School of Computer Science

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN, UTTARAKHAND

Digital Forensics Lab File

5th Semester

Submitted by:

Khushi Wadhawan
Sap ID: 500093673
Btech CSE CSF
Batch: 2

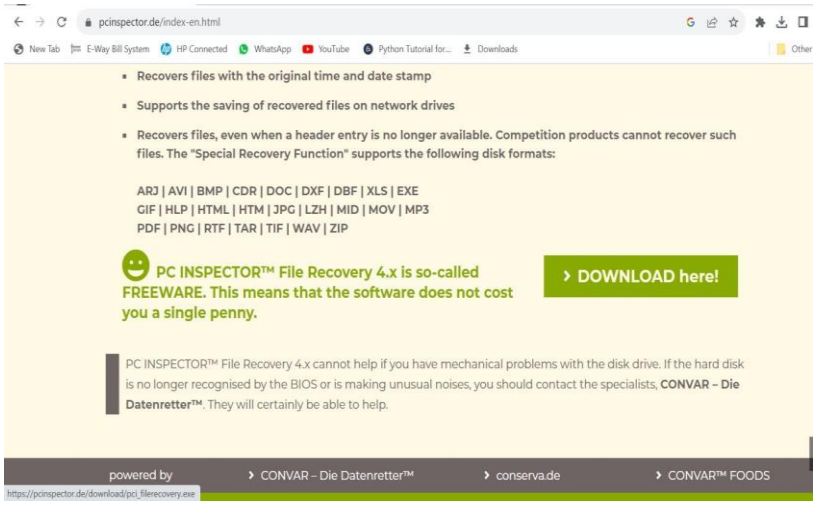
Submitted to:

Dr. Deepika Koundal

EXPERIMENT 1

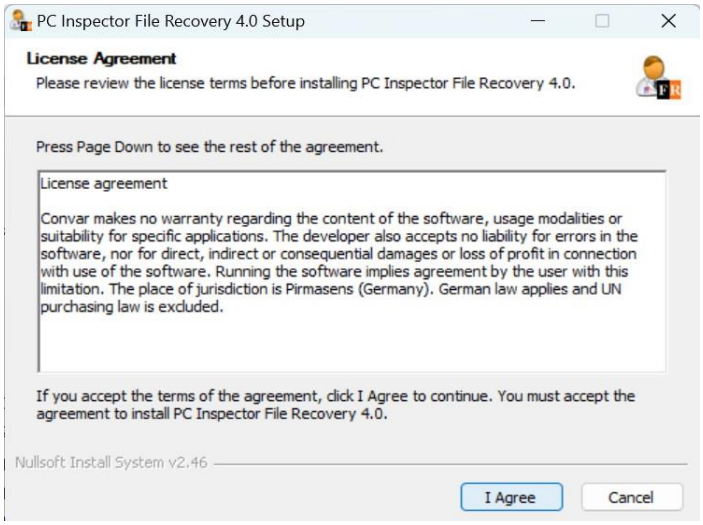
Lab Objective: Data Recovery using PC Inspector and other data recovery tools

Go to pcinspector.de site and install pc inspector

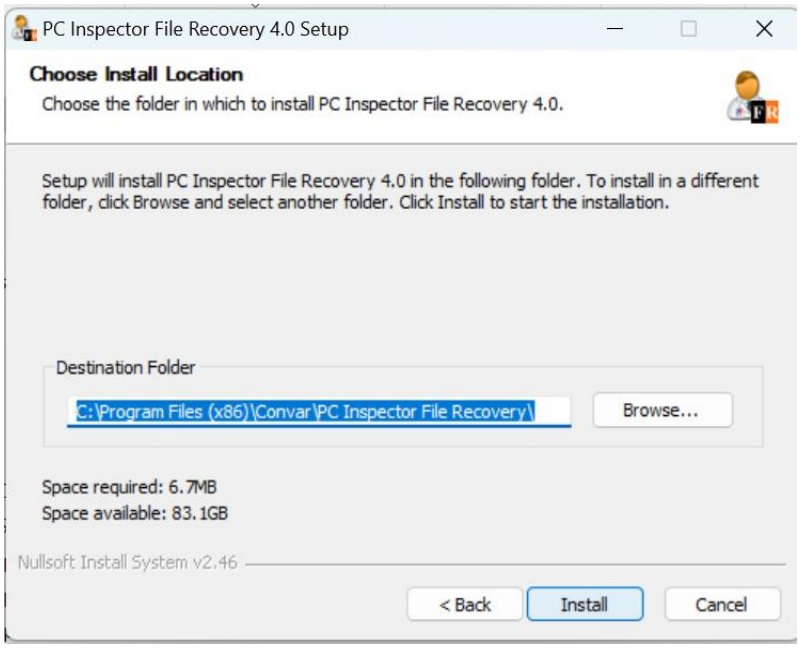


Choose the preferred language

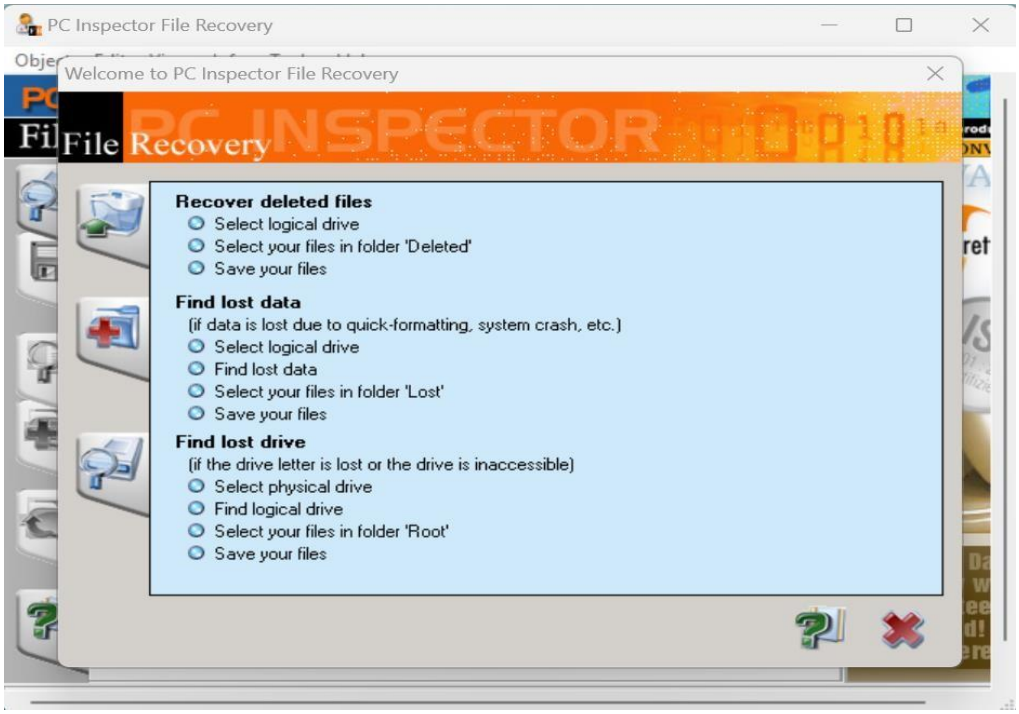
Accept terms and conditions and click on “I Agree”



Choose the location at which we want to install pc inspector

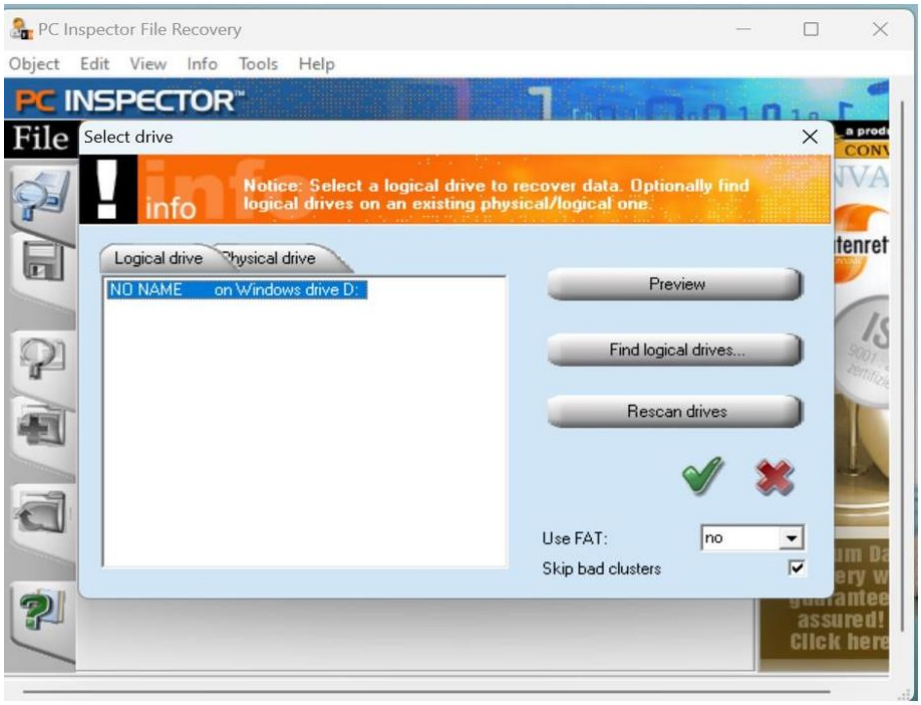


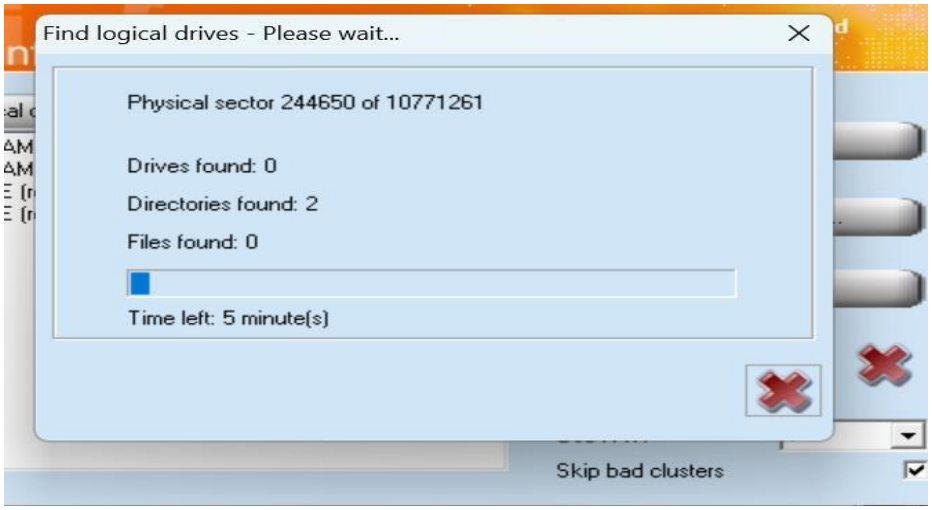
Click on select logical drive



Select your pen drive that will be used to perform the experiment

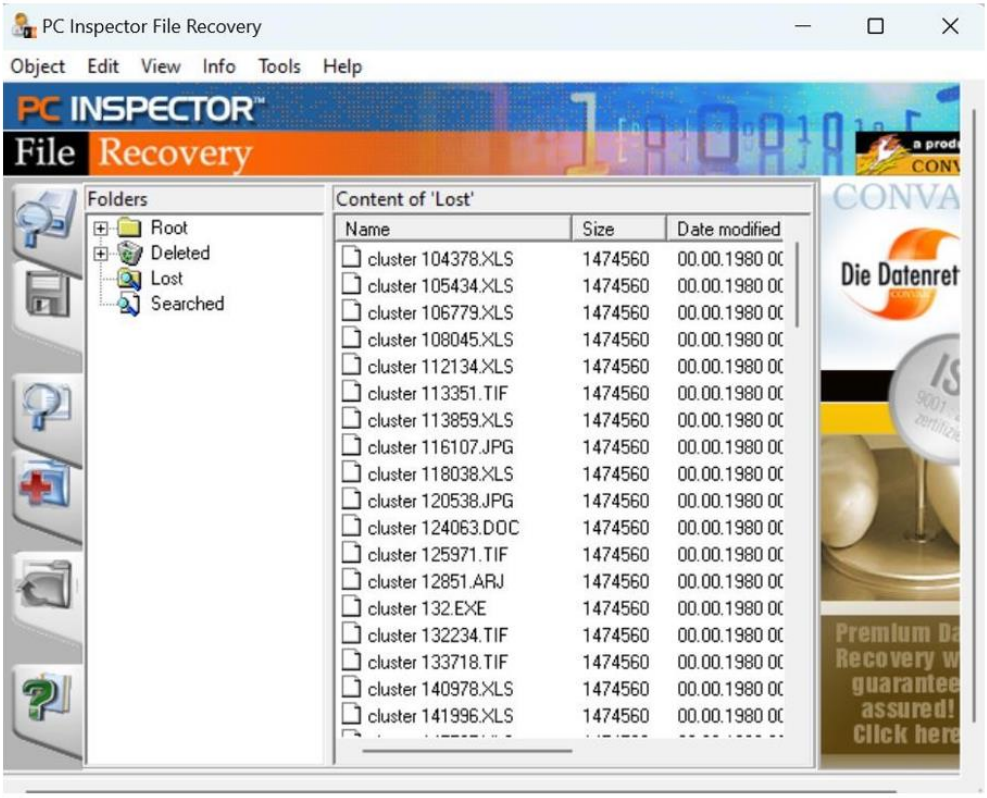
Click on find logical drives





•

Recovered files will be displayed

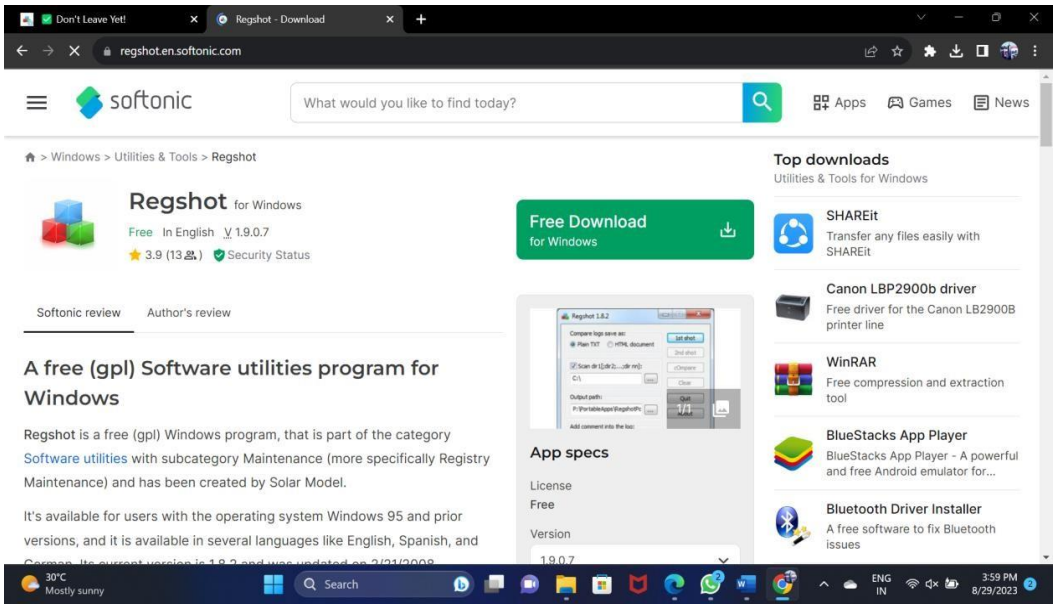


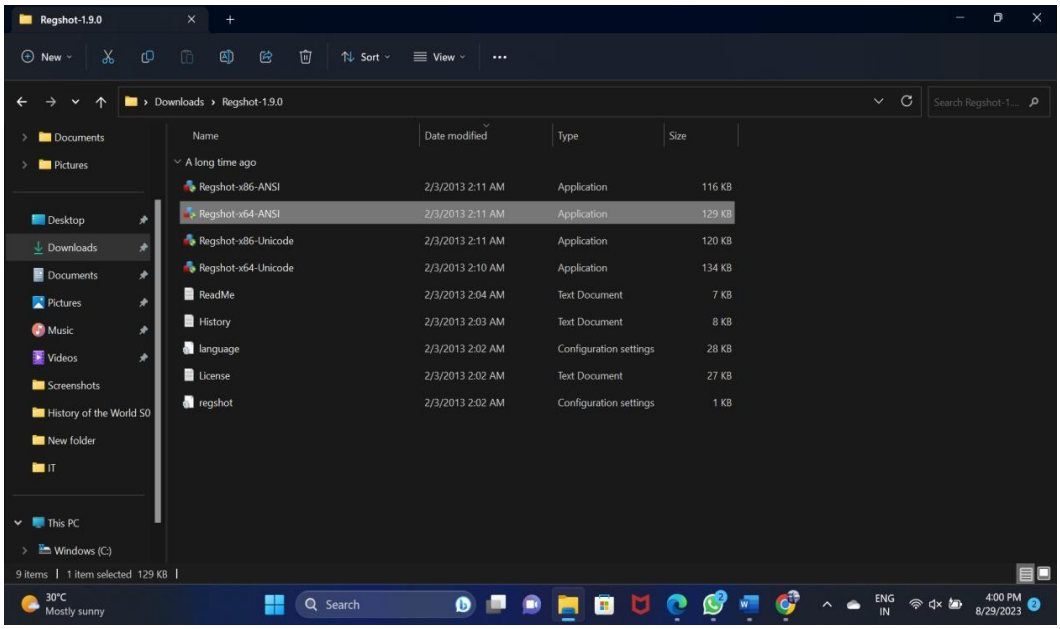
EXPERIMENT 2

Lab Objective: Identifying changes in registry files using Regshot

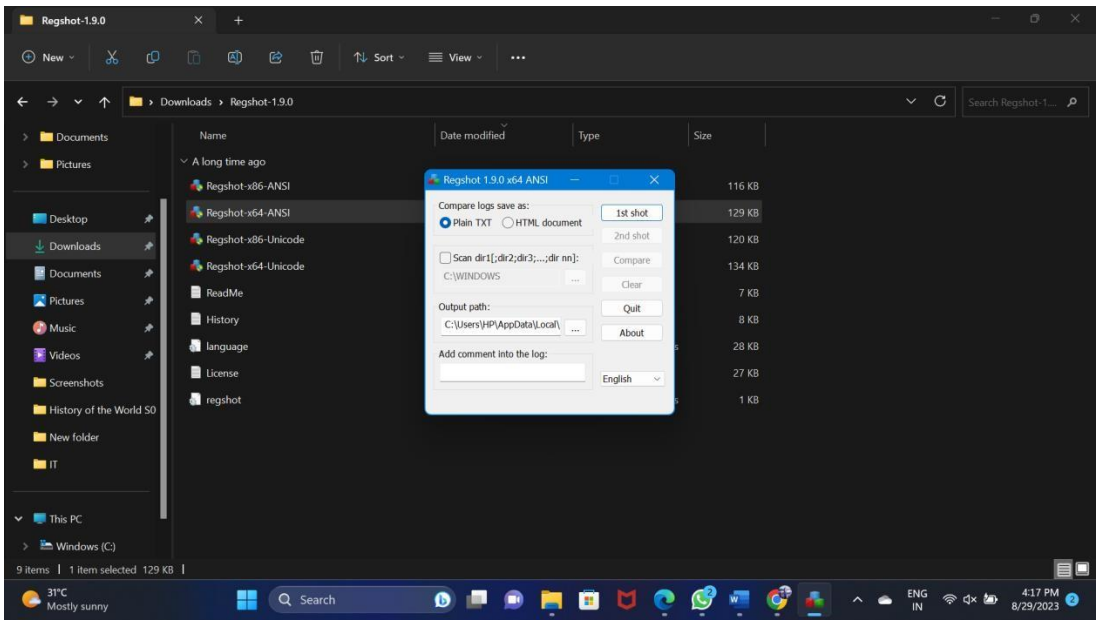
STEPS:

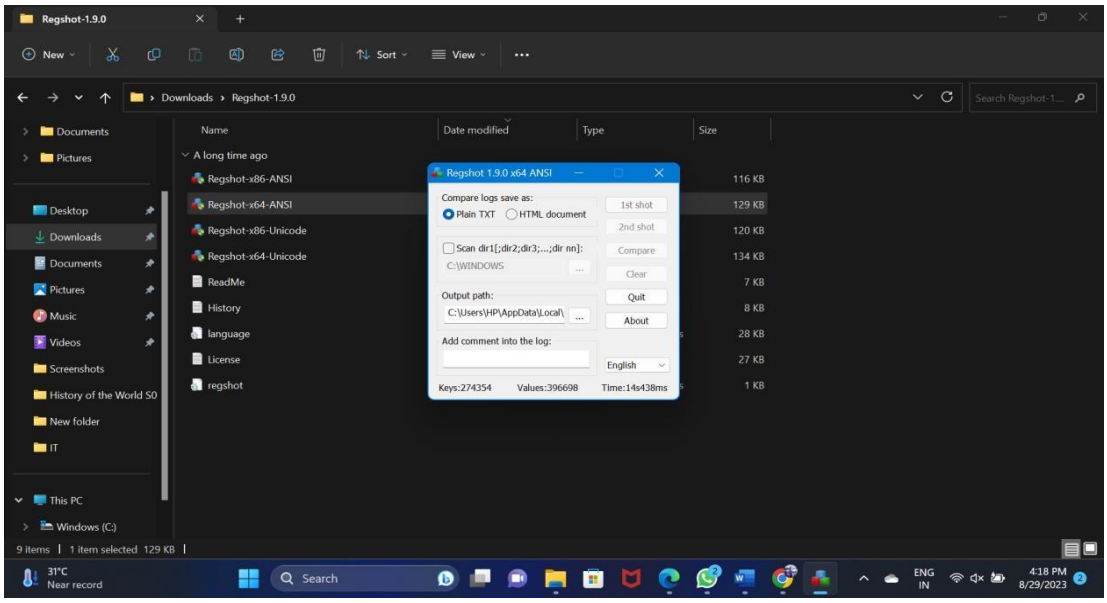
1. Download Regshot from https://regshot.en.softonic.com/

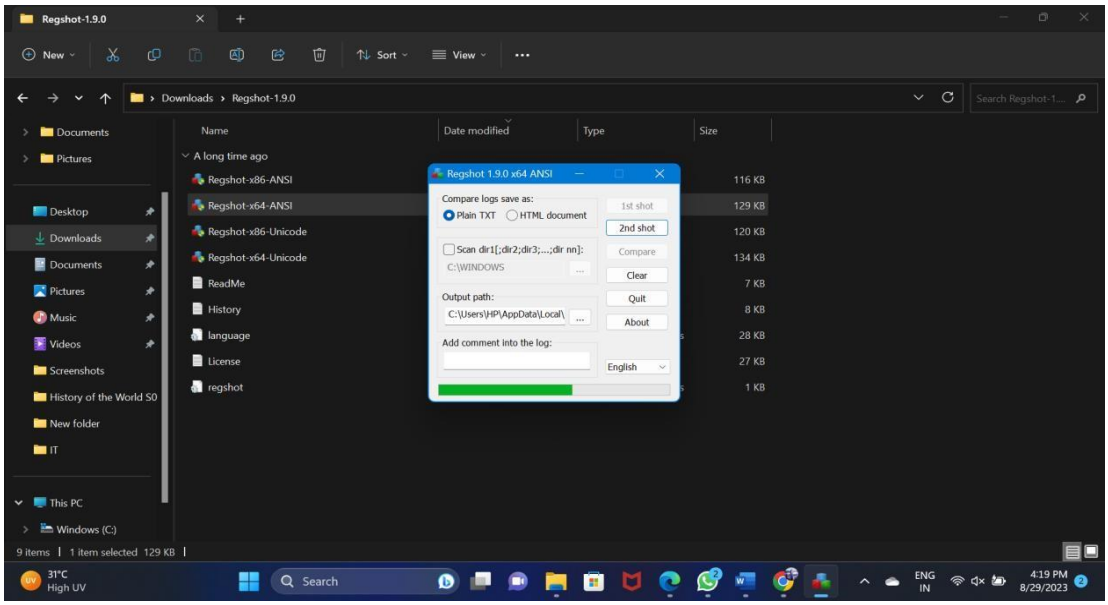




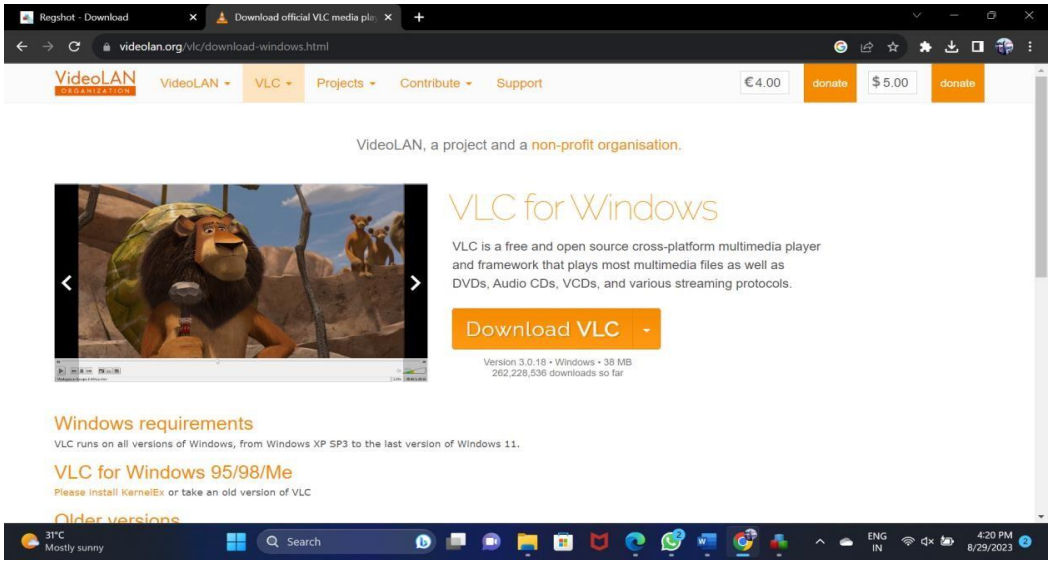
2. Running ANSI executable file from Regshot and taking the 1st shot

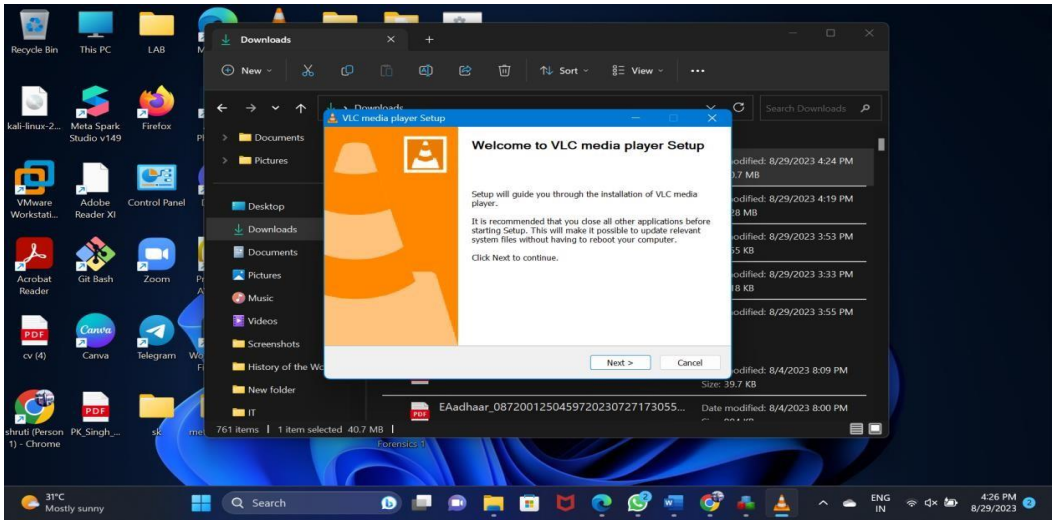


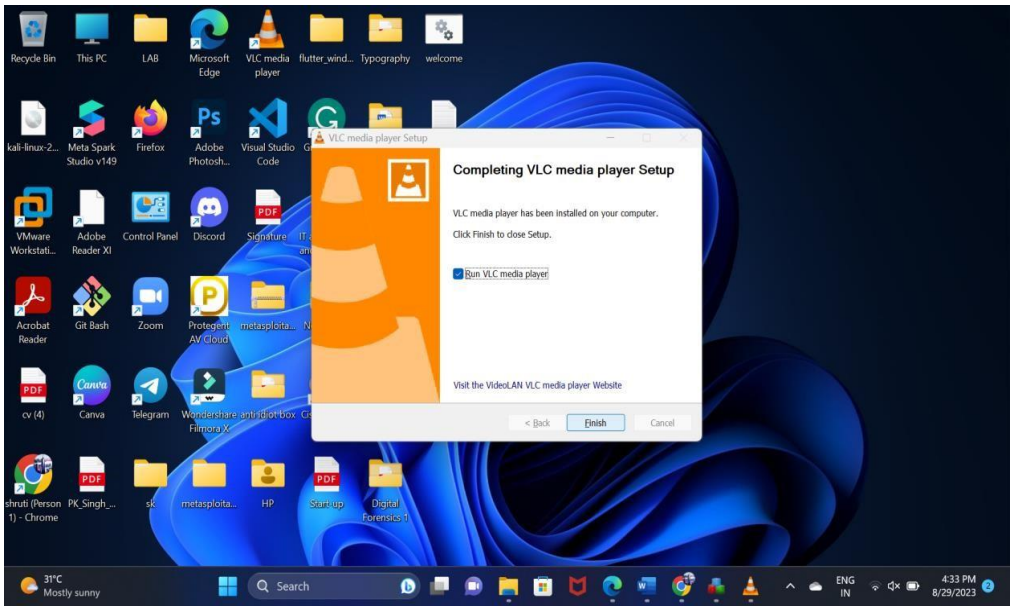




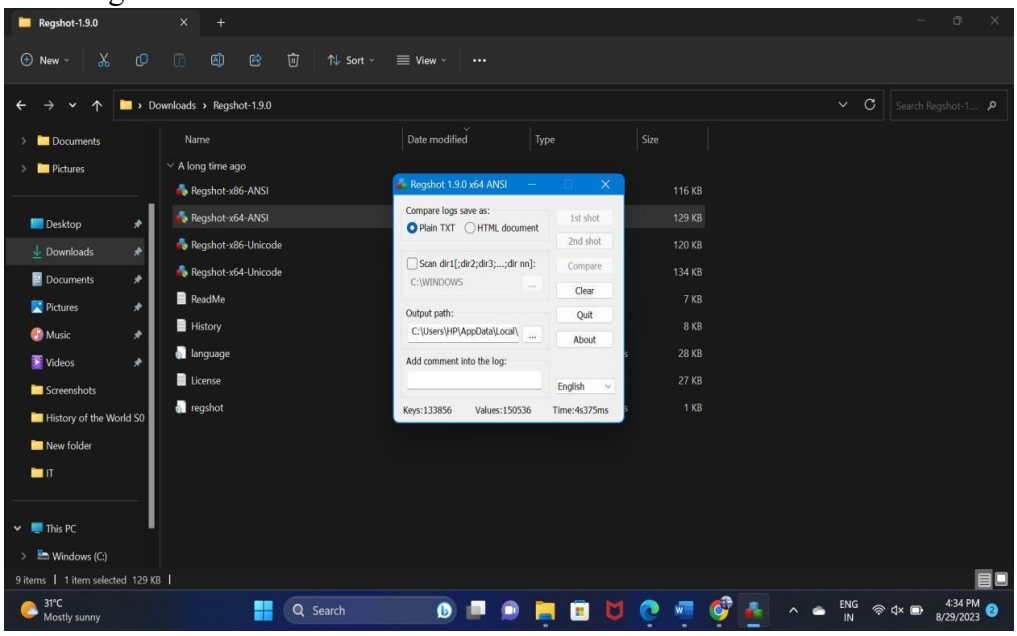
3. Installing VLC to change registry files

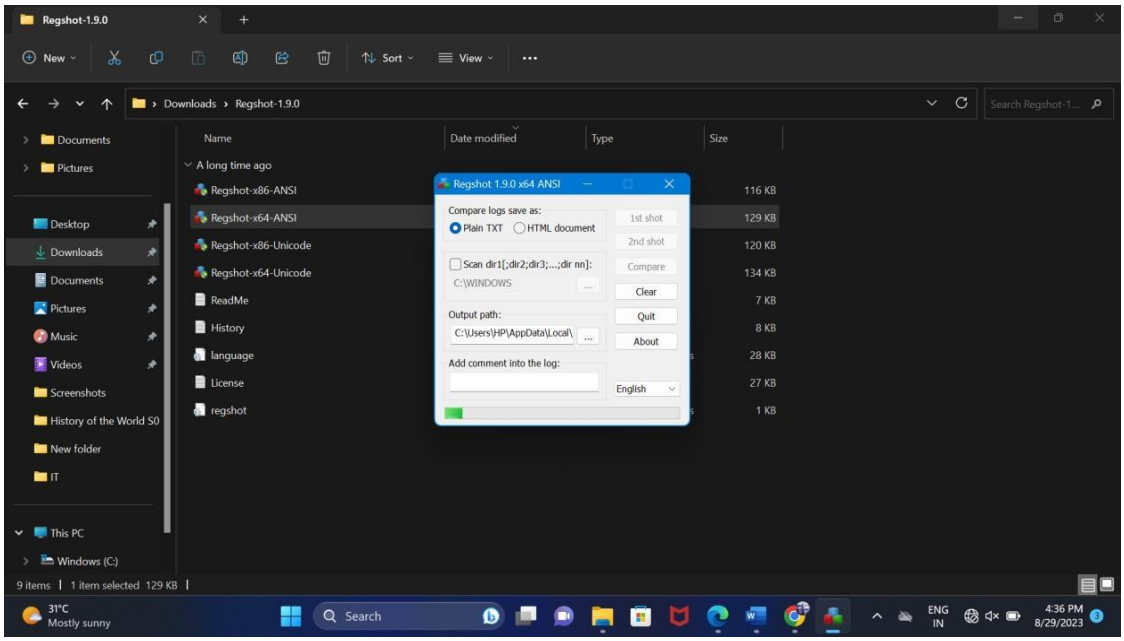




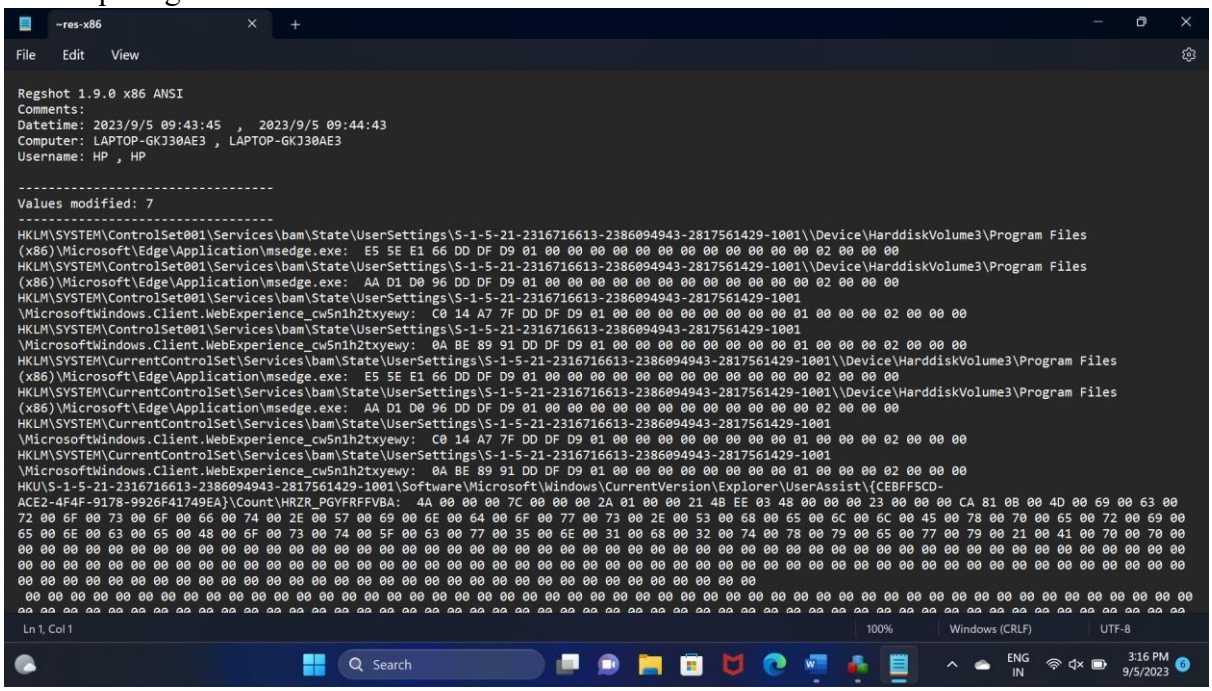


4. Taking the 2nd shot





5. Comparing the two shots



CONCLUSION: Through this experiment, I learnt about the tool REGSHOT, which can be used to identify changes in registry files. This can determine what kind of activities and changes are performed on the system and whether they can be harmful.

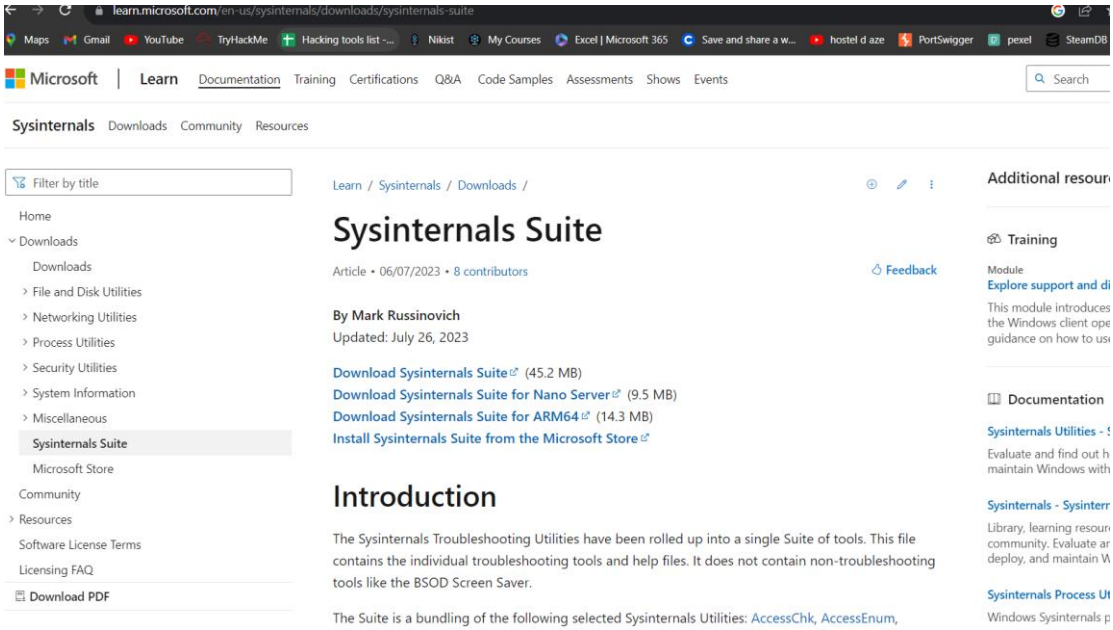
•

EXPERIMENT 3

Lab objective: Sysinternals tool kits to diagnosis, monitoring or analysis of windows machine.

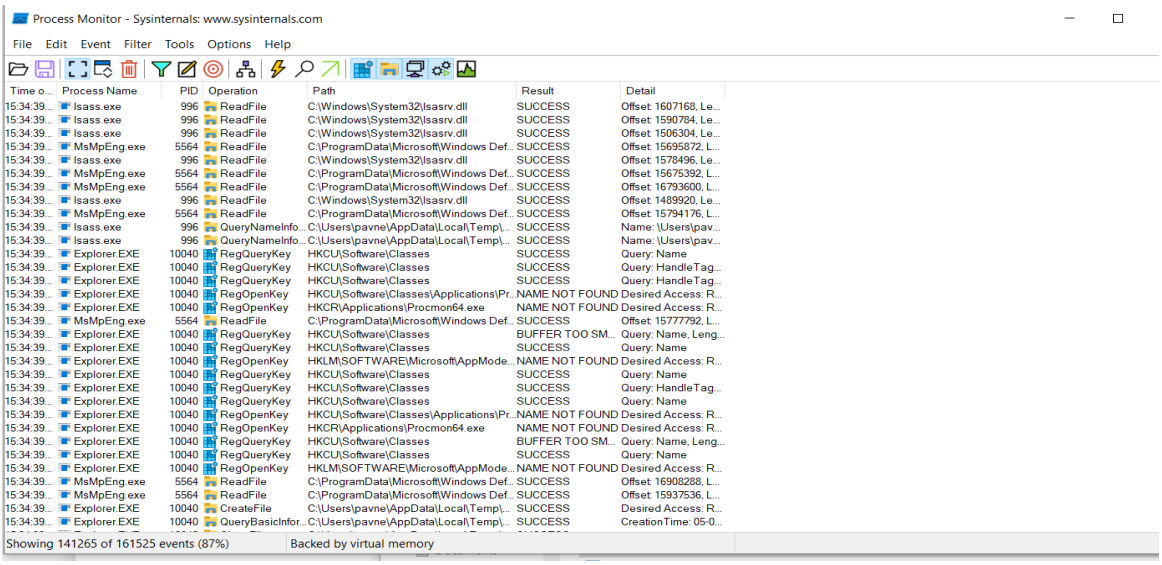
Sysinternals tool kits to diagnosis, monitoring or analysis of windows machine.

Install Sysinternals



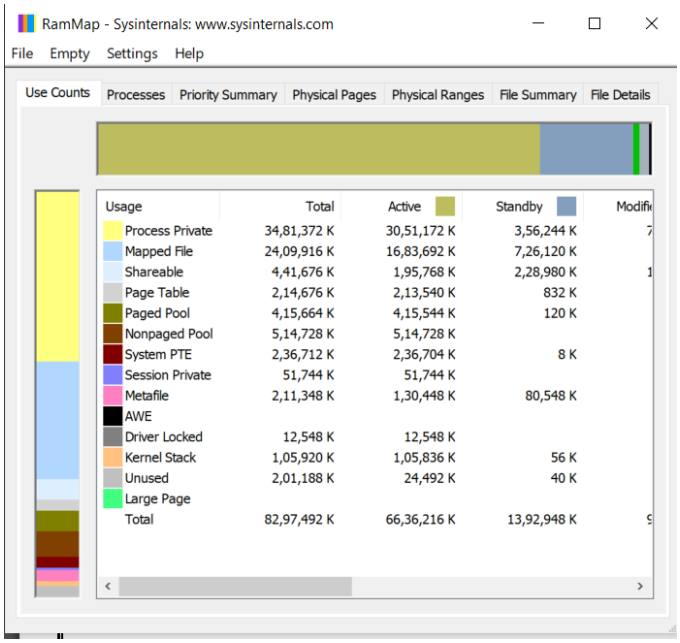
Exploring Procmon

Procmon is a downloadable utility for Microsoft Windows OS that captures and displays system and network activity. This includes file system activity, registry key activity, network, and threat activities.

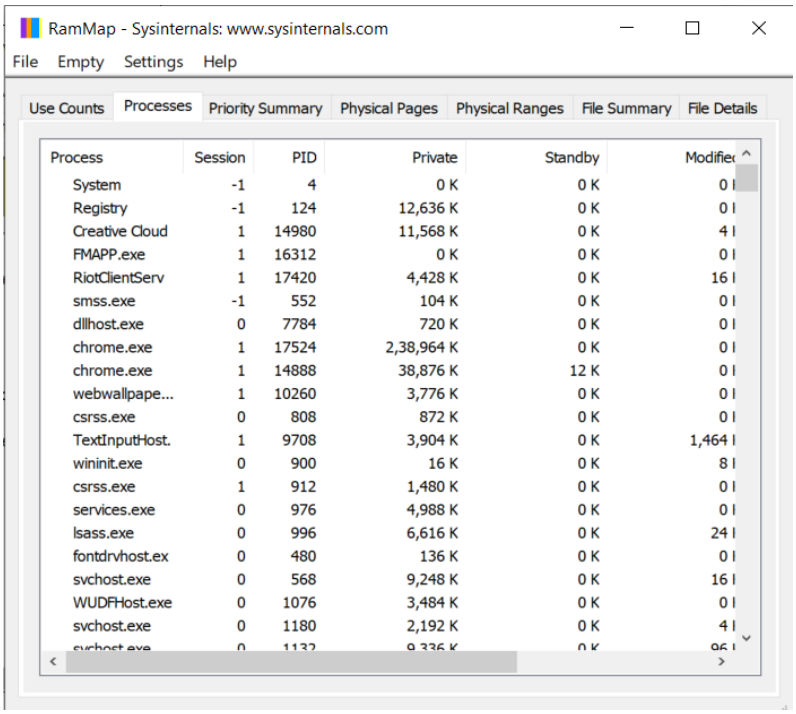


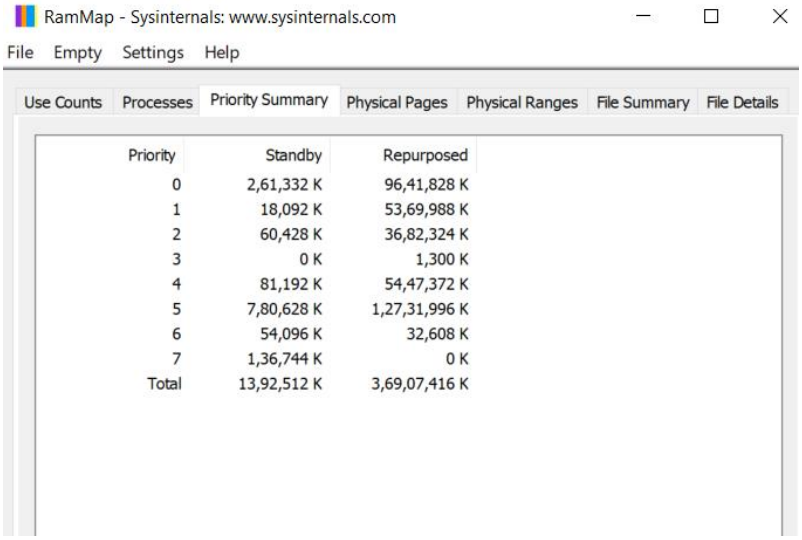
Exploring Rammap

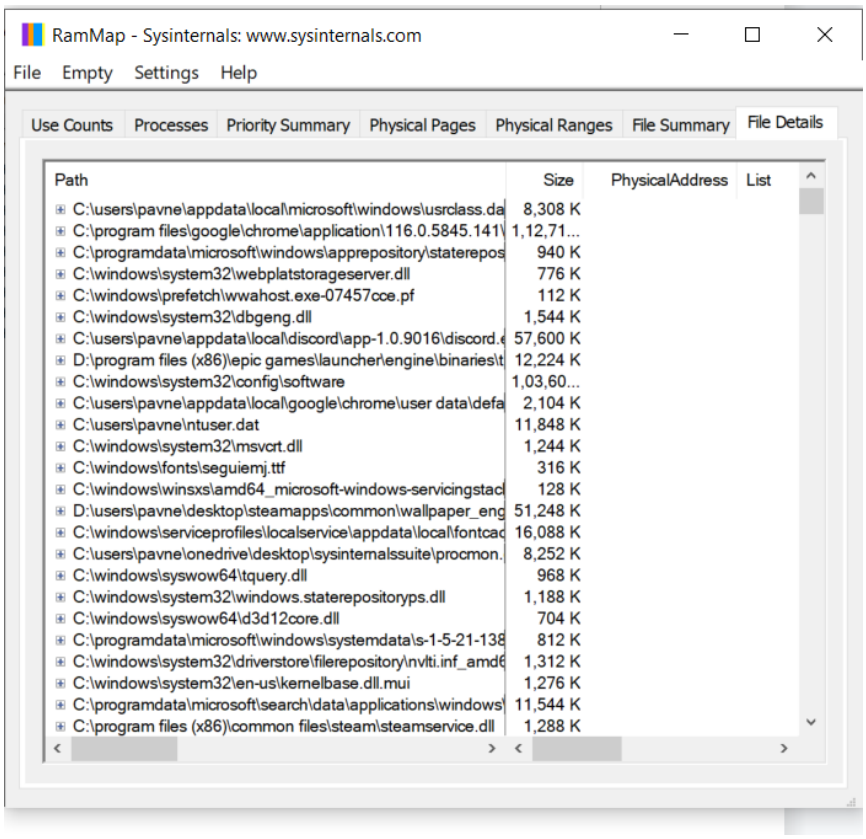
This tool provides us with details regarding how windows assign physical memory, how much data is cached in RAM, kernel, and device drivers' uses of RAM.



-

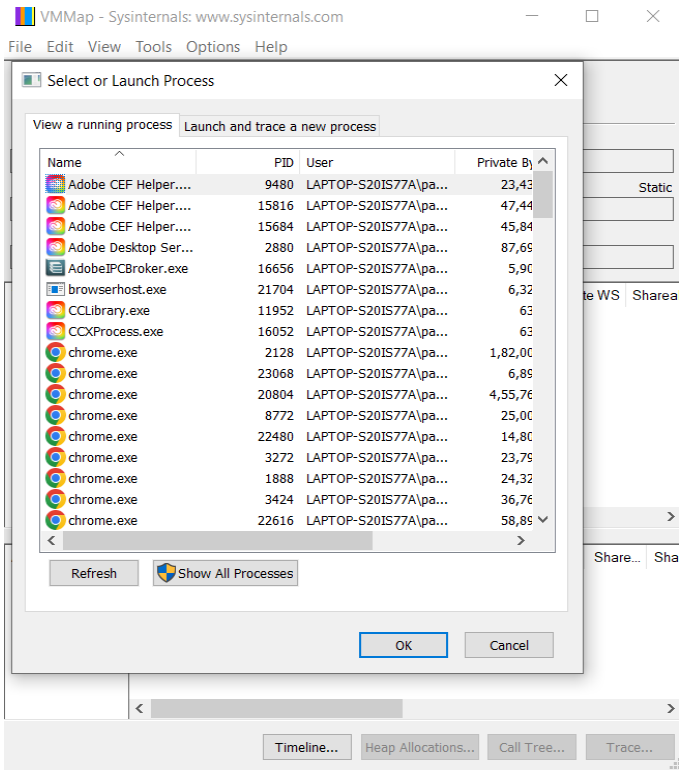

RamMap - Sysinternals: www.sysinternals.com
File Empty Settings Help
Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details
Process Session PID Private Standby Modifie
System -1 4 0 K 0 K 0 I
Registry -1 124 12,636 K 0 K 0 I
Creative Cloud 1 14980 11,568 K 0 K 4 I
FMAPP.exe 1 16312 0 K 0 K 0 I
RiotClientServ 1 17420 4,428 K 0 K 16 I
smss.exe -1 552 104 K 0 K 0 I
dllhost.exe 0 7784 720 K 0 K 0 I
chrome.exe 1 17524 2,38,964 K 0 K 0 I
chrome.exe 1 14888 38,876 K 12 K 0 I
webwallpape... 1 10260 3,776 K 0 K 0 I
csrss.exe 0 808 872 K 0 K 0 I
TextInputHost. 1 9708 3,904 K 0 K 1,464 I
wininit.exe 0 900 16 K 0 K 8 I
csrss.exe 1 912 1,480 K 0 K 0 I
services.exe 0 976 4,988 K 0 K 0 I
lsass.exe 0 996 6,616 K 0 K 24 I
fontdrvhost.ex 0 480 136 K 0 K 0 I
svchost.exe 0 568 9,248 K 0 K 16 I
WUDFHost.exe 0 1076 3,484 K 0 K 0 I
svchost.exe 0 1180 2,192 K 0 K 4 I


RamMap - Sysinternals: www.sysinternals.com
File Empty Settings Help
Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details
Priority Standby Repurposed
0 2,61,332 K 96,41,828 K
1 18,092 K 53,69,988 K
2 60,428 K 36,82,324 K
3 0 K 1,300 K
4 81,192 K 54,47,372 K
5 7,80,628 K 1,27,31,996 K
6 54,096 K 32,608 K
7 1,36,744 K 0 K
Total 13,92,512 K 3,69,07,416 K

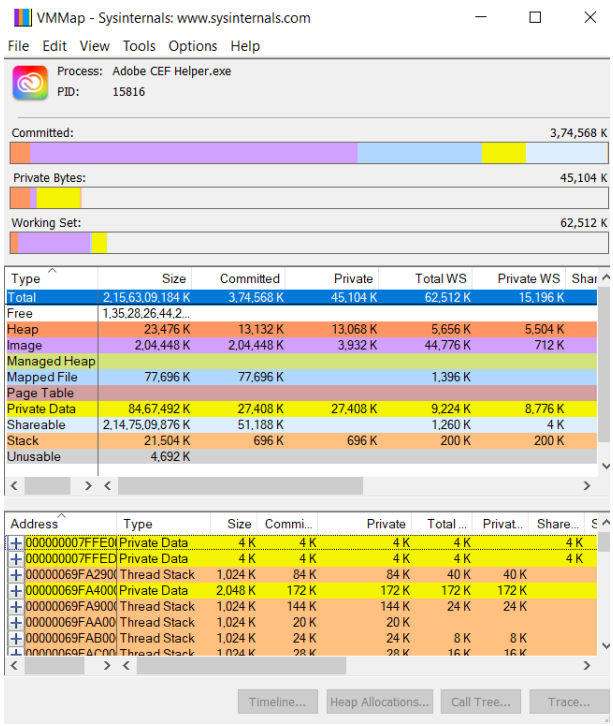


Exploring VMmap

It displays the processes committed to virtual memory types as well as the amount of physical memory assigned by the OS to VM types. It also shows summary information and a detailed process memory map.



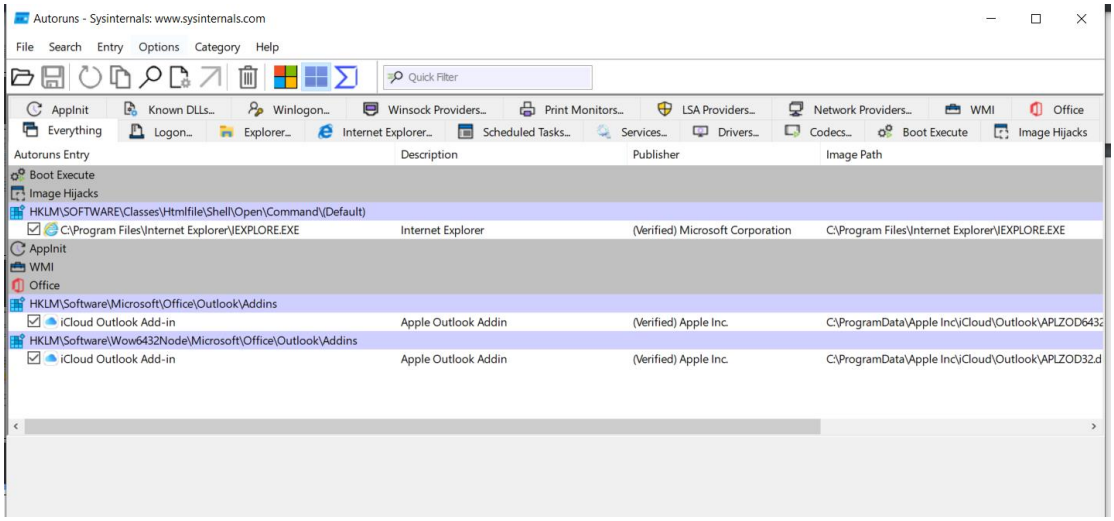
•



Exploring Autoruns

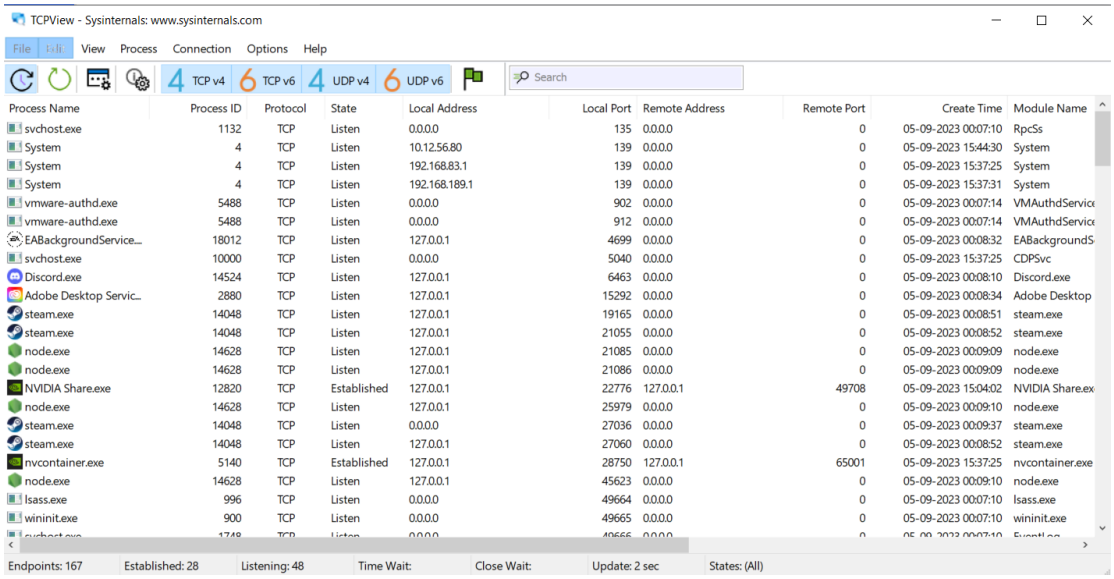
It shows which programs have permission to run during the system bootup or login. It shows which programs have auto run enabled and it also shows us a full list of registries and file system location available for auto-startup configuration.

It also has a virus-total feature which helps us flag out any malicious configuration.



Exploring TCP view

It provides us with a detailed listing of all TCP and UDP endpoints on our machine. These include local and remote connections as well as TCP connection state.

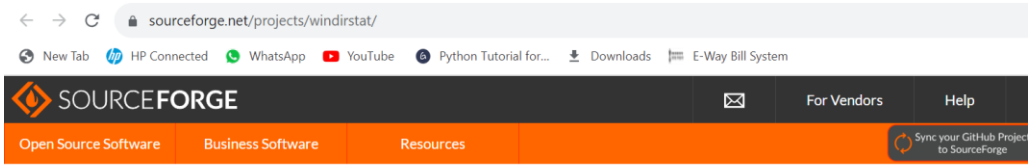


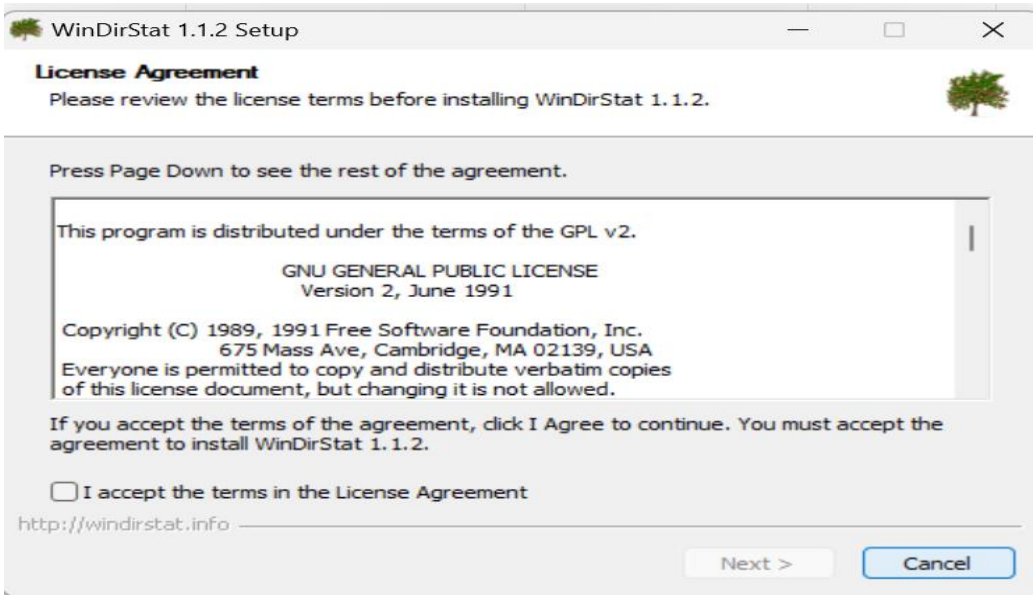
•

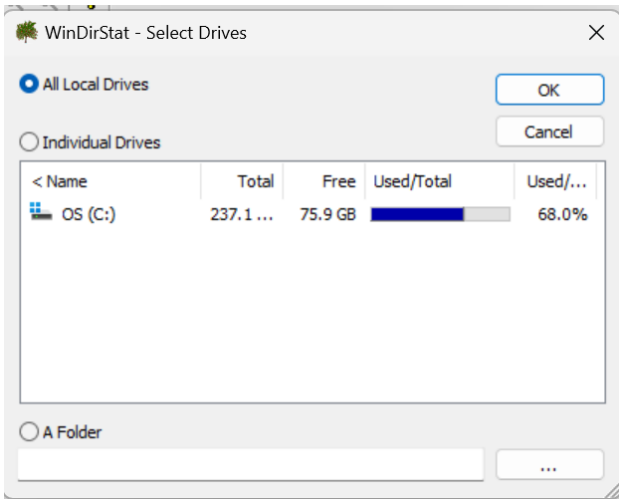
EXPERIMENT 4

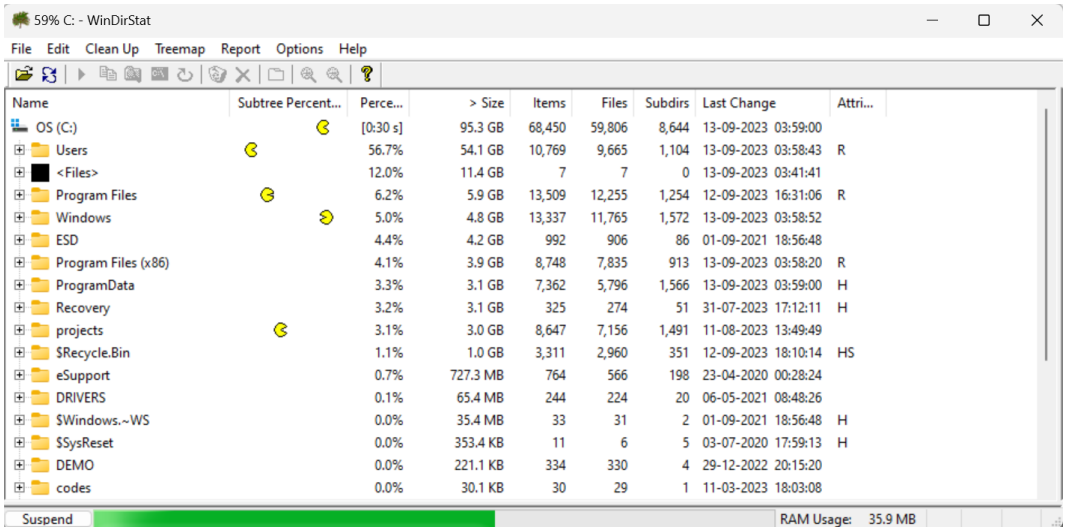
Lab Objectives: windows forensics using WinDirStat/ Kdirstst and PsTools**.**

Install WinDirStat:

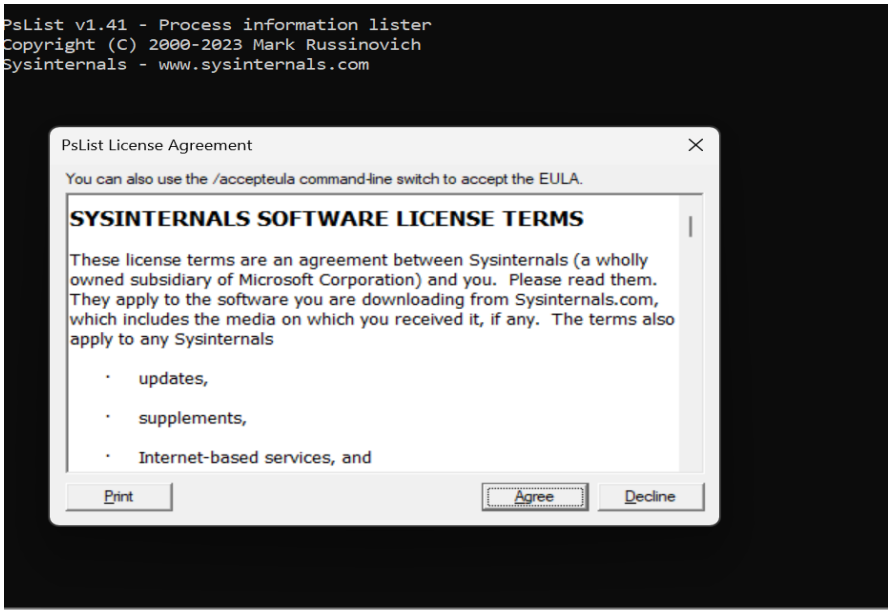





WinDirStat - Select Drives
All Local Drives
OK
Individual Drives
Cancel
< Name
Total
Free
Used/Total
Used/...
OS (C:)
237.1 ...
75.9 GB
68.0%
A Folder
...


59% C: - WinDirStat
File Edit Clean Up Treemap Report Options Help
Name Subtree Percent... Perce... > Size Items Files Subdirs Last Change Attri...
OS (C:) [0:30 s] 95.3 GB 68,450 59,806 8,644 13-09-2023 03:59:00
Users 56.7% 54.1 GB 10,769 9,665 1,104 13-09-2023 03:58:43 R
<Files> 12.0% 11.4 GB 7 7 0 13-09-2023 03:41:41
Program Files 6.2% 5.9 GB 13,509 12,255 1,254 12-09-2023 16:31:06 R
Windows 5.0% 4.8 GB 13,337 11,765 1,572 13-09-2023 03:58:52
ESD 4.4% 4.2 GB 992 906 86 01-09-2021 18:56:48
Program Files (x86) 4.1% 3.9 GB 8,748 7,835 913 13-09-2023 03:58:20 R
ProgramData 3.3% 3.1 GB 7,362 5,796 1,566 13-09-2023 03:59:00 H
Recovery 3.2% 3.1 GB 325 274 51 31-07-2023 17:12:11 H
projects 3.1% 3.0 GB 8,647 7,156 1,491 11-08-2023 13:49:49
$Recycle.Bin 1.1% 1.0 GB 3,311 2,960 351 12-09-2023 18:10:14 HS
eSupport 0.7% 727.3 MB 764 566 198 23-04-2020 00:28:24
DRIVERS 0.1% 65.4 MB 244 224 20 06-05-2021 08:48:26
$Windows.~WS 0.0% 35.4 MB 33 31 2 01-09-2021 18:56:48 H
$SysReset 0.0% 353.4 KB 11 6 5 03-07-2020 17:59:13 H
DEMO 0.0% 221.1 KB 334 330 4 29-12-2022 20:15:20
codes 0.0% 30.1 KB 30 29 1 11-03-2023 18:03:08
Suspend
RAM Usage: 35.9 MB

Pslist


PsList v1.41 - Process information lister
Copyright (C) 2000-2023 Mark Russinovich
Sysinternals - www.sysinternals.com
PsList License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
updates,
supplements,
Internet-based services, and
Print
Agree
Decline

```
Sysinternals - www.sysinternals.com

Process information for LAPTOP-8GR4A1LO:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0  16    0     60    34:32:05.718    22:00:50.656
System                4   8 276 5188     56     0:05:23.437    22:00:50.656
Registry            140   8   4    0   9240     0:00:01.031    22:00:52.449
smss                528  11   2   58   1108     0:00:00.500    22:00:50.631
csrss               864  13  12  762   2184     0:00:02.328    22:00:48.235
wininit             996  13   2  148   1588     0:00:00.046    22:00:47.602
services           1072   9   8  759   5816     0:00:11.453    22:00:47.516
lsass              1096   9  11 1792   9952     0:00:15.078    22:00:47.469
svchost            1228   8  28 1529  14332     0:00:21.046    22:00:47.264
fontdrvhost        1264   8   5   40   2408     0:00:00.312    22:00:47.248
svchost            1368   8  11 1430  10216     0:00:34.593    22:00:47.193
svchost            1420   8   7  323   3092     0:00:02.140    22:00:47.158
svchost            1576   8   4  257   3016     0:00:01.234    22:00:46.983
WUDFHost           1600   8   8  284   4428     0:00:00.937    22:00:46.971
svchost            1608   8   2  311   2112     0:00:00.109    22:00:46.970
svchost            1684   8   7  158   7572     0:00:05.359    22:00:46.937
svchost            1748   8  23 1059   8584     0:00:17.296    22:00:46.919
svchost            1856   8   7  454  19188     0:00:00.906    22:00:46.852
atiesrxx           1868   8   4  198   1524     0:00:00.015    22:00:46.851
svchost            1952   8  11  323   3936     0:00:31.703    22:00:46.826
svchost            1120   8   6  421   6504     0:00:03.015    22:00:46.743
svchost            1724   8  10  355   2684     0:00:00.046    22:00:46.716
svchost            2228   8   2  196   2224     0:00:00.343    22:00:46.608
svchost            2240   8   5  238   3892     0:00:18.031    22:00:46.606
svchost            2260   8   5  231   2644     0:00:31.390    22:00:46.602
svchost            2272   8   3  246   1252     0:00:00.171    22:00:46.602
svchost            2280   8   4  170   1900     0:00:00.234    22:00:46.602
Memory Compression 2424   8  70    0   1136     0:00:35.875    22:00:46.571
svchost            2472   8   2  177   1852     0:00:00.328    22:00:46.568
svchost            2480   8   8  278   3164     0:00:04.453    22:00:46.568
svchost            2576   8   5  194   2188     0:00:00.593    22:00:46.549
svchost            2584   8   5  175   1816     0:00:03.468    22:00:46.548
svchost            2724   8   5  326  17412     0:00:28.281    22:00:46.386
svchost            2748   8  11  411   3808     0:00:01.484    22:00:46.203
svchost            2776   8   3  160   1480     0:00:00.109    22:00:46.185
```

```
PsList v1.41 - Process information lister
Copyright (C) 2000-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Process memory detail for LAPTOP-8GR4A1LO:

Name                 Pid      VM      WS    Priv Priv Pk   Faults   NonP Page
cmd                12392 2151729656    3928    1900    3132     1294       4   32
cmd                 3672 2151729656    4160    1968    3120     1263       4   32
cmd                11724 2151739196    5844    2356    5132     2834       6   51
```

```
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

Usage: psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd]][-n s][-r se
rvicename][-h][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w directory][-d][-<priority
>][-g n][-a n,n,...][-verbose] cmd [arguments]
     -a         Separate processors on which the application can run with
                commas where 1 is the lowest numbered CPU. For example,
                to run the application on CPU 2 and CPU 4, enter:
                "-a 2,4"
     -c         Copy the specified program to the remote system for
                execution. If you omit this option the application
                must be in the system path on the remote system.
     -d         Don't wait for process to terminate (non-interactive).
     -e         Does not load the specified account's profile.
     -f         Copy the specified program even if the file already
                exists on the remote system.
     -g         Set the primary thread's processor group to the one specified
                (Only for systems with more than 64 processors).
     -i         Run the program so that it interacts with the desktop of the
                specified session on the remote system. If no session is
                specified the process runs in the console session.
     -h         If the target system is Vista or higher, has the process
                run with the account's elevated token, if available.
     -l         Run process as limited user (strips the Administrators group
                and allows only privileges assigned to the Users group).
                On Windows Vista the process runs with Low Integrity.
     -n         Specifies timeout in seconds connecting to remote computers.
     -p         Specifies optional password for user name. If you omit this
                you will be prompted to enter a hidden password.
     -r         Specifies the name of the remote service to create or interact.
                with.
     -s         Run the remote process in the System account.
```

```
PsKill v1.17 - Terminates processes on local or remote systems
Copyright (C) 1999-2023  Mark Russinovich
Sysinternals - www.sysinternals.com

Usage: pskill [-t] [\\computer [-u username [-p password]]] <process ID | name>
     -t    Kill the process and its descendants.
     -u    Specifies optional user name for login to
           remote computer.
     -p    Specifies optional password for user name. If you omit this
           you will be prompted to enter a hidden password.
     -nobanner Do not display the startup banner and copyright message.
```

```
PsService v2.26 - Service information and configuration utility
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: AJRouter
DISPLAY_NAME: AllJoyn Router Service
Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped th
e AllJoyn clients that do not have their own bundled routers will be unable to run.
        TYPE               : 20 WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
                                (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077 (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms

SERVICE_NAME: ALG
DISPLAY_NAME: Application Layer Gateway Service
Provides support for 3rd party protocol plug-ins for Internet Connection Sharing
        TYPE               : 10 WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
                                (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077 (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms

SERVICE_NAME: AMD External Events Utility
DISPLAY_NAME: AMD External Events Utility
        GROUP              : Event log
        TYPE               : 10 WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms
```

```
PsSuspend v1.08 - Process Suspender
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals

PsSuspend suspends or resumes processes on a local or remote NT system.

Usage: pssuspend [-r] [\\RemoteComputer [-u Username [-p Password]]] <process Id or name>
     -r    Resume.
     -u    Specifies optional user name for login to
           remote computer.
     -p    Specifies optional password for user name. If you omit this
           you will be prompted to enter a hidden password.
     -nobanner Do not display the startup banner and copyright message.
```

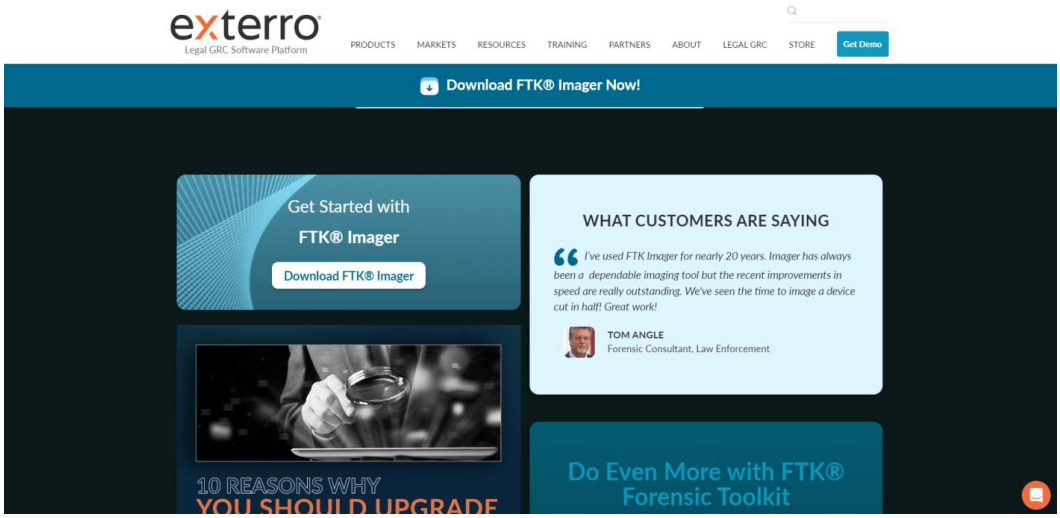
```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.7.14.148:52876      relay-61f2512e:https   ESTABLISHED
  TCP    10.7.14.148:52878      20.198.118.190:https   ESTABLISHED
  TCP    10.7.14.148:52977      20.187.186.89:https    ESTABLISHED
  TCP    10.7.14.148:53575      a104-90-7-81:https     CLOSE_WAIT
  TCP    10.7.14.148:53577      a104-90-7-178:https    CLOSE_WAIT
  TCP    10.7.14.148:53578      a104-90-7-178:https    CLOSE_WAIT
  TCP    10.7.14.148:53579      a104-90-7-83:https     CLOSE_WAIT
  TCP    10.7.14.148:53580      a104-90-7-83:https     CLOSE_WAIT
  TCP    10.7.14.148:53581      a104-90-7-83:https     CLOSE_WAIT
  TCP    10.7.14.148:53582      a104-90-7-83:https     CLOSE_WAIT
  TCP    10.7.14.148:53583      a104-90-7-81:https     CLOSE_WAIT
  TCP    10.7.14.148:53587      se-in-f188:5228        ESTABLISHED
  TCP    10.7.14.148:53592      ec2-3-6-163-125:https  ESTABLISHED
  TCP    10.7.14.148:53596      a104-90-7-81:https     LAST_ACK
  TCP    10.7.14.148:53599      a104-90-7-123:https    CLOSE_WAIT
```

```
Interface: 10.7.14.148 --- 0x2
  Internet Address      Physical Address      Type
  10.7.1.1              f8-b1-56-33-55-7d     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

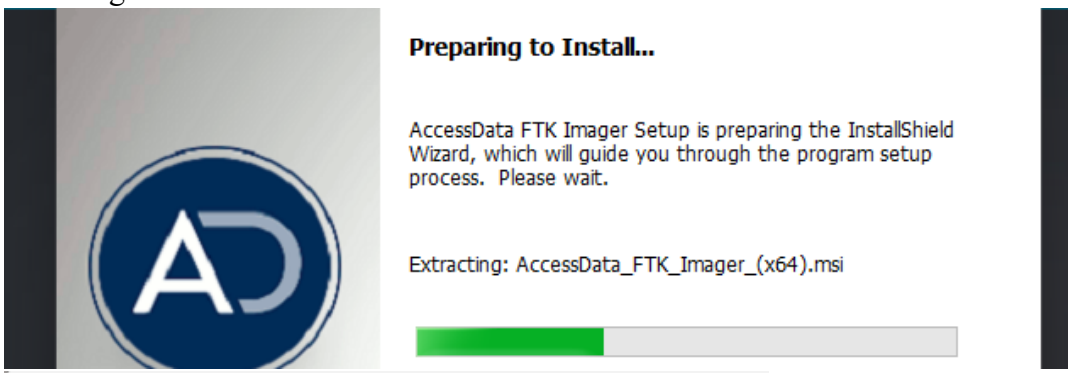
•

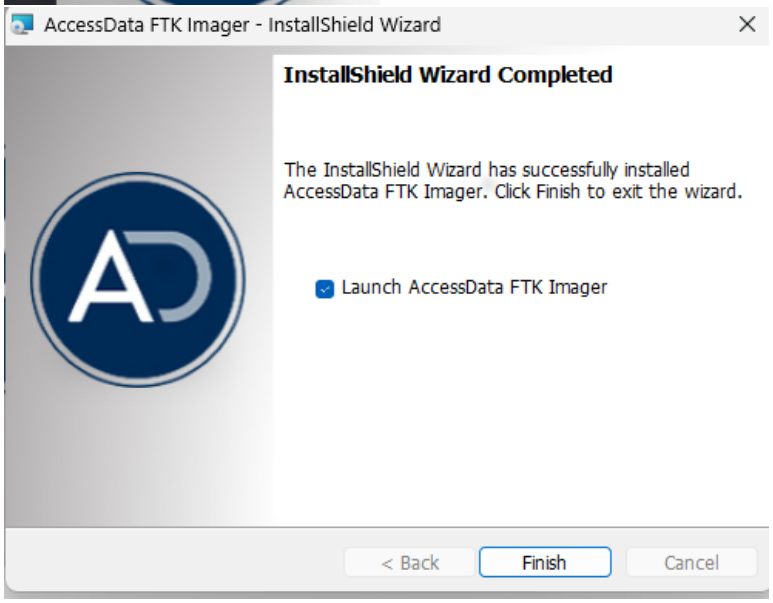
EXPERIMENT 5

Install FTK Imager

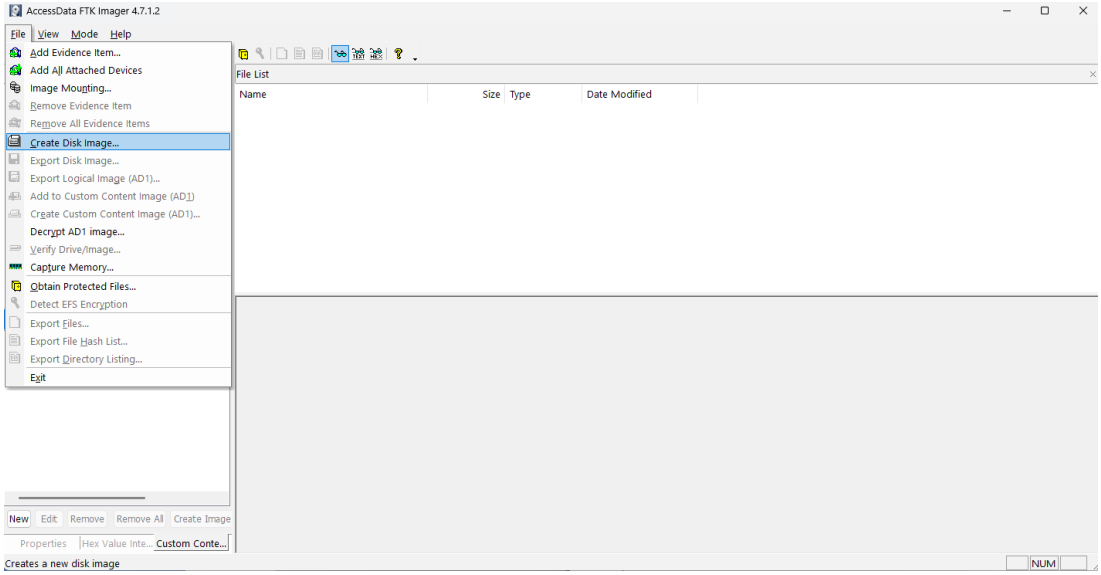


Installing

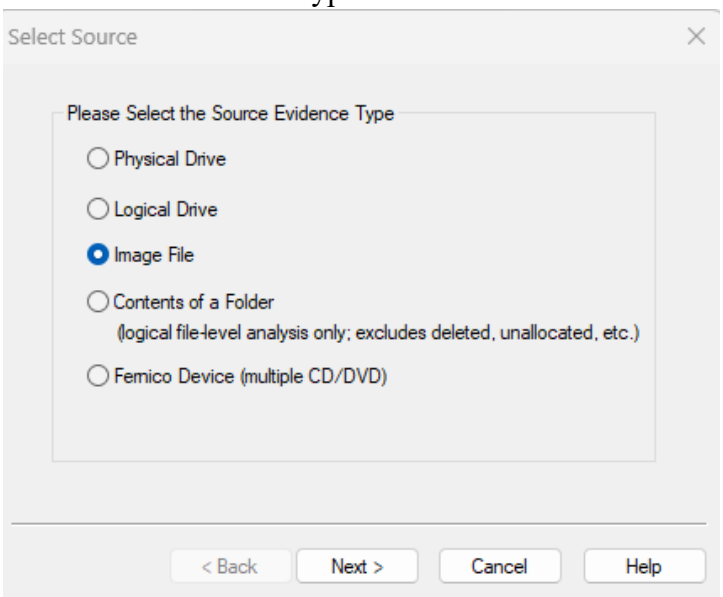




Executing FTK Imager
Open File -> Create Disk Storage

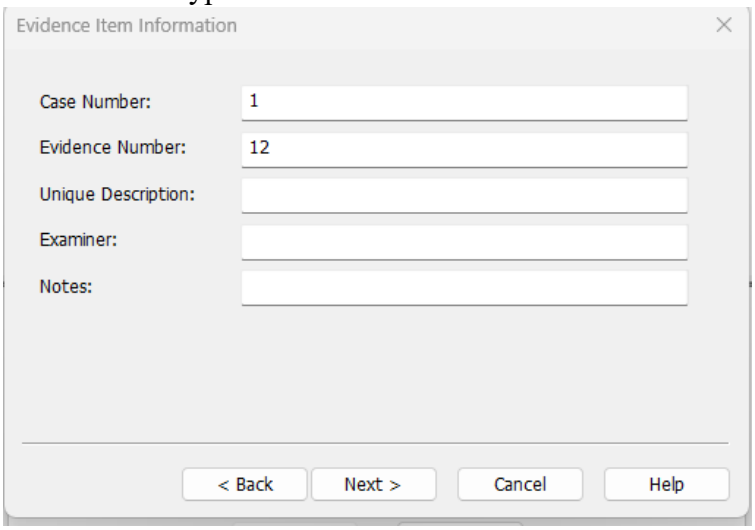


Select source evidence type

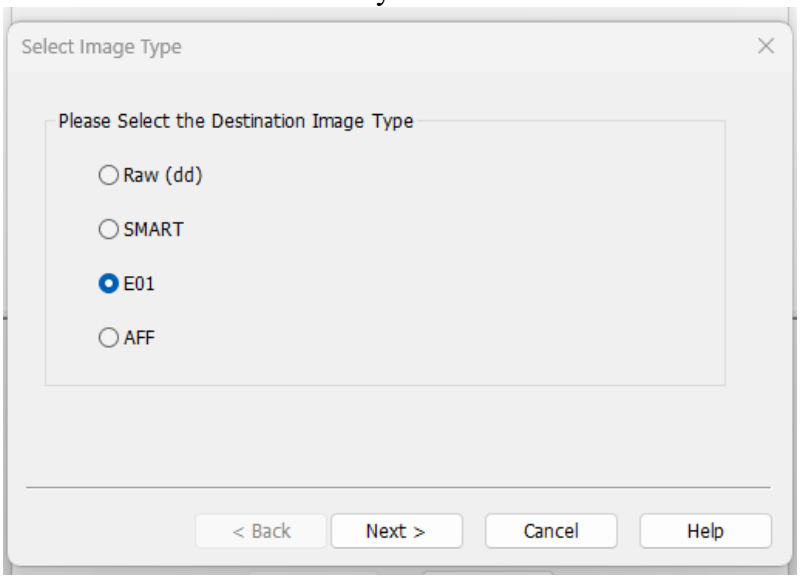


•

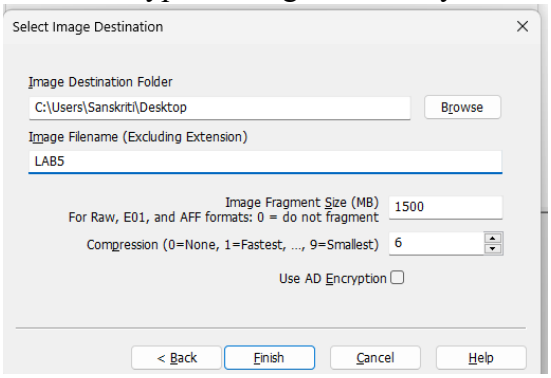
Select source type to clone information from



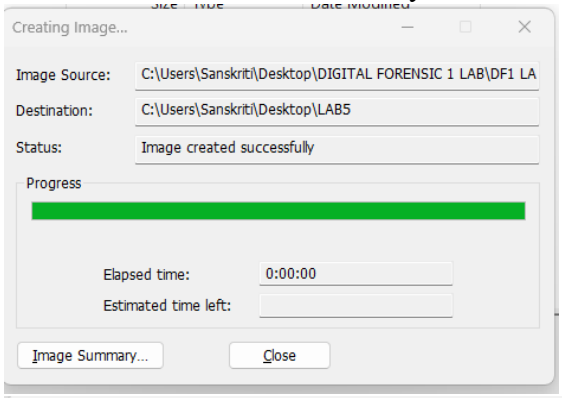
Select source drive of which you want to clone data from

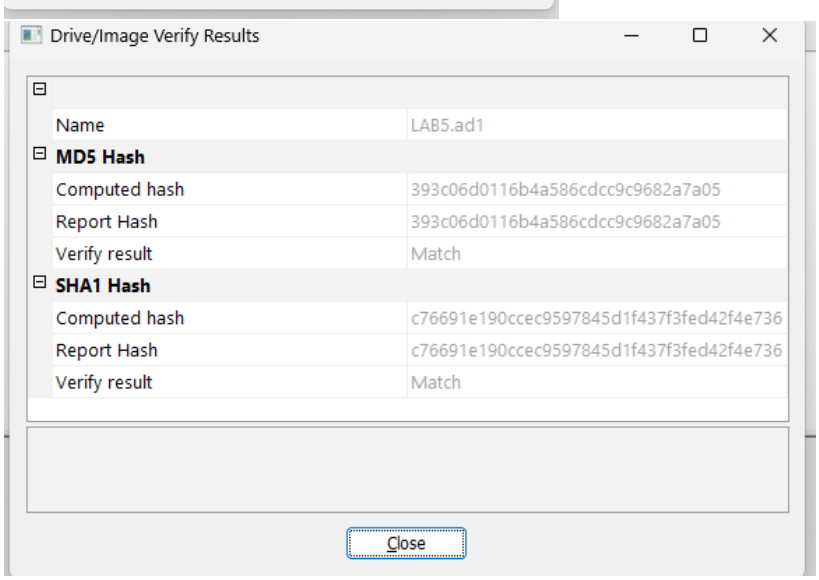


Select the type of image in which you want to clone data



Add a destination folder where you want to store the cloned image and start the process

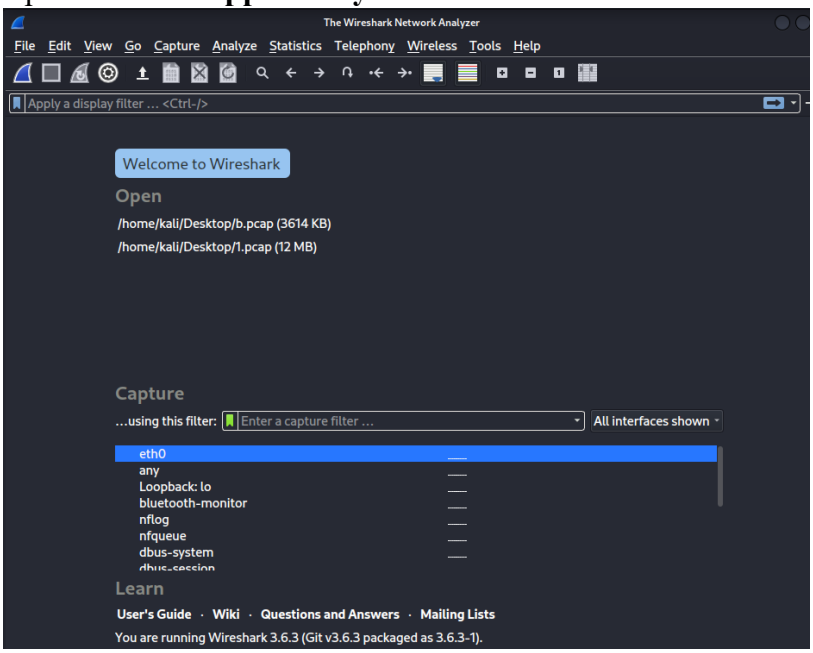




•

EXPERIMENT 6

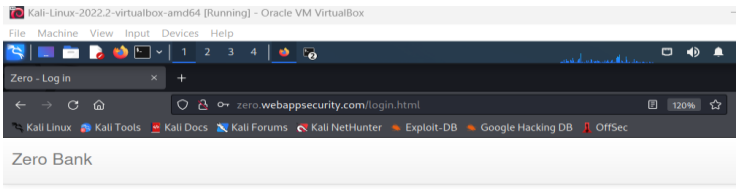
1) First, we will open **Wireshark** for tracing the packets in Kali Linux
Click on eth0
Open **zero.webappsecurity.com** in firefox

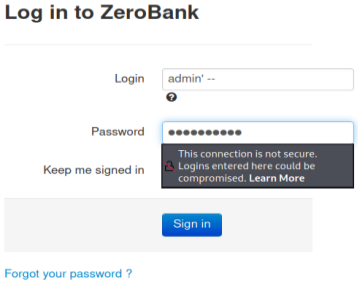


2) Capture the packets

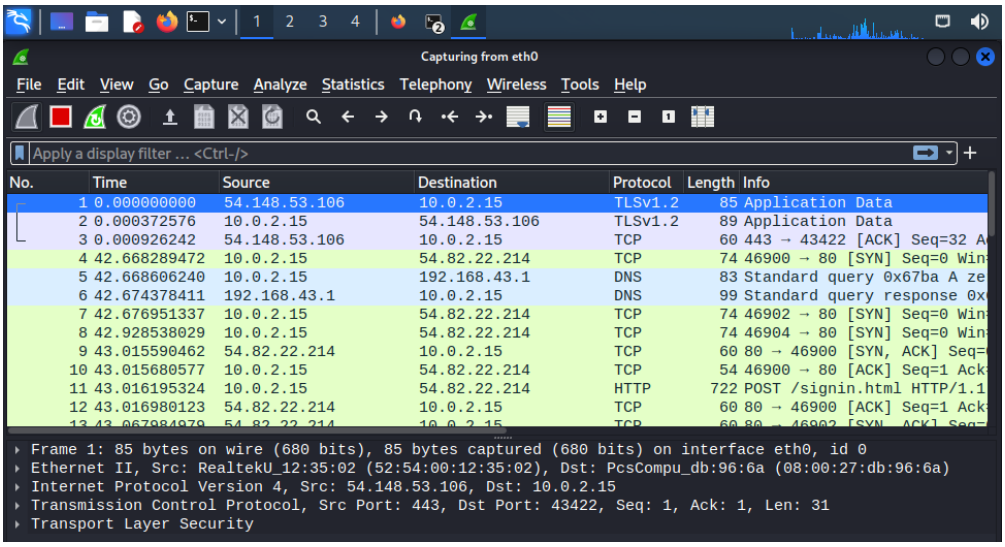
Then , we click on eth0 for start tracking the website packets , and at the same time we try to perform sql injection on website **zero.webappsecurity.com** to track the packets of login try attempt also .

We try to perform SQL Injection on the website zero.webappsecurity.com by entering login as **admin' - -** and Password as **' or 1=1--**



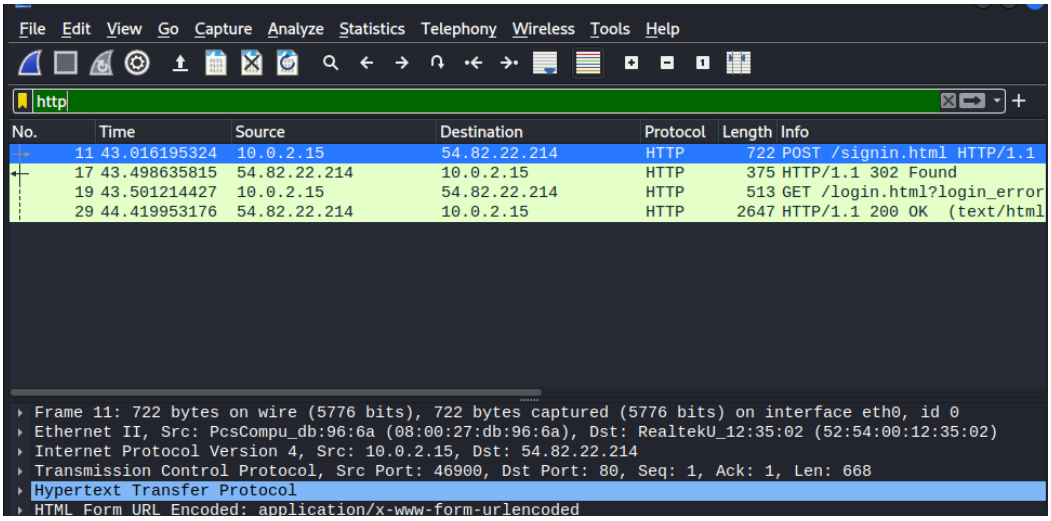


After trying wireshark packet tracking , we get the packets which are listed below.



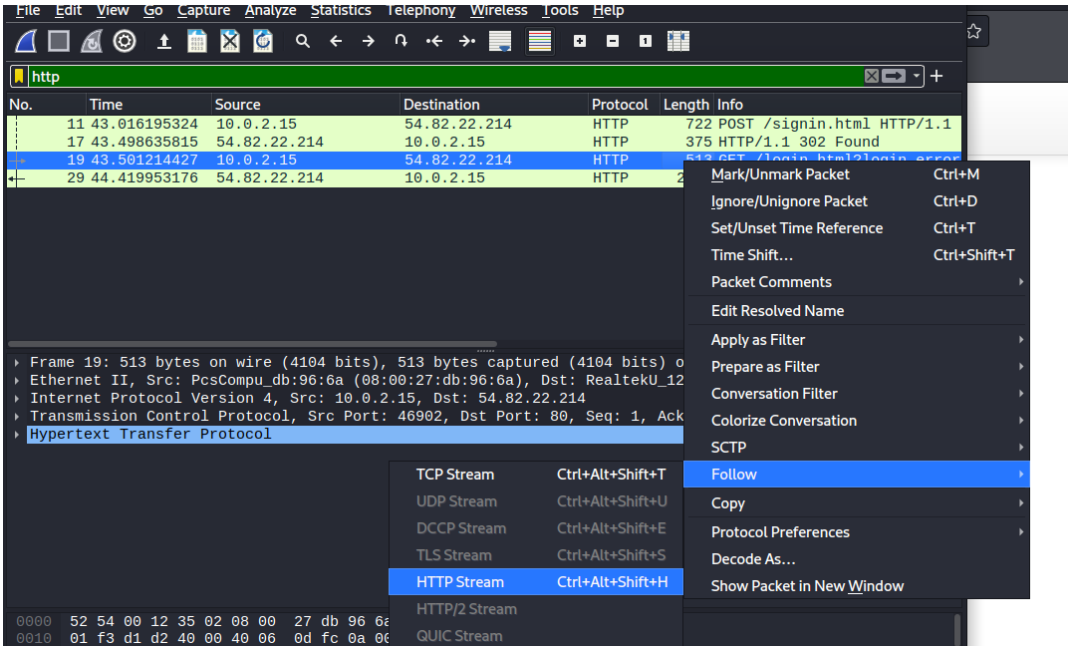
3) Check the login values

But , we want to get the packet trace of just sign in , which we can see in above screenshot **sign in** is working on **http** . So we apply a filter of http and as we get what we wanted so we stop the Wireshark by clicking on red button which is shown in the above screenshot.

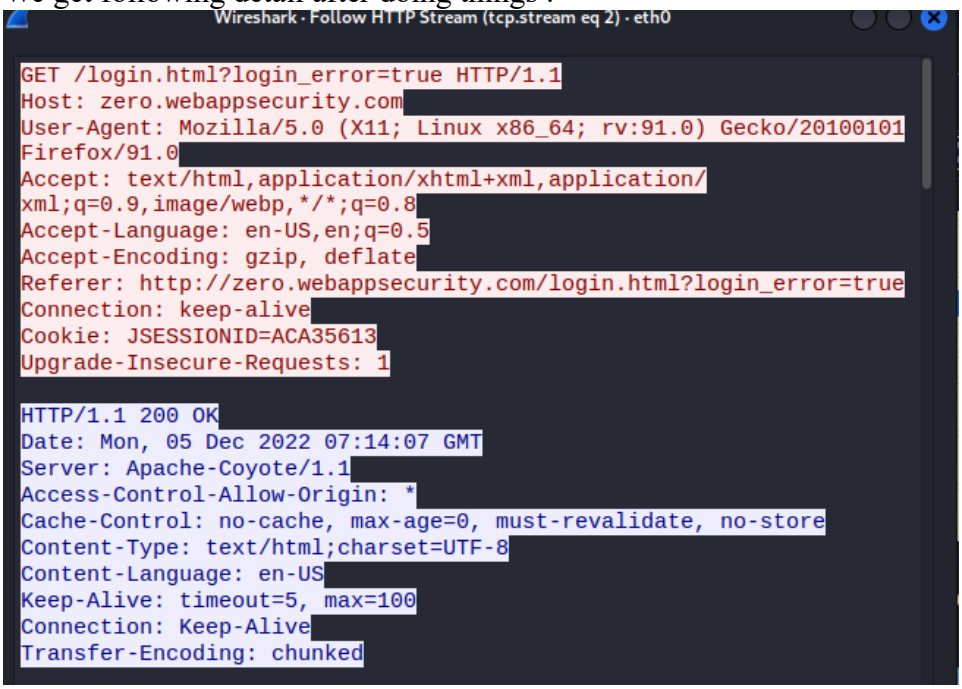


And then we right click on S.no. 19 which is based on login and then we click on **follow** and then we click on **Http Stream**

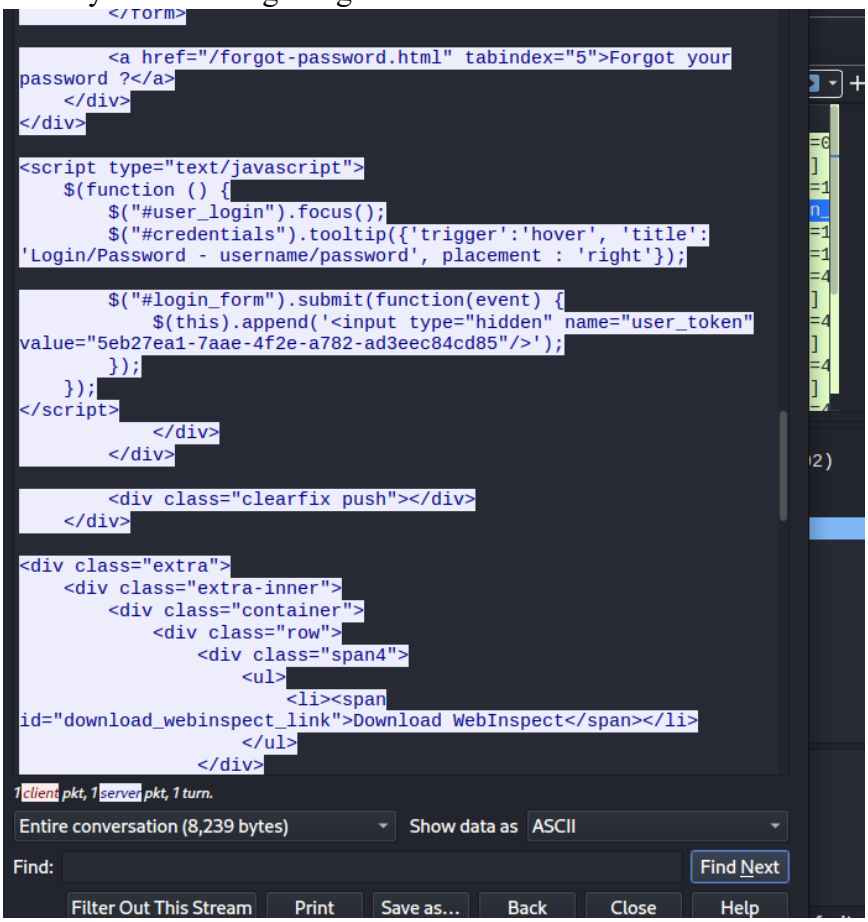
•



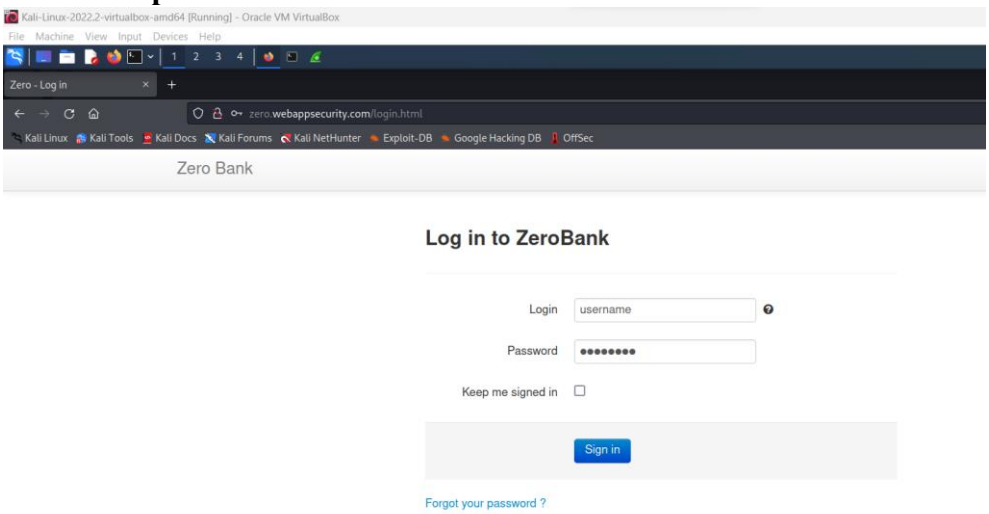
We get following detail after doing things .



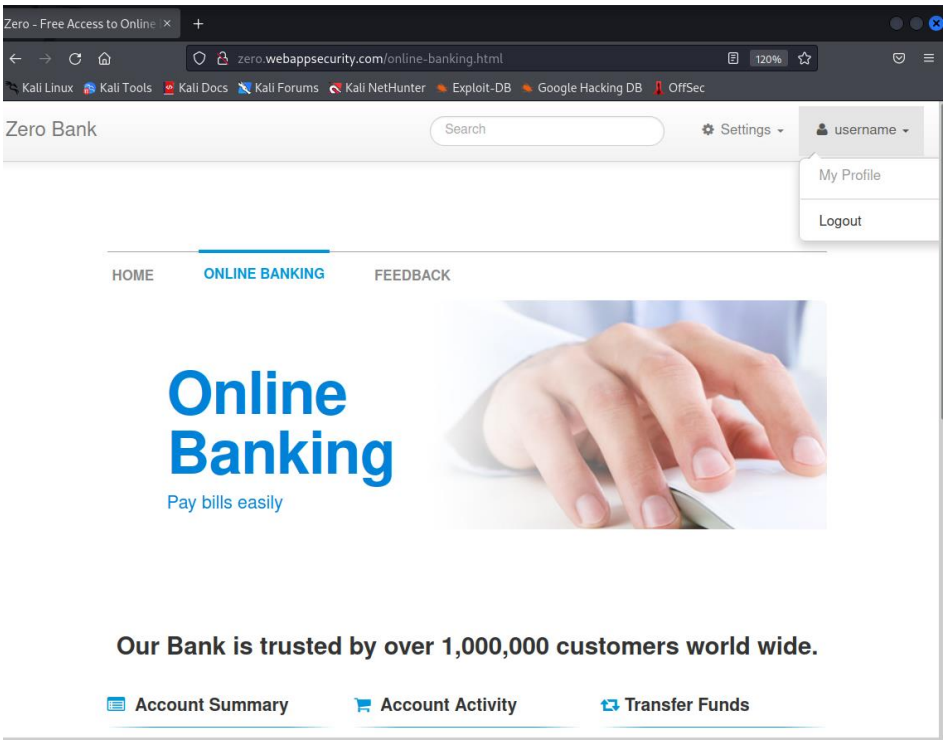
But as I scroll down to looking if username and passwords are written in Http Stream , I actually found the right login credentials of that website .



I tried entering the username and password to website and it worked .
Login : **username**
Password : **password**

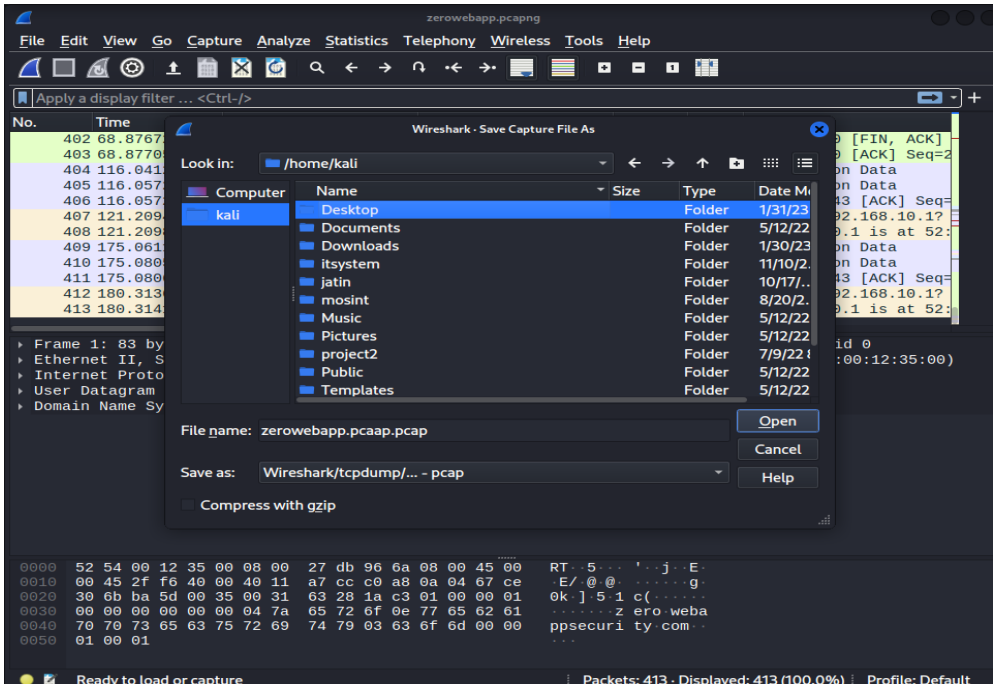


•

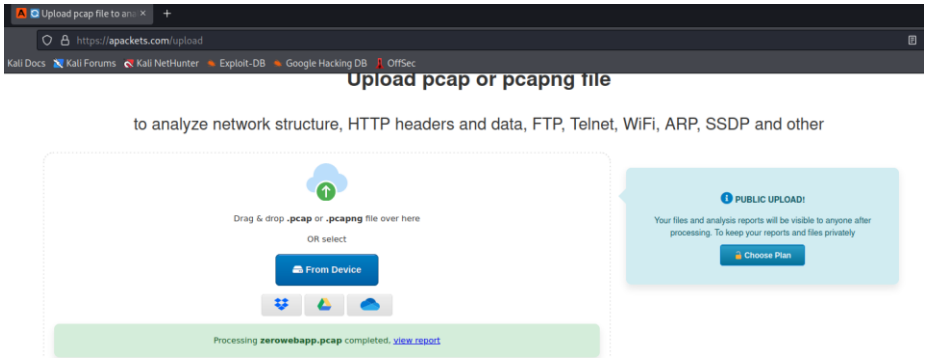


4) **Use A-packets**

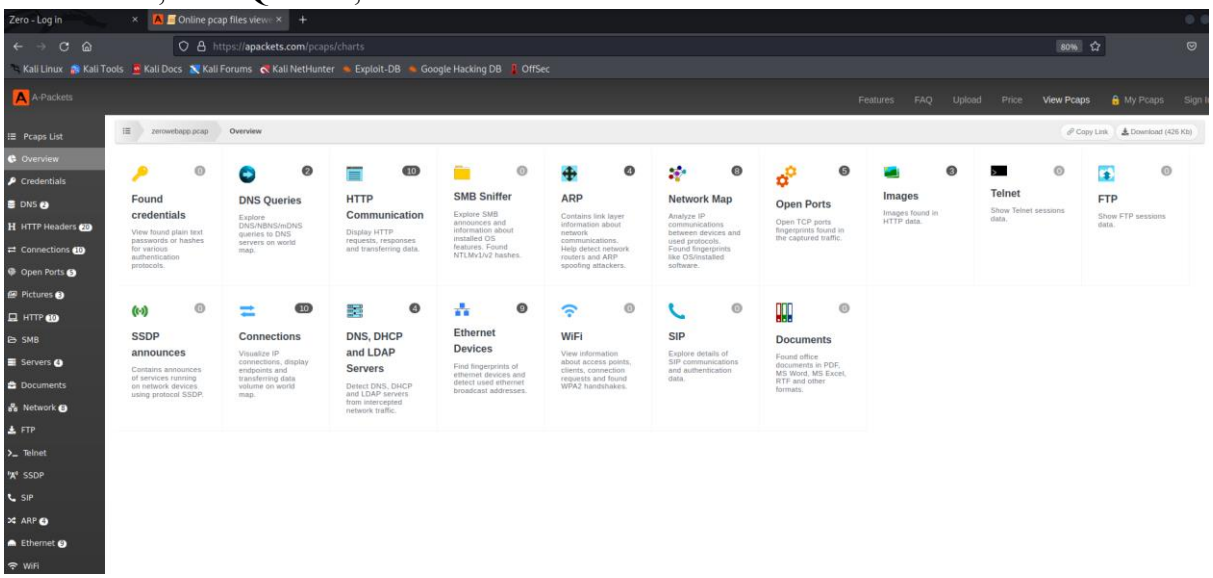
We click on red Button stop , and then save with file name as testfire.pcap



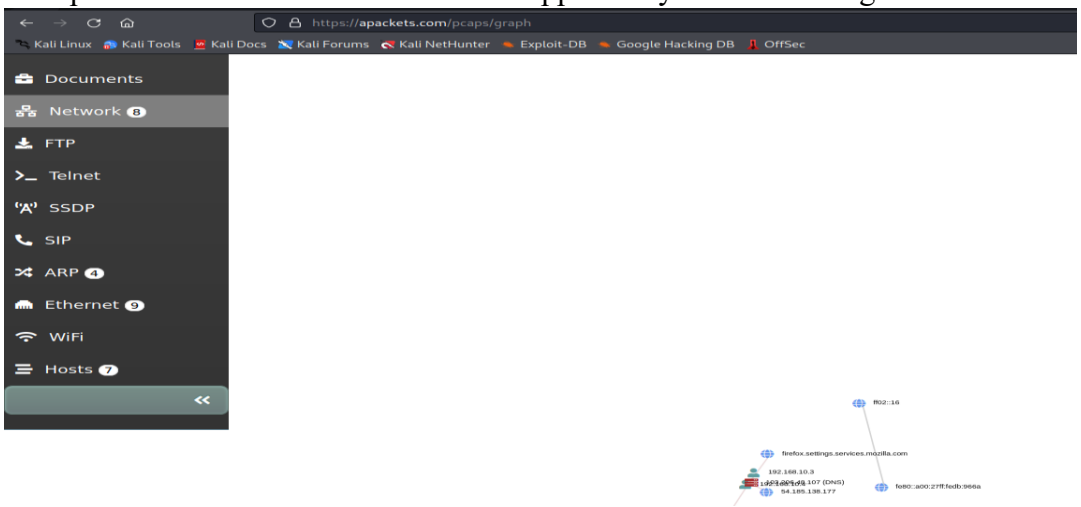
Now , we go to apackets.com and upload that file .



And here we go , after viewing reports , we can find lot of information such as Found Credentials , DNS Queries , Network Route and much more.



We open the Network Route of zero.webappsecurity.com which is given below.



•

EXPERIMENT 7

Lab Objective: Data Acquisition using Autopsy

Steps:

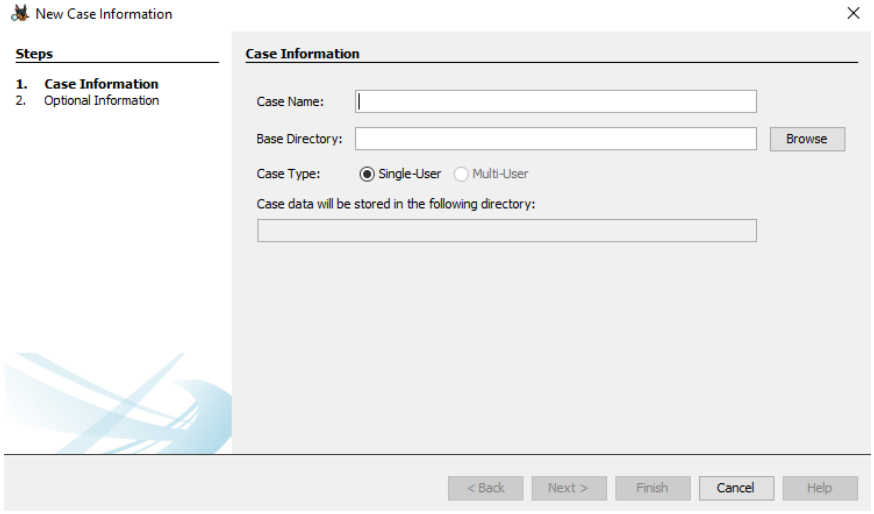
1. Download and install Autopsy.

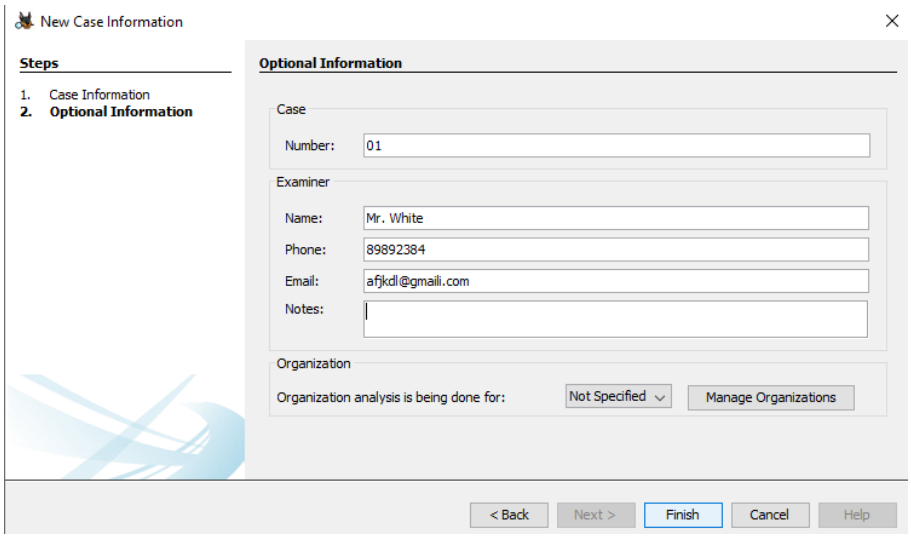
Downloading of Autopsy was done from the official website of Autopsy.

2. Filling out essential and optional details about the case.

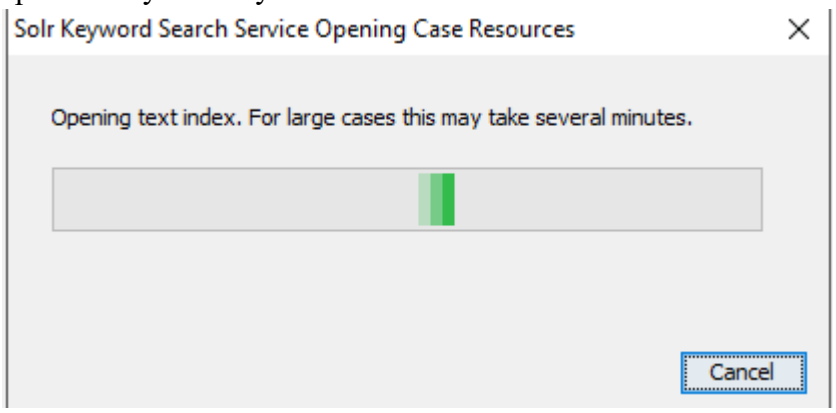
After installation Autopsy asked me to create a new case.

After creating a new case Autopsy asked me for the details related to the case.





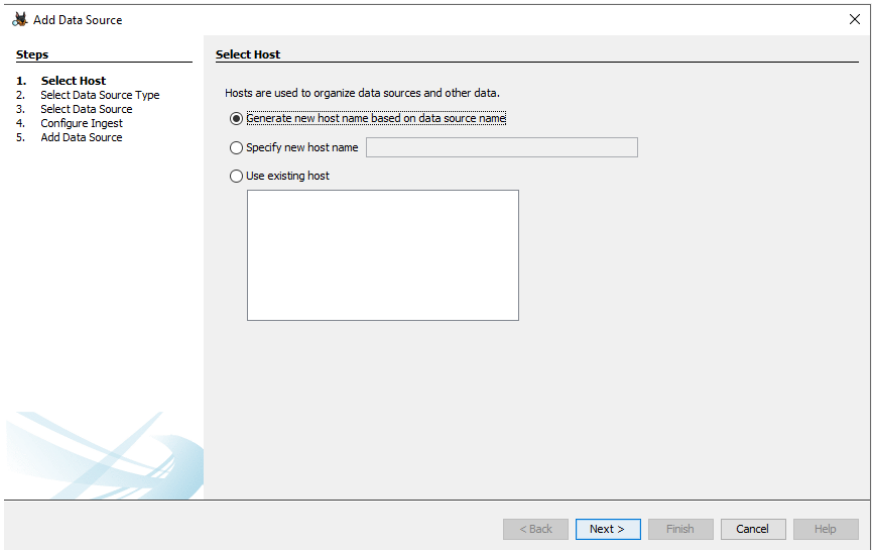
After filling essential and optional information. Autopsy created a database in the folder specified by me only.

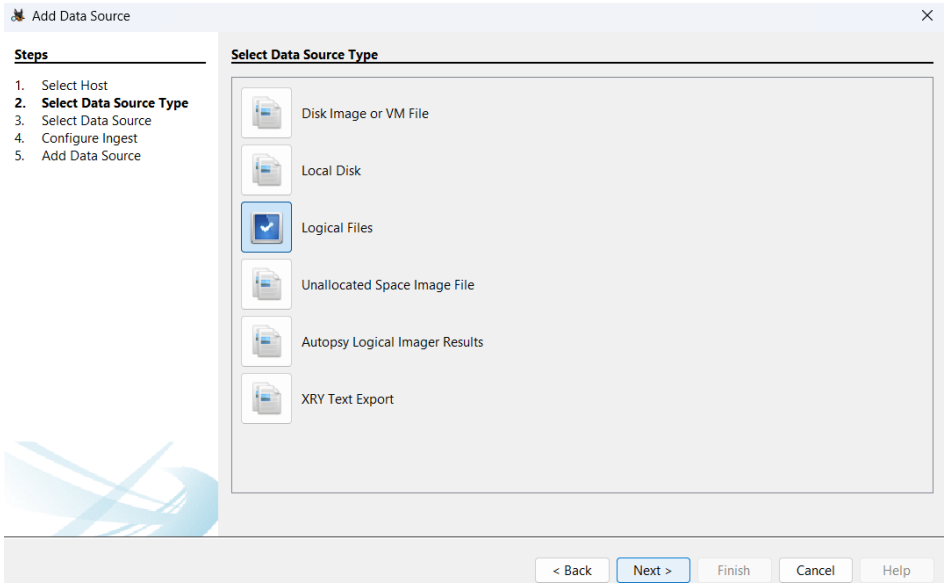


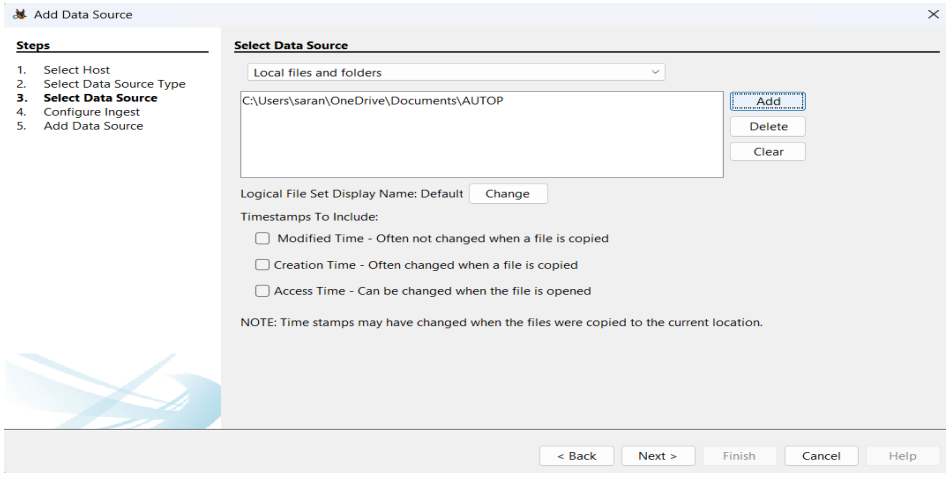
3. Selecting the evidence disk and starting the analysis.

Now, I needed to selected a file or drive as my evidence on which I need to perform.

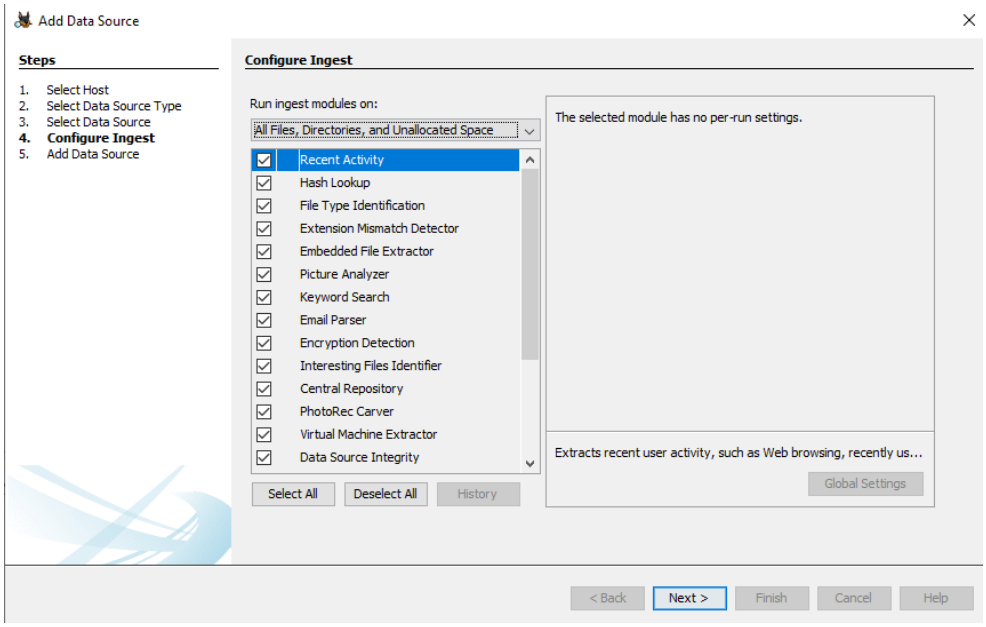
•


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Host
Hosts are used to organize data sources and other data.
Generate new host name based on data source name
Specify new host name
Use existing host
< Back
Next >
Finish
Cancel
Help

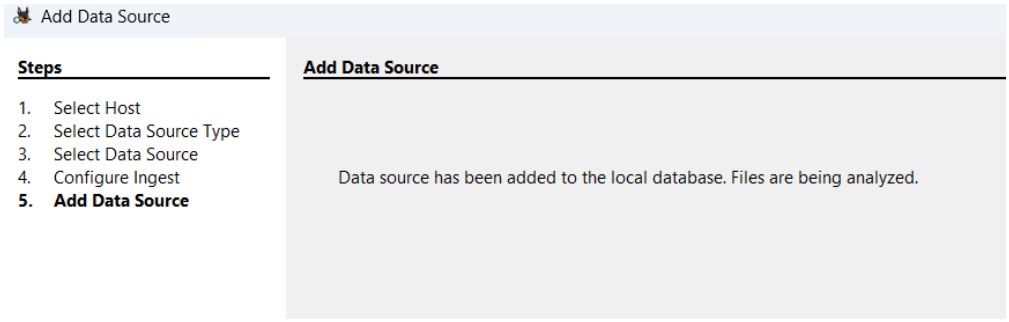

Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help


Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Local files and folders
C:\Users\saran\OneDrive\Documents\AUTOP
Add
Delete
Clear
Logical File Set Display Name: Default
Change
Timestamps To Include:
Modified Time - Often not changed when a file is copied
Creation Time - Often changed when a file is copied
Access Time - Can be changed when the file is opened
NOTE: Time stamps may have changed when the files were copied to the current location.
< Back
Next >
Finish
Cancel
Help

Autopsy can also apply filters. To search for a specific file.

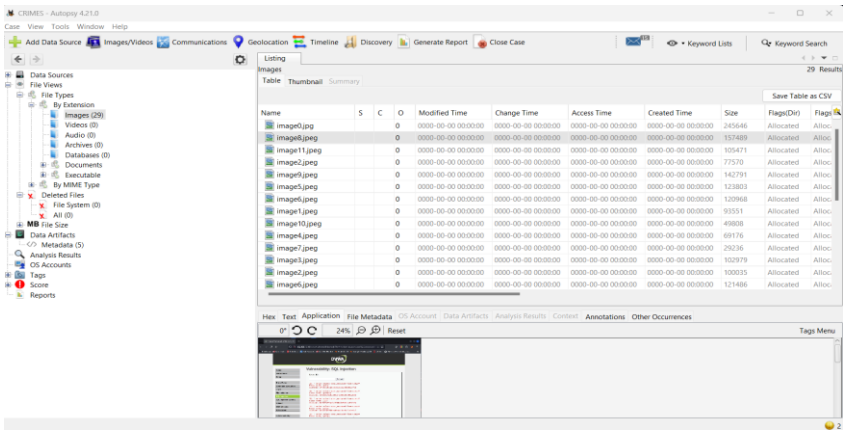


Scanning started.

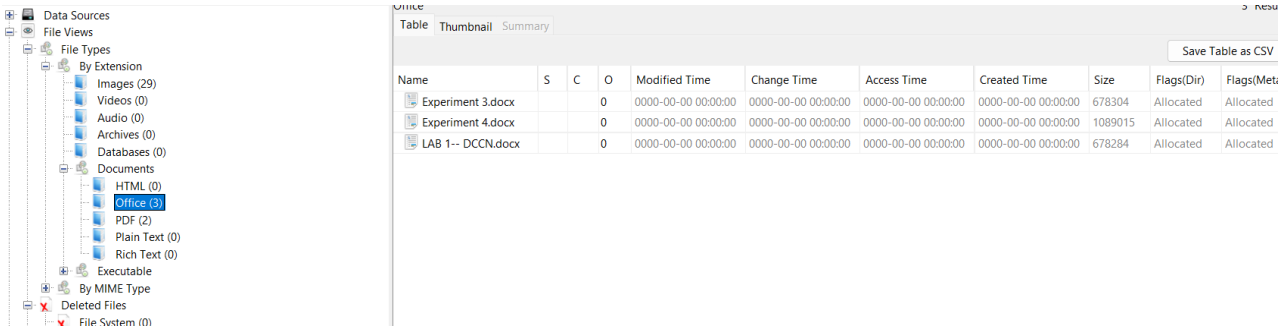


After scanning Autopsy was able to find file with extensions.

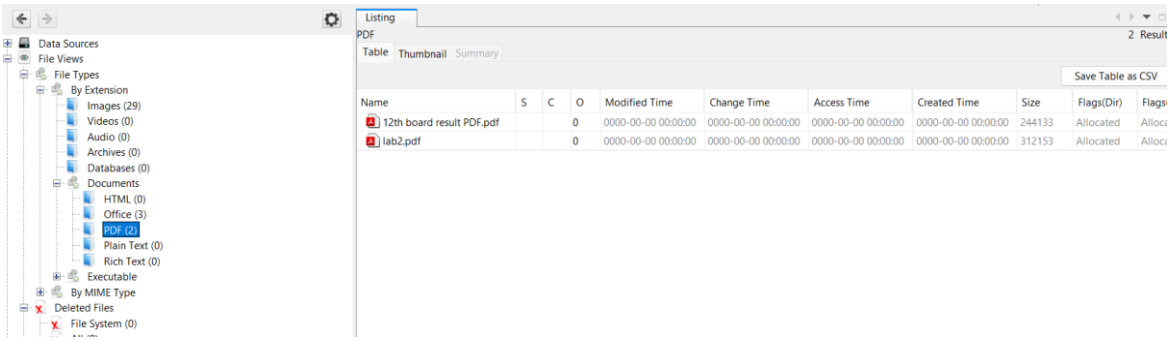
a) .jpg , .png



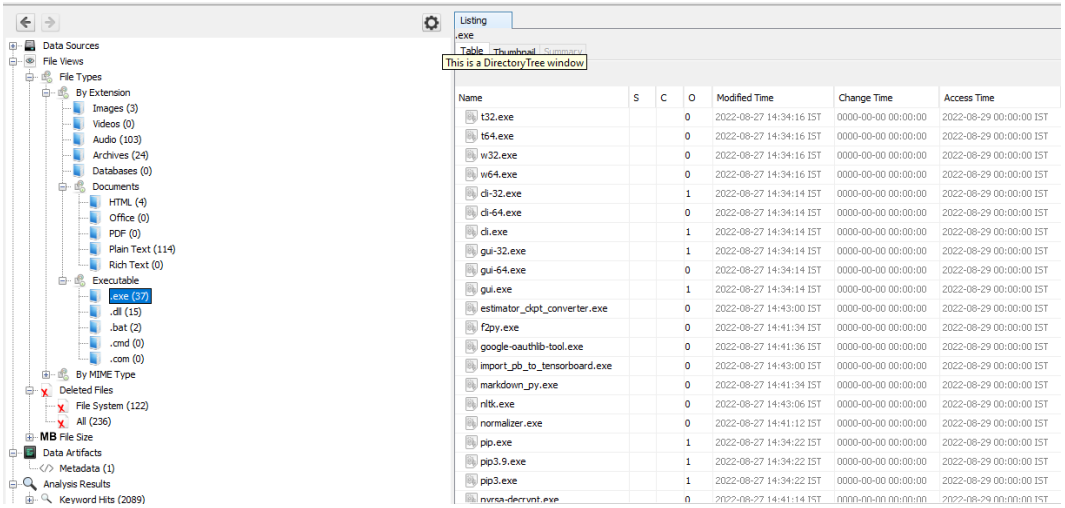
b) OFFICE



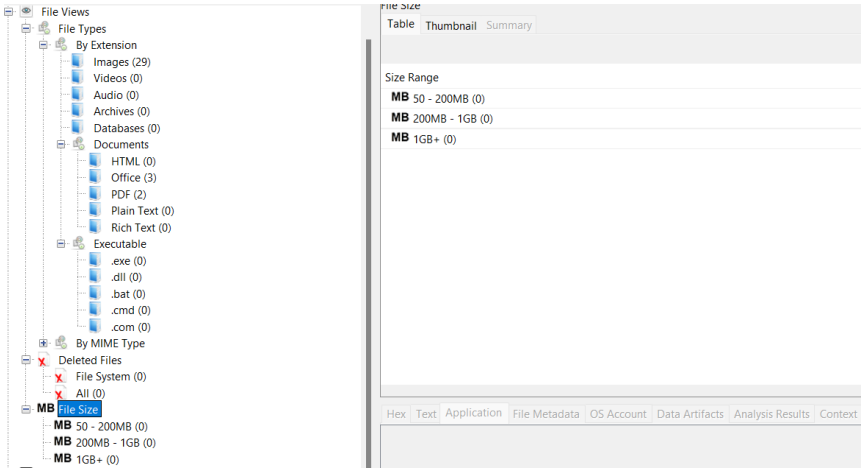
c) PDF



d) .exe

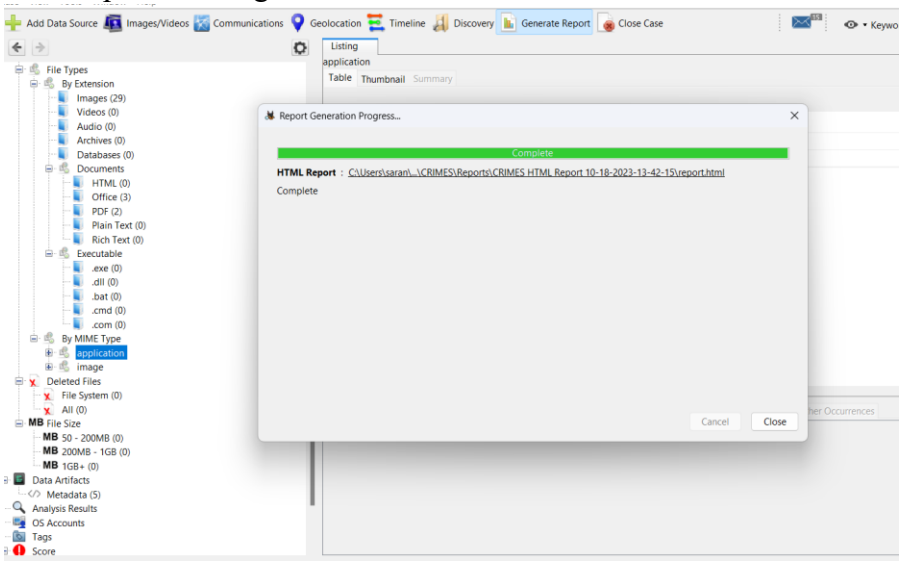


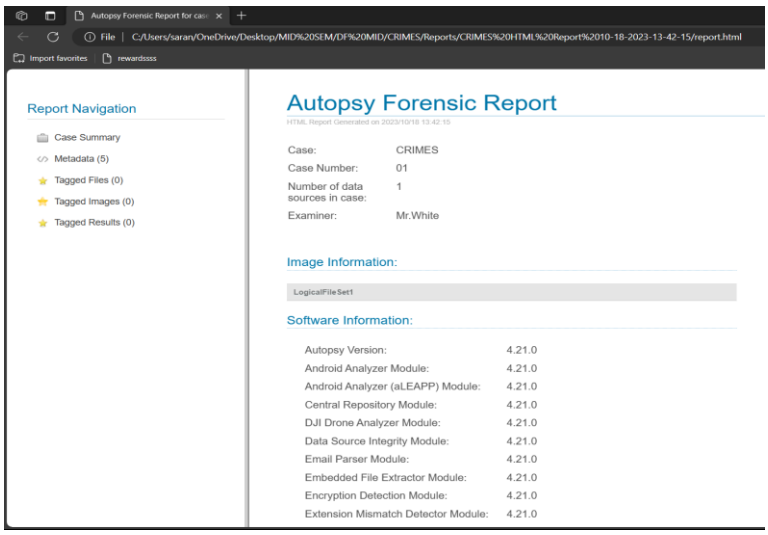
e) File Size



4. Final Report

Final report can be generated in HTML form.



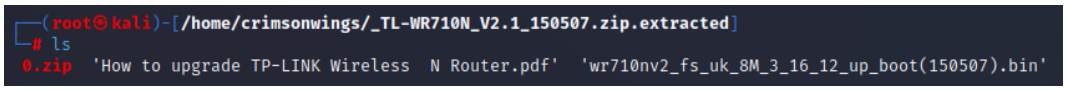


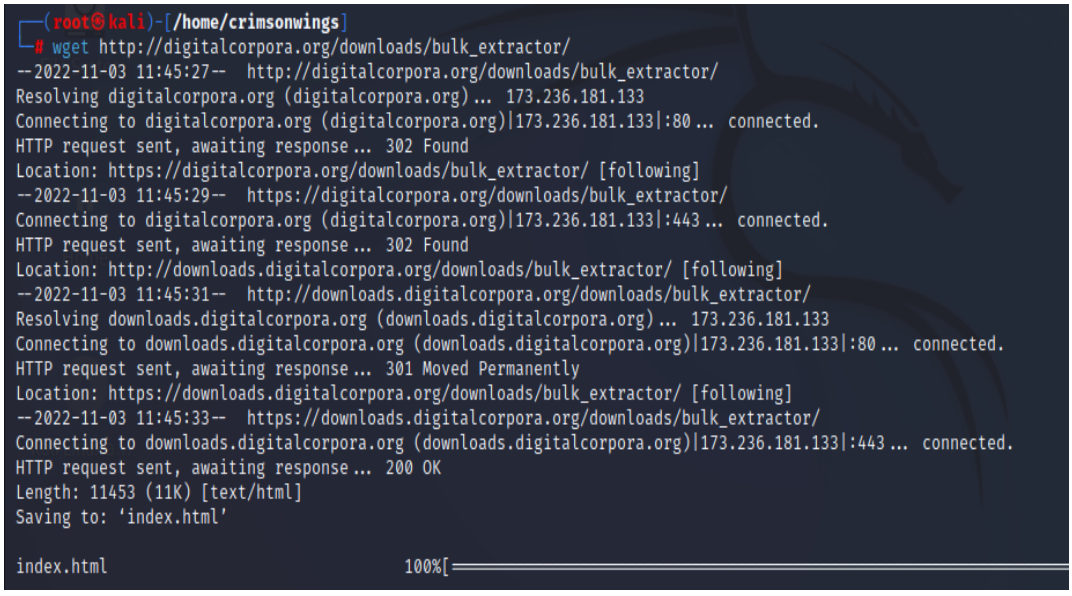
•

EXPERIMENT 8

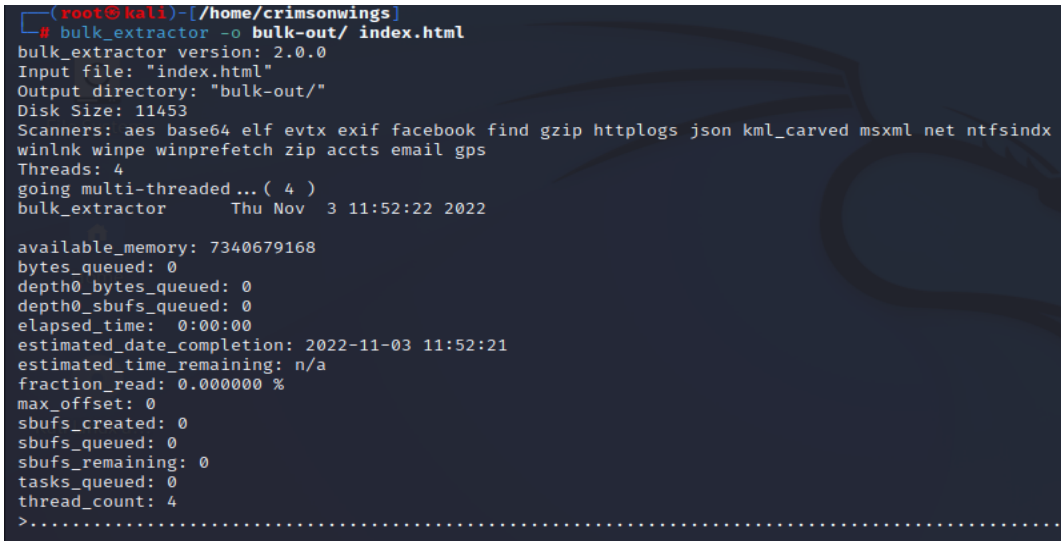
Lab Objective: Exploration of Digital Forensics Tools in Kali Linux

1.BULK WALK





2. BULK EXTRACTOR



```
┌──(root㉿kali)-[/home/kali/_TL-WR710N_V2.1_150507.zip.extracted]
└─# wget http://downloads.digitalcorpora.org/downloads/bulk_extractor
--2022-11-03 02:27:48--  http://downloads.digitalcorpora.org/downloads/bulk_extractor
Resolving downloads.digitalcorpora.org (downloads.digitalcorpora.org)... 173.236.181.133
Connecting to downloads.digitalcorpora.org (downloads.digitalcorpora.org)|173.236.181.133|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://downloads.digitalcorpora.org/downloads/bulk_extractor [following]
--2022-11-03 02:27:50--  https://downloads.digitalcorpora.org/downloads/bulk_extractor
Connecting to downloads.digitalcorpora.org (downloads.digitalcorpora.org)|173.236.181.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11453 (11K) [text/html]
Saving to: 'bulk_extractor'

bulk_extractor               100%[=========================================================>]  11.18K  --.-KB/s    in 0s

2022-11-03 02:27:52 (48.6 MB/s) - 'bulk_extractor' saved [11453/11453]
```

3. P0f

```
┌──(root㉿kali)-[/home/crimsonwings]
└─# apt install p0f
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  p0f
0 upgraded, 1 newly installed, 0 to remove and 228 not upgraded.
Need to get 81.0 kB of archives.
After this operation, 224 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 p0f amd64 3.09b-
Fetched 81.0 kB in 3s (25.4 kB/s)
Selecting previously unselected package p0f.
(Reading database ... 311160 files and directories currently installed.)
Preparing to unpack .../archives/p0f_3.09b-3_amd64.deb ...
Unpacking p0f (3.09b-3) ...
Setting up p0f (3.09b-3) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for kali-menu (2022.3.1) ...
```

```
.-[ 192.168.209.128/49846 -> 195.42.179.202/443 (syn) ]-
|
| client   = 192.168.209.128/49846
| os       = Linux 2.2.x-3.x
| dist     = 0
| params   = generic
| raw_sig  = 4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id+:0
|
`----

.-[ 192.168.209.128/49846 -> 195.42.179.202/443 (mtu) ]-
|
| client   = 192.168.209.128/49846
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----

.-[ 192.168.209.128/49846 -> 195.42.179.202/443 (syn+ack) ]-
|
| server   = 195.42.179.202/443
| os       = ???
| dist     = 0
| params   = none
| raw_sig  = 4:128+0:0:1460:mss*44,0:mss::0
|
`----

.-[ 192.168.209.128/49846 -> 195.42.179.202/443 (mtu) ]-
|
| server   = 195.42.179.202/443
| link     = Ethernet or modem
| raw_mtu  = 1500
|
`----
```

•

```
┌──(root㉿kali)-[/home/crimsonwings]
└─# p0f -i eth0 -p -o p0f.log
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[-] PROGRAM ABORT : 'p0f.log' is being used by another process.
```

4. BINWALK

Binwalk is a tool for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside of firmware images.

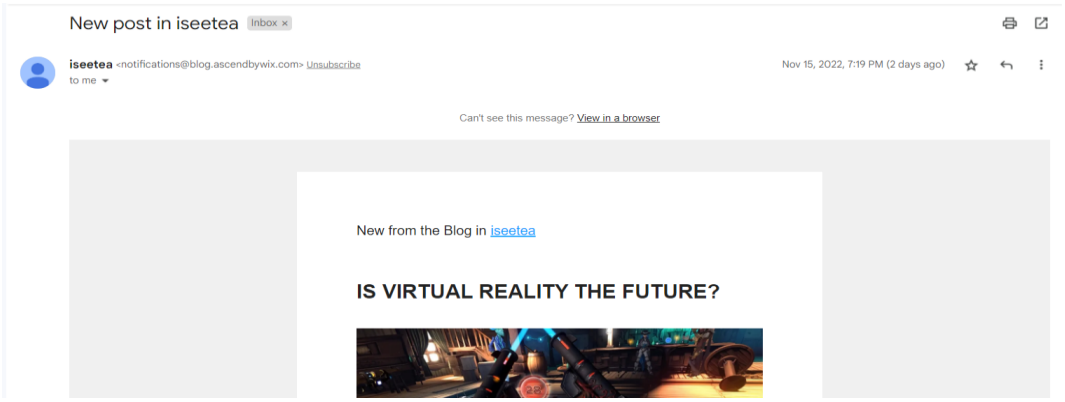
```
┌──(kali㉿kali)-[~]
└─$ sudo wget https://static.tp-link.com/res/down/soft/TL-WR710N_V2.1_150507.zip
[sudo] password for kali:
--2022-11-03 02:10:02--  https://static.tp-link.com/res/down/soft/TL-WR710N_V2.1_150507.zip
Resolving static.tp-link.com (static.tp-link.com)... 108.158.221.35, 108.158.221.38, 108.158.221.59, ...
Connecting to static.tp-link.com (static.tp-link.com)|108.158.221.35|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4044994 (3.9M) [application/x-zip-compressed]
Saving to: 'TL-WR710N_V2.1_150507.zip'

TL-WR710N_V2.1_150507.zip      100%[=========================================================>]   3.86M  3.41MB/s    in 1.1s

2022-11-03 02:10:03 (3.41 MB/s) - 'TL-WR710N_V2.1_150507.zip' saved [4044994/4044994]
```

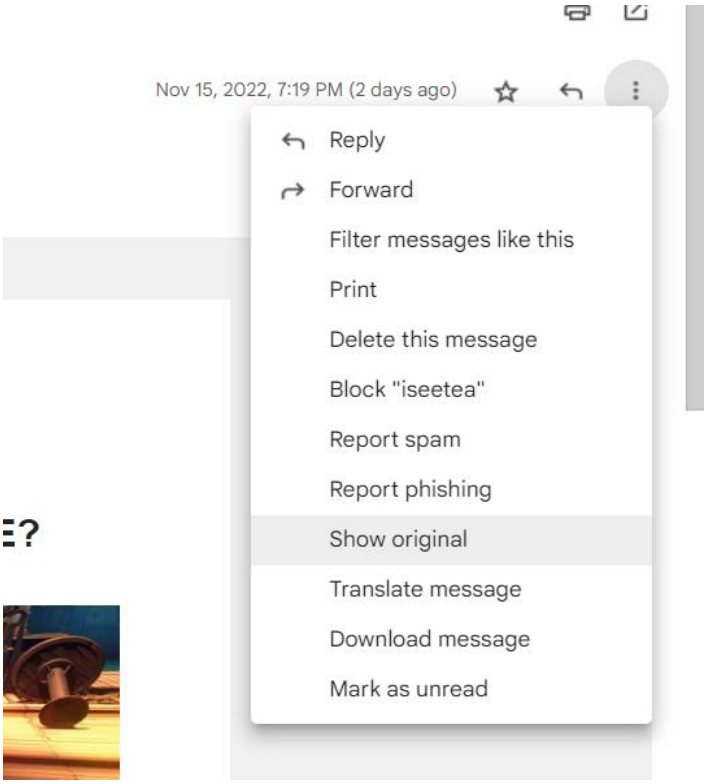
```
┌──(root㉿kali)-[/home/kali]
└─# binwalk -e --run-as=root TL-WR710N_V2.1_150507.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 3802215, uncompressed size: 82580
48, name: wr710nv2_fs_uk_8M_3_16_12_up_boot(150507).bin
3802290       0x3A04B2        Zip archive data, at least v2.0 to extract, compressed size: 242353, uncompressed size: 259952
, name: How to upgrade TP-LINK Wireless  N Router.pdf
4044972       0x3DB8AC        End of Zip archive, footer length: 22
```

```
┌──(root㉿kali)-[/home/kali]
└─# cd _TL-WR710N_V2.1_150507.zip.extracted

┌──(root㉿kali)-[/home/kali/_TL-WR710N_V2.1_150507.zip.extracted]
└─# ls
 0.zip  'How to upgrade TP-LINK Wireless  N Router.pdf'   'wr710nv2_fs_uk_8M_3_16_12_up_boot(150507).bin'

┌──(root㉿kali)-[/home/kali/_TL-WR710N_V2.1_150507.zip.extracted]
└─#
```

EXPERIMENT 9

Lab Objective : Email Forensics





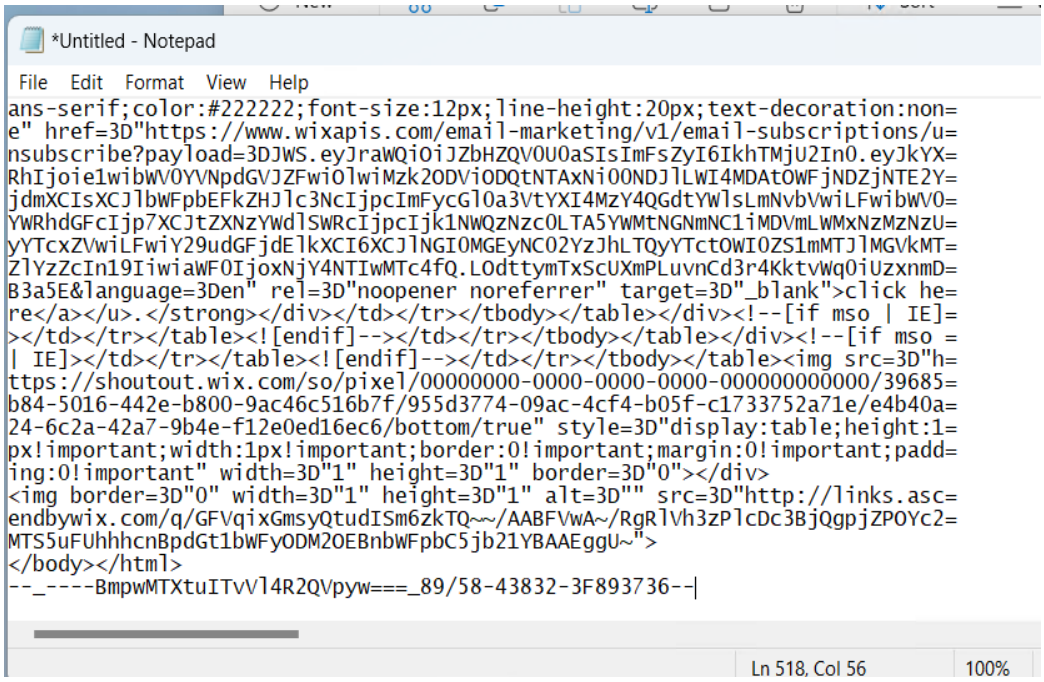
Original Message

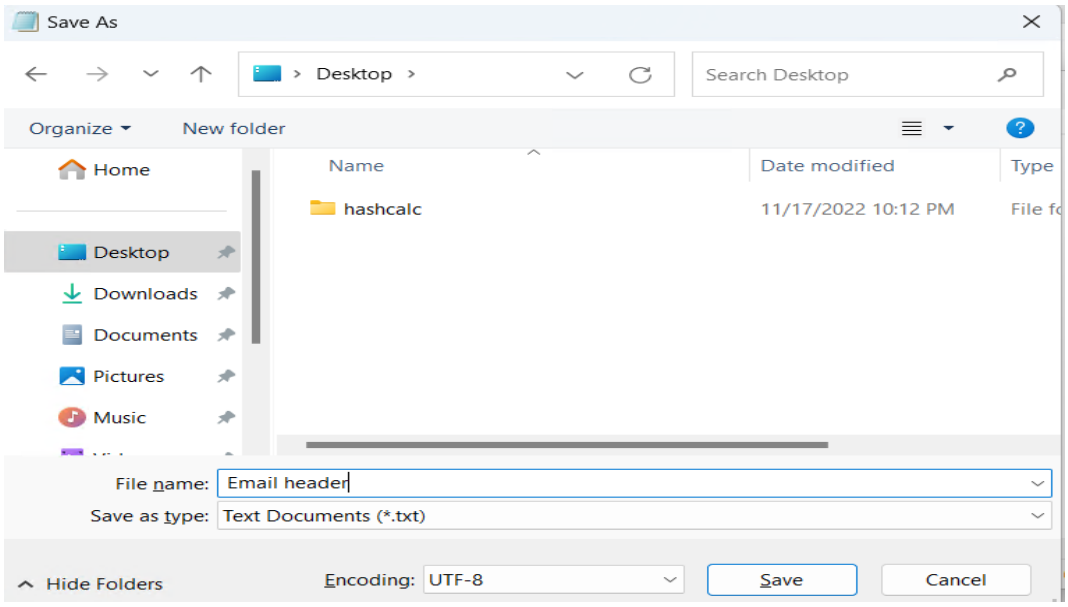
Message ID	<B9.58.43832.3F893736@jk.mta1vrest.cc.prd.sparkpost>
Created at:	Tue, Nov 15, 2022 at 7:19 PM (Delivered after 0 seconds)
From:	iseetea <notifications@blog.ascendbywix.com>
To:	Arpit Kumar <arpitkumar8368@gmail.com>
Subject:	New post in iseetea
SPF:	PASS with IP 156.70.25.18 Learn more
DKIM:	'PASS' with domain blog.ascendbywix.com Learn more
DMARC:	'PASS' Learn more

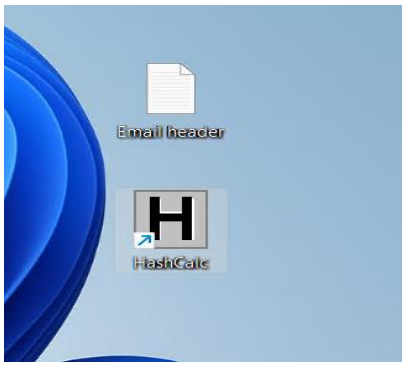
Download Original

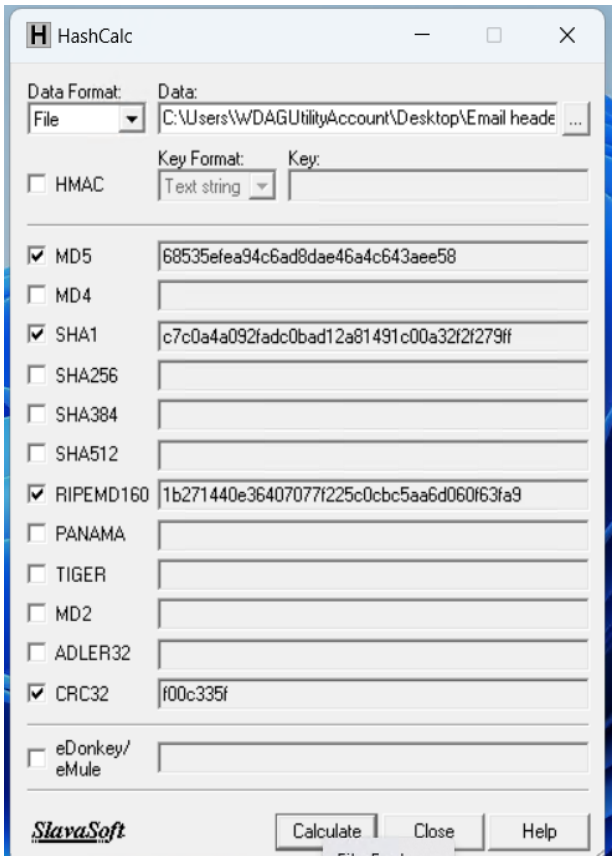
Copy to clipboard

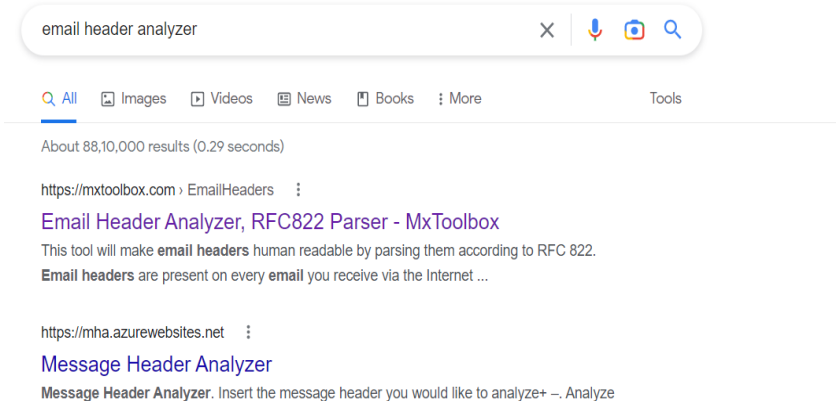
```
Delivered-To: arpitkumar8368@gmail.com
Received: by 2002:a9d:7c97:0:0:0:0:0 with SMTP id q23csp3667979otn;
        Tue, 15 Nov 2022 05:49:39 -0800 (PST)
X-Google-Smtp-Source: AA0mqf5jlgN9bcyQfpGRsqSLrxXfVHvTGBbRBPBzIOaUp0cLteWCKxvYtRf3rwOELkpxAQF5wTNz
X-Received: by 2002:a17:902:74cc:b0:17c:5b01:f227 with SMTP id f12-20020a17090274cc00b0017c5b01f227mr4203387plt.3.1668520179464;
        Tue, 15 Nov 2022 05:49:39 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1668520179; cv=none;
        d=google.com; s=arc-20160816;
        b=nXQOMKbRp+2gPJd4zRcQj3iU3WZcTHbCor3K+Jsjjx/vKr90ytWk8zJ3MBegwsc+c
         vr0UTKNLktXkJmC1wMhitnzO/hl51n2EwK+Z60XIWnZqzzwrhAgCBGDWwsxH4keAUMAl
         jn2pwePcKfPUEbD+Eq4c3+cmu2iqoPyNDr+FCnRc44as9/i1GPijBZm9u6zKOQCAC0f+
         BiLTs5qquSZ9IM9KiXkxDTS469BHiZ7vC/8R3diHVZ7KYzZGtf1OvhbiAQXBnpyLgFmT
         hb/xfY1hega7o1oGDMzCX5rHCH80naIOHtqOPWoAIHvaqjPPbkiRkpTau7rx4Fw5QBp8
         RR6w==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=feedback-id:precedence:from:list-unsubscribe:subject:mime-version
         :date:message-id:to:dkim-signature;
        bh=9ifxU5lXe/XhTWeosutVH3vVB2zIBGDdhCgD3DDKrAY=;
        b=niIpFUH0zJ+Xc+kdAjgIUZnYQKSDbfwA7D0Wx2PBwDXw2CydspyZs2jL0Hju49JVV3
         Lb469YXgw2Hgs4CzMJSNOM1D/LcSLodhMScBQVnuhh5c2pzG2BgPTdEWIWDoOIfkl3bJ
         fZsFxcmDTUKBBF/UZvI0yHFl2b94lyss+A4qOVibvqDRweDz8D4KufRA6FhtRp5PWE98
         oTBzFoeTnVawnvpxbOHLpmdxWAkmpBg7h3EfVTQoCy6zTouVpCVEa64KaweySmk8Q35C
         qkFiDwA34fIExtF6iwaAl0ABqriOOvjMRTDvHs0mZ8BadT9HYbr6Db+t6ZRE0lE70OsJ
         BgUA==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@blog.ascendbywix.com header.s=scph0420 header.b=nCRsowMU;
       spf=pass (google.com: domain of msprvs1=19318bgewwk2o=bounces-17751-295429@spmailtechno.com designates 156.70.25.18 as permitted
smtp.mailfrom="msprvs1=19318bgEwWK2O=bounces-17751-295429@spmailtechno.com";
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=ascendbywix.com
Return-Path: <msprvs1=19318bgEwWK2O=bounces-17751-295429@spmailtechno.com>
Received: from mta-70-25-18.wix-shared.com.sparkpostmail.com (mta-70-25-18.wix-shared.com.sparkpostmail.com. [156.70.25.18])
        by mx.google.com with ESMTPS id a5-20020a170902ecc500b0018694f6e90si13975658plb.529.2022.11.15.05.49.39
```






Email header
HashCalc


HashCalc
Data Format:
File
Data:
C:\Users\WDAGUtilityAccount\Desktop\Email heade
Key Format:
Text string
Key:
HMAC
MD5
68535efea94c6ad8dae46a4c643aee58
MD4
SHA1
c7c0a4a092fadc0bad12a81491c00a32f2f279ff
SHA256
SHA384
SHA512
RIPEMD160
1b271440e36407077f225c0cbc5aa6d060f63fa9
PANAMA
TIGER
MD2
ADLER32
CRC32
f00c335f
eDonkey/
eMule
SlavaSoft
Calculate
Close
Help


email header analyzer
All
Images
Videos
News
Books
More
Tools
About 88,10,000 results (0.29 seconds)
https://mxtoolbox.com › EmailHeaders
Email Header Analyzer, RFC822 Parser - MxToolbox
This tool will make email headers human readable by parsing them according to RFC 822.
Email headers are present on every email you receive via the Internet ...
https://mha.azurewebsites.net
Message Header Analyzer
Message Header Analyzer. Insert the message header you would like to analyze+ –. Analyze

MX TOOLBOX

SuperTool | MX Lookup | Blacklists | DMARC | Diagnostics | Email Health | DNS Lookup | Anal

Email Header Analyzer

Paste Header:

```
[ IE]></td></tr></table><![endif]--></td></tr></tbody></table><img src=3D"h=
ttps://shoutout.wix.com/so/pixel/00000000-0000-0000-0000-000000000000/39685=
b84-5016-442e-b800-9ac46c516b7f/955d3774-09ac-4cf4-b05f-c1733752a71e/e4b40a=
24-6c2a-42a7-9b4e-f12e0ed16ec6/bottom/true" style=3D"display:table;height:1=
px!important;width:1px!important;border:0!important;margin:0!important;padd=
ing:0!important" width=3D"1" height=3D"1" border=3D"0"></div>
<img border=3D"0" width=3D"1" height=3D"1" alt=3D"" src=3D"http://links.asc=
endbywix.com/q/GFVqixGmsyQtudISm6zkTQ~~/AABFVwA~/RgRlVh3zPlcDc3BjQgpjZPOYc2=
MTS5uFUhhhcnBpdGt1bWFyODM2OEBnbWFpbC5jb21YBAAEggU~">
</body></html>
--_----BmpwMTXtuITvVI4R2QVpyw===_89/58-43832-3F893736--
```

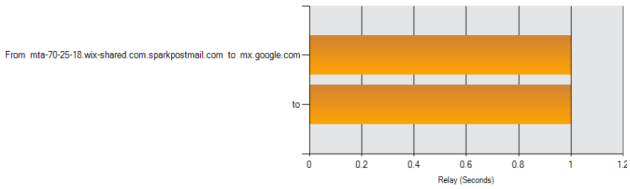
Analyze Header

Delivery Information

- DMARC Compliant
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Relay Information

Received Delay:	0 seconds



SPF and DKIM Information

dmarc:blog.ascendbywix.com

Show | Solve Email Delivery Problems

DMARC Record for blog.ascendbywix.com

```
No DMARC Record found for sub-domain.

Organization Domain of this sub-domain is: ascendbywix.com Inbox Receivers will apply ascendbywix.com DMARC record to mail sent from blog.ascendbywix.com

SP Tag '' found: Inbox Receivers will treat all mail sent from blog.ascendbywix.com that fails DMARC as suspicious.
```

DMARC Record for ascendbywix.com (organizational domain)

```
v=DMARC1;p=reject;rua=mailto:monitor@wixshoutout.com,mailto:wix@dmarc.postmastery.com,mailto:dmarc_agg@dmarc.everest.email;ruf=mailto:danny@wixshoutout.com,
```

spf:spmailtechno.com:156.70.25.18

Hide

```
v=spf1 exists:%{i}._spf.sparkpostmail.com ~all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	exists	%{i}._spf.sparkpostmail.com	Pass	This mechanism is used to construct an arbitrary host name that is used fo
~	all		SoftFail	Always matches. It goes at the end of your record.
	From Domain	blog.ascendbywix.com		The domain used in the From header field.
	Return Path Domain	spmailtechno.com		The domain used in the Return-Path header field.

	Test	Result
✗	SPF Alignment	Domain not found in SPF
✓	SPF Record Published	SPF Record found
✓	SPF Record Deprecated	No deprecated records found
✓	SPF Multiple Records	Less than two records found
✓	SPF Contains characters after ALL	No items after 'ALL'.
✓	SPF Syntax Check	The record is valid
✓	SPF Included Lookups	Number of included lookups is OK
✓	SPF Type PTR Check	No type PTR found

dkim:blog.ascendbywix.com:scph0420

Show

Dkim Public Record:

```
v=DKIM1;k=rsa;h=sha256;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCx0kyVU+mX21Ef3zRnHA3trLgmwUSUXgxenWtN
```

Dkim Signature:

```
v=1; a=rsa-sha256; c=relaxed/relaxed; d=blog.ascendbywix.com; s=scph0420; t=1668520179; i=@blog.ascend
```