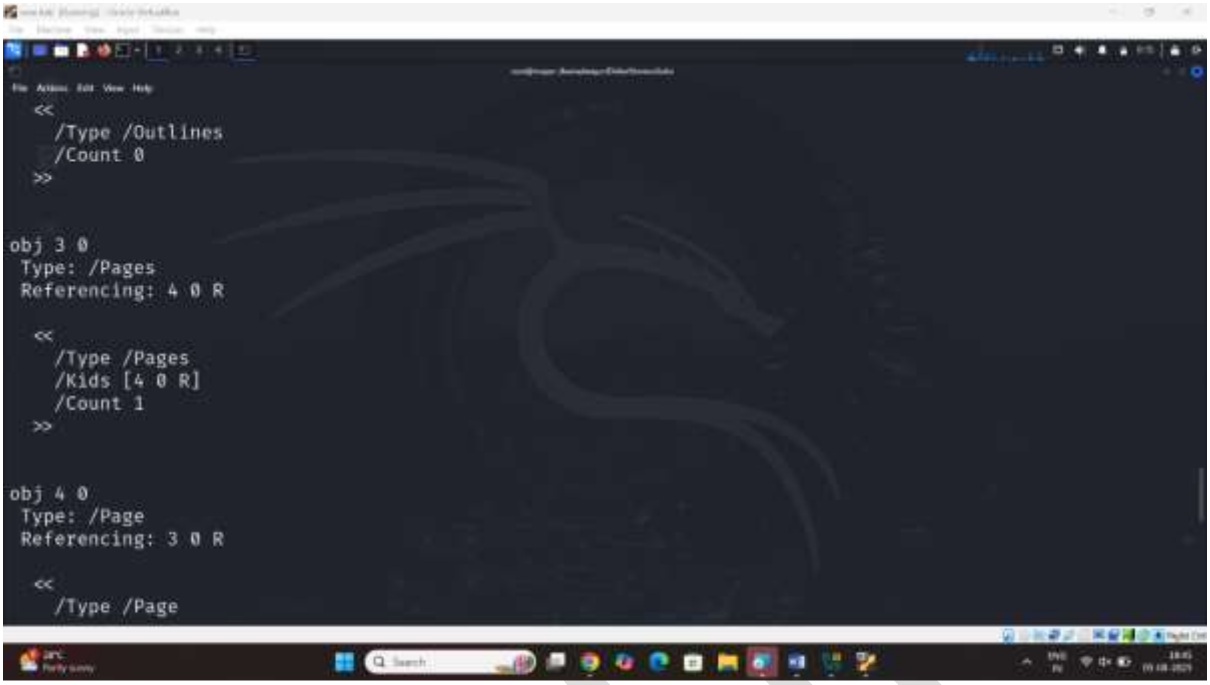
Second method malicious pdf file analysis

Command: python3 pdf-parser.py/home/kali/mayur/downloads/infecterd-pdf-master/malicious.pdf

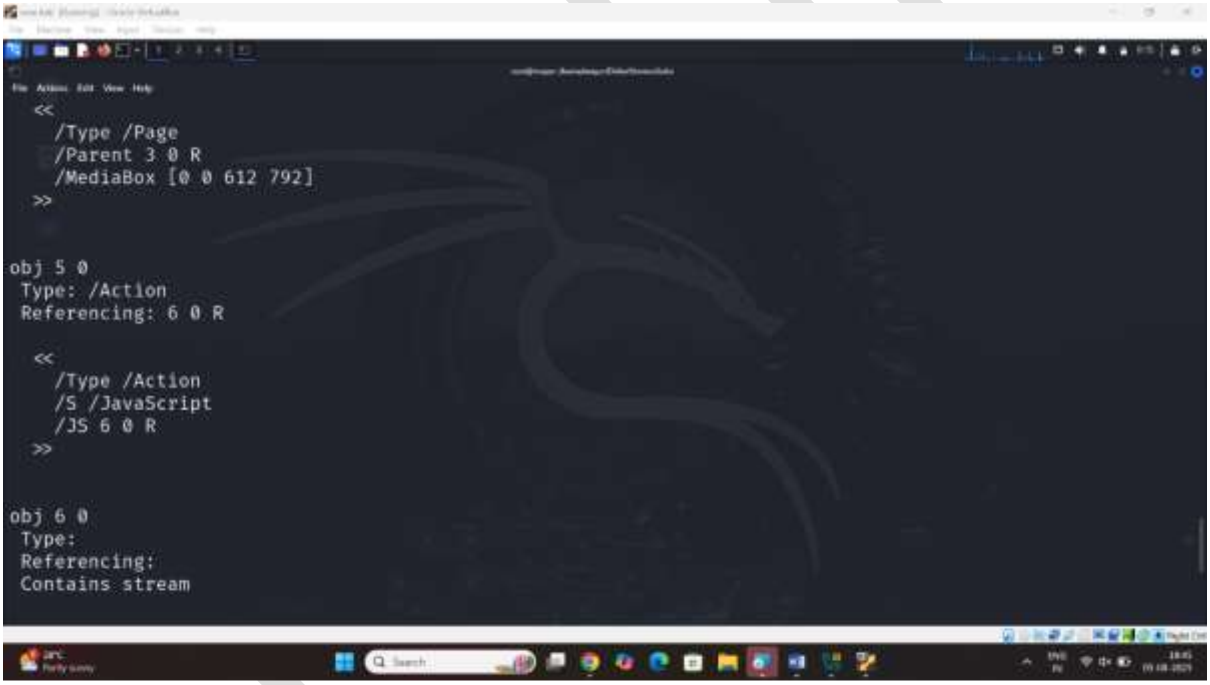
Result:



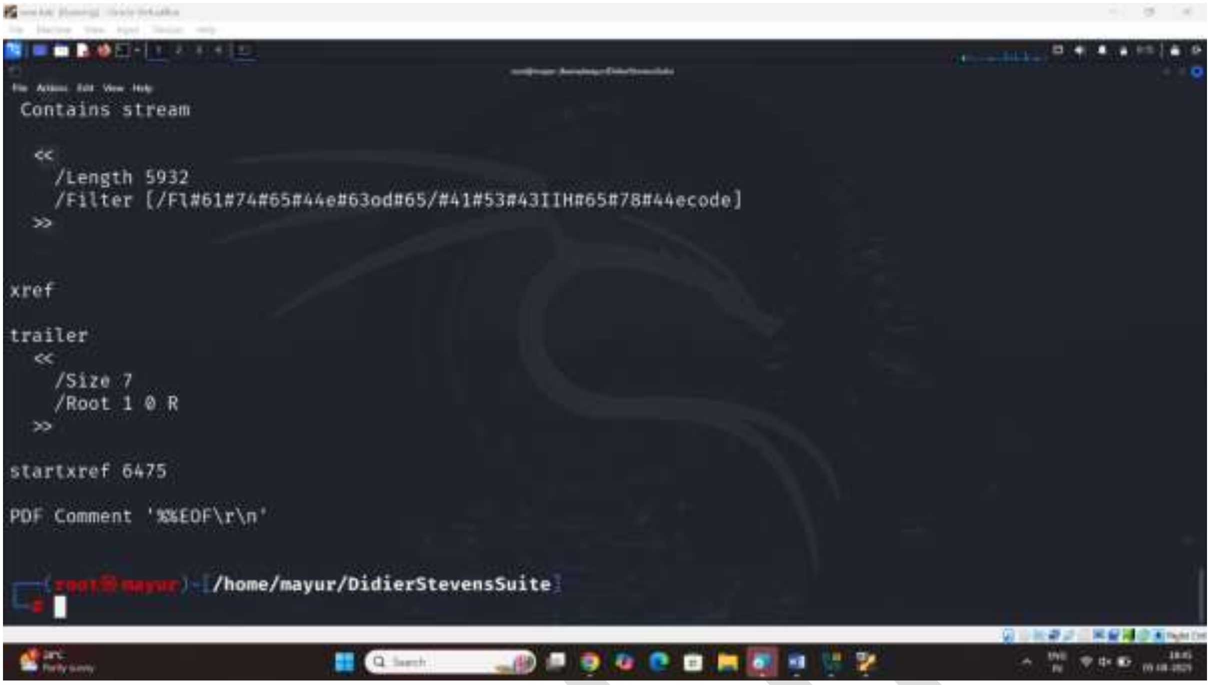
```
lookup-hosts.py

┌──(root㉿mayur)-[/home/mayur/DidierStevensSuite]
└─# python3 pdf-parser.py /home/mayur/Downloads/infected-pdf-master/malicious.pdf
PDF Comment '%PDF-1.5\r\n'

PDF Comment '%\xb4\xce\x8c\xe0\r\n'

obj 1 0
 Type: /Catalog
 Referencing: 2 0 R, 3 0 R, 5 0 R

  <<
    /Type /Catalog
    /Outlines 2 0 R
    /Pages 3 0 R
    /OpenAction 5 0 R
  >>


obj 2 0
 Type: /Outlines
 Referencing:
```



```
    <<
      /Type /Outlines
      /Count 0
    >>

obj 3 0
 Type: /Pages
 Referencing: 4 0 R

    <<
      /Type /Pages
      /Kids [4 0 R]
      /Count 1
    >>

obj 4 0
 Type: /Page
 Referencing: 3 0 R

    <<
      /Type /Page
```



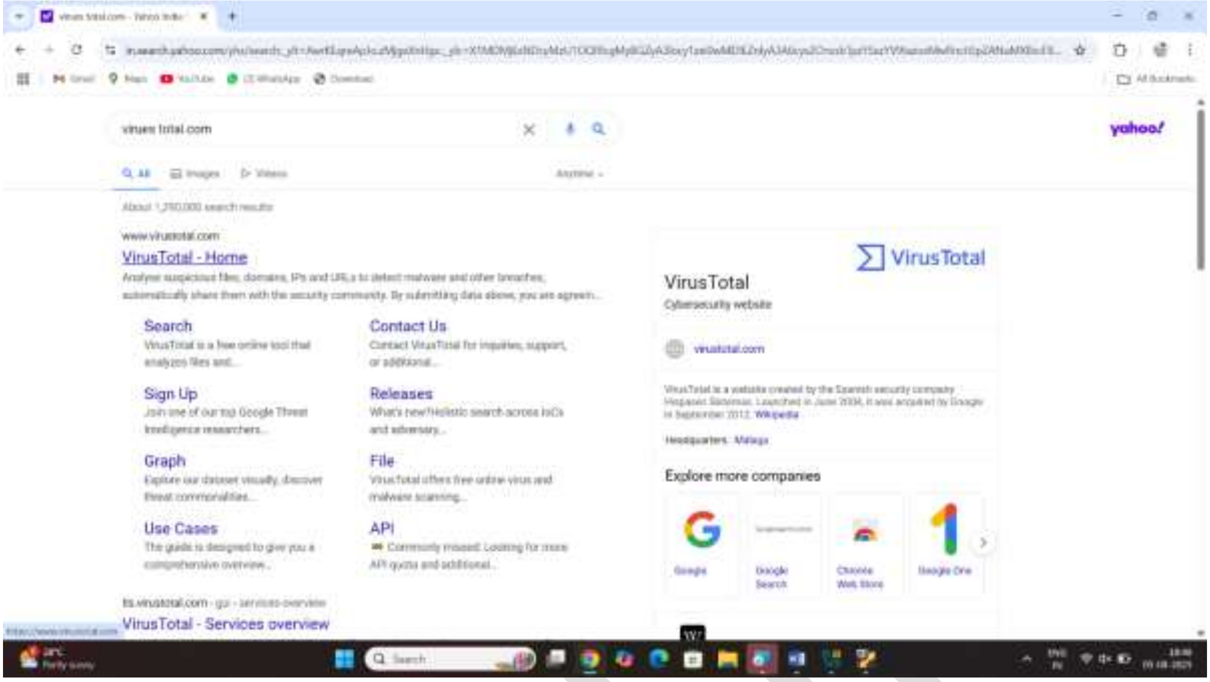
```
    <<
      /Type /Page
      /Parent 3 0 R
      /MediaBox [0 0 612 792]
    >>

obj 5 0
 Type: /Action
 Referencing: 6 0 R

    <<
      /Type /Action
      /S /JavaScript
      /JS 6 0 R
    >>

obj 6 0
 Type:
 Referencing:
 Contains stream
```



```
 Contains stream

  <<
    /Length 5932
    /Filter [/Fl#61#74#65#44e#63od#65/#41#53#43IIH#65#78#44ecode]
  >>


xref

trailer
  <<
    /Size 7
    /Root 1 0 R
  >>

startxref 6475

PDF Comment '%%EOF\r\n'

┌──(root㉿mayur)-[/home/mayur/DidierStevensSuite]
└─# 
```

Lab5 examine a suspicious file using online resource using virus total.com

Step1 open the google type the virus total.com



viruses total.com

About 1,250,000 search results

www.virustotal.com

VirusTotal - Home

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community. By submitting data above, you are agreein...

Search — VirusTotal is a free online tool that analyzes files and...

Contact Us — Contact VirusTotal for inquiries, support, or additional...

Sign Up — Join one of our top Google Threat Intelligence researchers...

Releases — What's new?Holistic search across IoCs and adversary...

Graph — Explore our dataset visually, discover threat commonalities...

File — VirusTotal offers free online virus and malware scanning...

Use Cases — The guide is designed to give you a comprehensive overview...

API — Commonly missed: Looking for more API quota and additional...

ts.virustotal.com › gui › services-overview

VirusTotal - Services overview

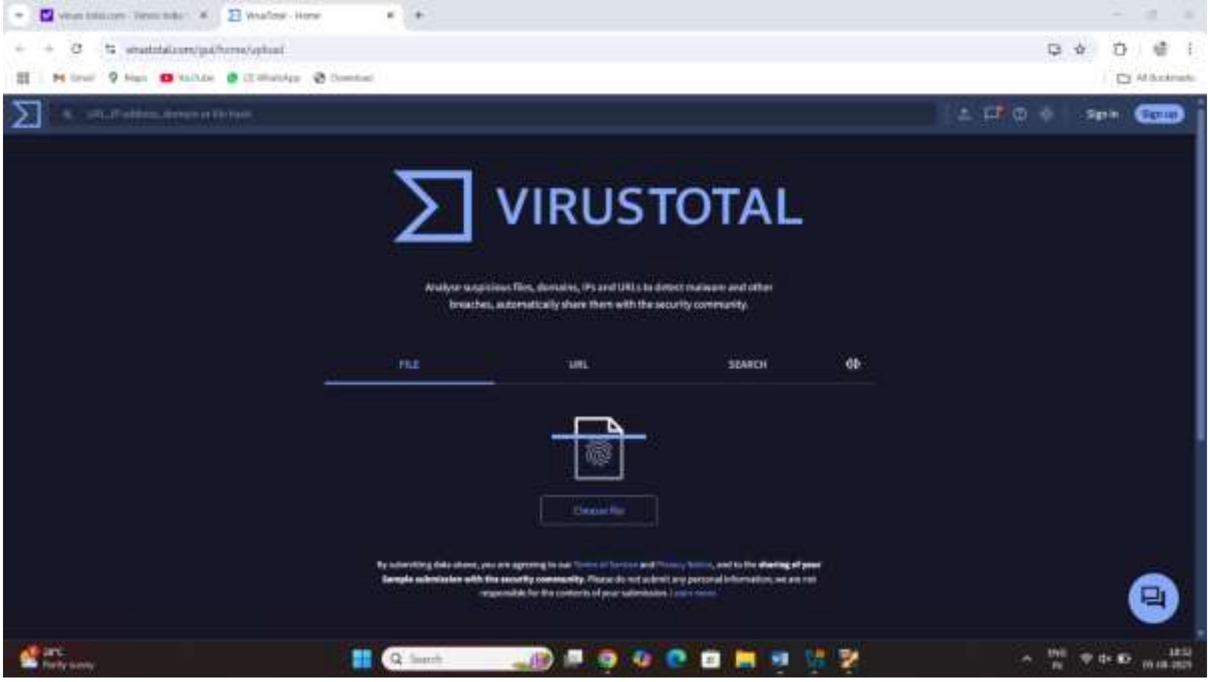
VirusTotal

Cybersecurity website

virustotal.com

VirusTotal is a website created by the Spanish security company Hispasec Sistemas. Launched in June 2004, it was acquired by Google in September 2012. Wikipedia

Headquarters: Malaga

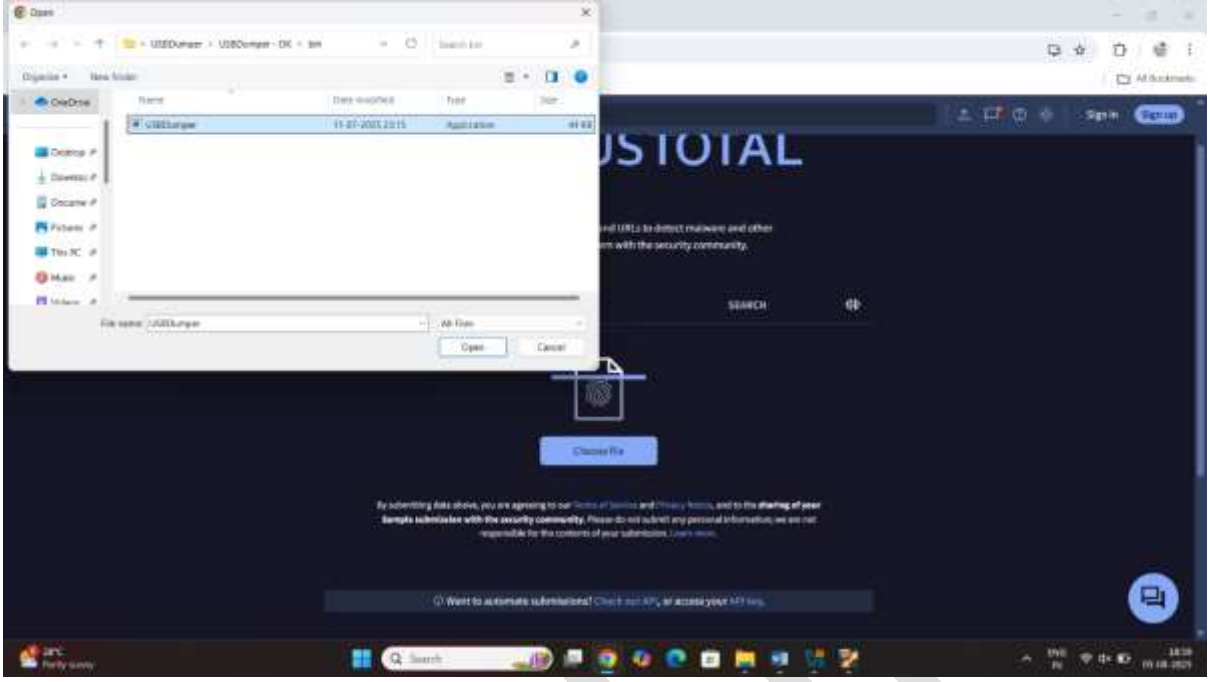


virustotal.com/gui/home/upload

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more

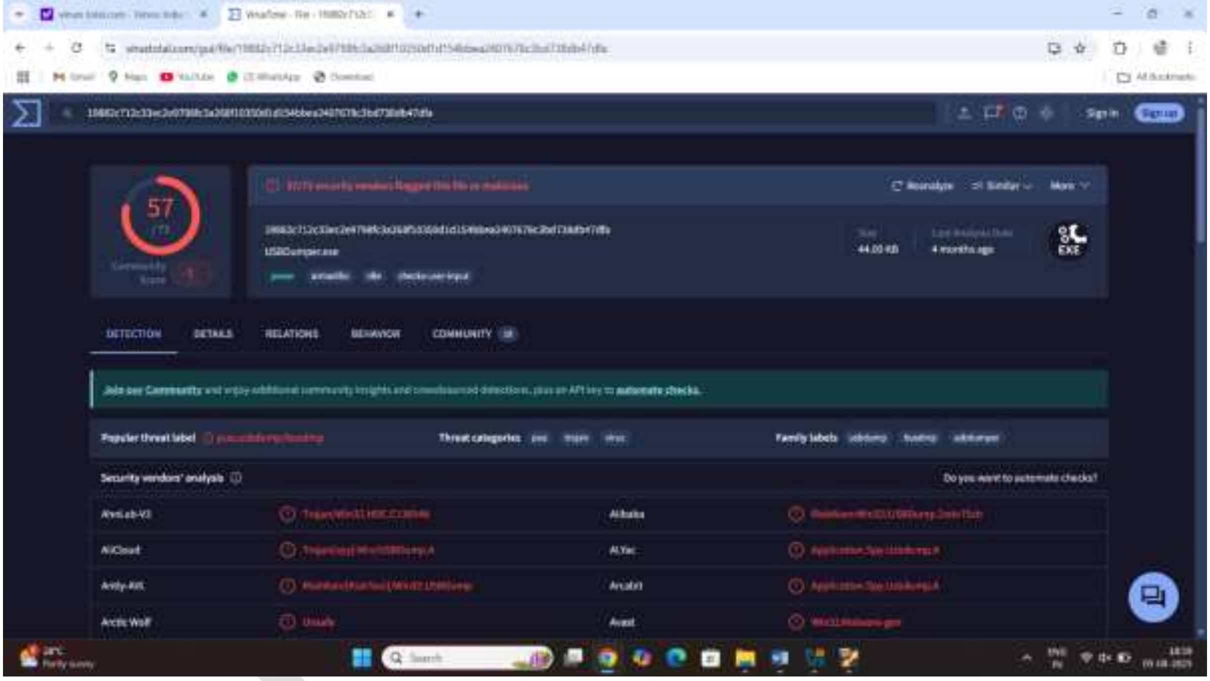
Step2 click on choose option



...nd URLs to detect malware and other ...m with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, or access your API key.



57/73 security vendors flagged this file as malicious

USBDumper.exe

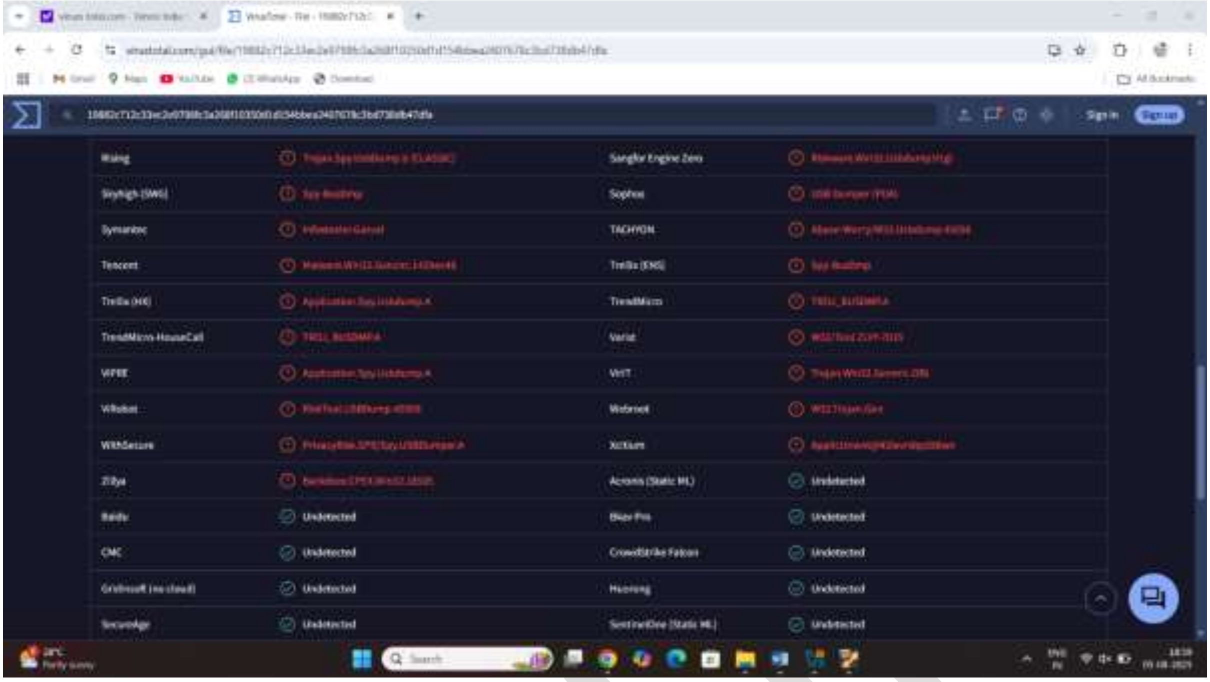
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label [illegible] Threat categories [illegible] Family labels [illegible]

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.HDC.C[illegible]	Alibaba	[illegible]
AliCloud	Trojan[illegible]:Win/USBDump.A	ALYac	Application.Spy.Usbdump.A
Antiy-AVL	[illegible]	Arcabit	Application.Spy.Usbdump.A
Arctic Wolf	Unsafe	Avast	Win32:Malware-gen

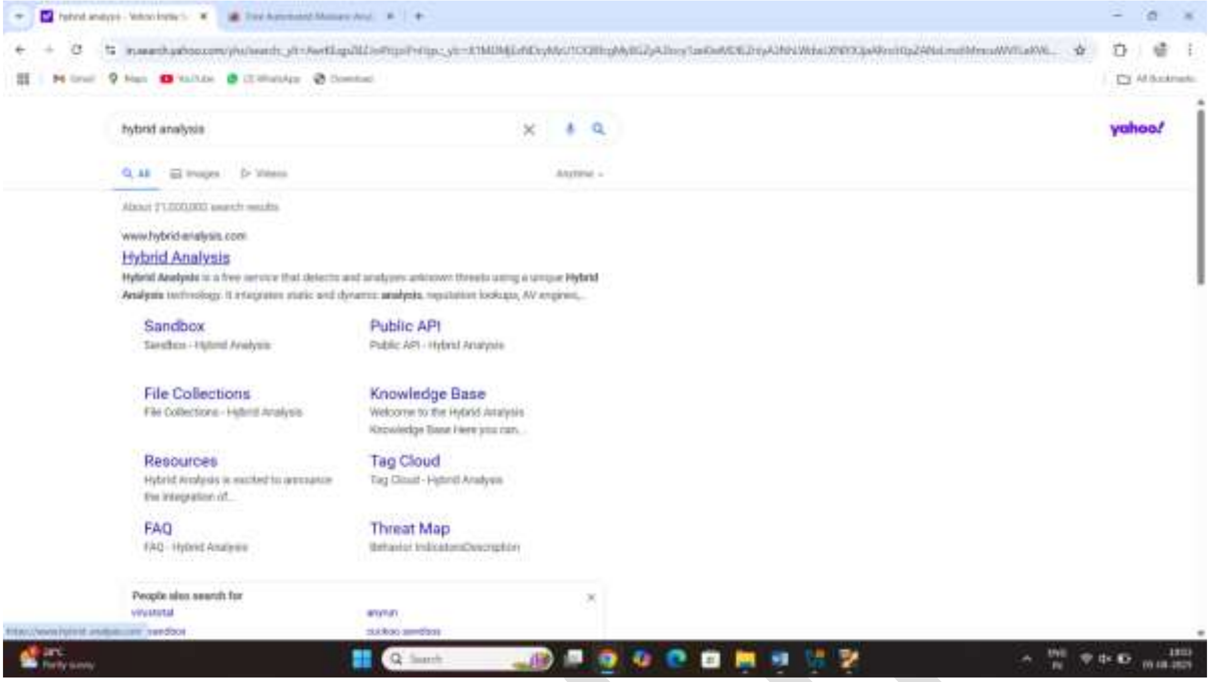


1068c712c33ec2e0798c3a268f10350d0d1546bea2407678c3bd738db47dfa

Rising	Trojan.Spy.UsbDump [illegible] (CLASSIC)	Sangfor Engine Zero	Malware.Win32.UsbDump.[illegible]
Skyhigh (SWG)	Spy-[illegible]	Sophos	USB Dumper (PUA)
Symantec	Infostealer.Gansol	TACHYON	Abuse-Worry/W32.UsbDump.[illegible]
Tencent	Malware.Win32.Gencirc.[illegible]	Trellix (ENS)	Spy-[illegible]
Trellix (HX)	Application.Spy.UsbDump.A	TrendMicro	TROJ_BUSDMP.A
TrendMicro-HouseCall	TROJ_BUSDMP.A	Varist	W32/Tool.ZGM-7015
VIPRE	Application.Spy.UsbDump.A	VirIT	Trojan.Win32.Generic.DBL
ViRobot	[illegible].USBDump.[illegible]	Webroot	W32.Trojan.Gen
WithSecure	PrivacyRisk.SPR/Spy.USBDumper.A	Xcitium	ApplicUnwnt@#[illegible]
Zillya	Backdoor.CPEX.Win32.[illegible]	Acronis (Static ML)	Undetected
Baidu	Undetected	Bkav Pro	Undetected
CMC	Undetected	CrowdStrike Falcon	Undetected
Gridinsoft (no cloud)	Undetected	Huorong	Undetected
SecureAge	Undetected	SentinelOne (Static ML)	Undetected

Lab6 examine a suspicious file using online resource using Haybrid analysis

Step1 open the google and type the hybrid analysis



hybrid analysis

All Images Videos Anytime

About 21,000,000 search results

www.hybrid-analysis.com

Hybrid Analysis

Hybrid Analysis is a free service that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology. It integrates static and dynamic **analysis**, reputation lookups, AV engines,...

Sandbox
Sandbox - Hybrid Analysis

Public API
Public API - Hybrid Analysis

File Collections
File Collections - Hybrid Analysis

Knowledge Base
Welcome to the Hybrid Analysis Knowledge Base Here you can...

Resources
Hybrid Analysis is excited to announce the integration of...

Tag Cloud
Tag Cloud - Hybrid Analysis

FAQ
FAQ - Hybrid Analysis

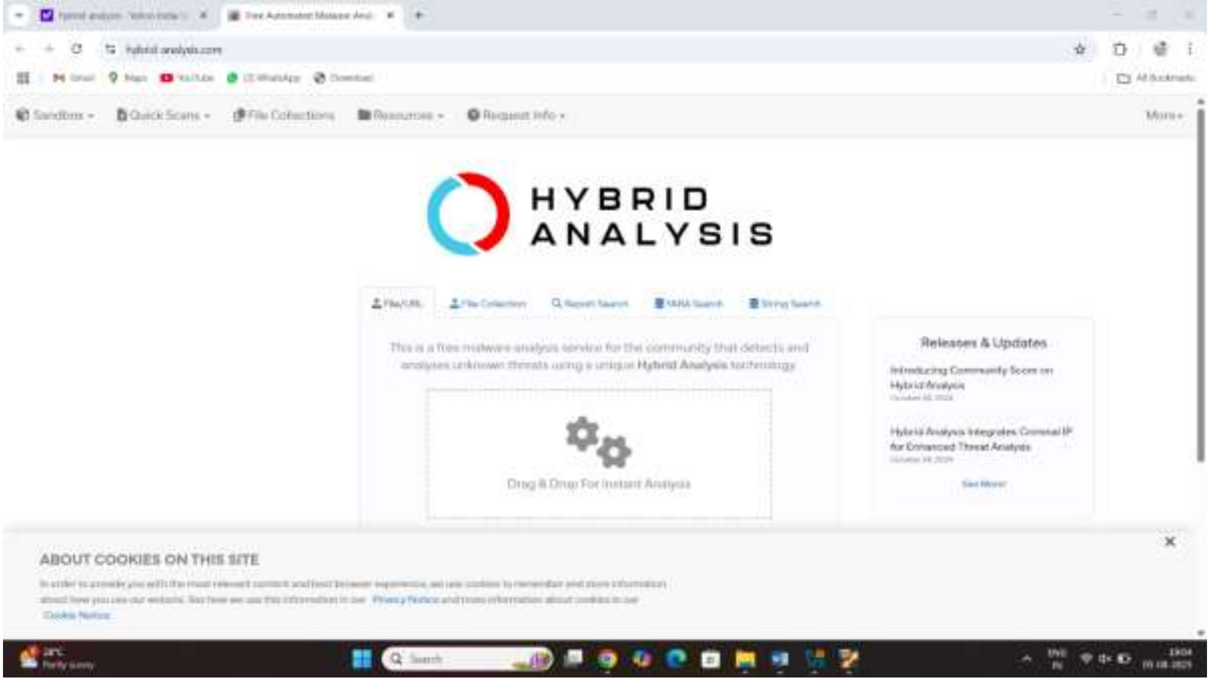
Threat Map
Behavior IndicatorsDescription

People also search for

virustotal anyrun

sandbox cuckoo sandbox

Step2 click on the link and open them



hybrid-analysis.com

Sandbox Quick Scans File Collections Resources Request Info More

HYBRID ANALYSIS

File/URL File Collection Report Search YARA Search String Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

Drag & Drop For Instant Analysis

Releases & Updates

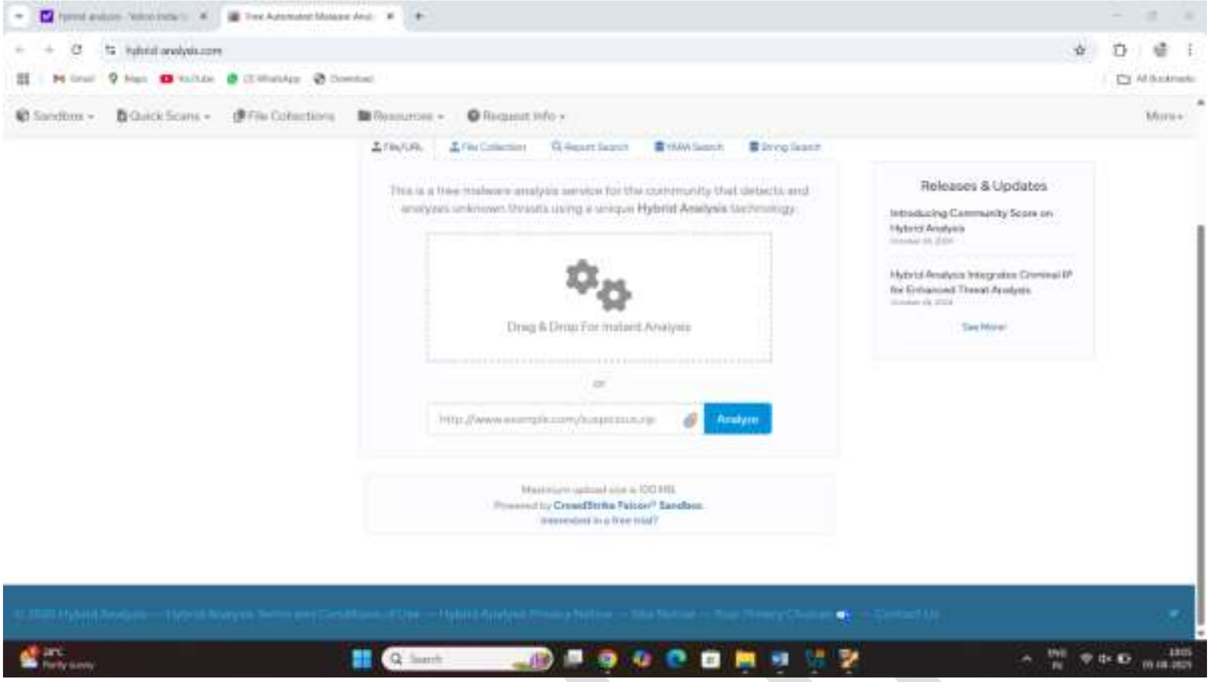
Introducing Community Score on Hybrid Analysis

Hybrid Analysis Integrates Criminal IP for Enhanced Threat Analysis

See More

ABOUT COOKIES ON THIS SITE

In order to provide you with the most relevant content and best browser experience, we use cookies to remember and store information about how you use our website. See how we use this information in our Privacy Notice and more information about cookies in our Cookie Notice.



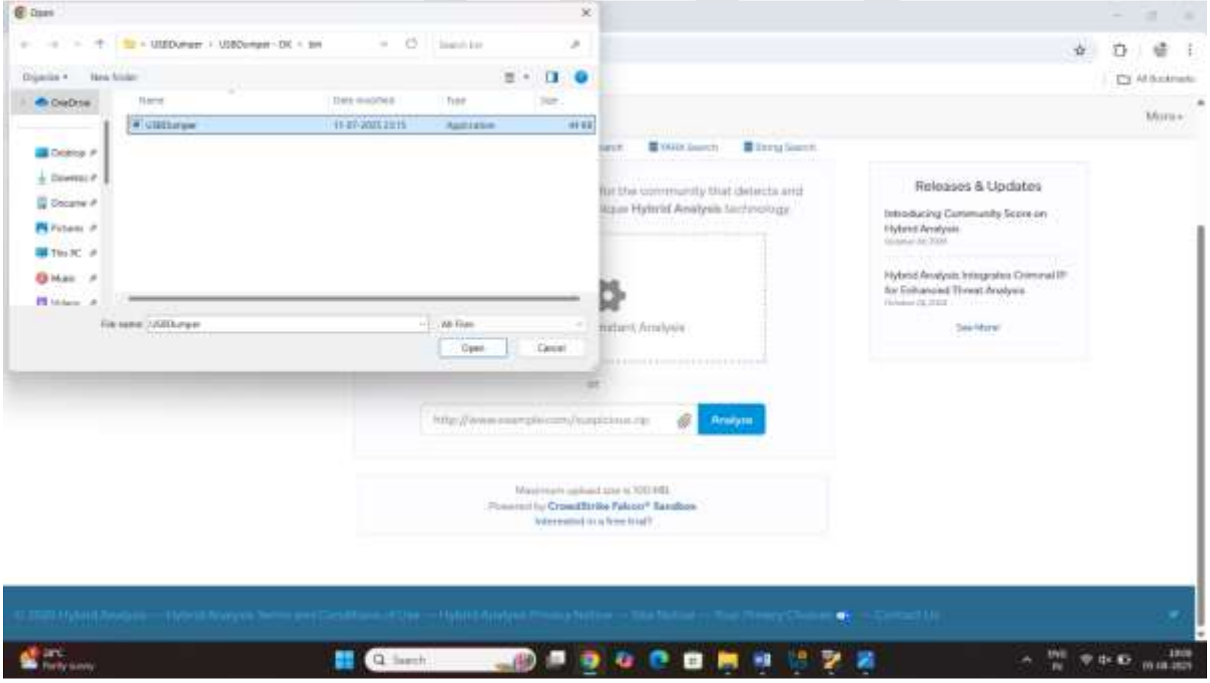
This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.

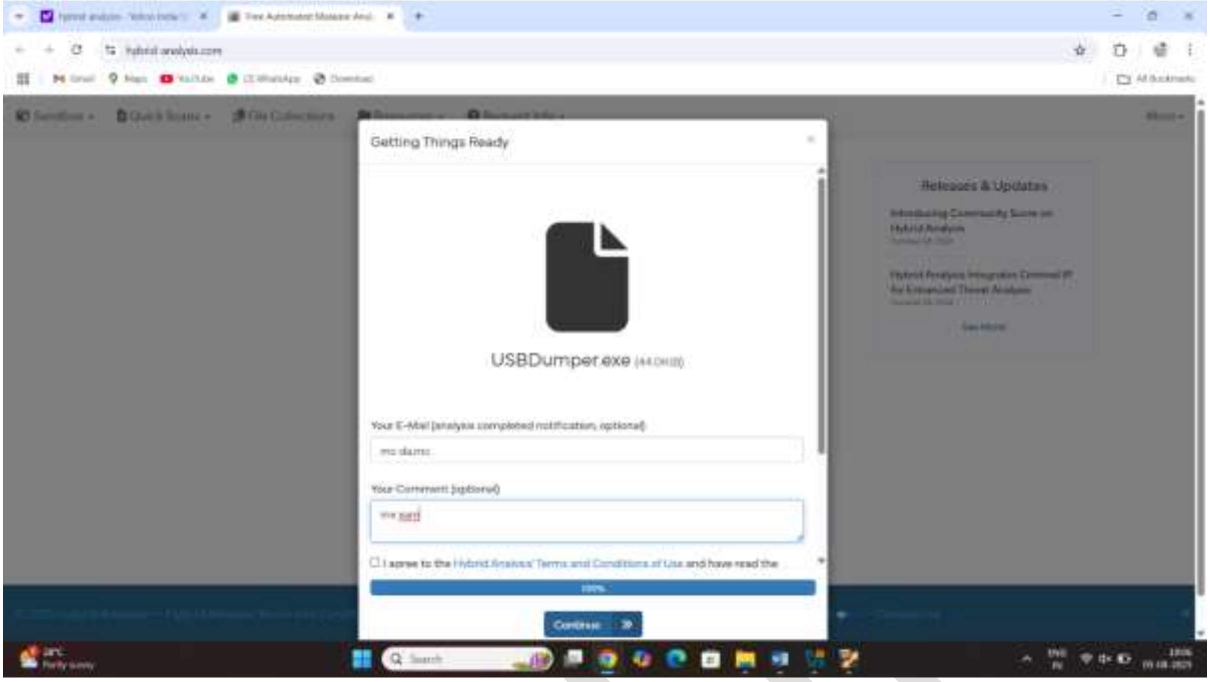
Introducing Community Score on Hybrid Analysis

Hybrid Analysis Integrates Criminal IP for Enhanced Threat Analysis

Maximum upload size is 100 MiB.
Powered by CrowdStrike Falcon® Sandbox.
Interested in a free trial?

Step3 click on the analysis option





Getting Things Ready

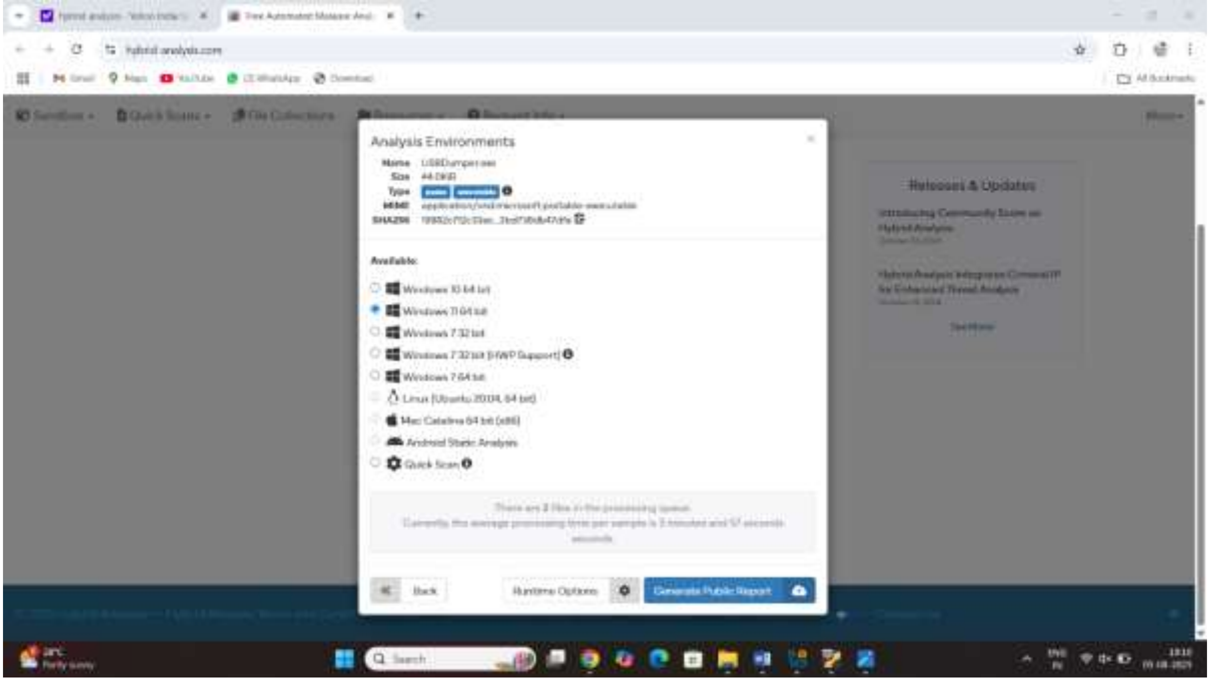
USBDumper.exe

Your E-Mail (analysis completed notification, optional)

Your Comment (optional)

□ I agree to the Hybrid Analysis' Terms and Conditions of Use and have read the

Step4 enter the email and apply the term and condition



Analysis Environments

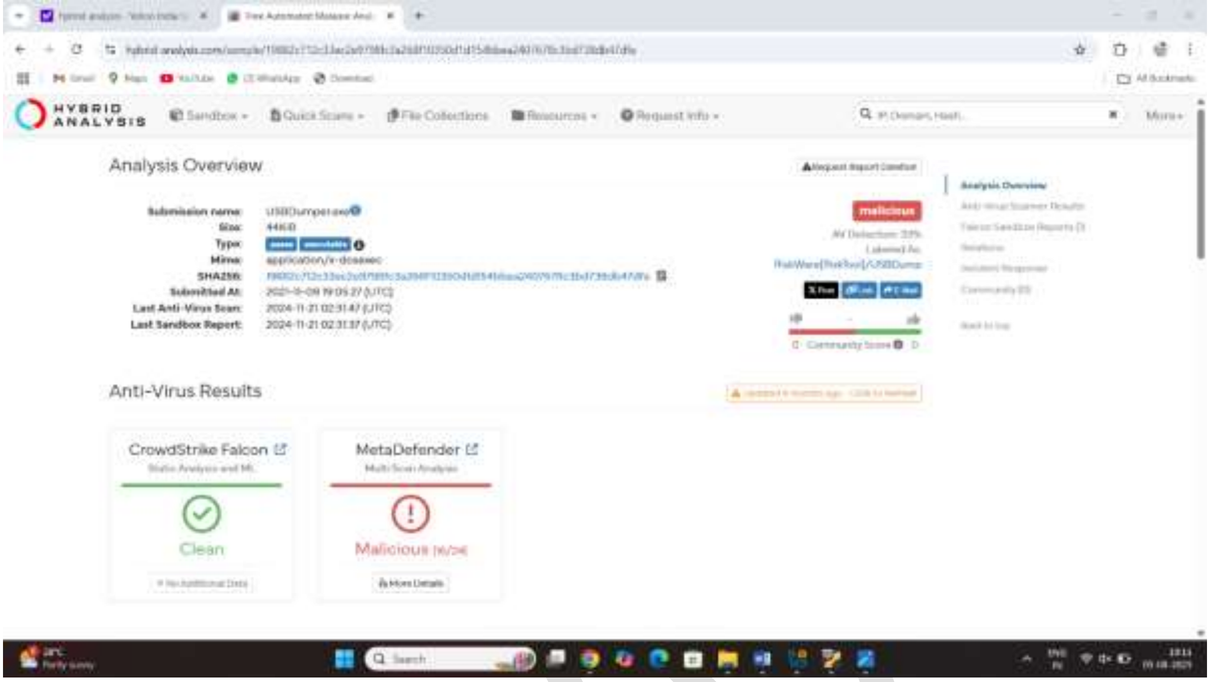
Name USBDumper.exe
Size 44.0KiB
Type
MIME application/vnd.microsoft.portable-executable

Available:

○ Windows 10 64 bit
● Windows 11 64 bit
○ Windows 7 32 bit
○ Windows 7 32 bit (HWP Support)
○ Windows 7 64 bit
○ Linux (Ubuntu 20.04, 64 bit)
○ Mac Catalina 64 bit (x86)
○ Android Static Analysis
○ Quick Scan

Step5 clcik on the generate public report option

Result:



Analysis Overview

Submission name: USBDumper.exe
Size: 446KiB
Mime: application/x-dosexec
SHA256: [illegible]
Submitted At: 2021-11-09 19:05:27 (UTC)
Last Anti-Virus Scan: 2024-11-21 02:31:47 (UTC)
Last Sandbox Report: 2024-11-21 02:31:37 (UTC)

malicious

Anti-Virus Results

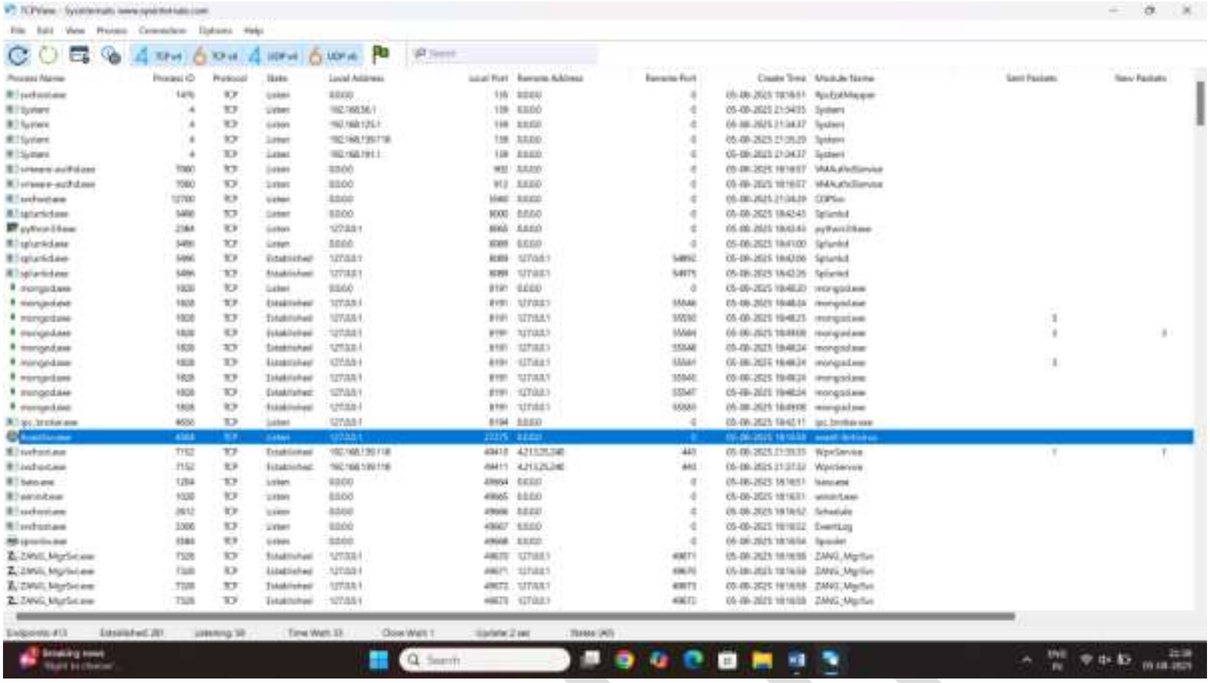
CrowdStrike Falcon — Clean

MetaDefender — Malicious

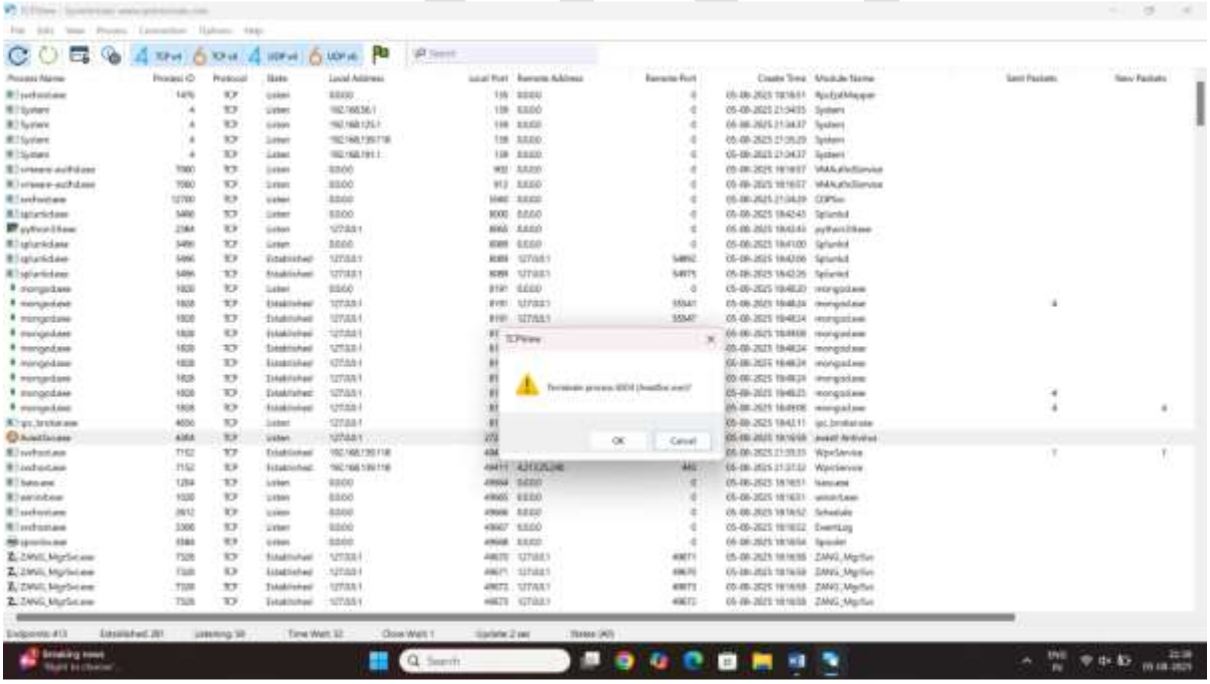
Lab8 emote malware analysis using TCP view

Dynamic malware analysis

Step1 start the TCP view program

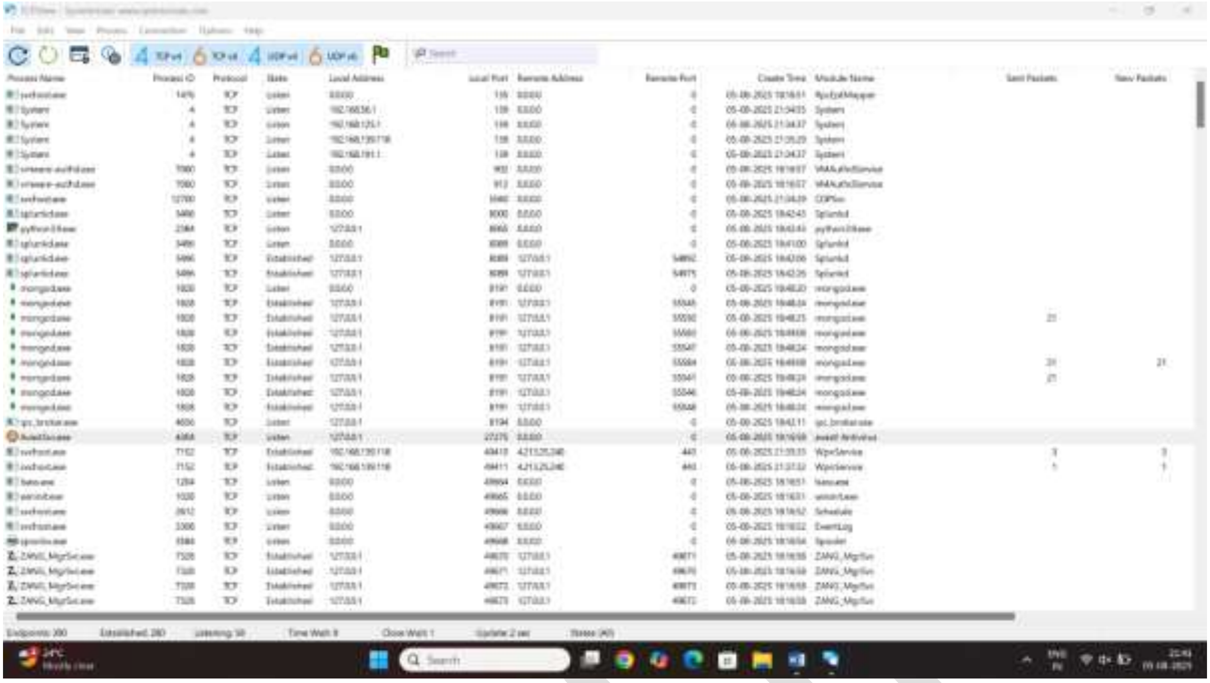


Step2 select the program to block program



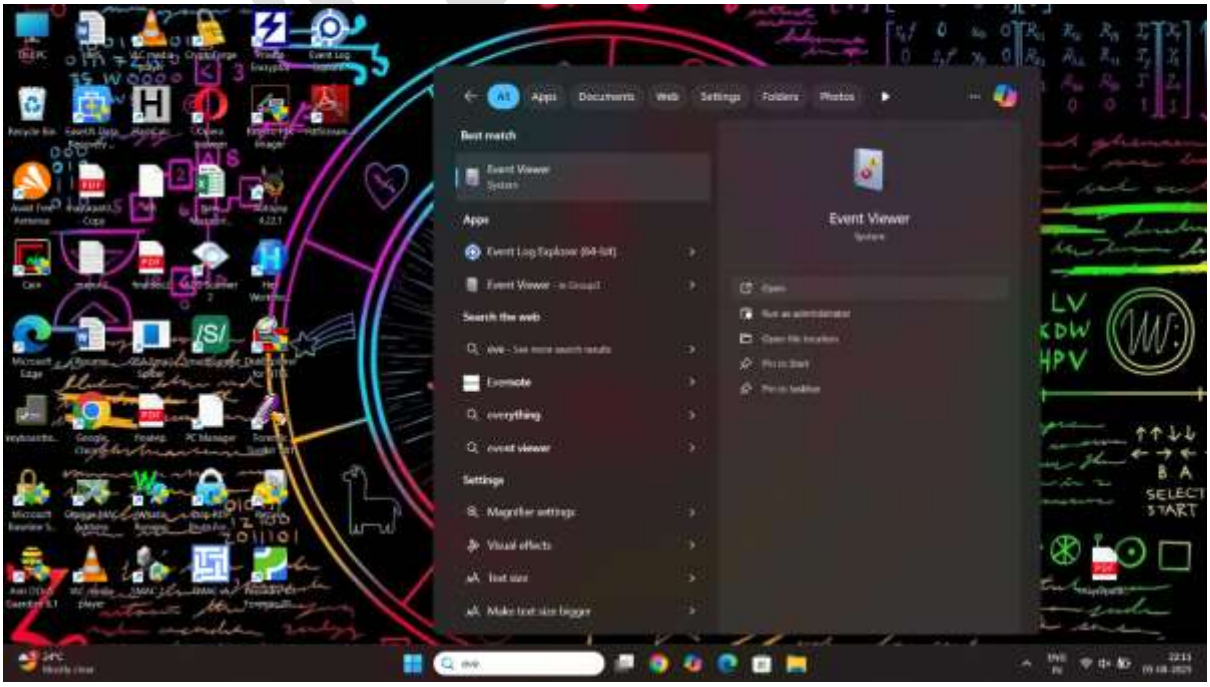
Click on ok

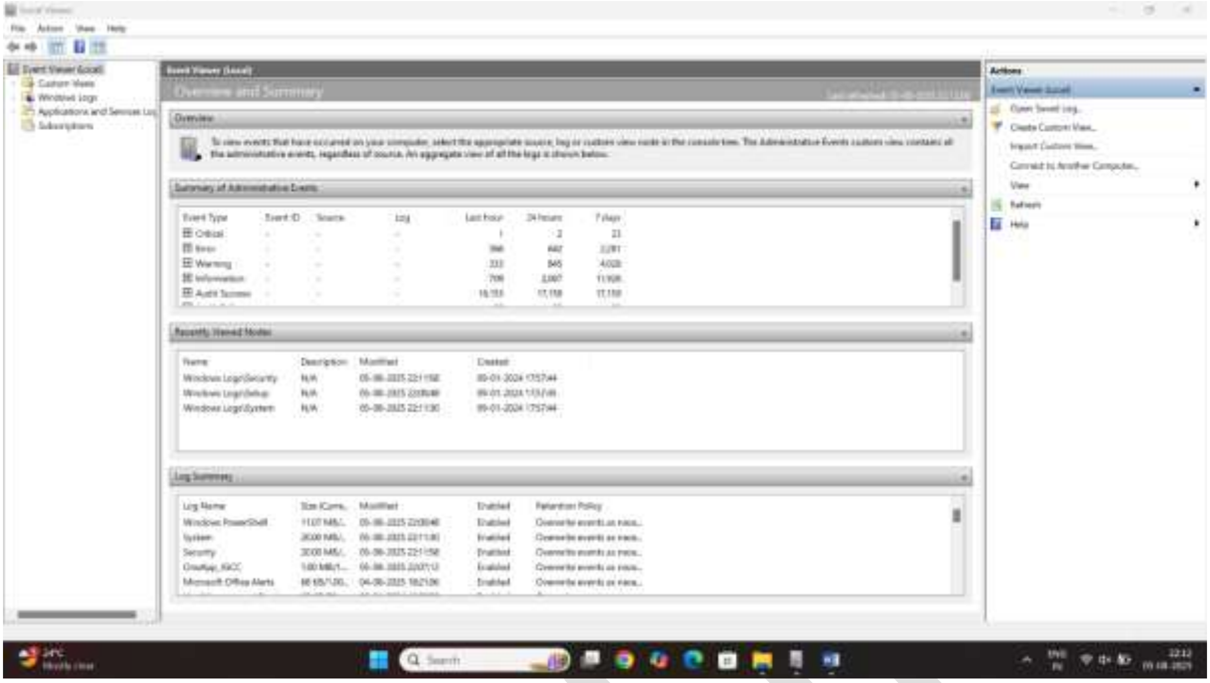
Result:



Lab8 examine windows event logs

Step1 start the windows machine search the event program on windows





Overview

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.

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	1	2	23
Error	-	-	-	366	442	2,281
Warning	-	-	-	333	845	4,028
Information	-	-	-	709	2,007	11,926
Audit Success	-	-	-	16,153	17,158	17,158

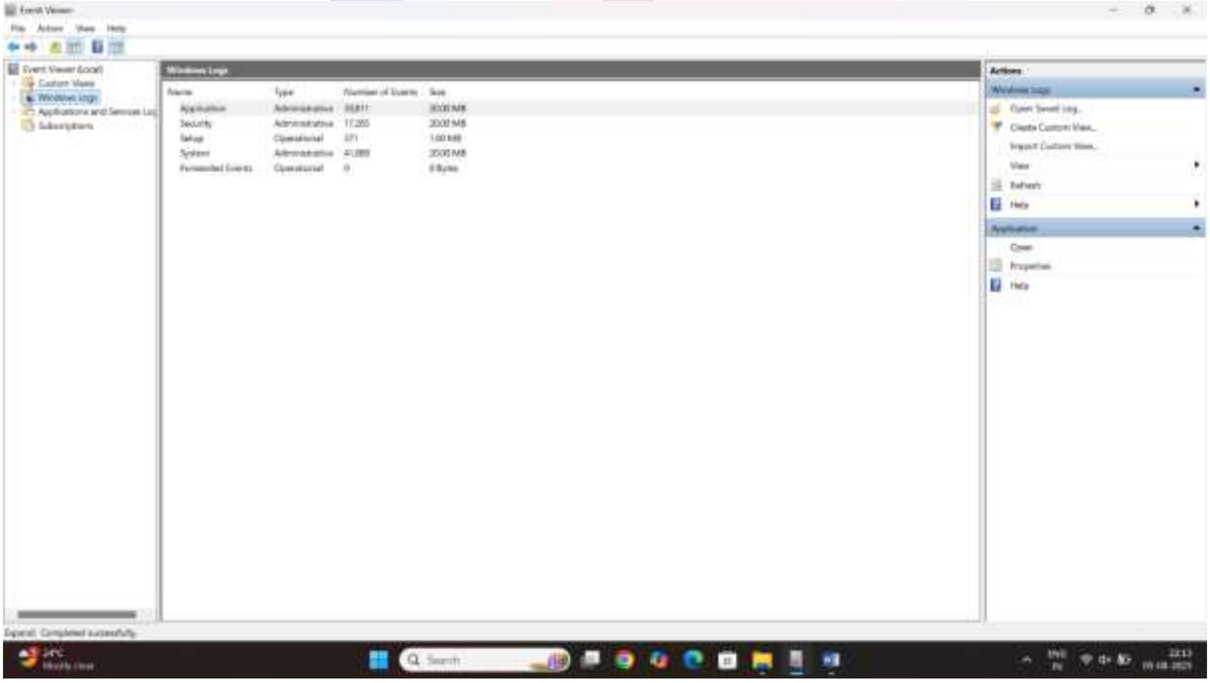
Recently Viewed Nodes

Name	Description	Modified	Created
Windows Logs\Security	N/A	05-08-2025 22:11:58	09-01-2024 17:57:44
Windows Logs\Setup	N/A	05-08-2025 22:08:48	09-01-2024 17:57:48
Windows Logs\System	N/A	05-08-2025 22:11:30	09-01-2024 17:57:44

Log Summary

Log Name	Size (Curre...	Modified	Enabled	Retention Policy
Windows PowerShell	11.07 MB/...	05-08-2025 22:08:48	Enabled	Overwrite events as nece...
System	20.00 MB/...	05-08-2025 22:11:30	Enabled	Overwrite events as nece...
Security	20.00 MB/...	05-08-2025 22:11:58	Enabled	Overwrite events as nece...
OneApp_IGCC	1.00 MB/1...	05-08-2025 22:07:12	Enabled	Overwrite events as nece...
Microsoft Office Alerts	68 KB/1.00...	04-08-2025 18:21:06	Enabled	Overwrite events as nece...

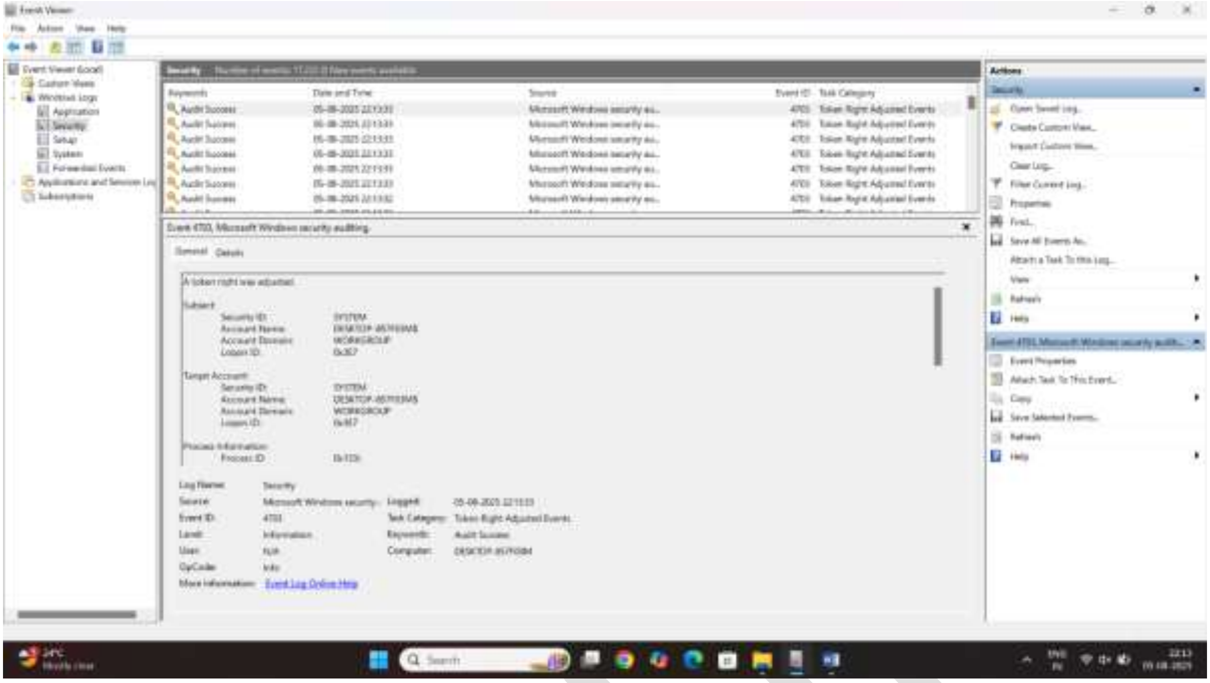
Step2 click on windows log



Name	Type	Number of Events	Size
Application	Administrative	35,811	20.00 MB
Security	Administrative	17,265	20.00 MB
Setup	Operational	371	1.00 MB
System	Administrative	41,089	20.00 MB
Forwarded Events	Operational	0	0 Bytes

Expand: Completed successfully.

Step3 click on the security option

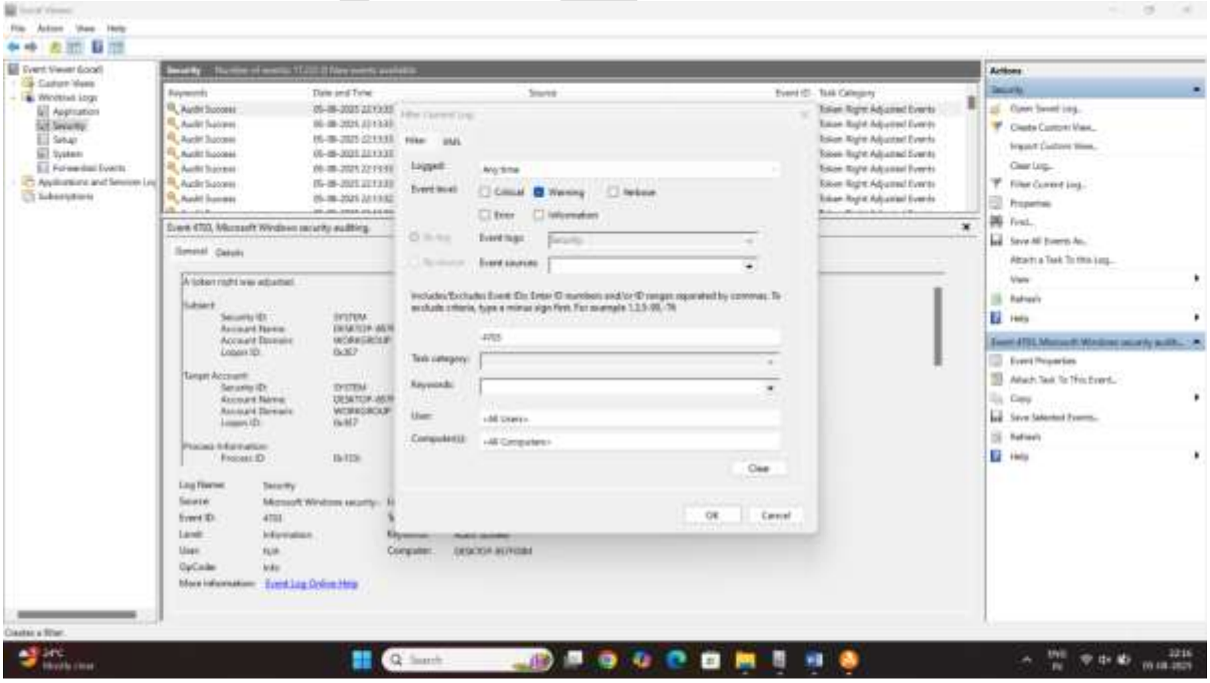


Event 4703, Microsoft Windows security auditing.

A token right was adjusted.

```
Subject:
        Security ID:        SYSTEM
        Account Name:       DESKTOP-8S7F0M$
        Account Domain:     WORKGROUP
        Logon ID:           0x3E7

Target Account:
        Security ID:        SYSTEM
        Account Name:       DESKTOP-8S7F0M$
        Account Domain:     WORKGROUP
        Logon ID:           0x3E7

Process Information:
        Process ID:         0x1134

Log Name:          Security
Source:            Microsoft Windows security   Logged:         05-08-2025 22:13:33
Event ID:          4703                         Task Category:  Token Right Adjusted Events
Level:             Information                  Keywords:       Audit Success
User:              N/A                          Computer:       DESKTOP-8S7F0M
OpCode:            Info
More Information:  Event Log Online Help
```

Step4 check the event id and apply the filter option

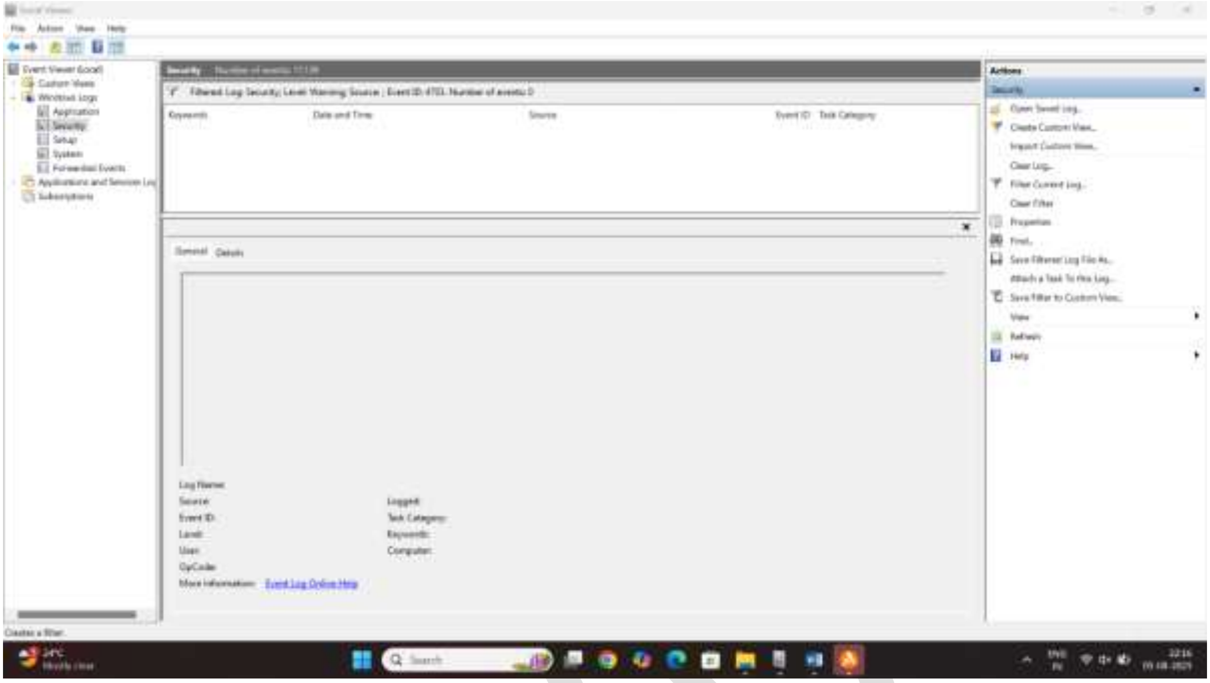


Filter Current Log

```
Logged:        Any time
Event level:   ☐ Critical  ☑ Warning  ☐ Verbose
               ☐ Error     ☐ Information
Event logs:    Security
Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To
exclude criteria, type a minus sign first. For example 1,3,5-99,-76

               4703
Task category:
Keywords:
User:          <All Users>
Computer(s):   <All Computers>
```

Step5 type the event id and click on next

Result:



Security Number of events: 17,139

Filtered: Log: Security; Level: Warning; Source: ; Event ID: 4703. Number of events: 0

Keywords | Date and Time | Source | Event ID | Task Category

Log Name:
Source: Logged:
Event ID: Task Category:
Level: Keywords:
User: Computer:
OpCode:
More Information: Event Log Online Help

Creates a filter.