AIM: Use the following tools to perform footprinting and reconnaissance.

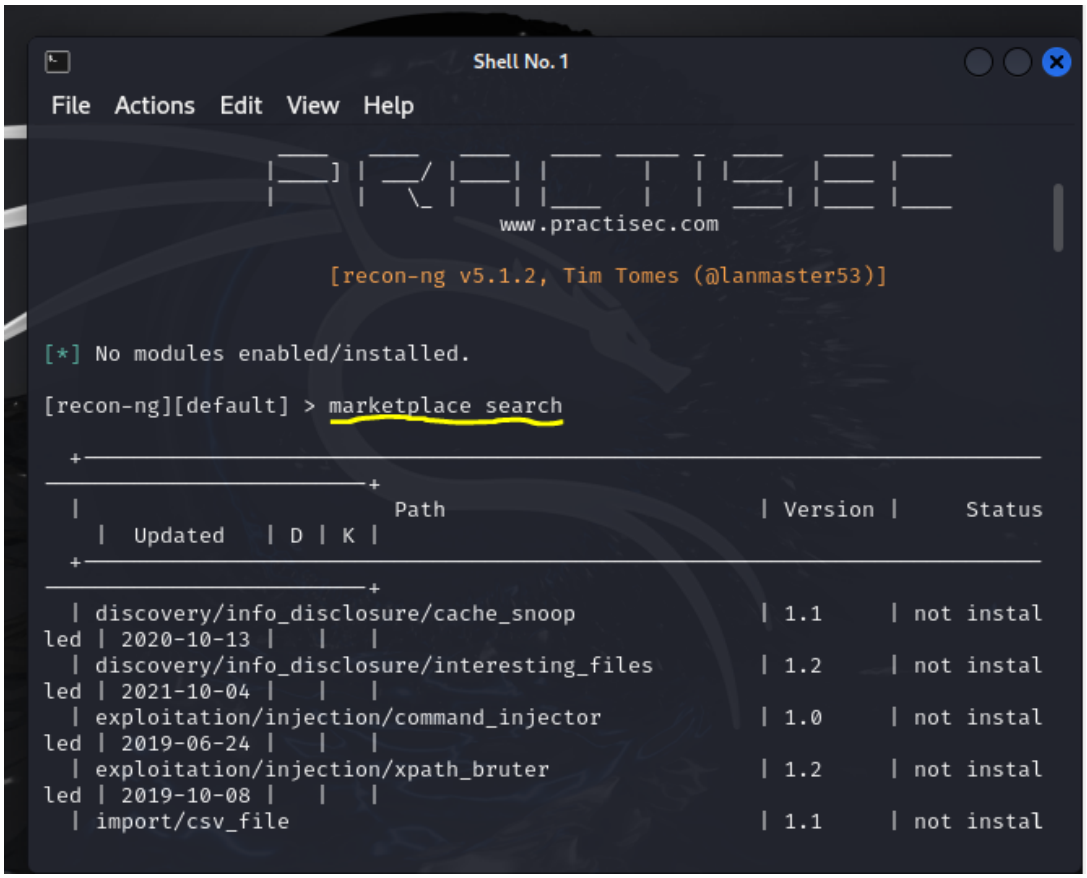
Practical-1

Aim: Recon -ng

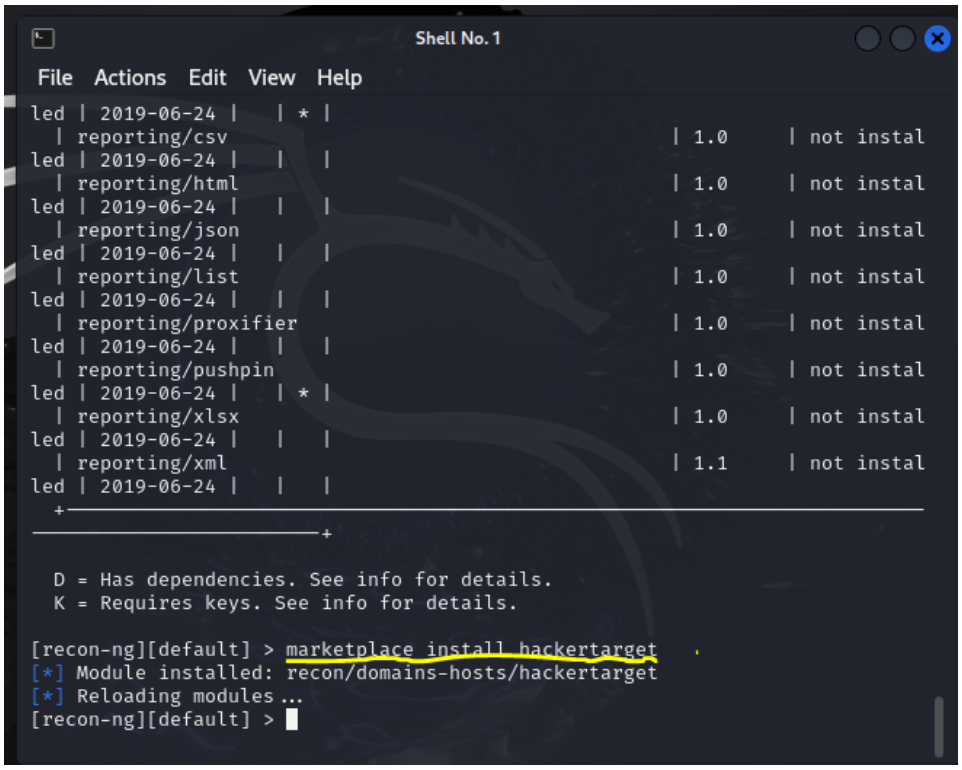
Commands:

1. marketplace search
2. --marketplace search ssl
3. --marketplace info ssltools
4. marketplace install hackertarget
5. modules load hackertarget
6. show options
7. options set SOURCE tesla.com
8. run

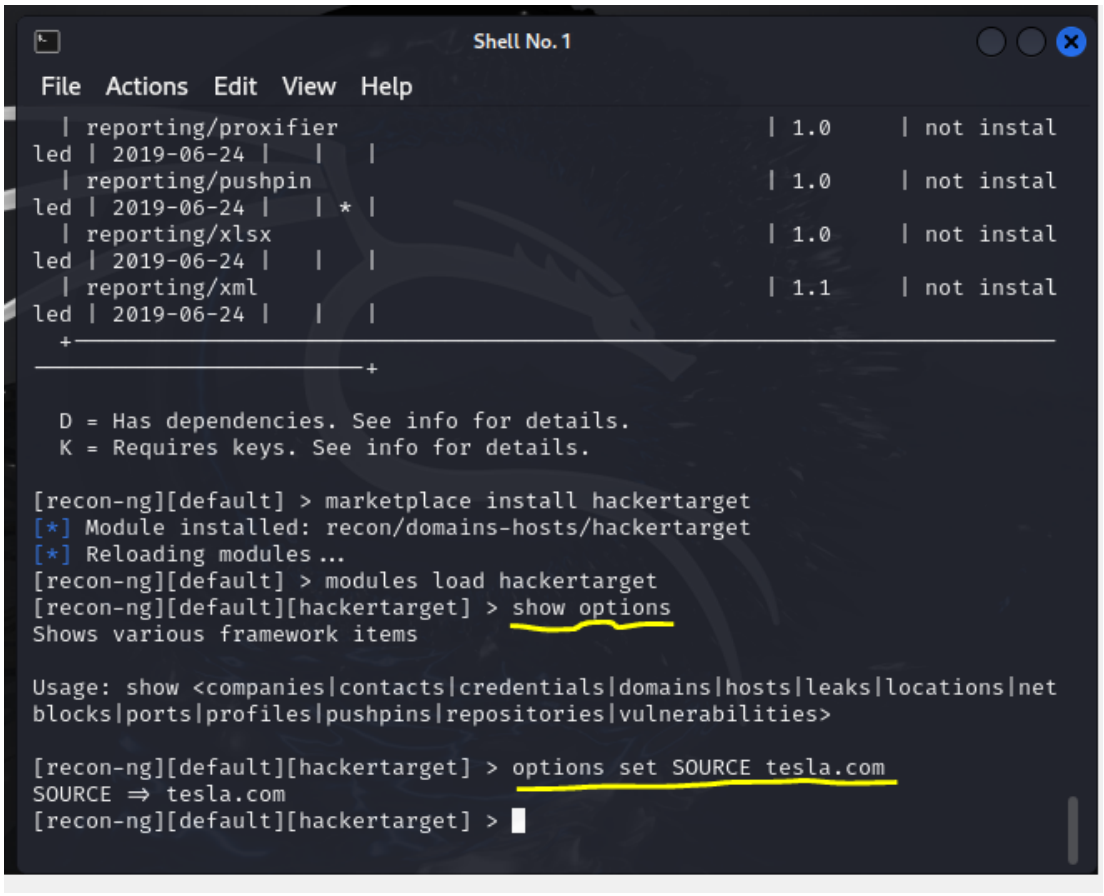
Step 1: Open Recon-ng in the Kali linux, enter below command to search the library. Command “marketplace search”



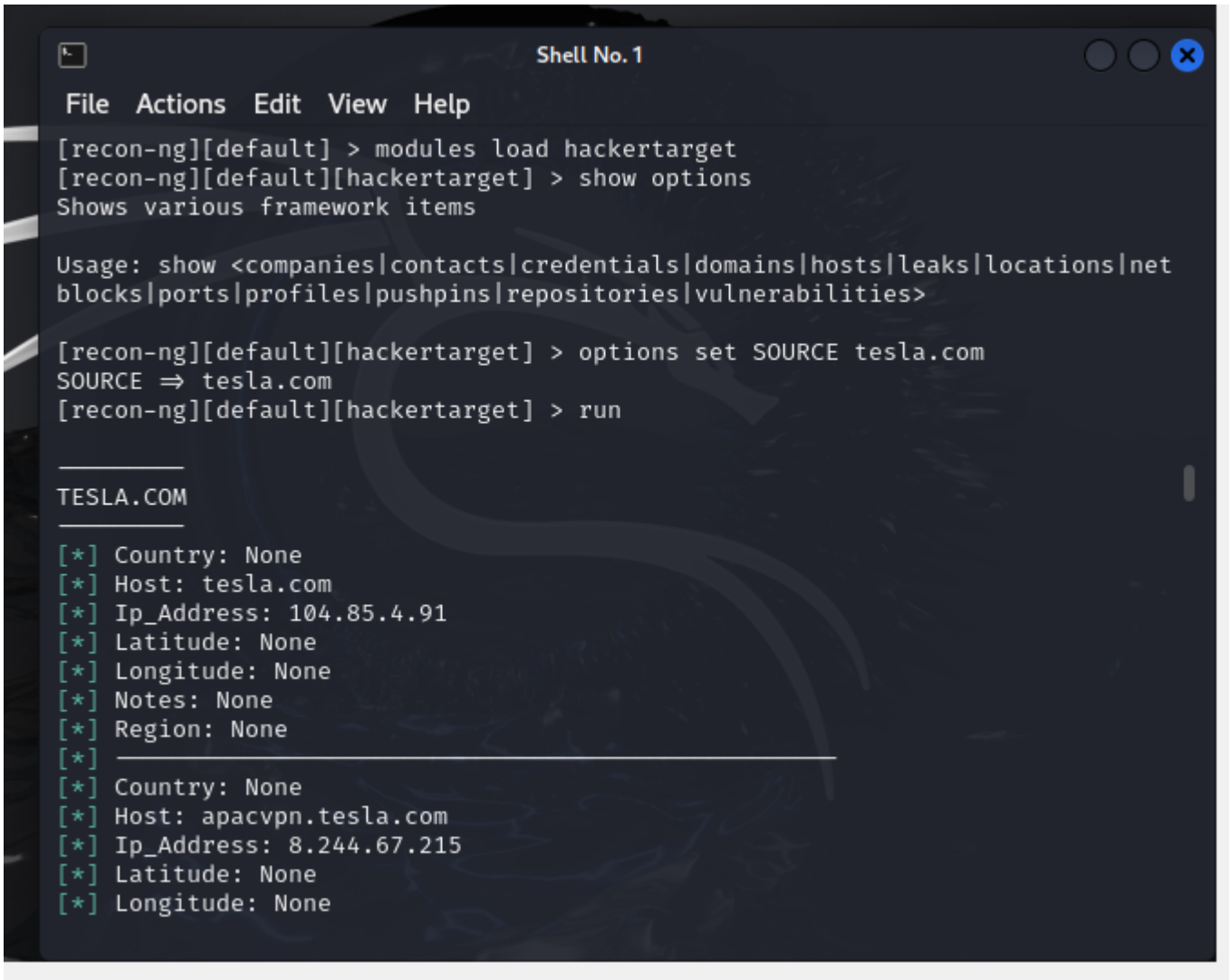
Step2: Use the command to install the package “marketplace install hackertarget”



Step 3 : Now load the package using command "modules load hackertarget" and run next command "options set SOURCE tesla.com" to set the address we desire scan.



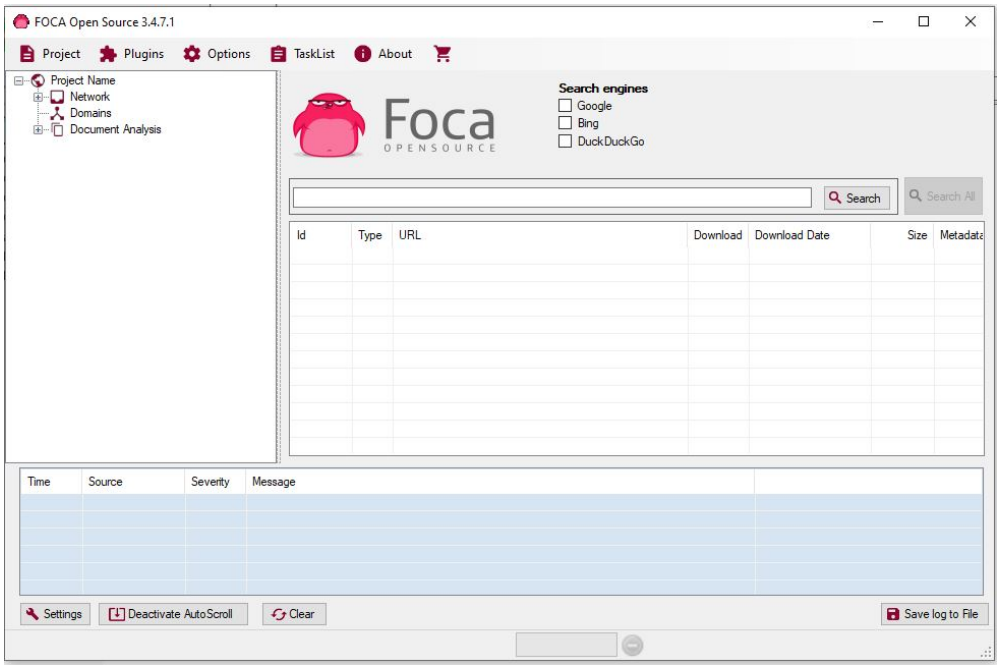
Step 6: Use command run to execute the scan.


Shell No. 1
File Actions Edit View Help
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > show options
Shows various framework items
Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|net
blocks|ports|profiles|pushpins|repositories|vulnerabilities>
[recon-ng][default][hackertarget] > options set SOURCE tesla.com
SOURCE ⇒ tesla.com
[recon-ng][default][hackertarget] > run
TESLA.COM
[*] Country: None
[*] Host: tesla.com
[*] Ip_Address: 104.85.4.91
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] Country: None
[*] Host: apacvpn.tesla.com
[*] Ip_Address: 8.244.67.215
[*] Latitude: None
[*] Longitude: None

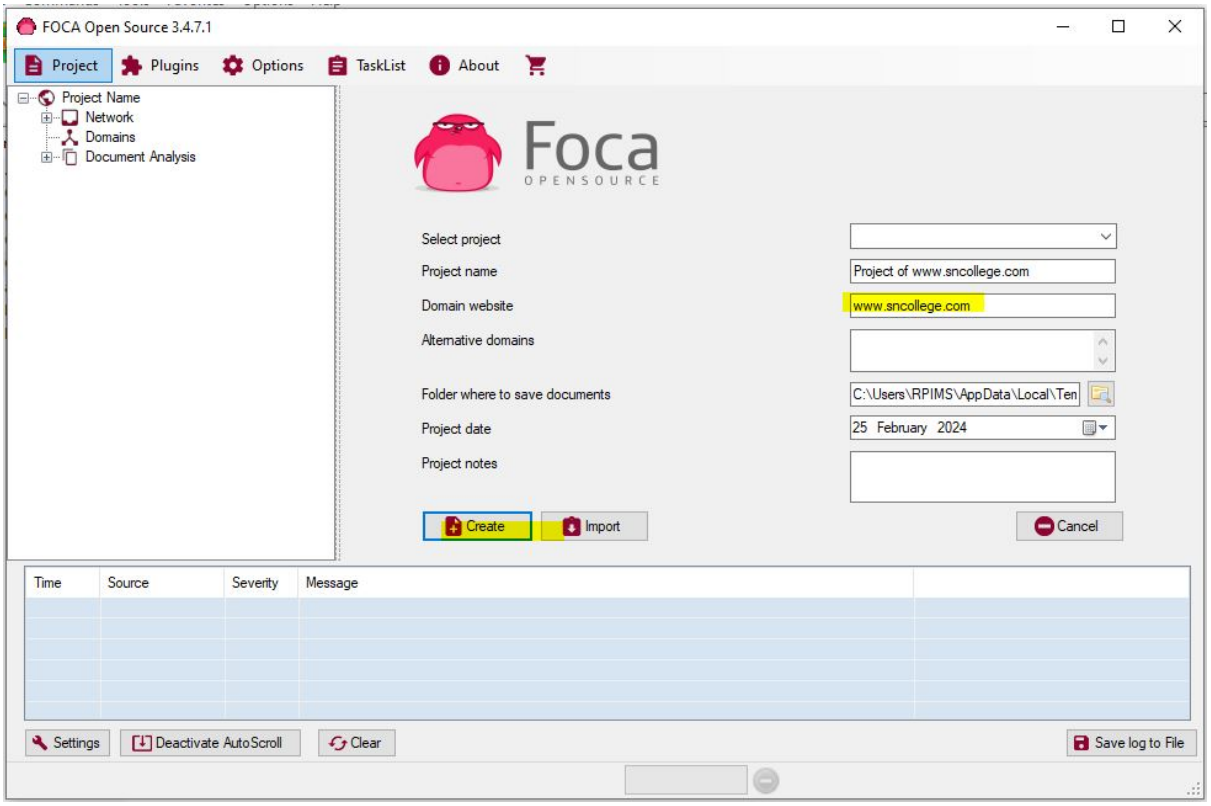
Practical 2:

Aim:- Use of **FOCA Tools**.

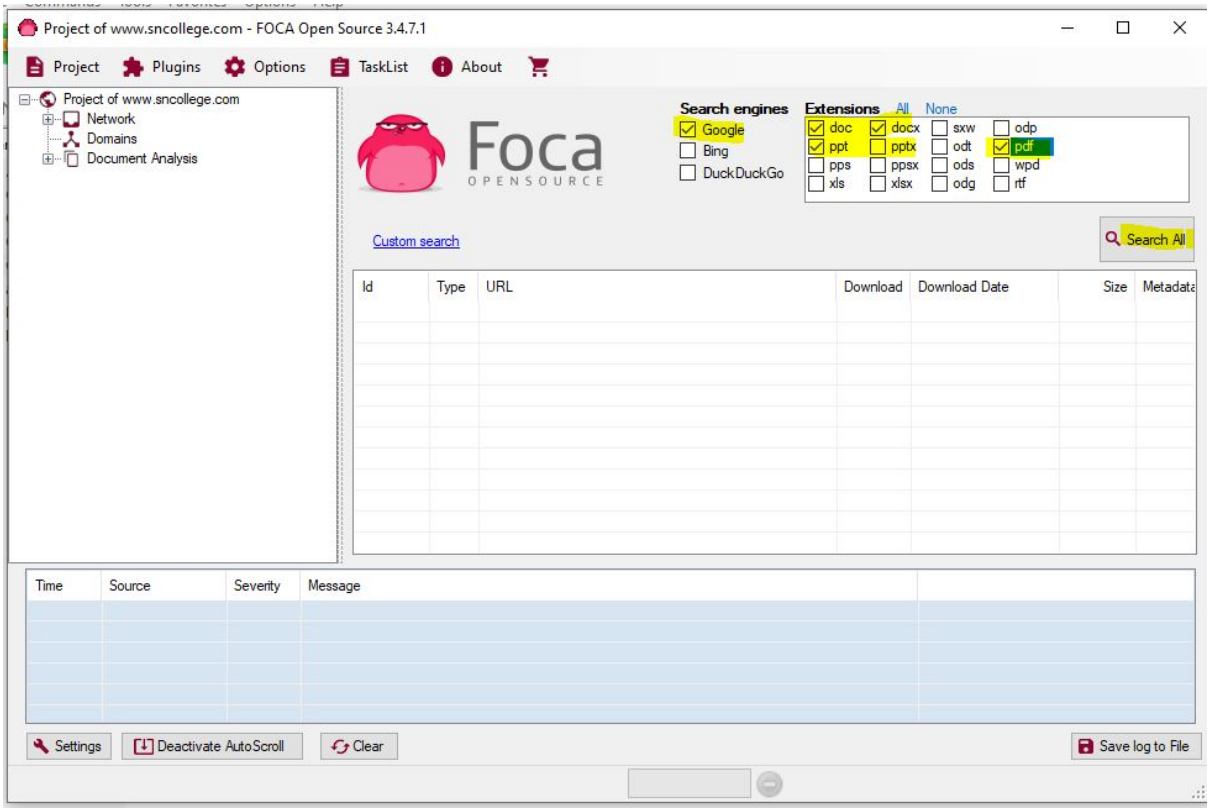
Step 1: Open FOCA Tool, goto project -> select new project.



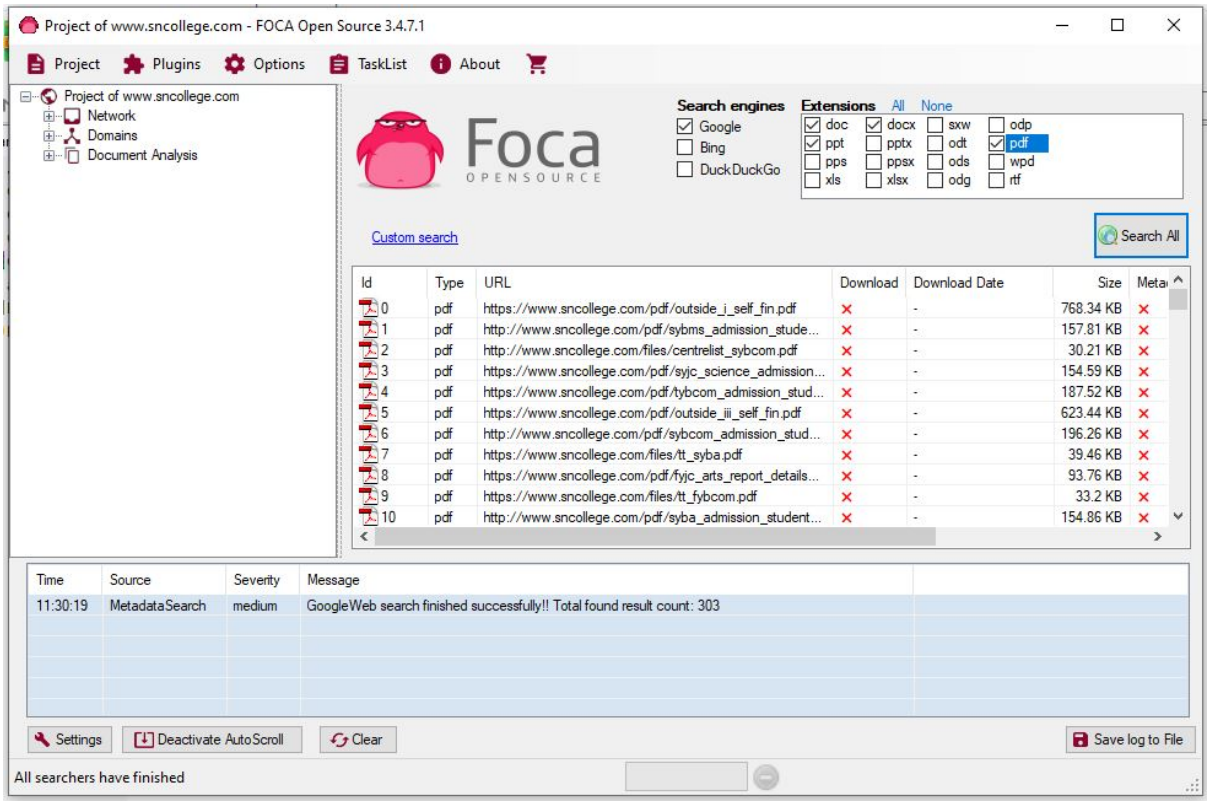
Step 2: Enter the URL then click the “Create” button.



Step 3: Select the search engine and add the extension. Click on the "Search all" button.



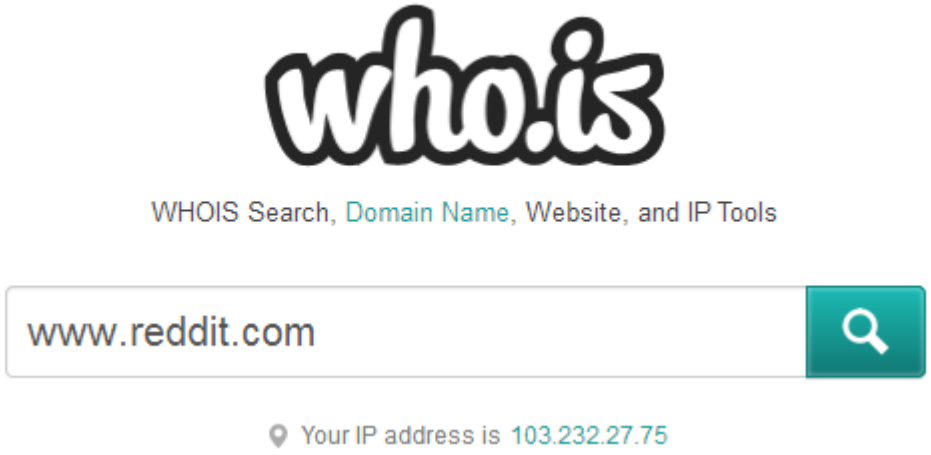
Step 4: You will find the document getting the download.



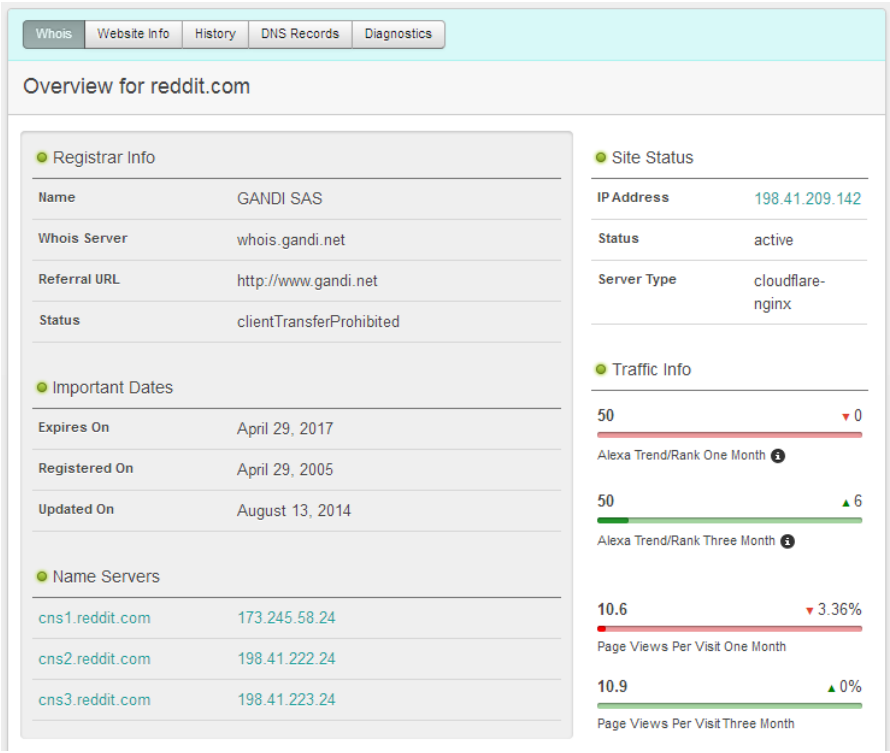
Practical 3:

Step 1: Open the WHOis website.

Step 2: Enter the website name and hit the “enter button”.



Step 3: Show you information about reddit.com in whois tab.



Whois | Website Info | History | DNS Records | Diagnostics

Overview for reddit.com

Registrar Info

Name	GANDI SAS
Whois Server	whois.gandi.net
Referral URL	http://www.gandi.net
Status	clientTransferProhibited

Important Dates

Expires On	April 29, 2017
Registered On	April 29, 2005
Updated On	August 13, 2014

Name Servers

cns1.reddit.com	173.245.58.24
cns2.reddit.com	198.41.222.24
cns3.reddit.com	198.41.223.24

Site Status

IP Address	198.41.209.142
Status	active
Server Type	cloudflare-nginx

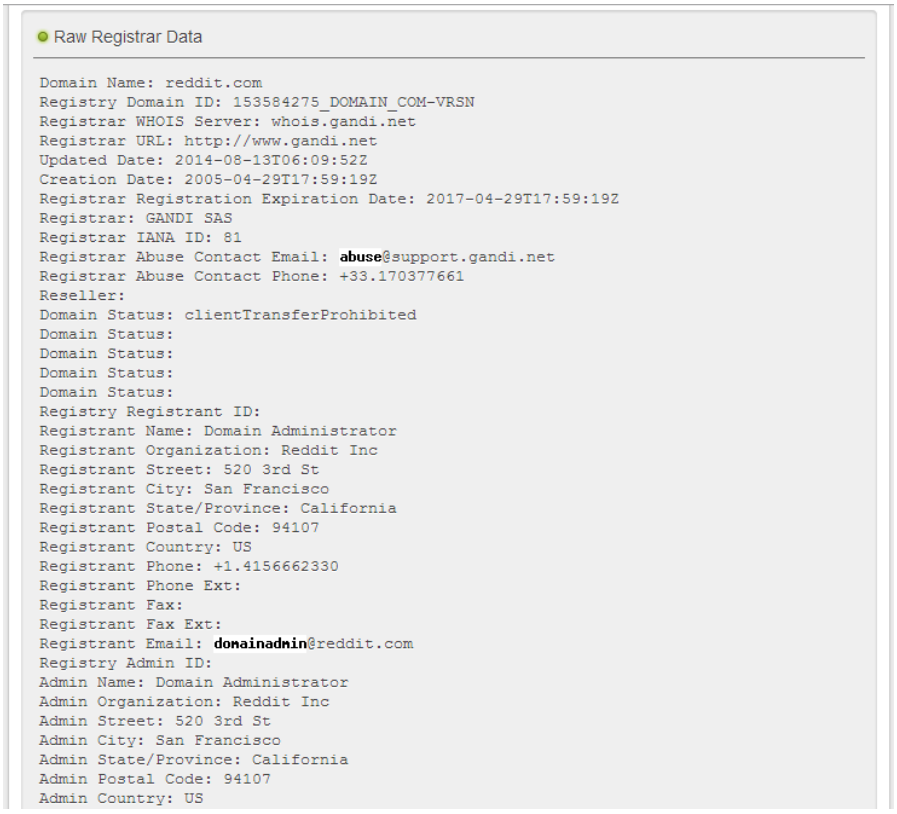
Traffic Info

50 ▼0
Alexa Trend/Rank One Month

50 ▲6
Alexa Trend/Rank Three Month

10.6 ▼3.36%
Page Views Per Visit One Month

10.9 ▲0%
Page Views Per Visit Three Month



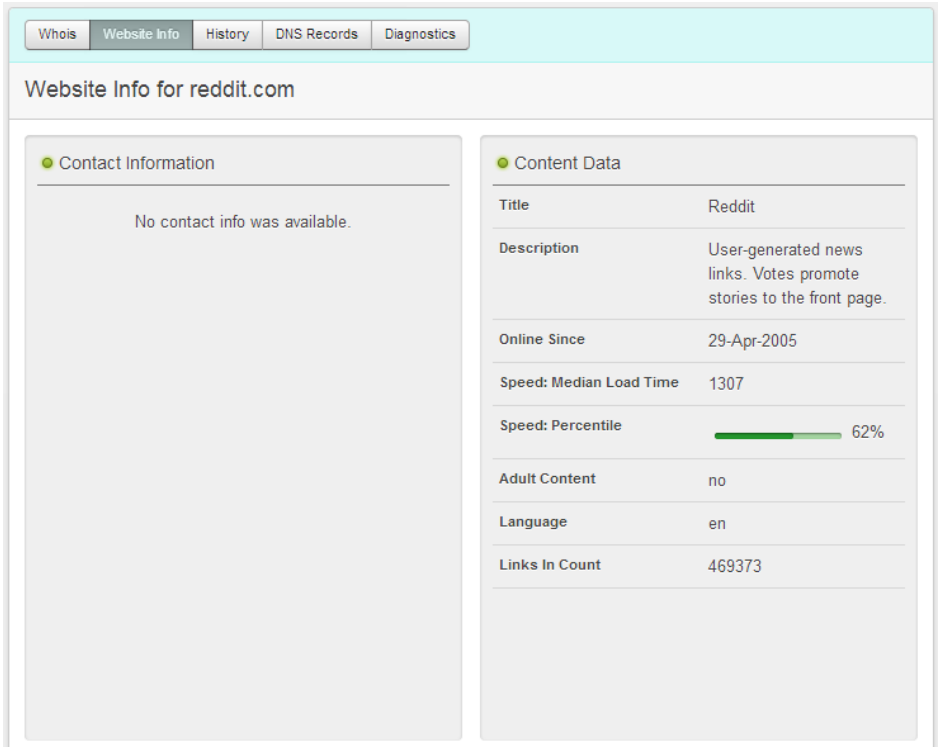
Raw Registrar Data

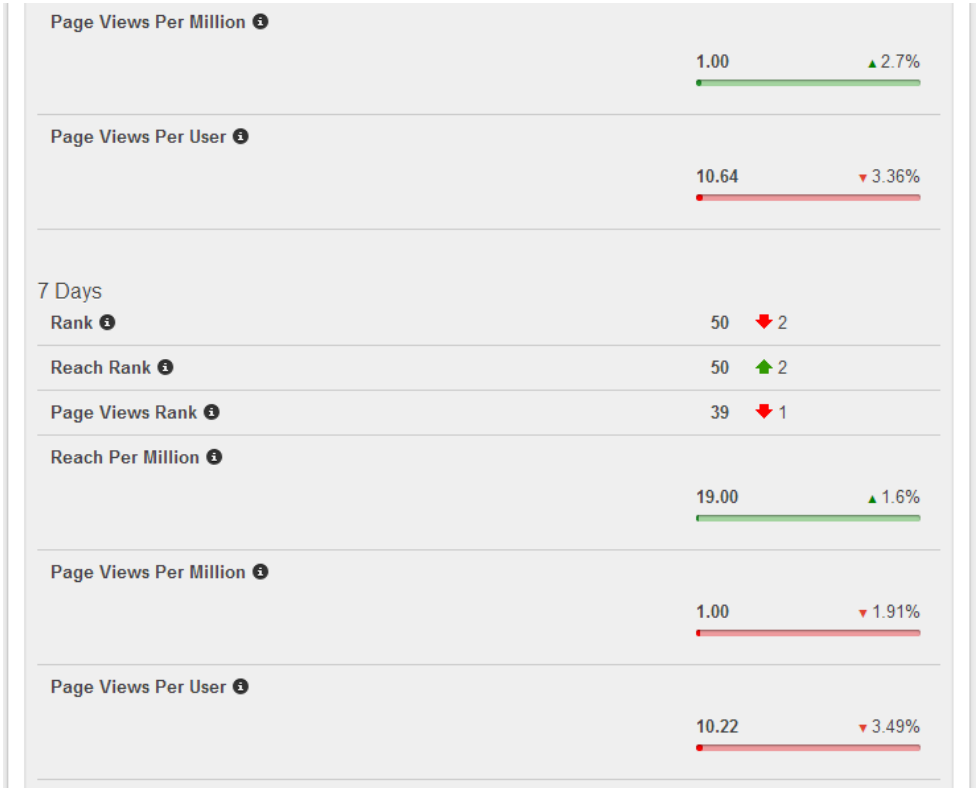
```
Domain Name: reddit.com
Registry Domain ID: 153584275_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2014-08-13T06:09:52Z
Creation Date: 2005-04-29T17:59:19Z
Registrar Registration Expiration Date: 2017-04-29T17:59:19Z
Registrar: GANDI SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Reseller:
Domain Status: clientTransferProhibited
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Reddit Inc
Registrant Street: 520 3rd St
Registrant City: San Francisco
Registrant State/Province: California
Registrant Postal Code: 94107
Registrant Country: US
Registrant Phone: +1.4156662330
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domainadmin@reddit.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Reddit Inc
Admin Street: 520 3rd St
Admin City: San Francisco
Admin State/Province: California
Admin Postal Code: 94107
Admin Country: US
```

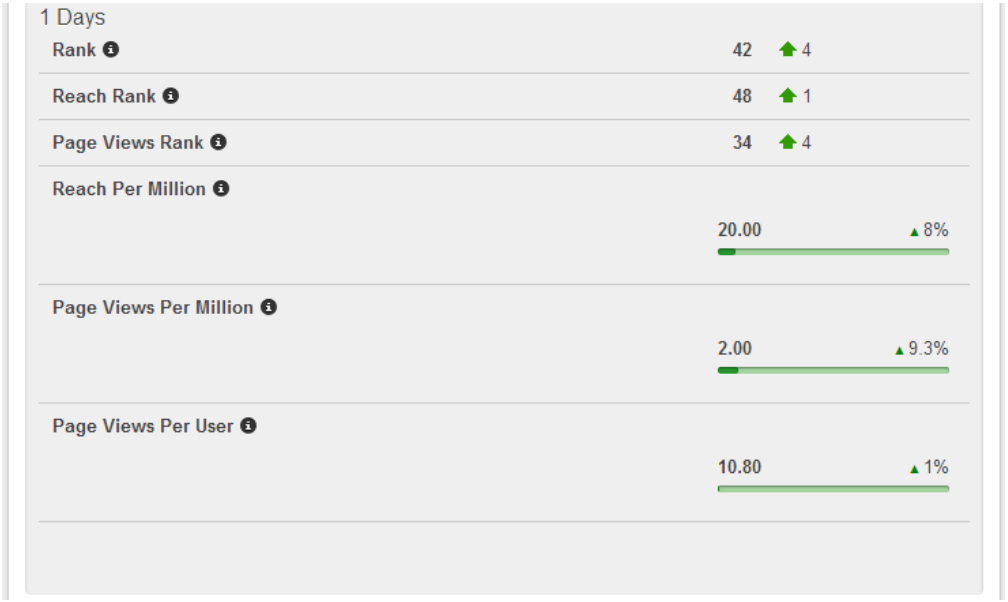
```
Admin Country: US
Admin Phone: +1.4156662330
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domainadmin@reddit.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: Reddit Inc
Tech Street: 520 3rd St
Tech City: San Francisco
Tech State/Province: California
Tech Postal Code: 94107
Tech Country: US
Tech Phone: +1.4156662330
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domainadmin@reddit.com
Name Server: CNS1.REDDIT.COM
Name Server: CNS2.REDDIT.COM
Name Server: CNS3.REDDIT.COM
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2014-09-02T06:18:01Z <<<

Reseller Email:
Reseller URL:

Personal data access and use are governed by French law, any use for
the purpose of unsolicited mass commercial advertising as well as any
mass or automated inquiries (for any intent other than the
registration or modification of a domain name) are strictly forbidden.
Copy of whole or part of our database without Gandi's endorsement is
```

```
Personal data access and use are governed by French law, any use for
the purpose of unsolicited mass commercial advertising as well as any
mass or automated inquiries (for any intent other than the
registration or modification of a domain name) are strictly forbidden.
Copy of whole or part of our database without Gandi's endorsement is
strictly forbidden.
The owner of a domain is the person specified as "Registrant Name" for
a natural person and "Registrant Organization" for a legal person.
Domain ownership disputes should be settled using ICANN's Uniform
Dispute Resolution Policy: http://www.icann.org/en/help/dndr#udrp

Information Updated: Tue, 2 Sep 2014 06:18:01 UTC
```

Step 4: Show you information about reddit.com in website information tab




Page Views Per Million
1.00
▲2.7%
Page Views Per User
10.64
▼3.36%
7 Days
Rank
50
2
Reach Rank
50
2
Page Views Rank
39
1
Reach Per Million
19.00
▲1.6%
Page Views Per Million
1.00
▼1.91%
Page Views Per User
10.22
▼3.49%


1 Days
Rank
42
4
Reach Rank
48
1
Page Views Rank
34
4
Reach Per Million
20.00
▲8%
Page Views Per Million
2.00
▲9.3%
Page Views Per User
10.80
▲1%

Subdomains

	Reach	Page Views	Page Views Per User
reddit.com	98.91%	97.78%	10.73
np.reddit.com	3.67%	0.86%	2.55
ssl.reddit.com	2.74%	0.38%	1.51
pay.reddit.com	0.17%	0.23%	15.2
fr.reddit.com	0.20%	0.23%	12.6
us.reddit.com	0.10%	0.14%	15
nl.reddit.com	0.03%	0.07%	22
OTHER		0.30%	

Step 5: Show you information about reddit.com in history tab.

Whois | Website Info | History | DNS Records | Diagnostics

Domain History Info for reddit.com

Want this archived information removed?

Old Registrar Info May 16, 2007

Name	DSTR ACQUISITION PA I, LLC DBA DOMAINBANK.COM
Whois Server	rs.domainbank.net
Referral URL	http://www.domainbank.net

Important Dates

Expires On	April 29, 2008
Registered On	April 29, 2005
Updated On	December 13, 2006

Name Servers

Registrar Info September 02, 2014

Name	GANDI SAS
Whois Server	whois.gandi.net
Referral URL	http://www.gandi.net
Status	clientTransferProhibited

Important Dates

Expires On	April 29, 2017
Registered On	April 29, 2005
Updated On	August 13, 2014

Name Servers

cns1.reddit.com	173.245.58.24
cns2.reddit.com	198.41.222.24
cns3.reddit.com	198.41.223.24

g

Old Raw Registrar Data May 16, 2007

```
The information in this whois database
is provided for the sole
purpose of assisting you in obtaining
information about domain
name registration records. This
information is available "as is,"
and we do not guarantee its accuracy.
By submitting a whois
query, you agree that you will use this
data only for lawful
purposes and that, under no
circumstances will you use this data
to: (1) enable high volume, automated,
electronic processes that
stress or load this whois database
system providing you this
information; or (2) allow,enable, or
otherwise support the
transmission of mass, unsolicited,
commercial advertising or
solicitations via facsimile, electronic
mail, or by telephone to
entitites other than your own existing
customers.  The
compilation, repackaging, dissemination
or other use of this data
is expressly prohibited without prior
written consent from this
company. We reserve the right to modify
these terms at any
time. By submitting an inquiry, you
agree to these terms of usage
and limitations of warranty.  Please
limit your queries to 10 per
minute and one connection.

   Domain Services Provided By:
      Domain Bank, support
      @domainbank.com
      http:///www.domainbank.com

Registrant:
   CONDENET INC
   Four Times Square
   New York, NY  10036
   US

   Registrar: DOMAINBANK
   Domain Name: REDDIT.COM
      Created on: 29-APR-05
      Expires on: 29-APR-08
      Last Updated on: 13-DEC-06

   Administrative Contact:
      ,    domain_admin@advancemags.com
      Advance Magazine Group
      4 Times Square
      23rd Floor
      New York, New York  10036
      US
      2122862860

   Technical Contact:
      ,    domains@advancemags.com
      Advance Magazine Group
      1201 N. Market St
      Wilmington, DE  19801
      US
      3028304630


   Domain servers in listed order:
      NS2.ADVANCEMAGS.COM
      NS3.ADVANCEMAGS.COM
      NS4.ADVANCEPUBS.NET

End of Whois Information
```

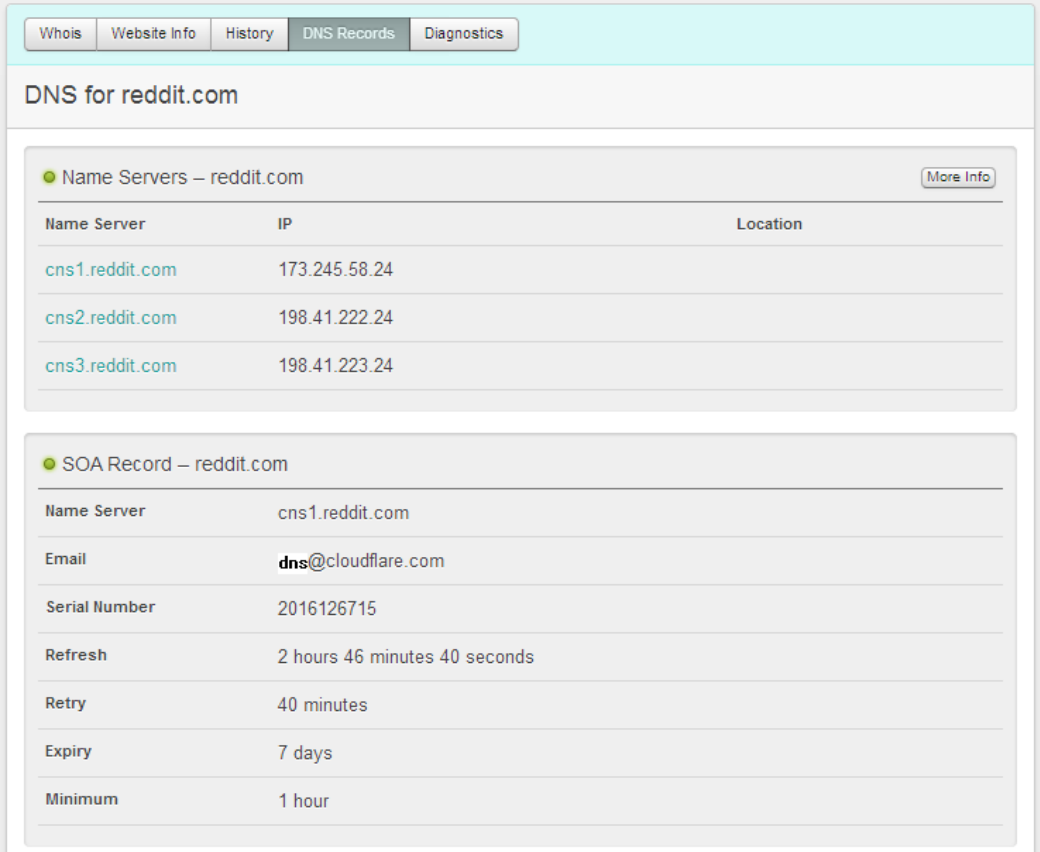
Raw Registrar Data September 02, 2014

```
Domain Name: reddit.com
Registry Domain ID:
153584275_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2014-08-13T06:09:52Z
Creation Date: 2005-04-29T17:59:19Z
Registrar Registration Expiration Date:
2017-04-29T17:59:19Z
Registrar: GANDI SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse
@support.gandi.net
Registrar Abuse Contact Phone:
+33.170377661
Reseller:
Domain Status: clientTransferProhibited
Domain Status:
Domain Status:
Domain Status:
Domain Status:
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Reddit Inc
Registrant Street: 520 3rd St
Registrant City: San Francisco
Registrant State/Province: California
Registrant Postal Code: 94107
Registrant Country: US
Registrant Phone: +1.4156662330
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: domainadmin@reddit.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Reddit Inc
Admin Street: 520 3rd St
Admin City: San Francisco
Admin State/Province: California
Admin Postal Code: 94107
Admin Country: US
Admin Phone: +1.4156662330
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: domainadmin@reddit.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: Reddit Inc
Tech Street: 520 3rd St
Tech City: San Francisco
Tech State/Province: California
Tech Postal Code: 94107
Tech Country: US
Tech Phone: +1.4156662330
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: domainadmin@reddit.com
Name Server: CNS1.REDDIT.COM
Name Server: CNS2.REDDIT.COM
Name Server: CNS3.REDDIT.COM
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
Name Server:
DNSSEC: Unsigned
URL of the ICANN WHOIS Data Problem
Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database:
2014-09-02T06:18:01Z <<<
```

```
End of Whois Information

Information Updated: Tue, 2 Sep 2014
06:18:01 UTC
```

```
Reseller Email:
Reseller URL:

Personal data access and use are
governed by French law, any use for
the purpose of unsolicited mass
commercial advertising as well as any
mass or automated inquiries (for any
intent other than the
registration or modification of a
domain name) are strictly forbidden.
Copy of whole or part of our database
without Gandi's endorsement is
strictly forbidden.
The owner of a domain is the person
specified as "Registrant Name" for
a natural person and "Registrant
Organization" for a legal person.
Domain ownership disputes should be
settled using ICANN's Uniform
Dispute Resolution Policy:
http://www.icann.org/en/help/dndr#udrp

Information Updated: Tue, 2 Sep 2014
06:18:01 UTC
```

Step 6: Show you information about reddit.com in dns records tab.



DNS Records – REDDIT.COM

Record	Type	TTL	Priority	Content
reddit.com	A	5 minutes		198.41.209.140 ()
reddit.com	A	5 minutes		198.41.209.143 ()
reddit.com	A	5 minutes		198.41.208.140 ()
reddit.com	A	5 minutes		198.41.208.142 ()
reddit.com	A	5 minutes		198.41.209.136 ()
reddit.com	A	5 minutes		198.41.209.137 ()
reddit.com	A	5 minutes		198.41.208.143 ()
reddit.com	A	5 minutes		198.41.208.138 ()
reddit.com	A	5 minutes		198.41.209.141 ()
reddit.com	A	5 minutes		198.41.208.141 ()
reddit.com	A	5 minutes		198.41.209.139 ()
reddit.com	A	5 minutes		198.41.209.138 ()
reddit.com	A	5 minutes		198.41.208.139 ()
reddit.com	A	5 minutes		198.41.209.142 ()
reddit.com	A	5 minutes		198.41.208.137 ()
reddit.com	MX	5 minutes	5	alt2.aspmx.l.google.com
reddit.com	MX	5 minutes	10	aspmx3.googlemail.com
reddit.com	MX	5 minutes	10	aspmx3.googlemail.com
reddit.com	MX	5 minutes	1	aspmx.l.google.com
reddit.com	MX	5 minutes	5	alt1.aspmx.l.google.com
reddit.com	MX	5 minutes	10	aspmx2.googlemail.com
reddit.com	NS	1 day		cns3.reddit.com
reddit.com	NS	1 day		cns2.reddit.com
reddit.com	NS	1 day		cns1.reddit.com
cns3.reddit.com	A	15 minutes		198.41.223.24 ()
cns3.reddit.com	AAAA	15 minutes		2400:cb00:2049:1::c629:df18
cns2.reddit.com	AAAA	15 minutes		2400:cb00:2049:1::c629:de18
cns2.reddit.com	A	15 minutes		198.41.222.24 ()
cns1.reddit.com	A	15 minutes		173.245.58.24 ()
cns1.reddit.com	AAAA	15 minutes		2400:cb00:2049:1::adf5:3a18
reddit.com	SOA	1 day		cns1.reddit.com. dns.cloudflare.com. 2016126715 10000 2400 604800 3600
reddit.com	TXT	5 minutes		v=spf1 include:_spf.google.com a:mail.reddit.com include:helpscoutemail.com -all
*.reddit.com	A	5 minutes		198.41.209.139 ()
*.reddit.com	A	5 minutes		198.41.208.140 ()
*.reddit.com	A	5 minutes		198.41.208.143 ()

*.reddit.com	A	5 minutes	198.41.209.136 ()
*.reddit.com	A	5 minutes	198.41.209.138 ()
*.reddit.com	A	5 minutes	198.41.209.143 ()
*.reddit.com	A	5 minutes	198.41.208.139 ()
*.reddit.com	A	5 minutes	198.41.209.140 ()
*.reddit.com	A	5 minutes	198.41.209.142 ()
*.reddit.com	A	5 minutes	198.41.208.137 ()
*.reddit.com	A	5 minutes	198.41.209.141 ()
*.reddit.com	A	5 minutes	198.41.208.141 ()
*.reddit.com	A	5 minutes	198.41.208.138 ()
*.reddit.com	A	5 minutes	198.41.209.137 ()
*.reddit.com	A	5 minutes	198.41.208.142 ()
blog.reddit.com	A	5 minutes	198.41.209.138 ()
blog.reddit.com	A	5 minutes	198.41.209.141 ()
blog.reddit.com	A	5 minutes	198.41.208.138 ()
blog.reddit.com	A	5 minutes	198.41.208.140 ()
blog.reddit.com	A	5 minutes	198.41.209.137 ()
blog.reddit.com	A	5 minutes	198.41.209.140 ()
blog.reddit.com	A	5 minutes	198.41.209.136 ()

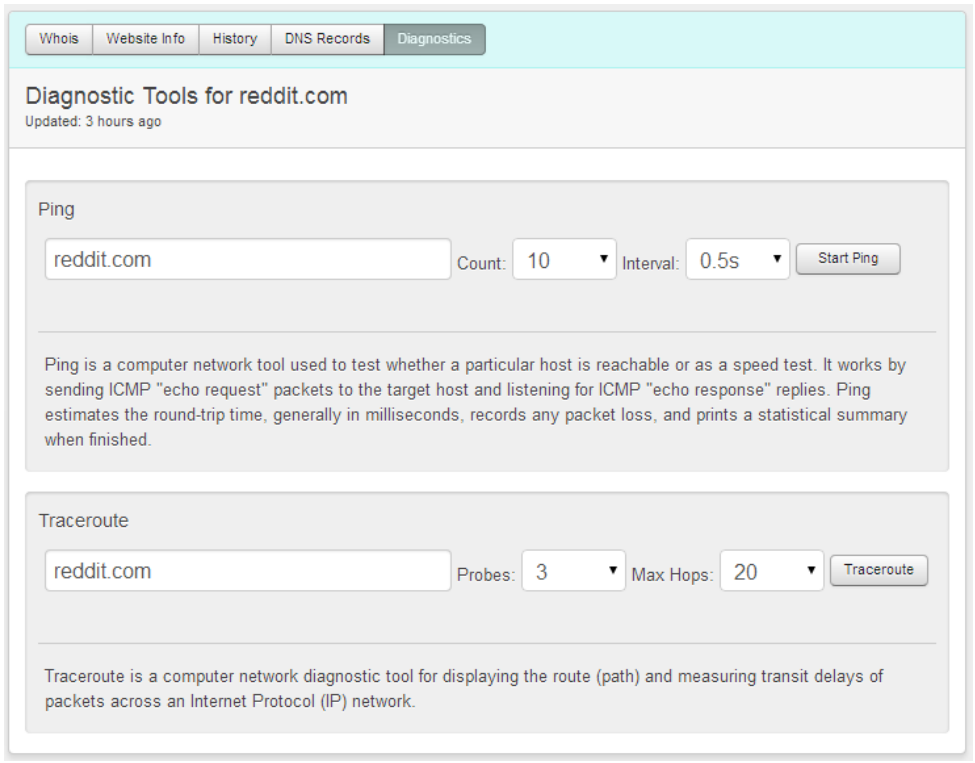
blog.reddit.com	A	5 minutes	198.41.209.136 ()
blog.reddit.com	A	5 minutes	198.41.209.143 ()
blog.reddit.com	A	5 minutes	198.41.208.139 ()
blog.reddit.com	A	5 minutes	198.41.208.137 ()
blog.reddit.com	A	5 minutes	198.41.209.139 ()
blog.reddit.com	A	5 minutes	198.41.208.143 ()
blog.reddit.com	A	5 minutes	198.41.208.141 ()
blog.reddit.com	A	5 minutes	198.41.209.142 ()
forum.reddit.com	A	5 minutes	198.41.209.137 ()
forum.reddit.com	A	5 minutes	198.41.208.137 ()
forum.reddit.com	A	5 minutes	198.41.209.142 ()
forum.reddit.com	A	5 minutes	198.41.209.139 ()
forum.reddit.com	A	5 minutes	198.41.208.139 ()
forum.reddit.com	A	5 minutes	198.41.209.141 ()
forum.reddit.com	A	5 minutes	198.41.208.143 ()
forum.reddit.com	A	5 minutes	198.41.208.140 ()
forum.reddit.com	A	5 minutes	198.41.209.138 ()
forum.reddit.com	A	5 minutes	198.41.209.136 ()
forum.reddit.com	A	5 minutes	198.41.209.140 ()

forum.reddit.com	A	5 minutes	198.41.208.138 ()
forum.reddit.com	A	5 minutes	198.41.209.143 ()
forum.reddit.com	A	5 minutes	198.41.208.141 ()
help.reddit.com	A	5 minutes	198.41.209.141 ()
help.reddit.com	A	5 minutes	198.41.208.143 ()
help.reddit.com	A	5 minutes	198.41.208.137 ()
help.reddit.com	A	5 minutes	198.41.209.142 ()
help.reddit.com	A	5 minutes	198.41.208.140 ()
help.reddit.com	A	5 minutes	198.41.209.137 ()
help.reddit.com	A	5 minutes	198.41.209.136 ()
help.reddit.com	A	5 minutes	198.41.209.139 ()
help.reddit.com	A	5 minutes	198.41.209.138 ()
help.reddit.com	A	5 minutes	198.41.209.143 ()
help.reddit.com	A	5 minutes	198.41.208.139 ()
help.reddit.com	A	5 minutes	198.41.209.140 ()
help.reddit.com	A	5 minutes	198.41.208.141 ()
help.reddit.com	A	5 minutes	198.41.208.138 ()
mail.reddit.com	A	5 minutes	174.129.203.189 (Seattle, WA, US)
test.reddit.com	A	5 minutes	198.41.209.140 ()

test.reddit.com	A	5 minutes	198.41.209.140 ()
test.reddit.com	A	5 minutes	198.41.208.139 ()
test.reddit.com	A	5 minutes	198.41.209.141 ()
test.reddit.com	A	5 minutes	198.41.209.136 ()
test.reddit.com	A	5 minutes	198.41.208.141 ()
test.reddit.com	A	5 minutes	198.41.208.140 ()
test.reddit.com	A	5 minutes	198.41.209.137 ()
test.reddit.com	A	5 minutes	198.41.209.143 ()
test.reddit.com	A	5 minutes	198.41.208.143 ()
test.reddit.com	A	5 minutes	198.41.209.139 ()
test.reddit.com	A	5 minutes	198.41.209.142 ()
test.reddit.com	A	5 minutes	198.41.209.138 ()
test.reddit.com	A	5 minutes	198.41.208.138 ()
test.reddit.com	A	5 minutes	198.41.208.137 ()
www.reddit.com	A	5 minutes	198.41.208.137 ()
www.reddit.com	A	5 minutes	198.41.209.138 ()
www.reddit.com	A	5 minutes	198.41.208.139 ()
www.reddit.com	A	5 minutes	198.41.209.140 ()
www.reddit.com	A	5 minutes	198.41.209.136 ()

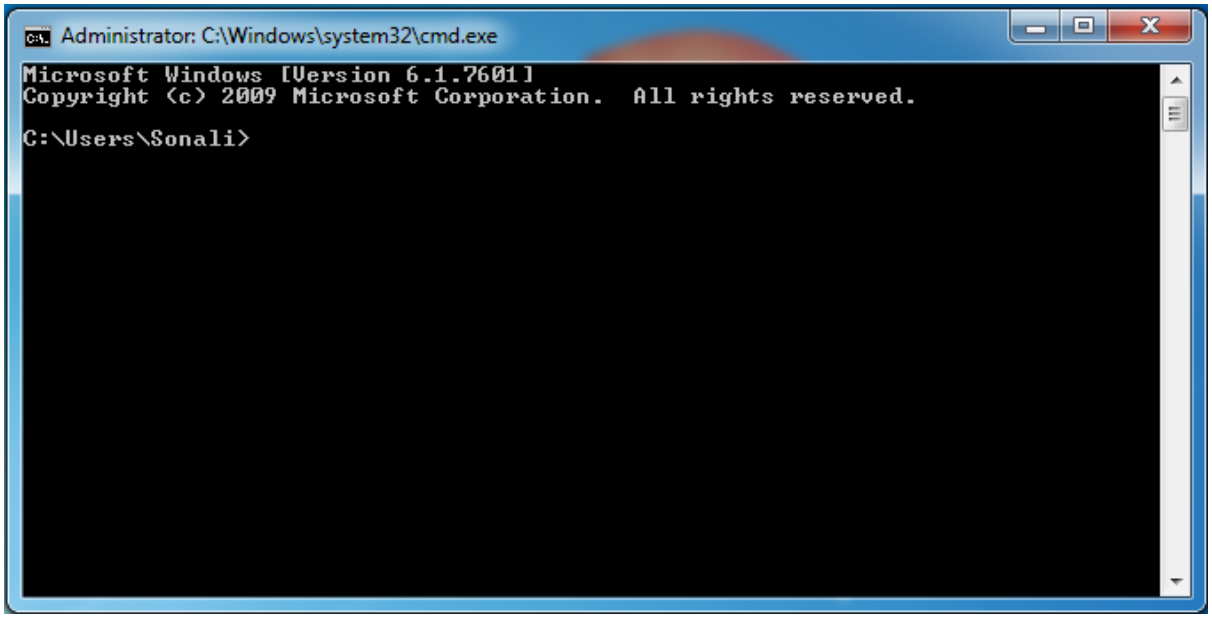
www.reddit.com	A	5 minutes	198.41.209.136 ()
www.reddit.com	A	5 minutes	198.41.208.141 ()
www.reddit.com	A	5 minutes	198.41.209.143 ()
www.reddit.com	A	5 minutes	198.41.208.140 ()
www.reddit.com	A	5 minutes	198.41.209.142 ()
www.reddit.com	A	5 minutes	198.41.208.143 ()
www.reddit.com	A	5 minutes	198.41.208.138 ()
www.reddit.com	A	5 minutes	198.41.209.141 ()
www.reddit.com	A	5 minutes	198.41.209.139 ()
www.reddit.com	A	5 minutes	198.41.209.137 ()

Step 7: Show you information about reddit.com in diagnosis tab.

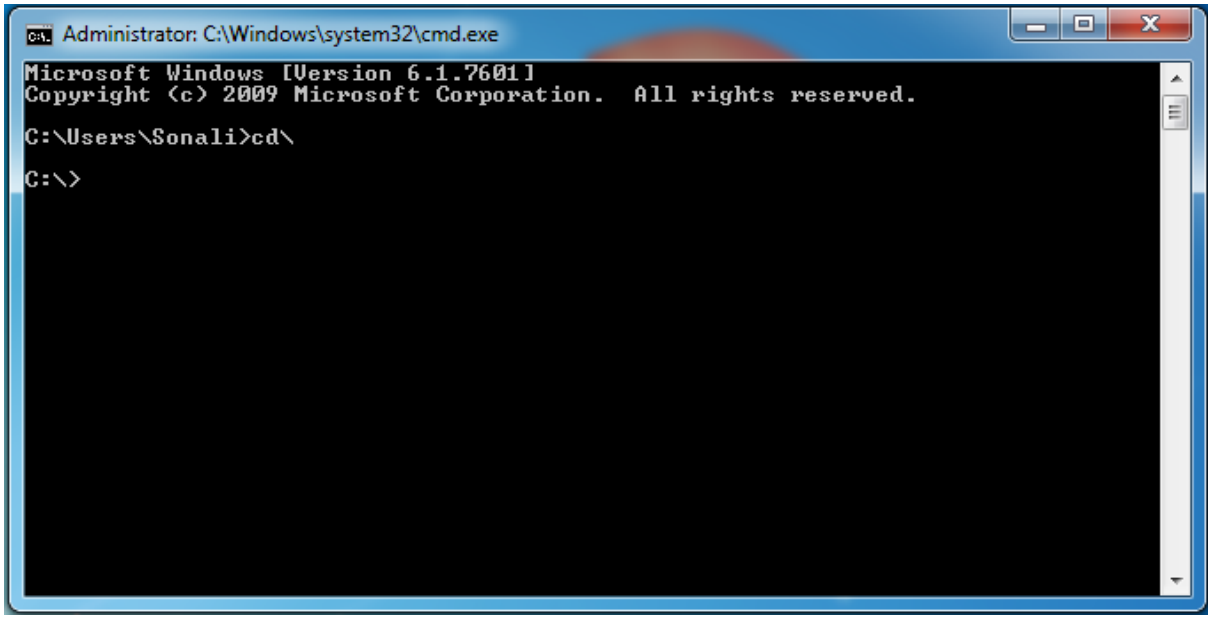


USING TRACE ROUTE

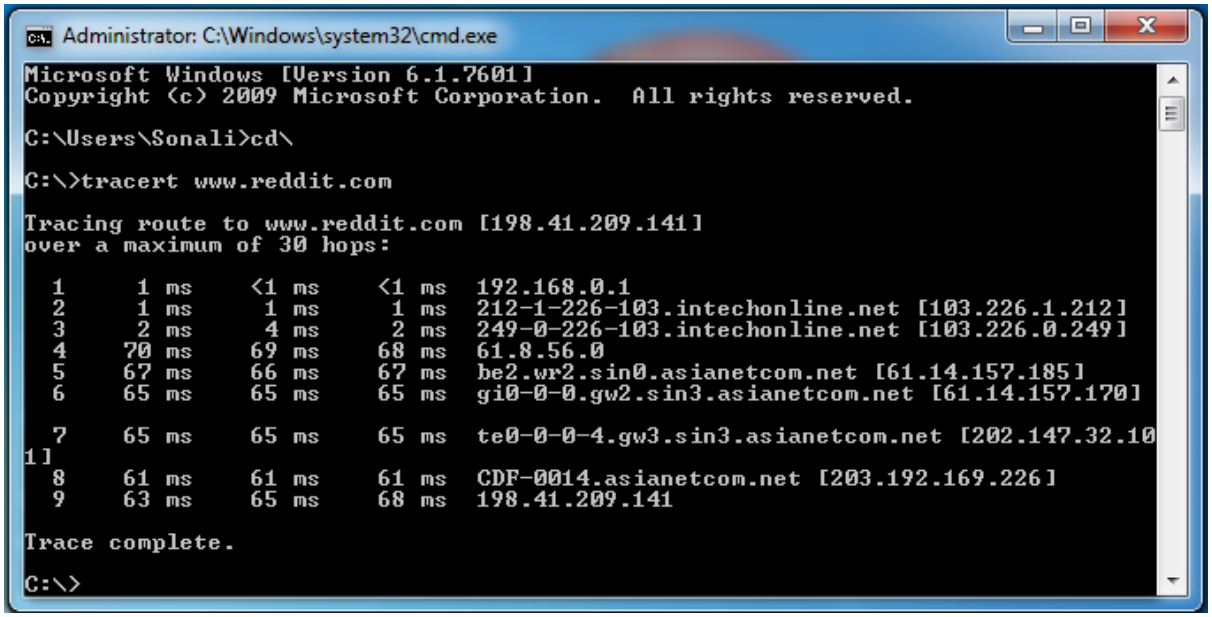
Step 1: Open cmd prompt.



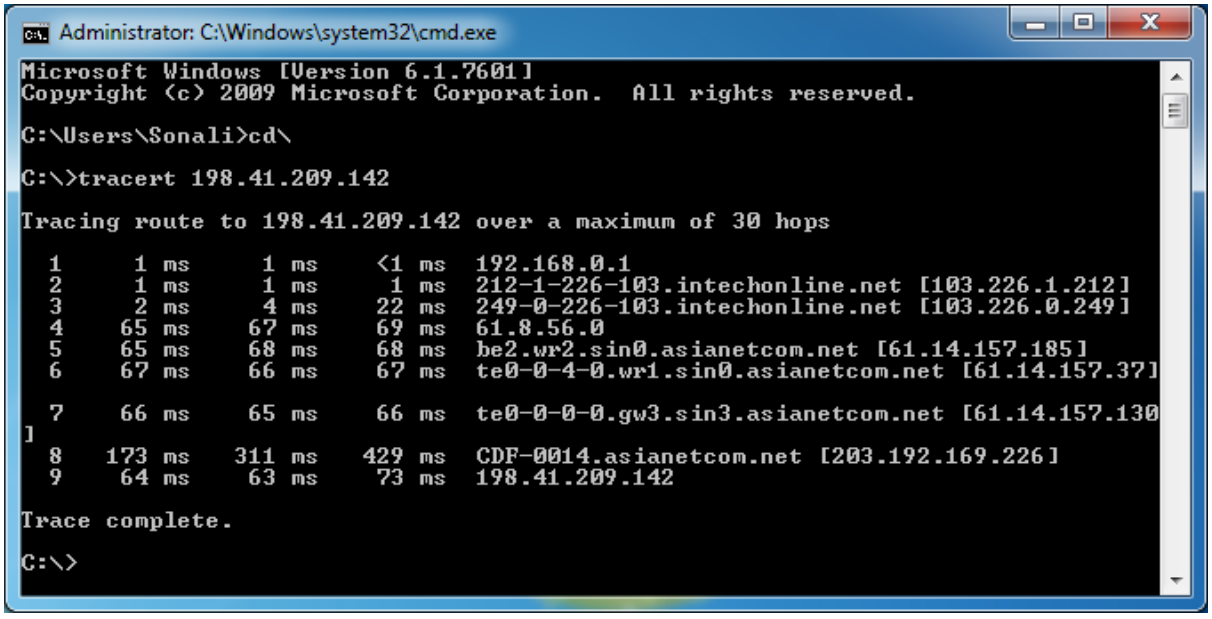
Step 2: Type cd\ and enter it will redirect to "C/directory".



Step 3: Type tracert command and type www.reddit.com and press "Enter".



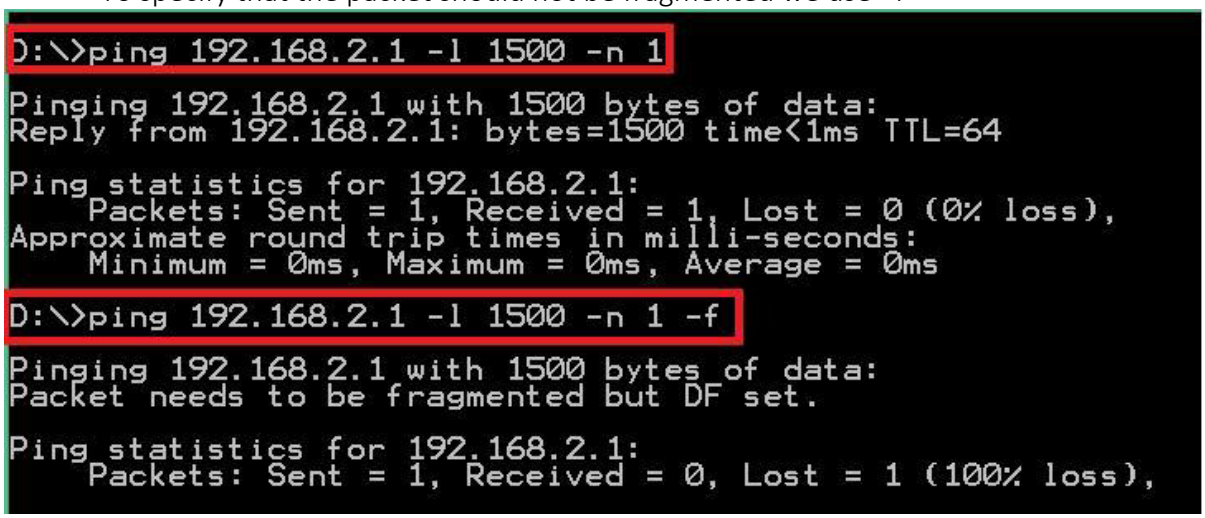
Step 4: Type tracert command and type ipaddress of reddit.com and press "Enter".



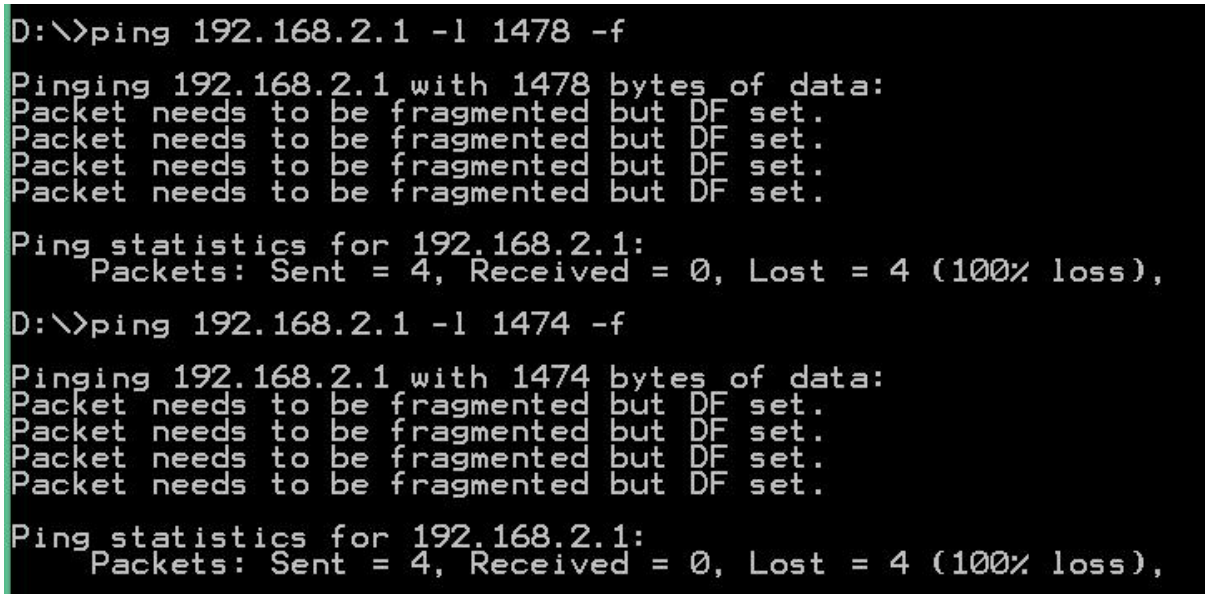
5. Ping

This practical is used to find out the MTU of the destination machine. □

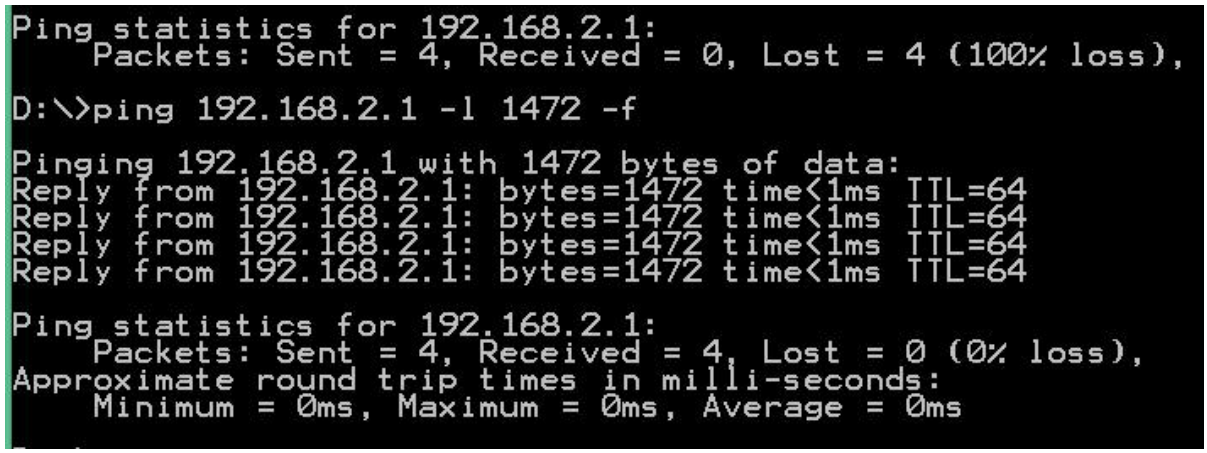
- We ping a computer using the 'p
- To specify the data length in bytes we use –lswitch □
- To specify that the packet should not be fragmented we use –f



- We now have to adjust the –lvalue till we get a reply. The border where the reply is received is said to be its MTU



- Response is received at –l1472, hence the MTU size is 1472 Bytes


Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
D:\>ping 192.168.2.1 -l 1472 -f
Pinging 192.168.2.1 with 1472 bytes of data:
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Reply from 192.168.2.1: bytes=1472 time<1ms TTL=64
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

TraceRoute using Ping

- We can perform traceroute by using the –n and –Iswitches.
- -n means number of replies to show and –Imeans obtain reply from the machine in the next hop
- Open command prompt ☐
- Ping certifiedhacker.com –n 1 –I1

```
D:\>ping certifiedhacker.com -n 1 -i 1

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 192.168.0.1: TTL expired in transit.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

- Above, the local router replies back.
- Keep on increasing the I value until the certiedhacker.com site directly replies to the ping.
- At each I value, the device in the route will reply back

```
D:\>ping certifiedhacker.com -n 1 -i 2

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Request timed out.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

D:\>ping certifiedhacker.com -n 1 -i 3

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Request timed out.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

D:\>ping certifiedhacker.com -n 1 -i 4

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 121.241.80.6: TTL expired in transit.

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

- At i=4, reply comes back from 121.241.80.6
- At i=14, the reply comes from the server hosting the certifiedhacker site

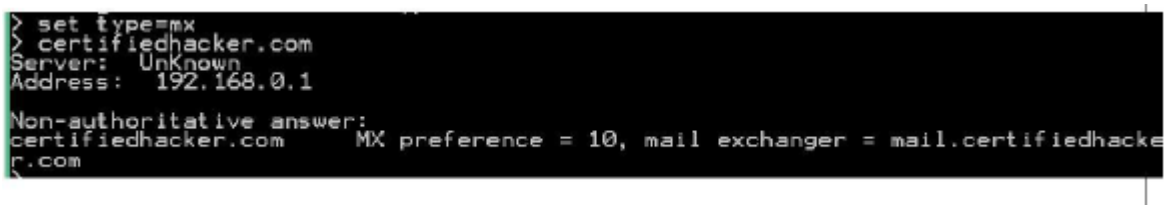
```
D:\>ping certifiedhacker.com -n 1 -i 14

Pinging certifiedhacker.com [202.75.54.101] with 32 bytes of data:
Reply from 202.75.54.101: bytes=32 time=155ms TTL=114

Ping statistics for 202.75.54.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 155ms, Maximum = 155ms, Average = 155ms
```

Node	IP
1	192.168.0.1
2	219.91.185.1
3	203.187.223.1
4	121.241.80.6
5	172.17.169.202
6	Timed Out
7	180.87.12.53
8	180.87.12.2
9	180.87.112.1
10	116.0.67.174
11	10.55.208.148
12	1.9.244.26
13	Timed Out
14	202.75.54.101 (Destination)

NSLookup

- NSLookup is used to perform DNS Foorprinting by using the windows command **nslookup**
- When we type nslookup, it shows us our current DNS Server

- To specify the DNS query type we want, we use the command
  set type = <recordname> followed by the website name on the next line
  Set type = mx Certifiedhacker.com



- We can set the **query type** as A, ANY, CNAME, MX, NS, PTR, SOA, SRV
  A Record

SOA Record

```
> set type=soa
> certifiedhacker.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
certifiedhacker.com
        primary name server = ns3.noyearlyfees.com
        responsible mail addr = hostmaster.noyearlyfees.com
        serial  = 10
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
>
```

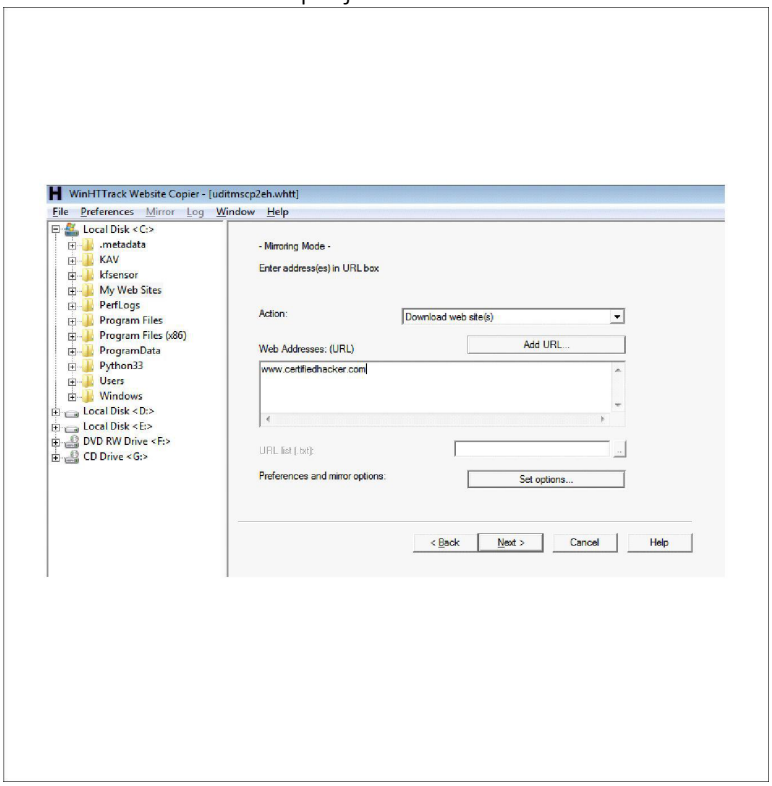
NameServer (NS) Record

```
> set type=ns
> certifiedhacker.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
certifiedhacker.com     nameserver = ns3.noyearlyfees.com
certifiedhacker.com     nameserver = ns0.noyearlyfees.com
>
```

Aim:HTTrack Website Copier

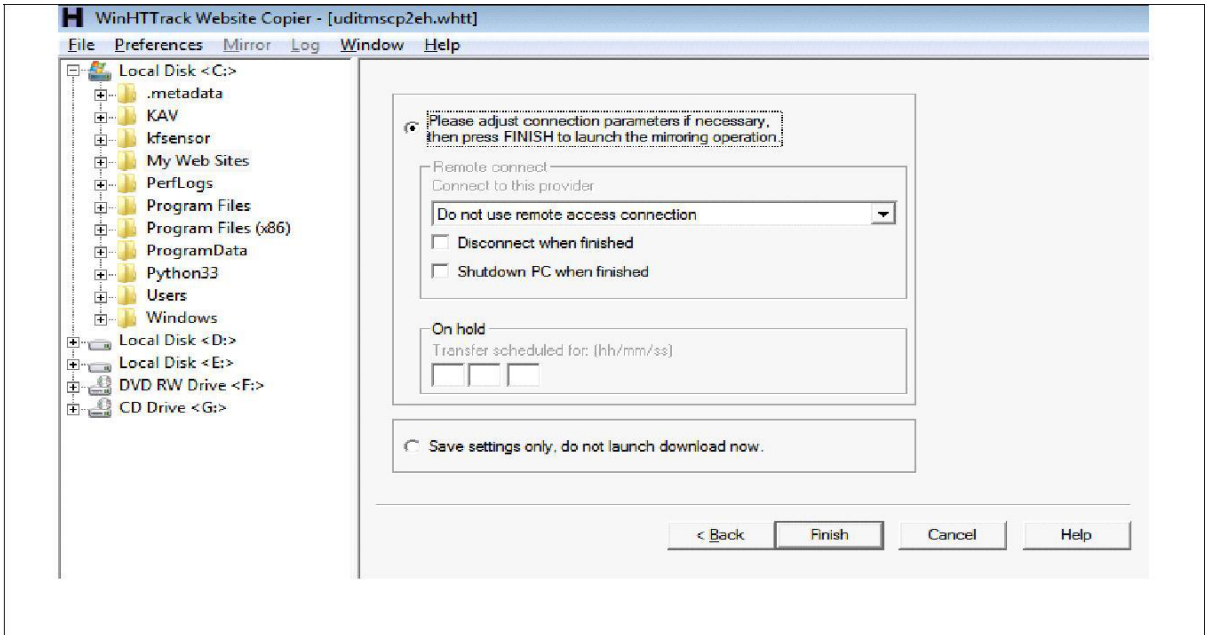
Start > Programs >

- HTTrack Website Copier
- Click on 'Next' to create Project
- Give a name to project Click on 'Next'

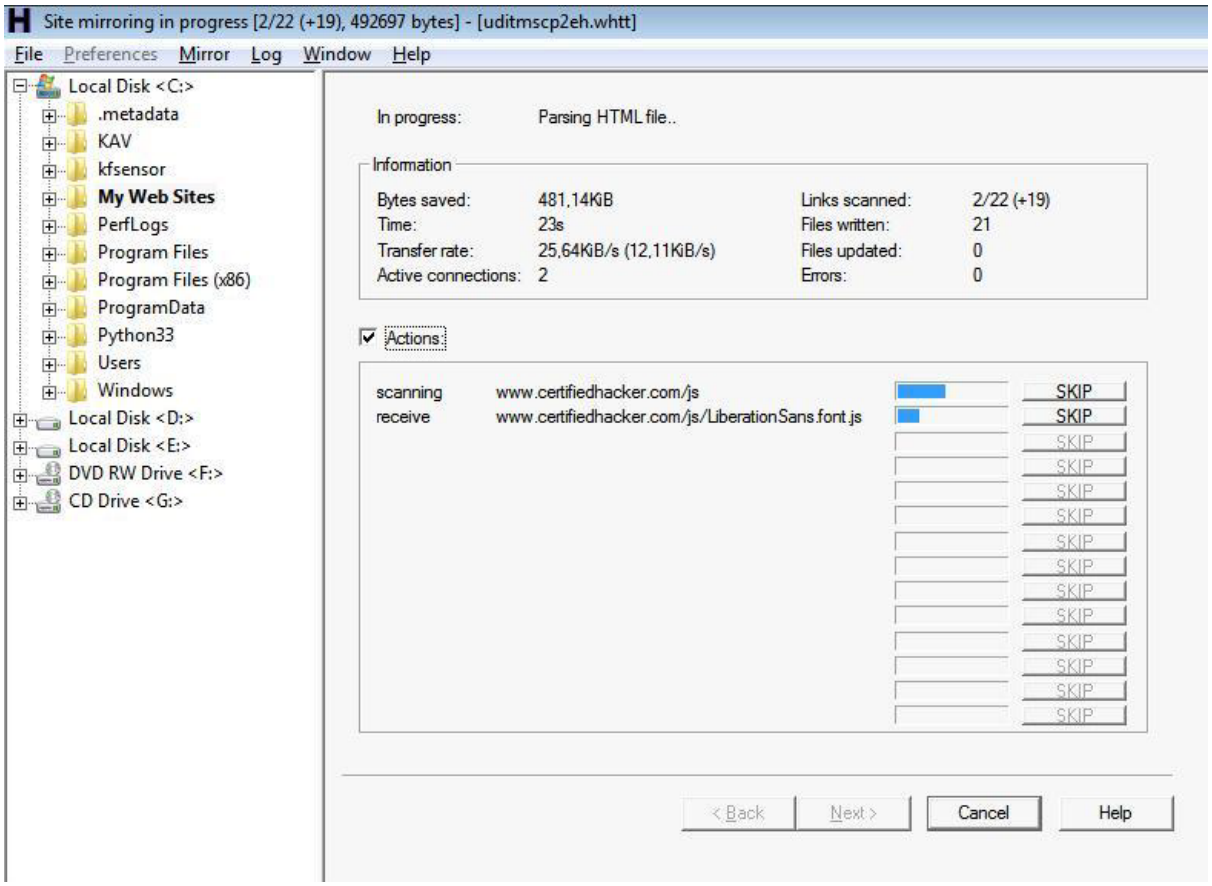


- Click on ‘Add URL’ and give the UR ☐
- Any additional options that need t ☐
- Then click 'Next'

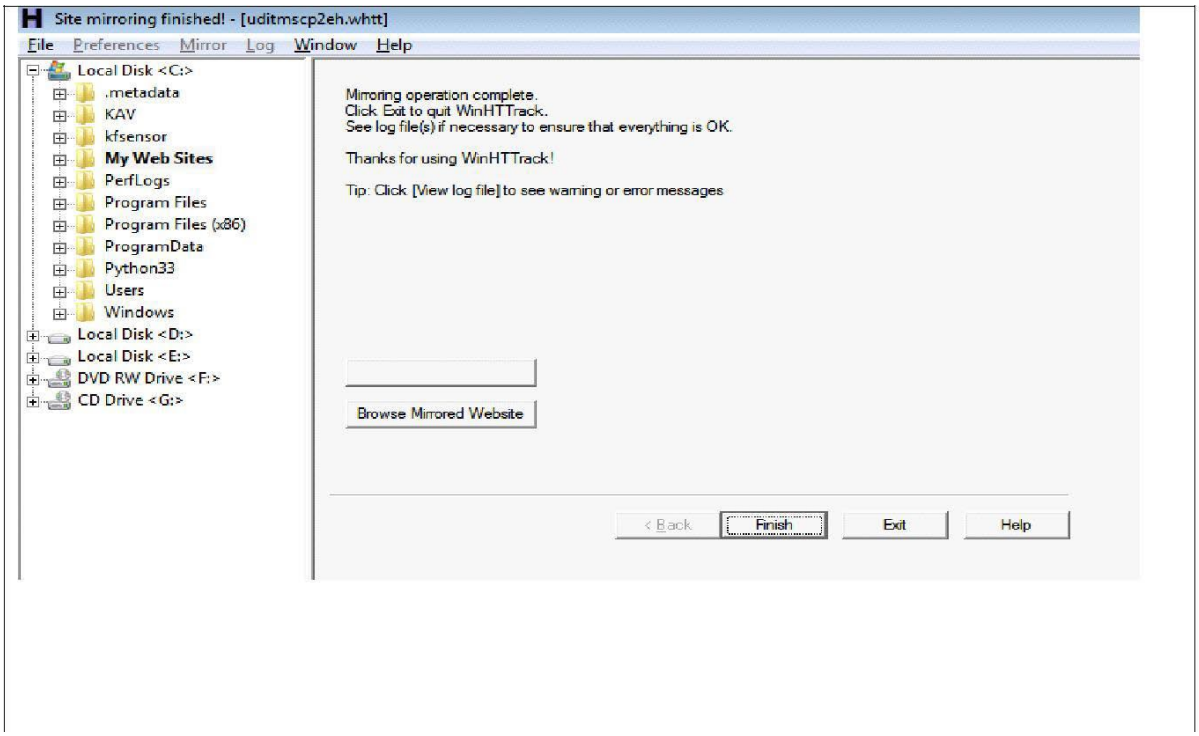
- By default, the radio button will be selected for Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.



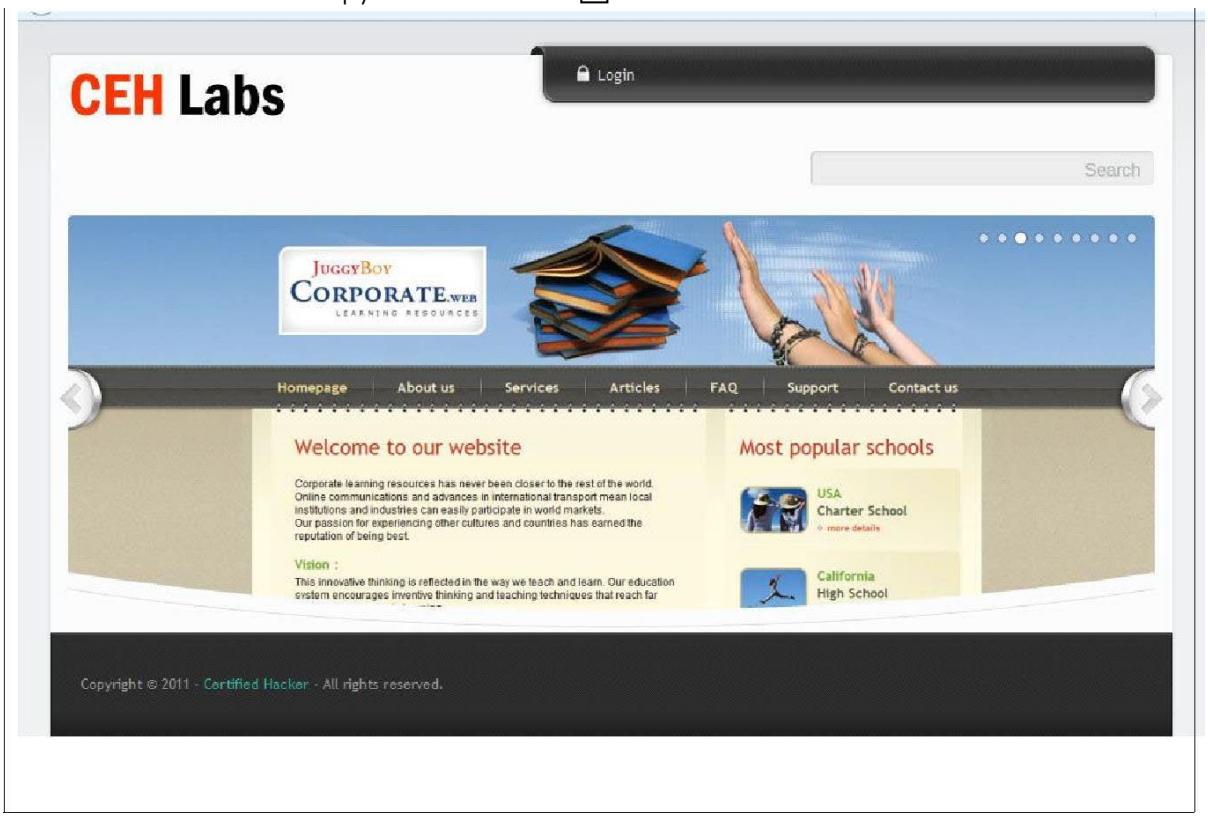
The mirroring of the site now begins. The site will be downloaded and be saved in the C:\My Web Sites\<Project Name> ☐



☐Process of mirroring the website.

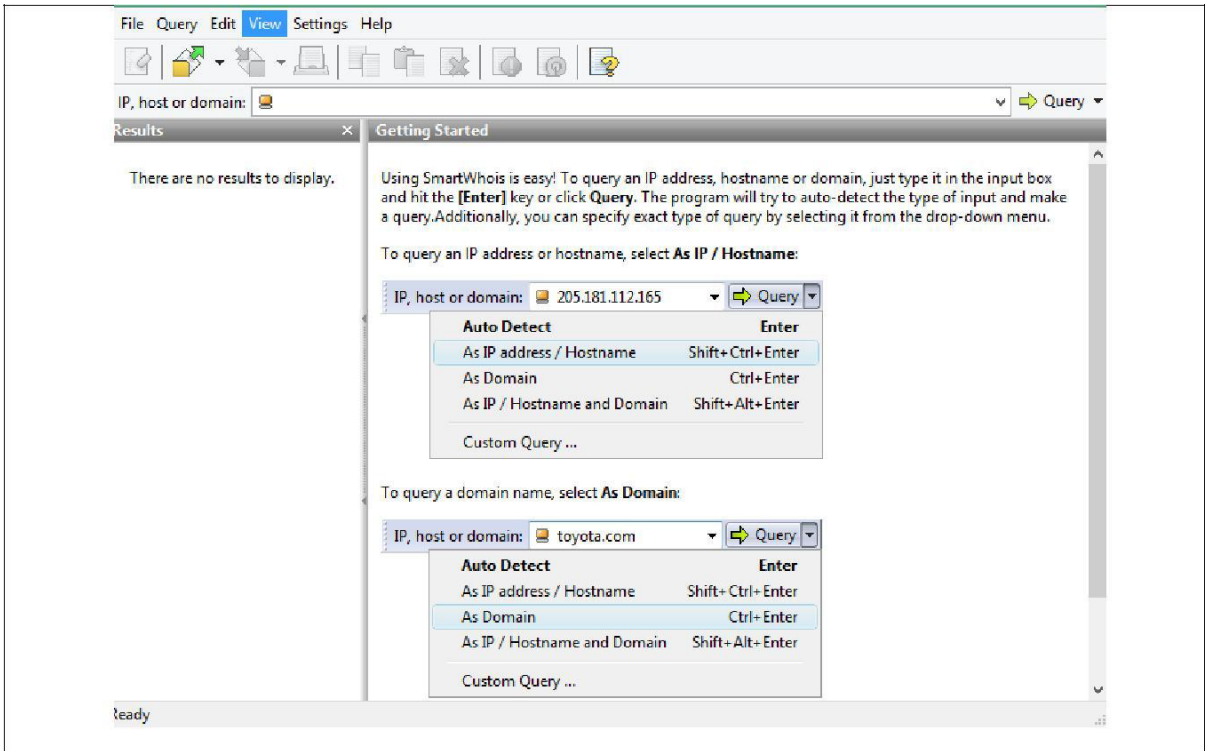


Once the Website Mirroring has been completed, you can click on the Browse Mirrored Website button and then browse the offline copy of the website. ☐

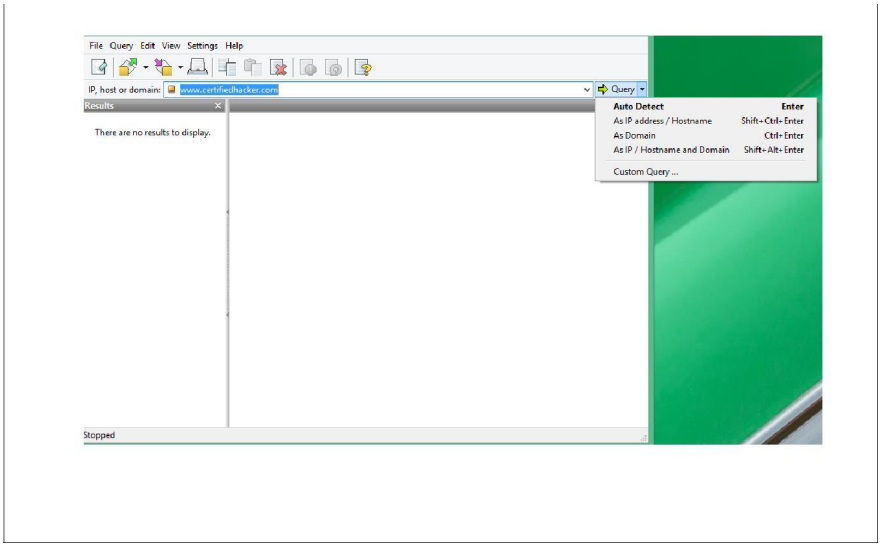


SmartWHOis

- SmartWHOis is used to perform WHOIS Footprinting against an entered IP Address or a Domain Name
- Run it from, Start > Programs > SmartWhois

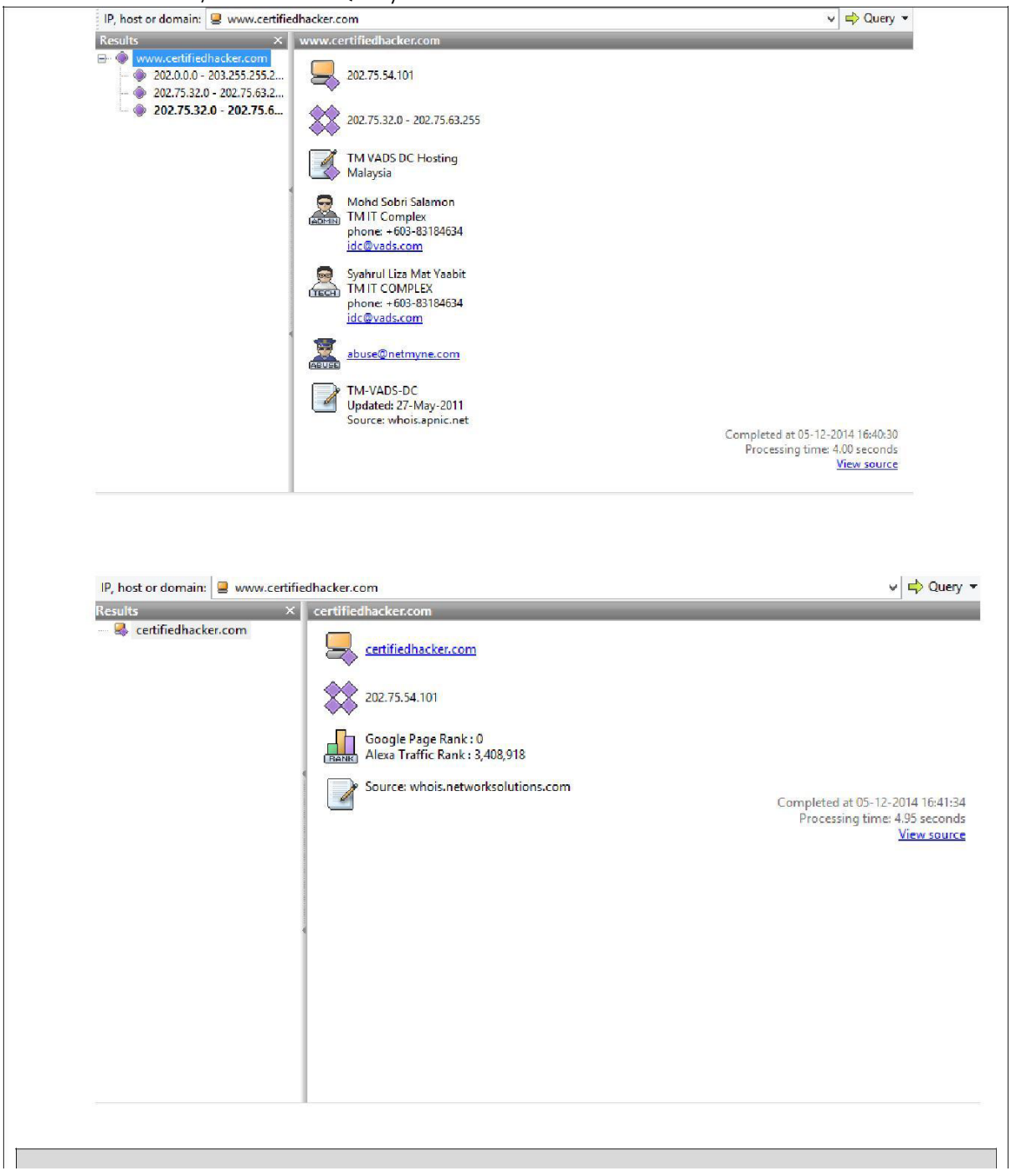


Type an IP address, hostname, or domain name in the address bar



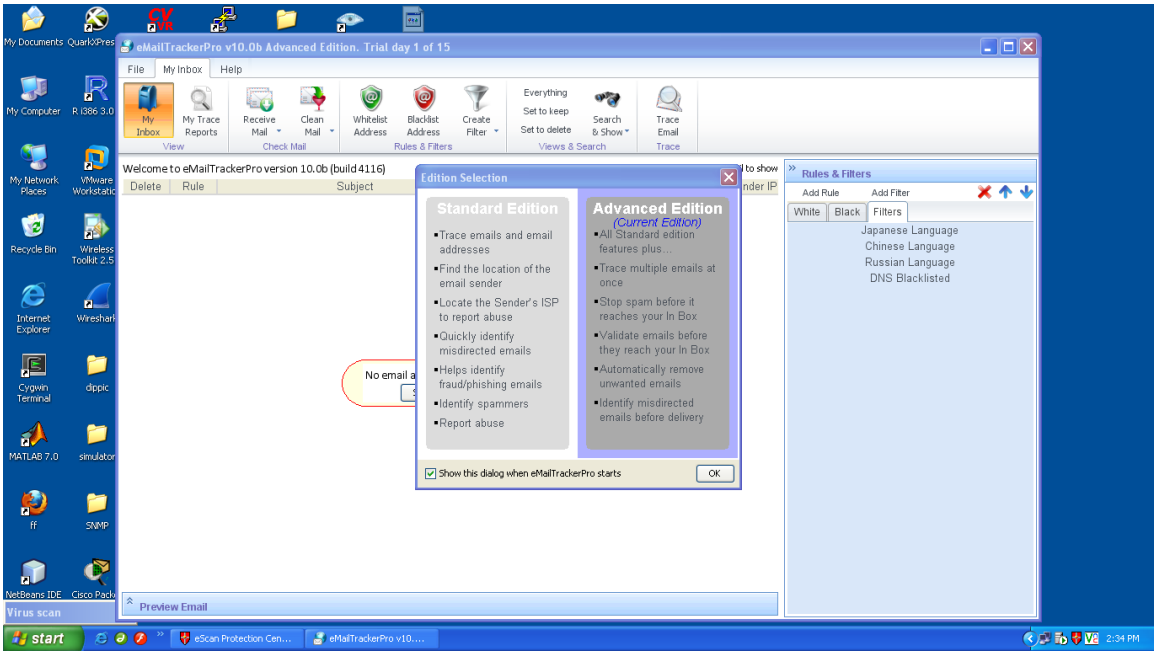
- Different queries will return different results.

- IP Address / Hostname Query results

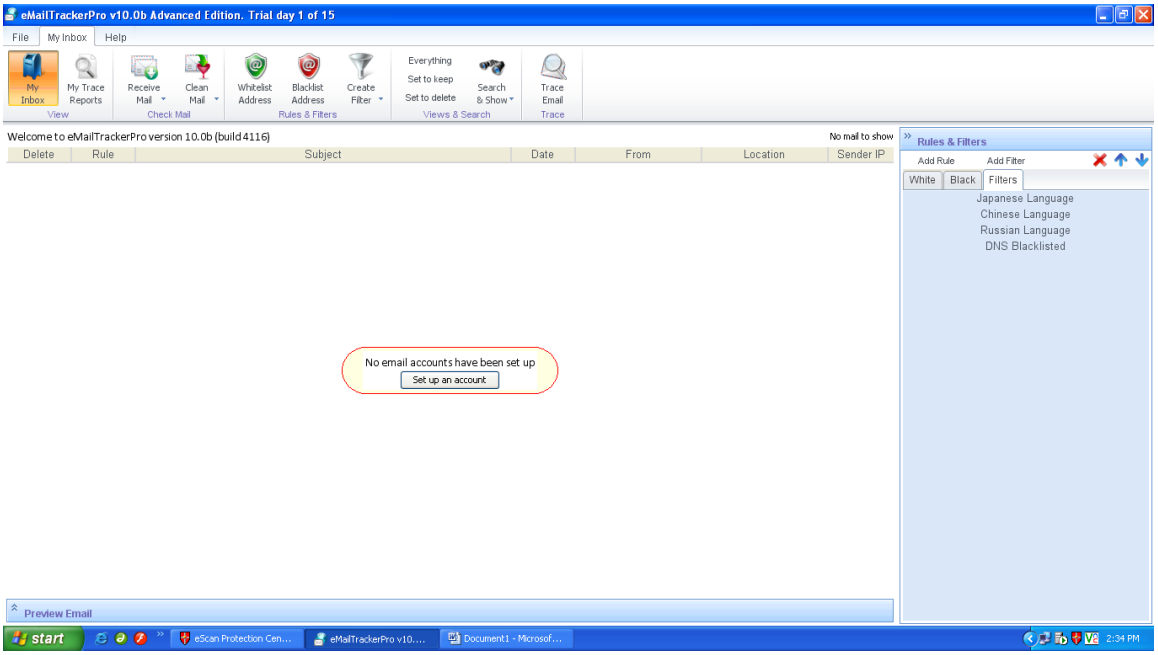


USING EMAIL TRACKER

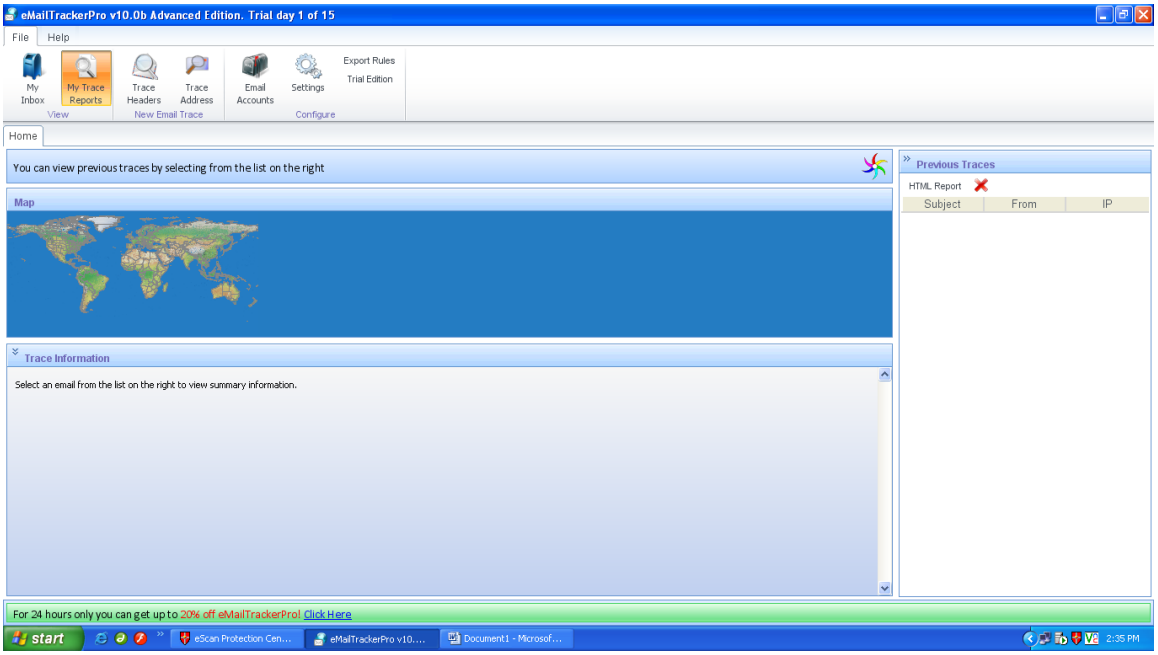
Step 1: Open emailTracker.



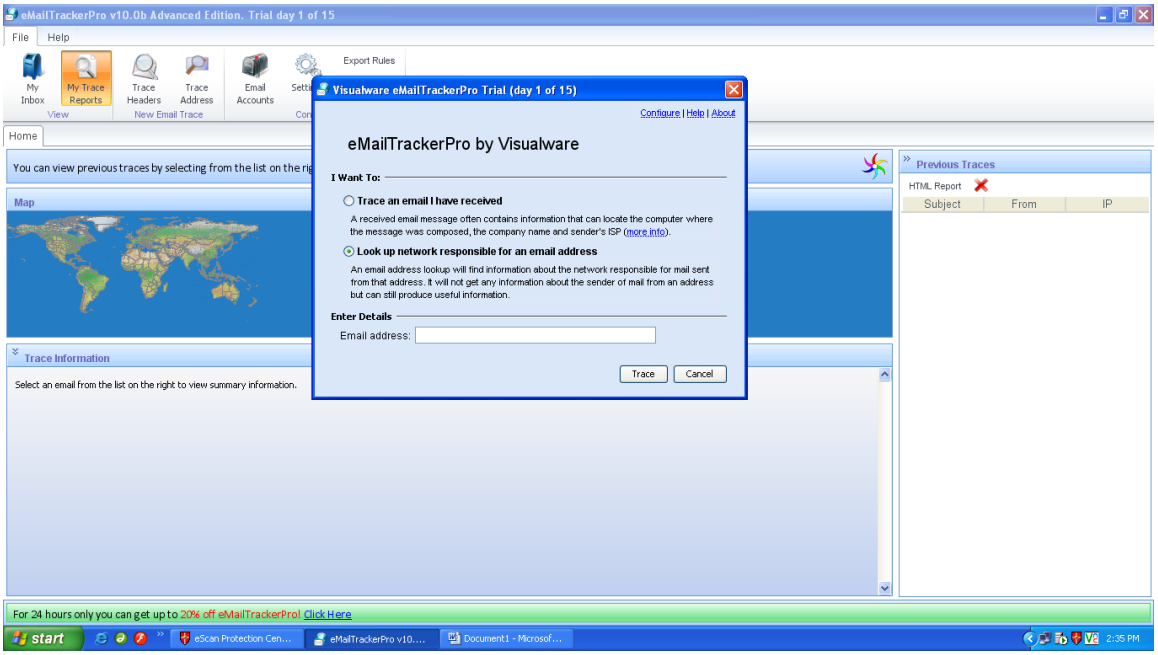
Step 2: Check if there are any reports generated previously.



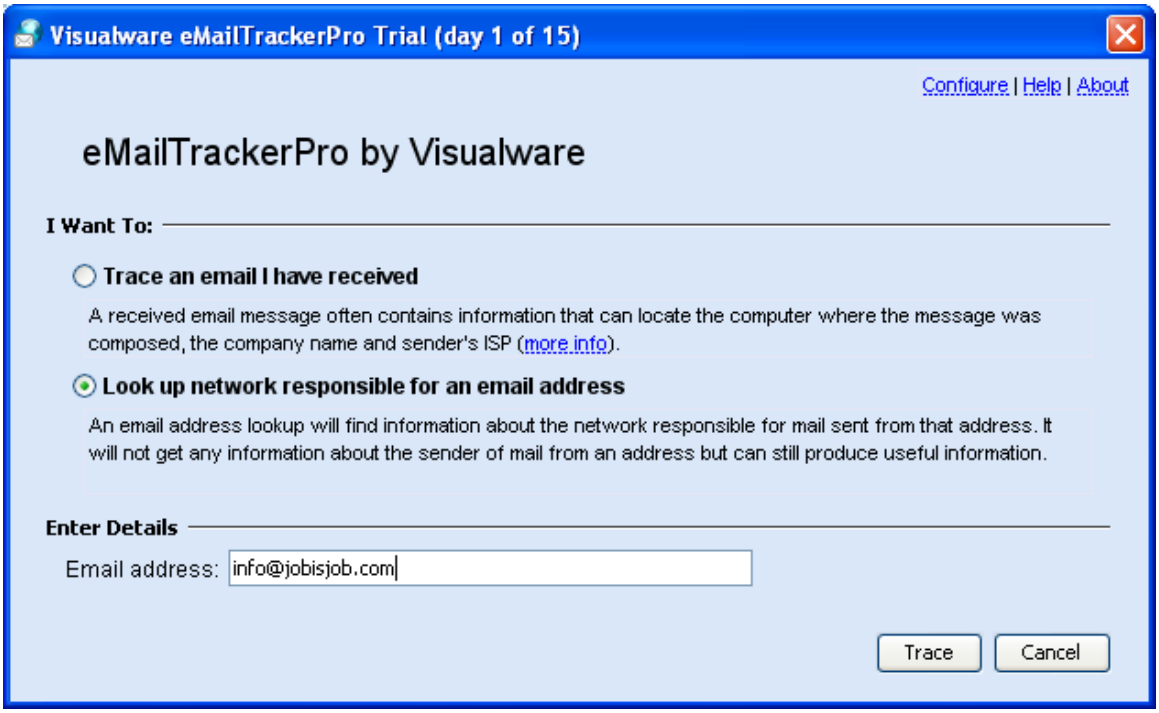
Step 3: Check for My trace Reports.



Step 4: Click on Trace address, a new window will open.



Step 5: Click on second option and enter email address you want to trace and click on trace button.



Step 6: The eMailTracker will search for the location and information about the email address entered.

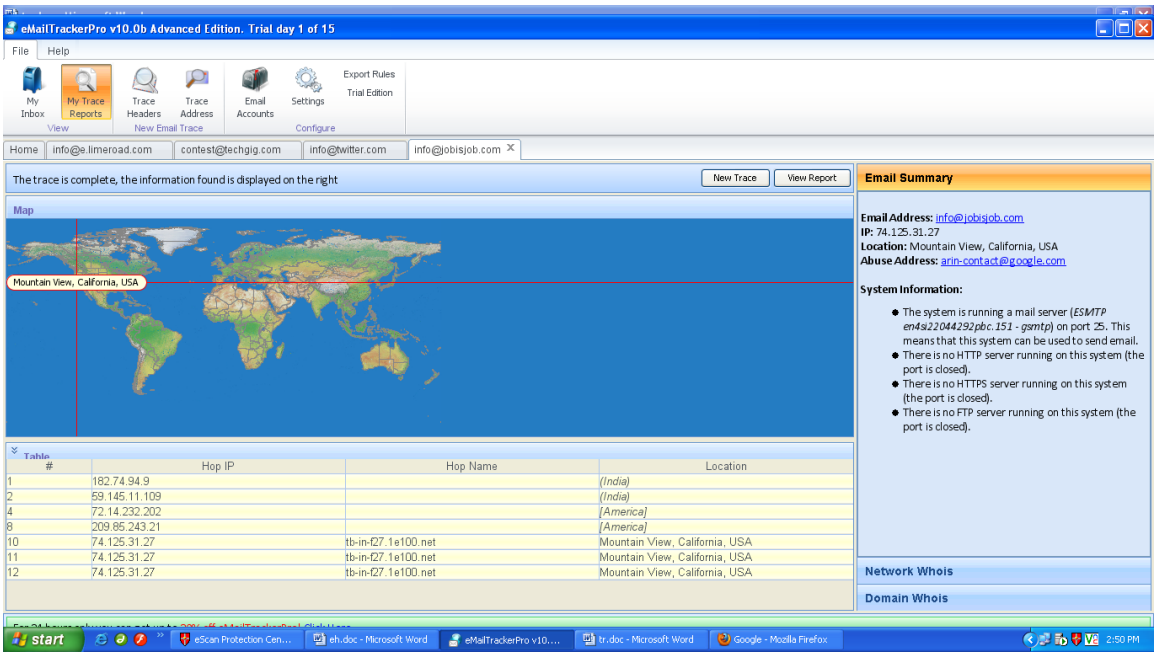


Figure: Location details and email summary.

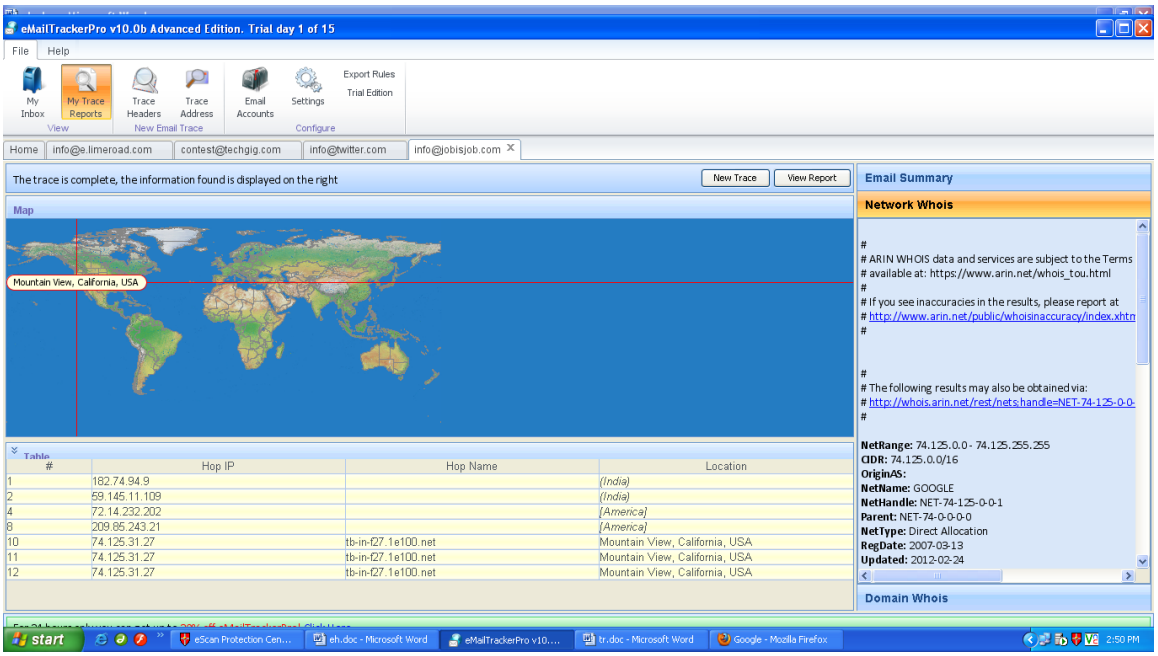


Figure: Location details and network summary.

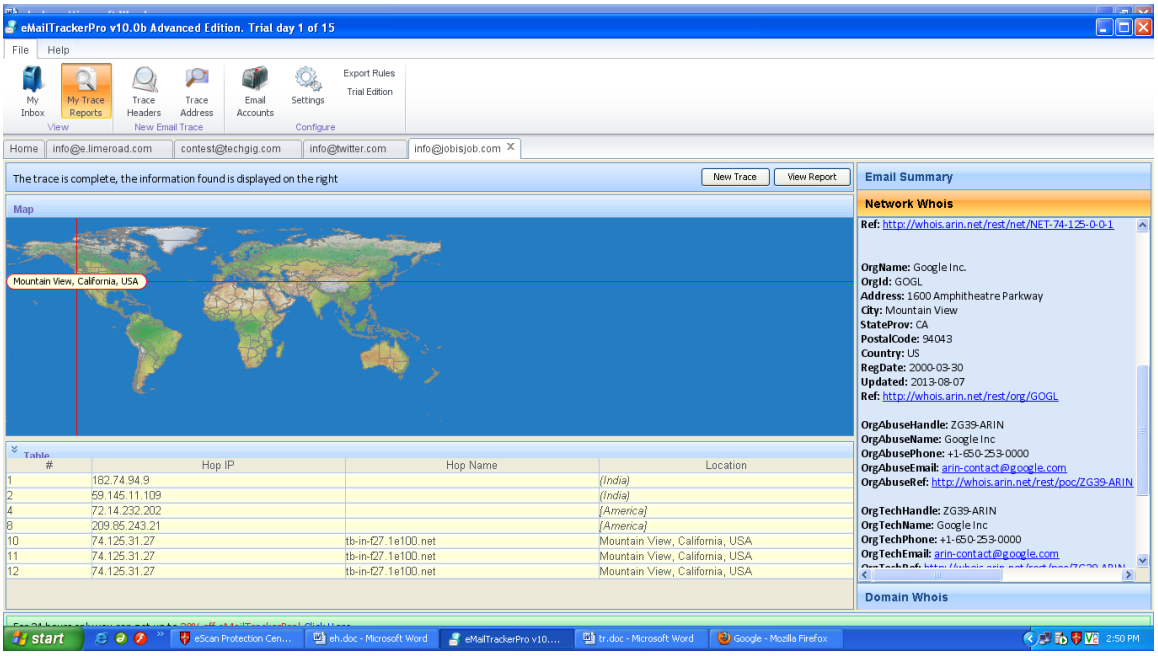


Figure: Location details and network summary.

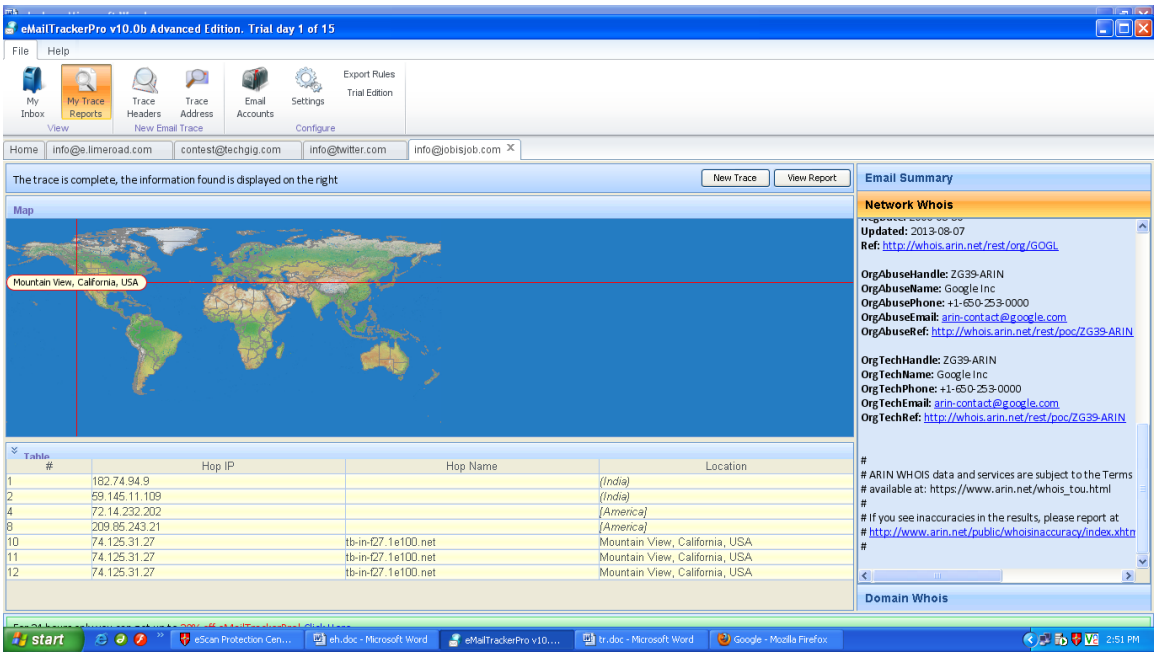


Figure: Location details and network summary.

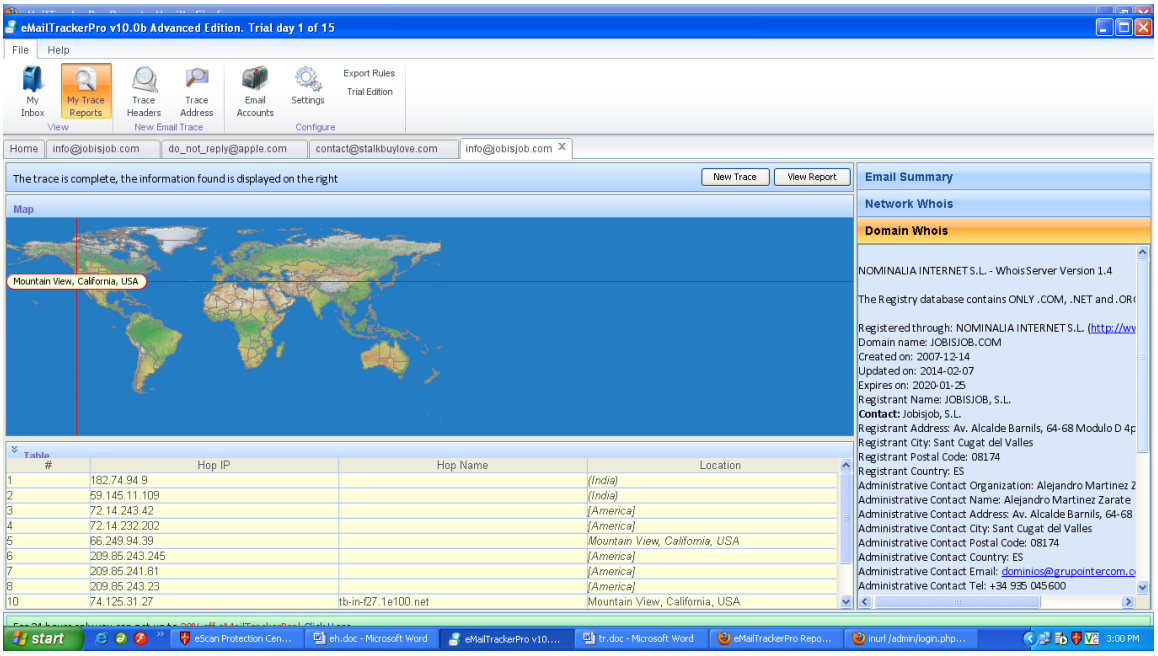


Figure: Location details and domain summary.

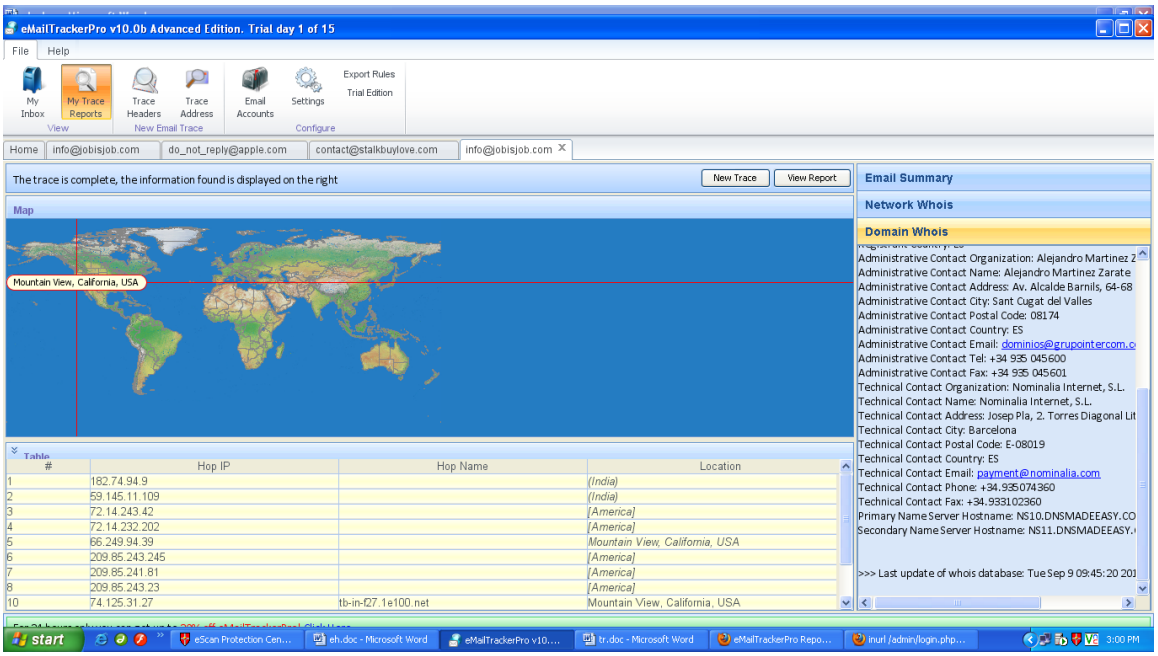
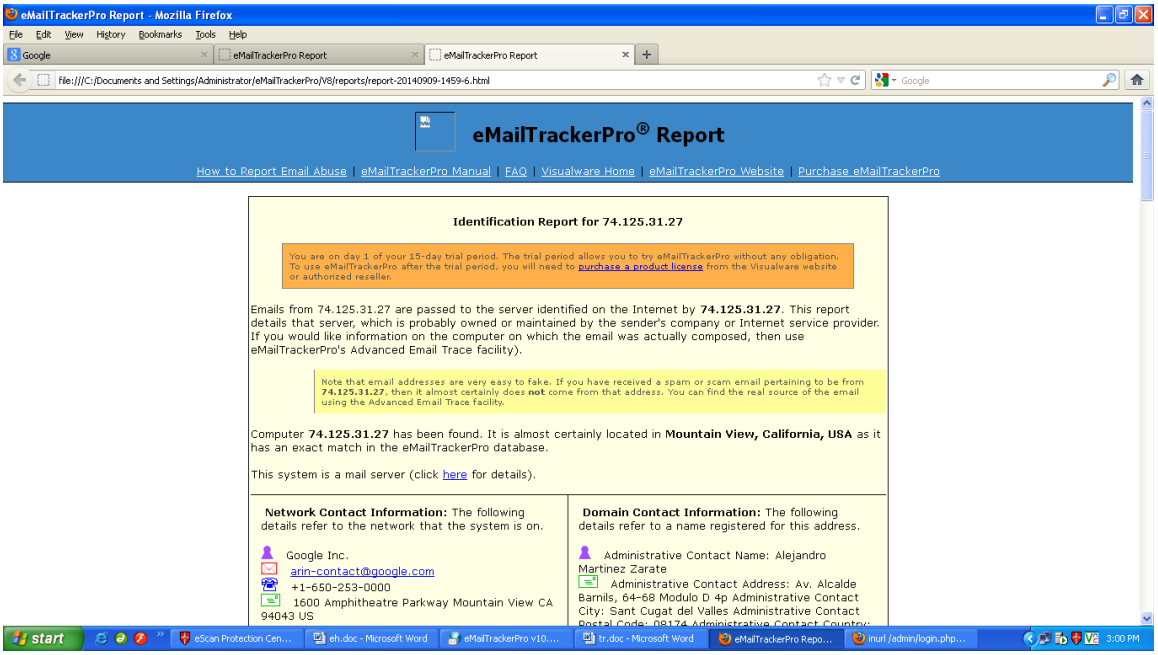
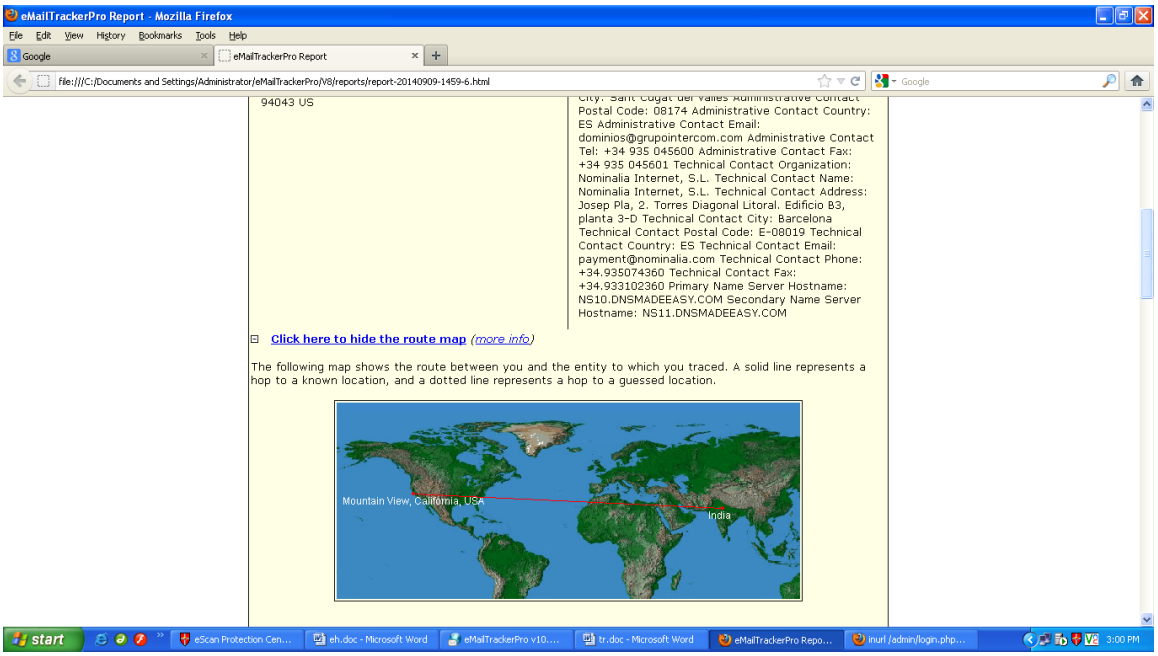
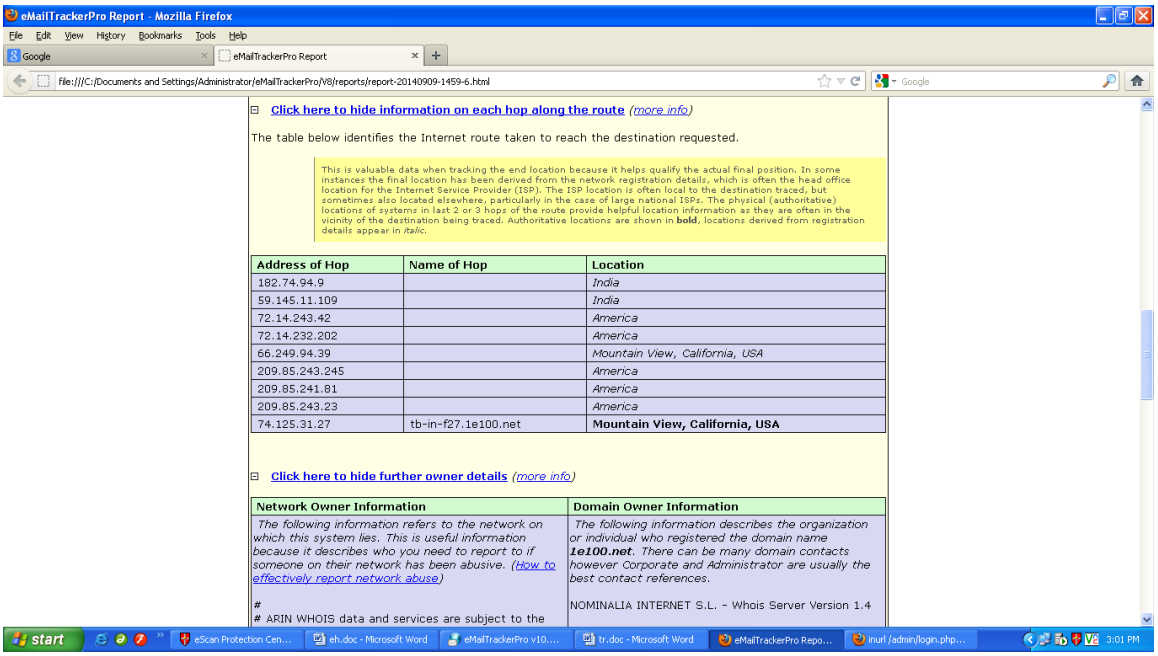


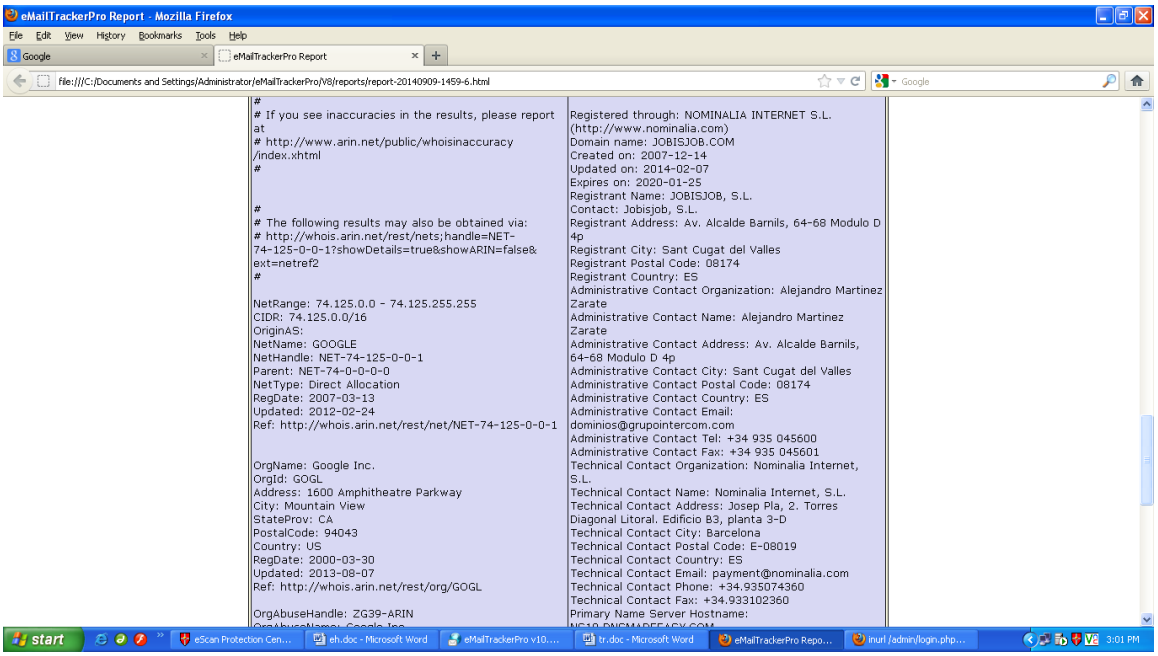
Figure: Location details and domain summary.

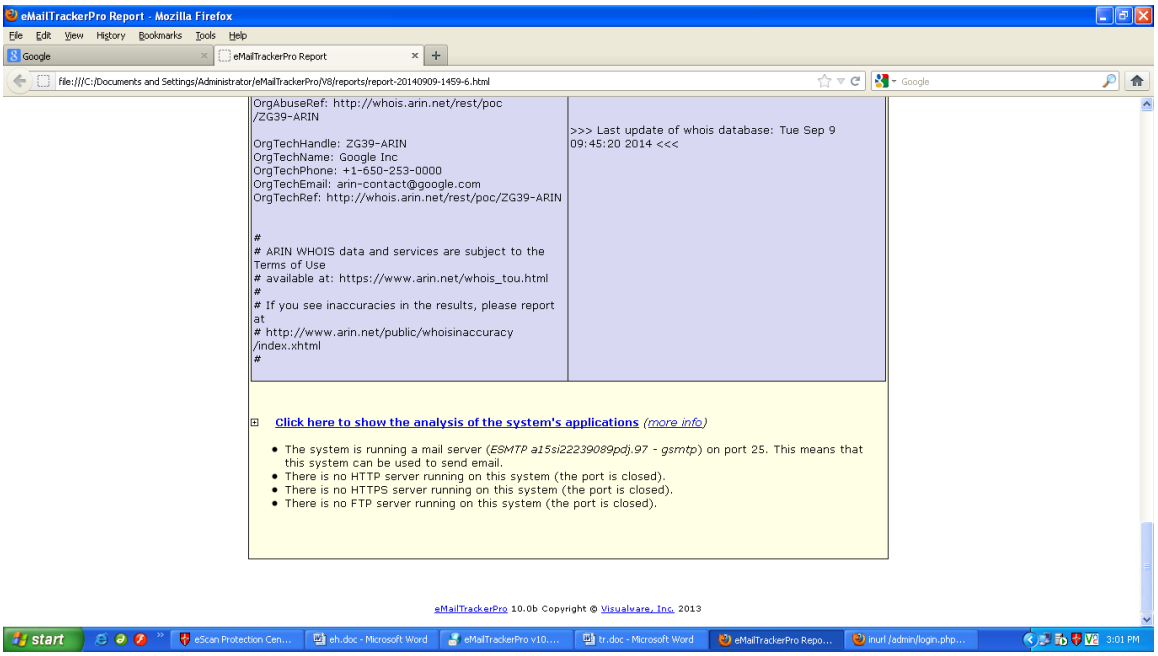
Step 7: Now click on View report and the following report will be generated in browser.




eMailTrackerPro Report - Mozilla Firefox
94043 US
Postal Code: 08174 Administrative Contact Country: ES Administrative Contact Email: dominios@grupointercom.com Administrative Contact Tel: +34 935 045600 Administrative Contact Fax: +34 935 045601 Technical Contact Organization: Nominalia Internet, S.L. Technical Contact Name: Nominalia Internet, S.L. Technical Contact Address: Josep Pla, 2. Torres Diagonal Litoral. Edificio B3, planta 3-D Technical Contact City: Barcelona Technical Contact Postal Code: E-08019 Technical Contact Country: ES Technical Contact Email: payment@nominalia.com Technical Contact Phone: +34.935074360 Technical Contact Fax: +34.933102360 Primary Name Server Hostname: NS10.DNSMADEEASY.COM Secondary Name Server Hostname: NS11.DNSMADEEASY.COM
Click here to hide the route map (more info)
The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.
Mountain View, California, USA
India


eMailTrackerPro Report - Mozilla Firefox
Click here to hide information on each hop along the route (more info)
The table below identifies the Internet route taken to reach the destination requested.
This is valuable data when tracking the end location because it helps qualify the actual final position. In some instances the final location has been derived from the network registration details, which is often the head office location for the Internet Service Provider (ISP). The ISP location is often local to the destination traced, but sometimes also located elsewhere, particularly in the case of large national ISPs. The physical (authoritative) locations of systems in last 2 or 3 hops of the route provide helpful location information as they are often in the vicinity of the destination being traced. Authoritative locations are shown in bold, locations derived from registration details appear in italic.
Address of Hop | Name of Hop | Location
182.74.94.9 | | India
59.145.11.109 | | India
72.14.243.42 | | America
72.14.232.202 | | America
66.249.94.39 | | Mountain View, California, USA
209.85.243.245 | | America
209.85.241.81 | | America
209.85.243.23 | | America
74.125.31.27 | tb-in-f27.1e100.net | Mountain View, California, USA
Click here to hide further owner details (more info)
Network Owner Information
The following information refers to the network on which this system lies. This is useful information because it describes who you need to report to if someone on their network has been abusive. (How to effectively report network abuse)
Domain Owner Information
The following information describes the organization or individual who registered the domain name 1e100.net. There can be many domain contacts however Corporate and Administrator are usually the best contact references.
NOMINALIA INTERNET S.L. - Whois Server Version 1.4
ARIN WHOIS data and services are subject to the


eMailTrackerPro Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
eMailTrackerPro Report
file:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html
#
If you see inaccuracies in the results, please report at
http://www.arin.net/public/whoisinaccuracy/index.xhtml
#
#
The following results may also be obtained via:
http://whois.arin.net/rest/nets;handle=NET-74-125-0-0-1?showDetails=true&showARIN=false&ext=netref2
#
NetRange: 74.125.0.0 - 74.125.255.255
CIDR: 74.125.0.0/16
OriginAS:
NetName: GOOGLE
NetHandle: NET-74-125-0-0-1
Parent: NET-74-0-0-0-0
NetType: Direct Allocation
RegDate: 2007-03-13
Updated: 2012-02-24
Ref: http://whois.arin.net/rest/net/NET-74-125-0-0-1
OrgName: Google Inc.
OrgId: GOGL
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2000-03-30
Updated: 2013-08-07
Ref: http://whois.arin.net/rest/org/GOGL
OrgAbuseHandle: ZG39-ARIN
Registered through: NOMINALIA INTERNET S.L. (http://www.nominalia.com)
Domain name: JOBISJOB.COM
Created on: 2007-12-14
Updated on: 2014-02-07
Expires on: 2020-01-25
Registrant Name: JOBISJOB, S.L.
Contact: Jobisjob, S.L.
Registrant Address: Av. Alcalde Barnils, 64-68 Modulo D 4p
Registrant City: Sant Cugat del Valles
Registrant Postal Code: 08174
Registrant Country: ES
Administrative Contact Organization: Alejandro Martinez Zarate
Administrative Contact Name: Alejandro Martinez Zarate
Administrative Contact Address: Av. Alcalde Barnils, 64-68 Modulo D 4p
Administrative Contact City: Sant Cugat del Valles
Administrative Contact Postal Code: 08174
Administrative Contact Country: ES
Administrative Contact Email: dominios@grupointercom.com
Administrative Contact Tel: +34 935 045600
Administrative Contact Fax: +34 935 045601
Technical Contact Organization: Nominalia Internet, S.L.
Technical Contact Name: Nominalia Internet, S.L.
Technical Contact Address: Josep Pla, 2. Torres Diagonal Litoral. Edificio B3, planta 3-D
Technical Contact City: Barcelona
Technical Contact Postal Code: E-08019
Technical Contact Country: ES
Technical Contact Email: payment@nominalia.com
Technical Contact Phone: +34.935074360
Technical Contact Fax: +34.933102360
Primary Name Server Hostname:
start
3:01 PM


eMailTrackerPro Report - Mozilla Firefox
File Edit View History Bookmarks Tools Help
eMailTrackerPro Report
file:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html
OrgAbuseRef: http://whois.arin.net/rest/poc/ZG39-ARIN
OrgTechHandle: ZG39-ARIN
OrgTechName: Google Inc
OrgTechPhone: +1-650-253-0000
OrgTechEmail: arin-contact@google.com
OrgTechRef: http://whois.arin.net/rest/poc/ZG39-ARIN
#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/whois_tou.html
#
If you see inaccuracies in the results, please report at
http://www.arin.net/public/whoisinaccuracy/index.xhtml
#
>>> Last update of whois database: Tue Sep 9 09:45:20 2014 <<<
Click here to show the analysis of the system's applications (more info)
The system is running a mail server (ESMTP a15si22239089pdj.97 - gsmtp) on port 25. This means that this system can be used to send email.
There is no HTTP server running on this system (the port is closed).
There is no HTTPS server running on this system (the port is closed).
There is no FTP server running on this system (the port is closed).
eMailTrackerPro 10.0b Copyright © Visualware, Inc. 2013
start
3:01 PM

Scan the network using the following tools:

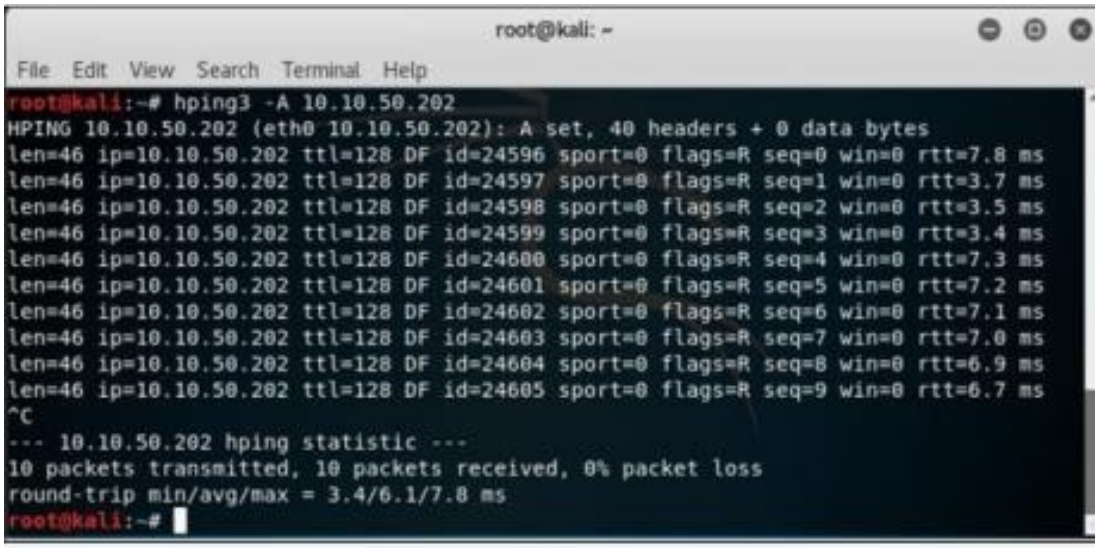
i. Hping2 / Hping3

Hping is a command-line TCP/IP packet assembler and analyzer 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: -

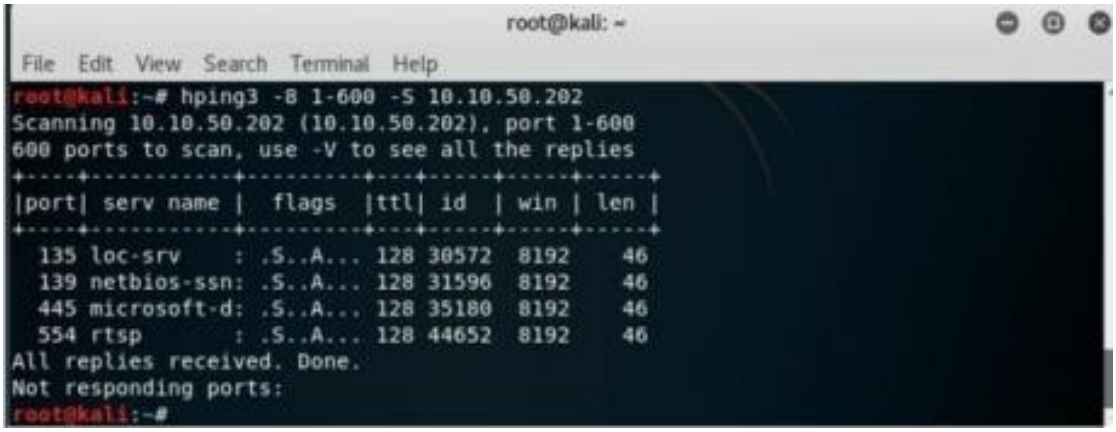
- ☐ Test firewall rules.
- ☐ Advanced port scanning.
- ☐ Testing net performance.
- ☐ Path MTU discovery.
- ☐ Transferring files between even fascist firewall rules.
- ☐ Traceroute-like under different protocols.
- ☐ Remote OS fingerprinting & others

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

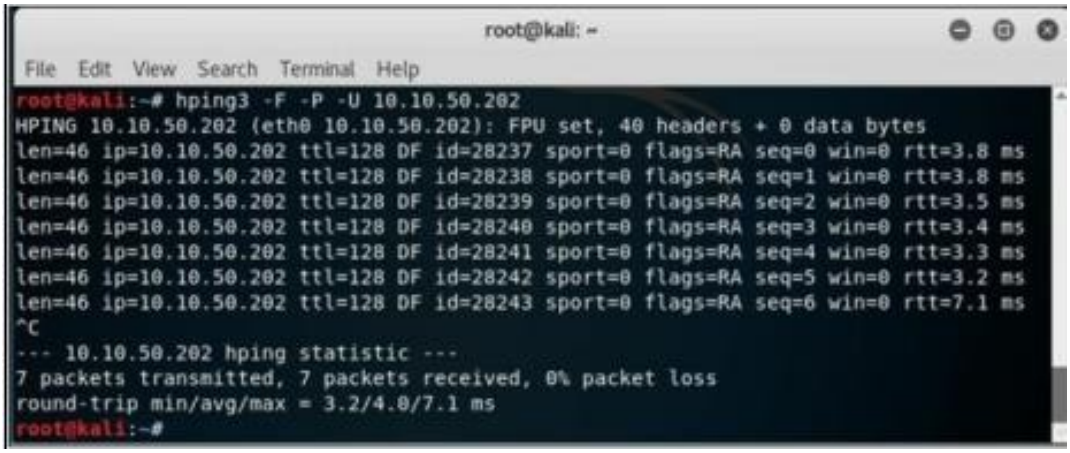
- To create an ACK packet:
  root@kali:~# hping3 –A 192.168.0.1



- To create SYN scan against different ports:
  root@kali:~# hping3 -8 1-600 –S 10.10.50.202

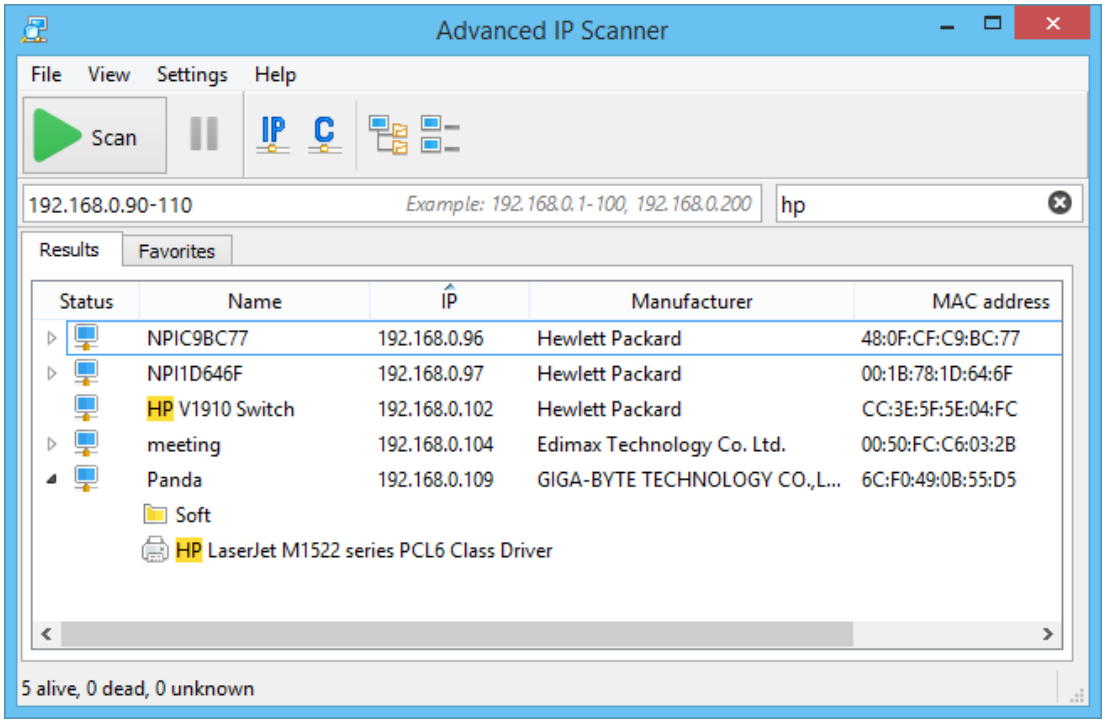


- To create a packet with FIN, URG, and PSH flags sets
  root@kali:~# hping3 –F –P -U 10.10.50.202



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.

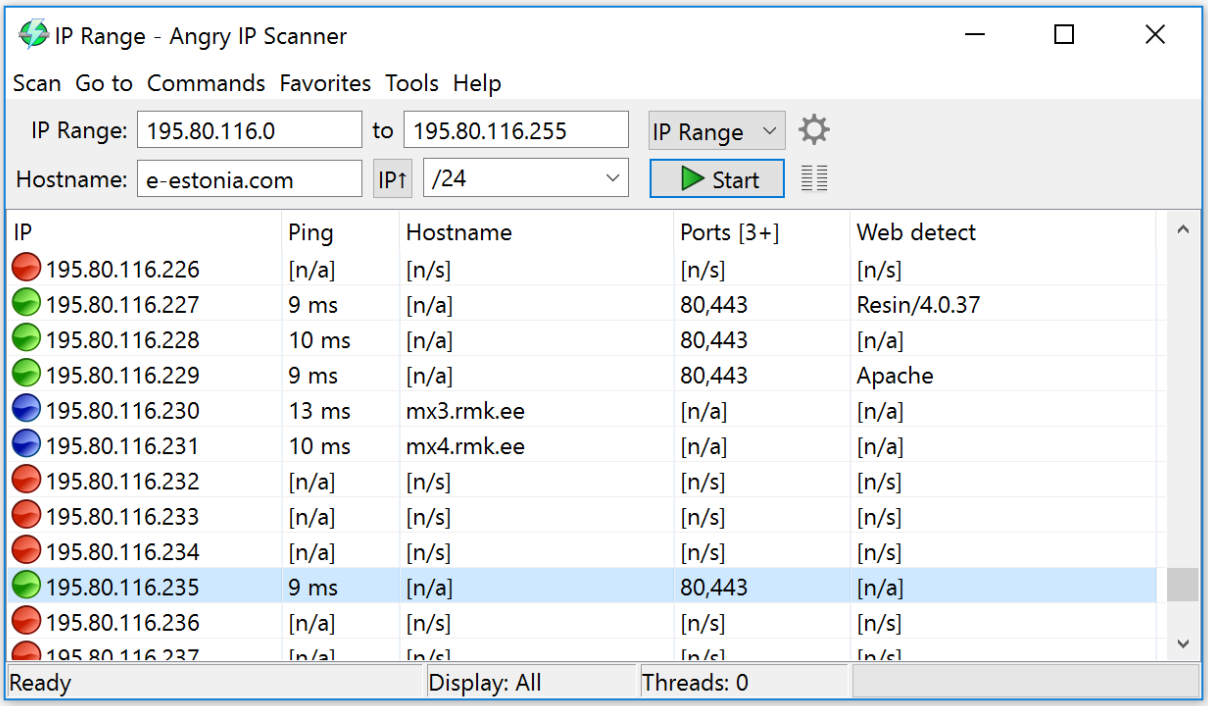


iii. Angry IP Scanner

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 otherfeatures.

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.



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 morelike scanrand, unicornscan, and ZMap, using asynchronous transmission. It's a flexible utility that allows arbitrary address and port ranges.

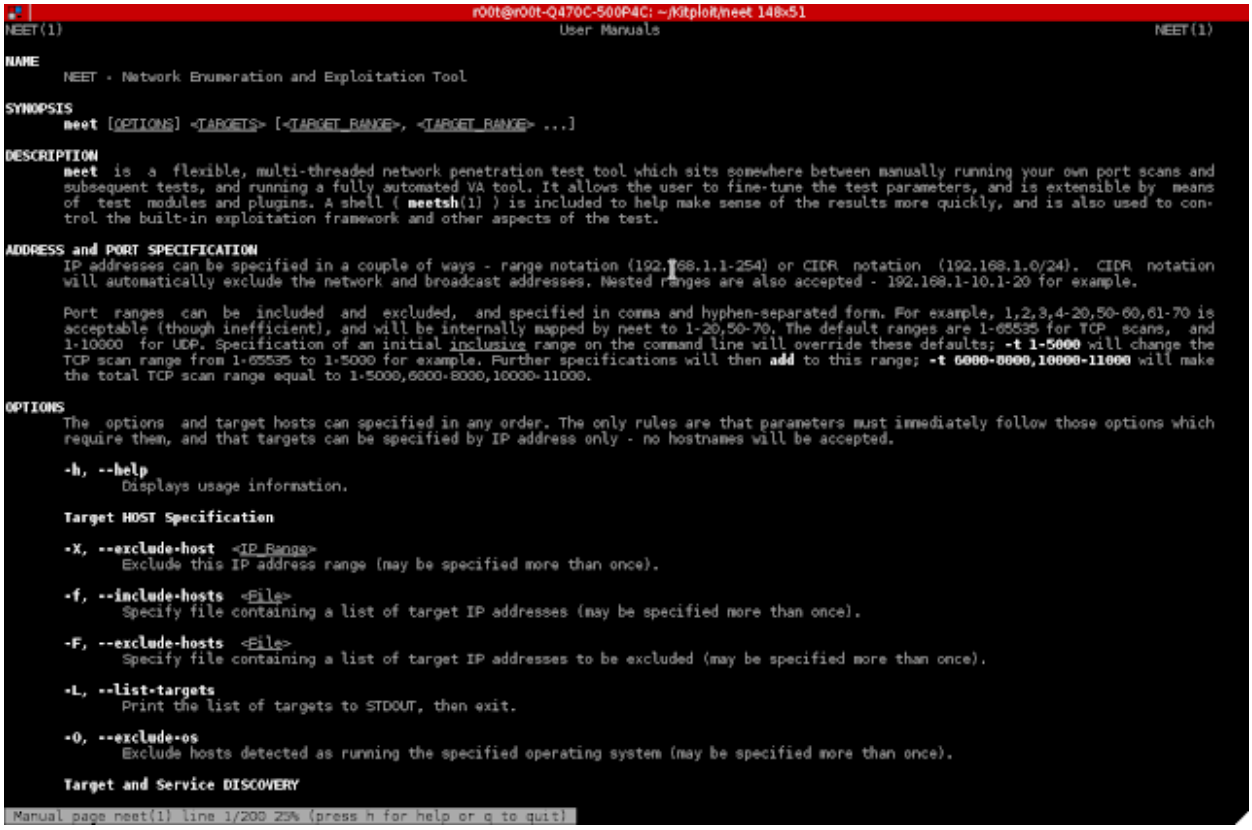
Scan for a selection of ports (-p22,80,445) across a given subnet (192.168.1.0/24):
root@kali:~# masscan -p22,80,445 192.168.1.0/24

```
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2014-05-13 21:35:12 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [3 ports/host]
Discovered open port 22/tcp on 192.168.1.217
Discovered open port 445/tcp on 192.168.1.220
Discovered open port 80/tcp on 192.168.1.230
```

v. NEET

Neet is a flexible, multi-threaded tool for network penetration testing. It runs on Linux and co-ordinates 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.



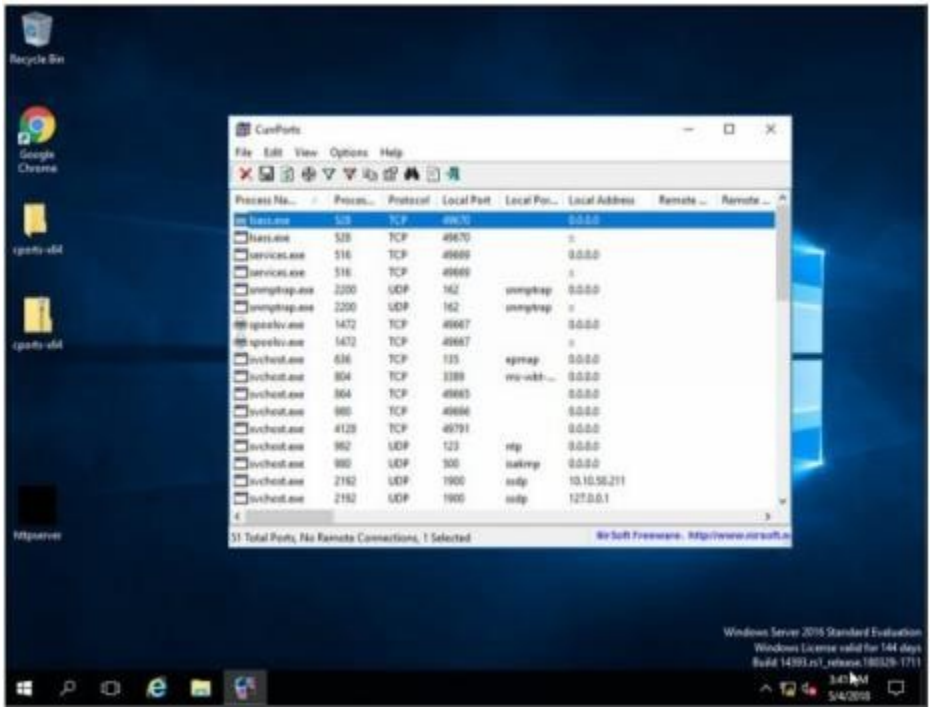
vi. CurrPorts

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.

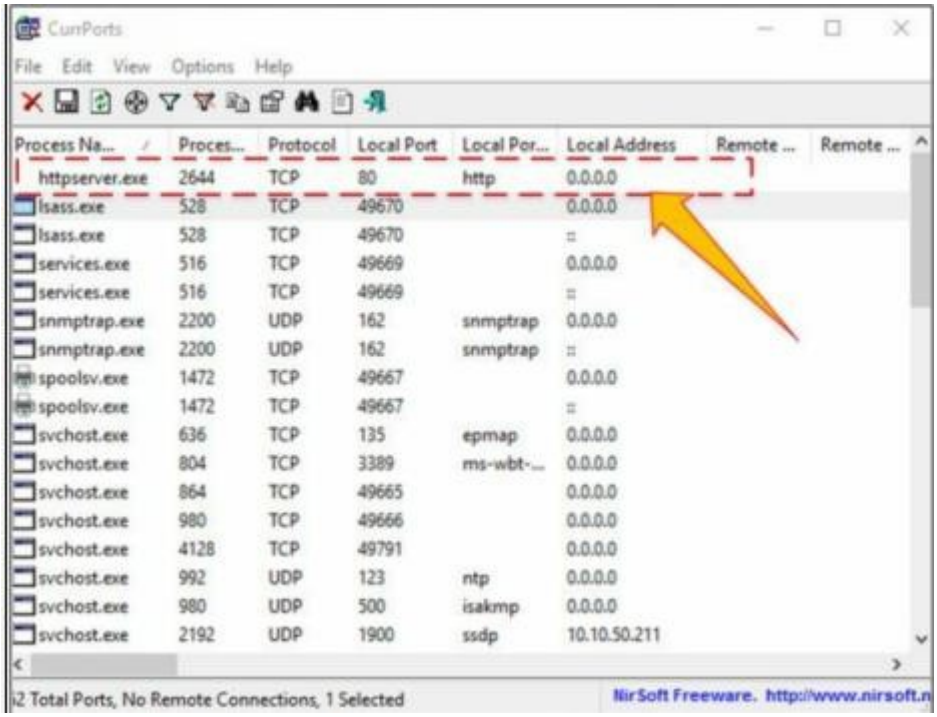
Topology:

Configuration:

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

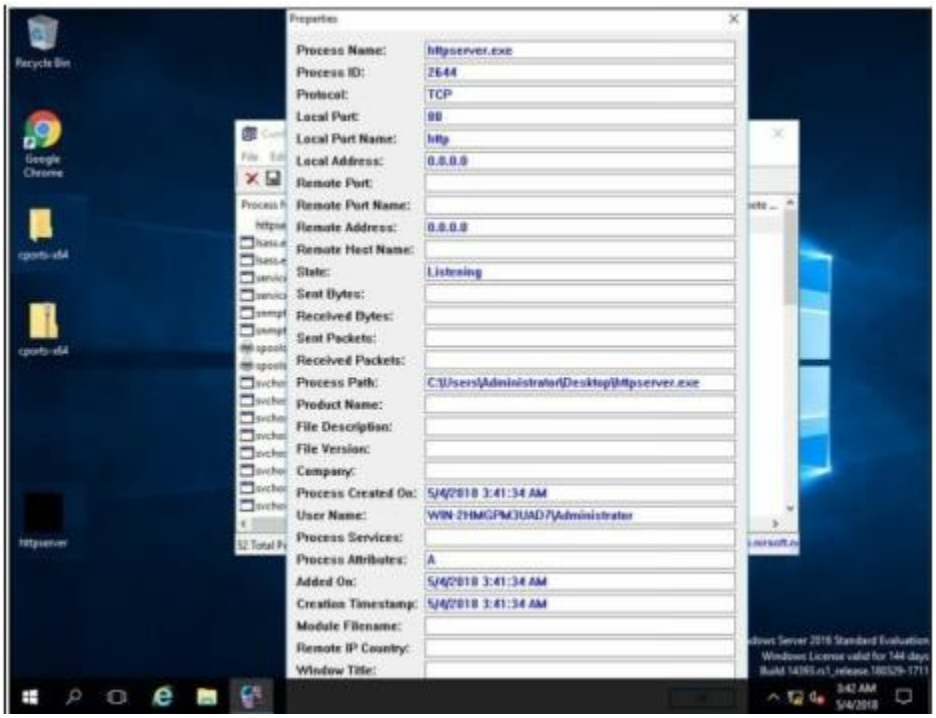


2.Run the HTTP Trojan created in the previous lab



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

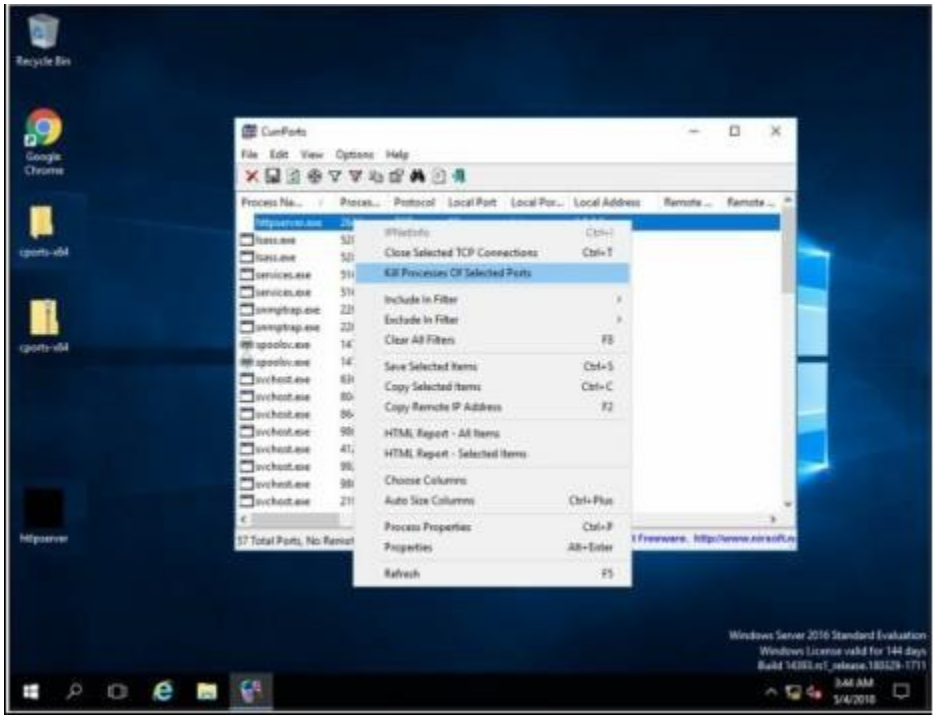


Properties are showing more details about tcp connection.

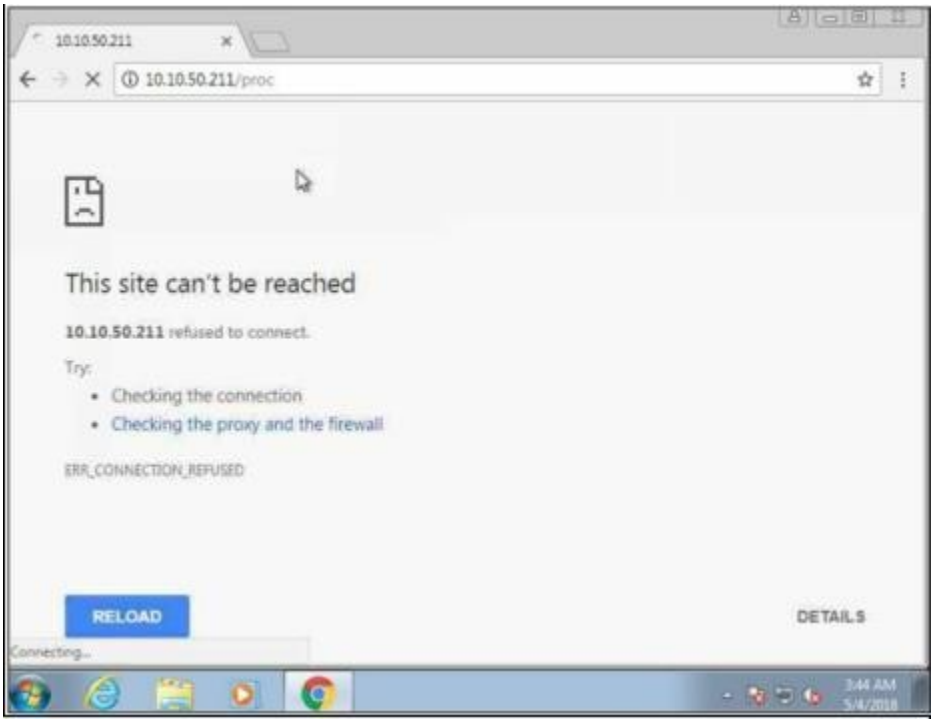
4. Go to Windows 7 machine and initiate the connection as mentioned in the previous lab using aweb browser.

Connection successfully established.

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



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



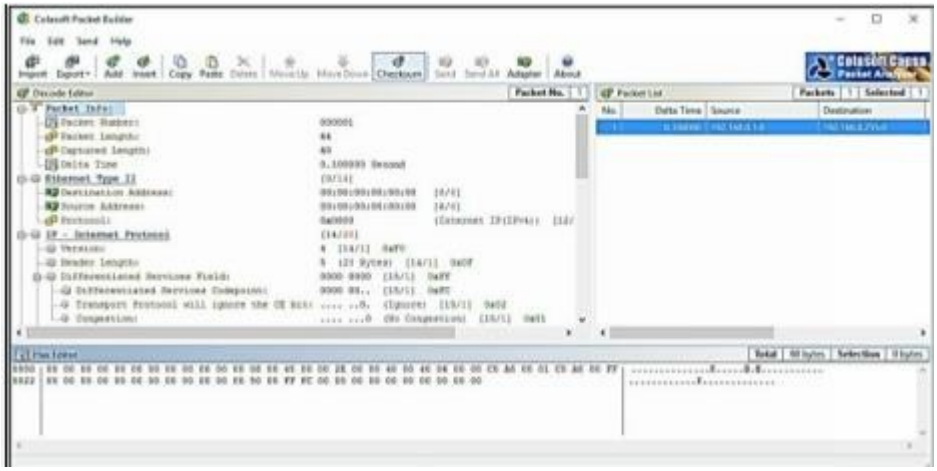
vii. Colasoft Packet Builder

Colasoft Packet Builder software enables to create the customized network packets. These

Customized Network packets can penetrate the network for attacks. Customization can also useto 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



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

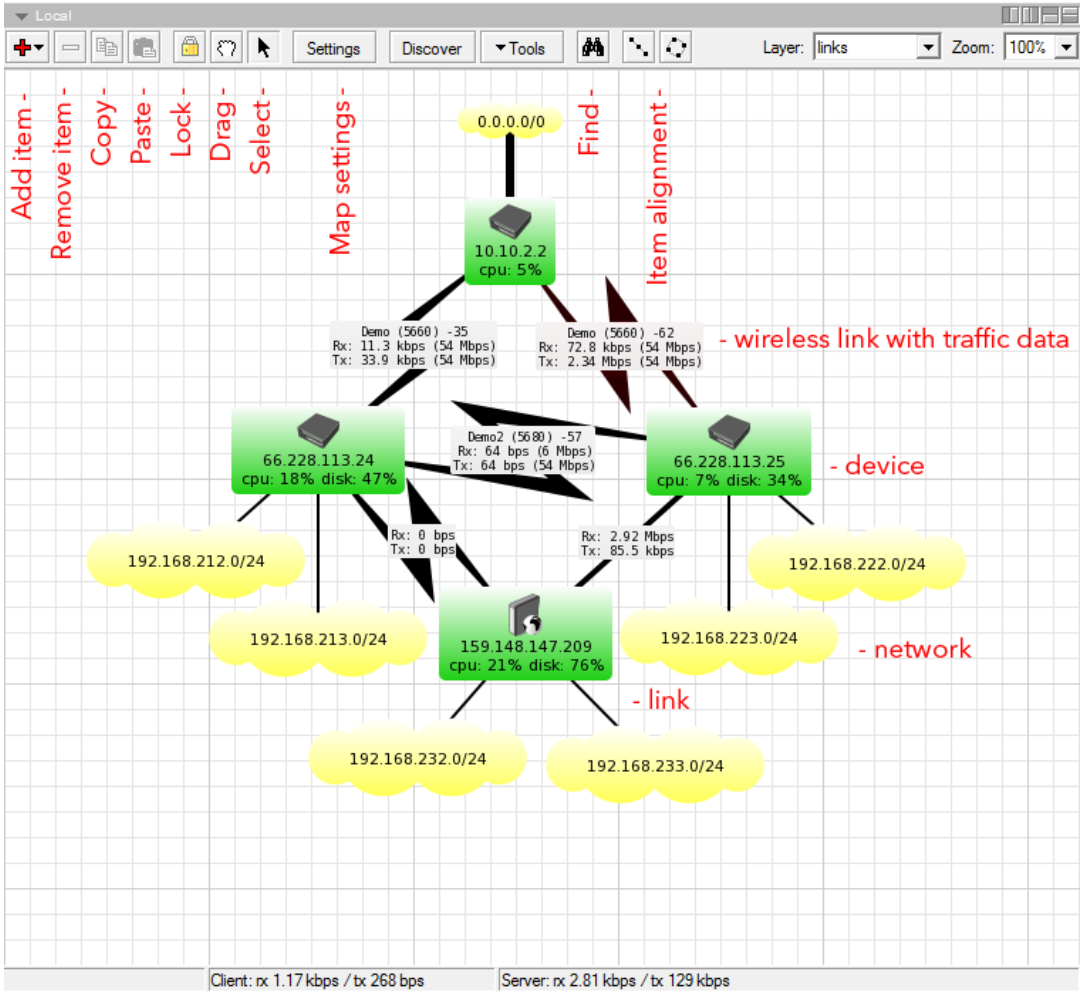
viii. The Dude

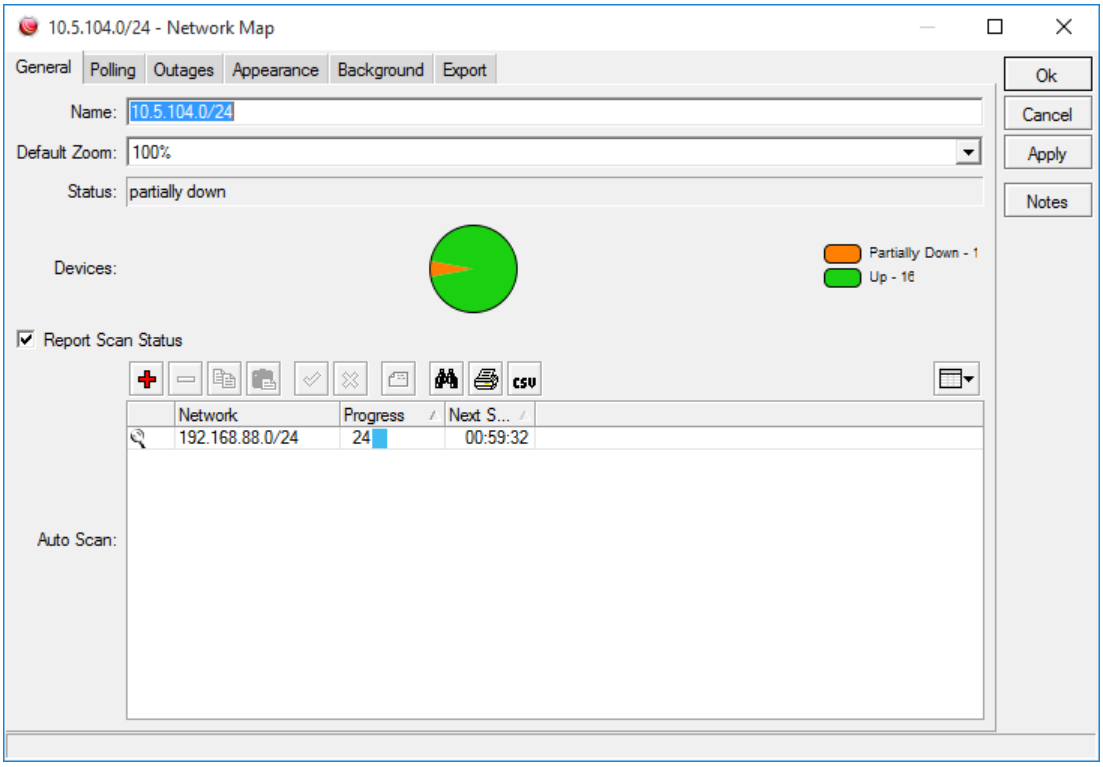
The Dude network monitor is a new application by MikroTik which can dramatically improve the way you manage your network environment. It will automatically scan all devices within

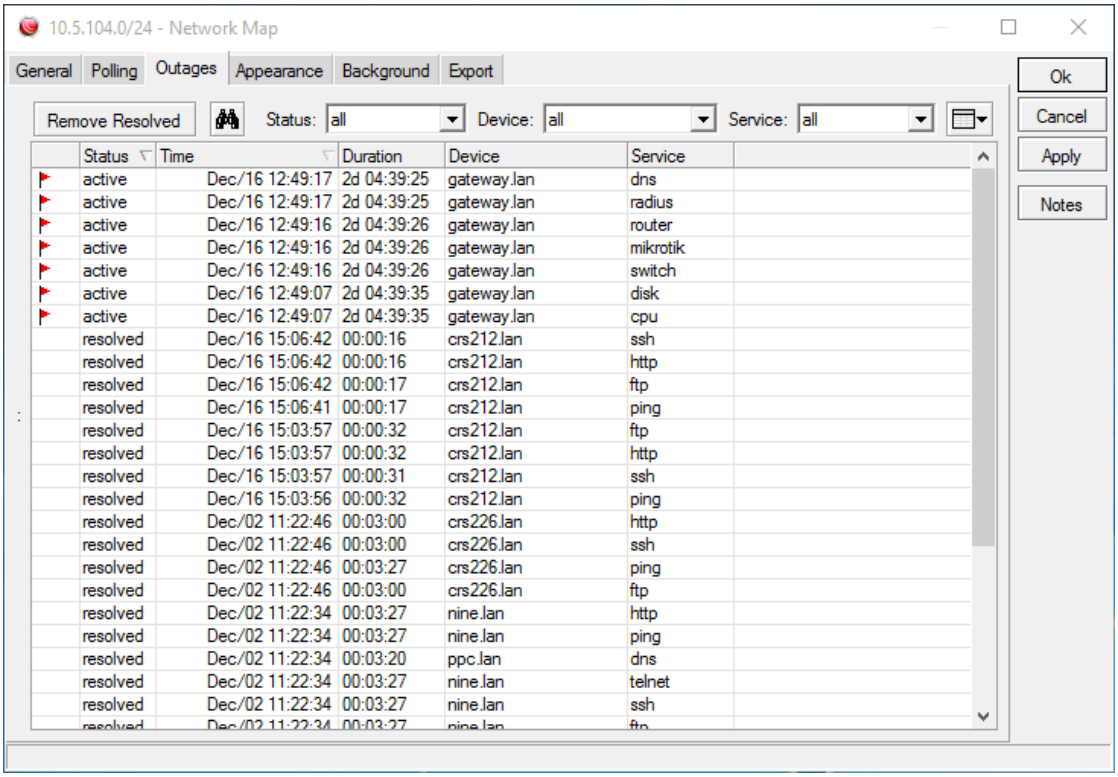
specified subnets, draw and layout a map of your networks, monitor services of your devices and alert you in case some service has problems.

Main Features:

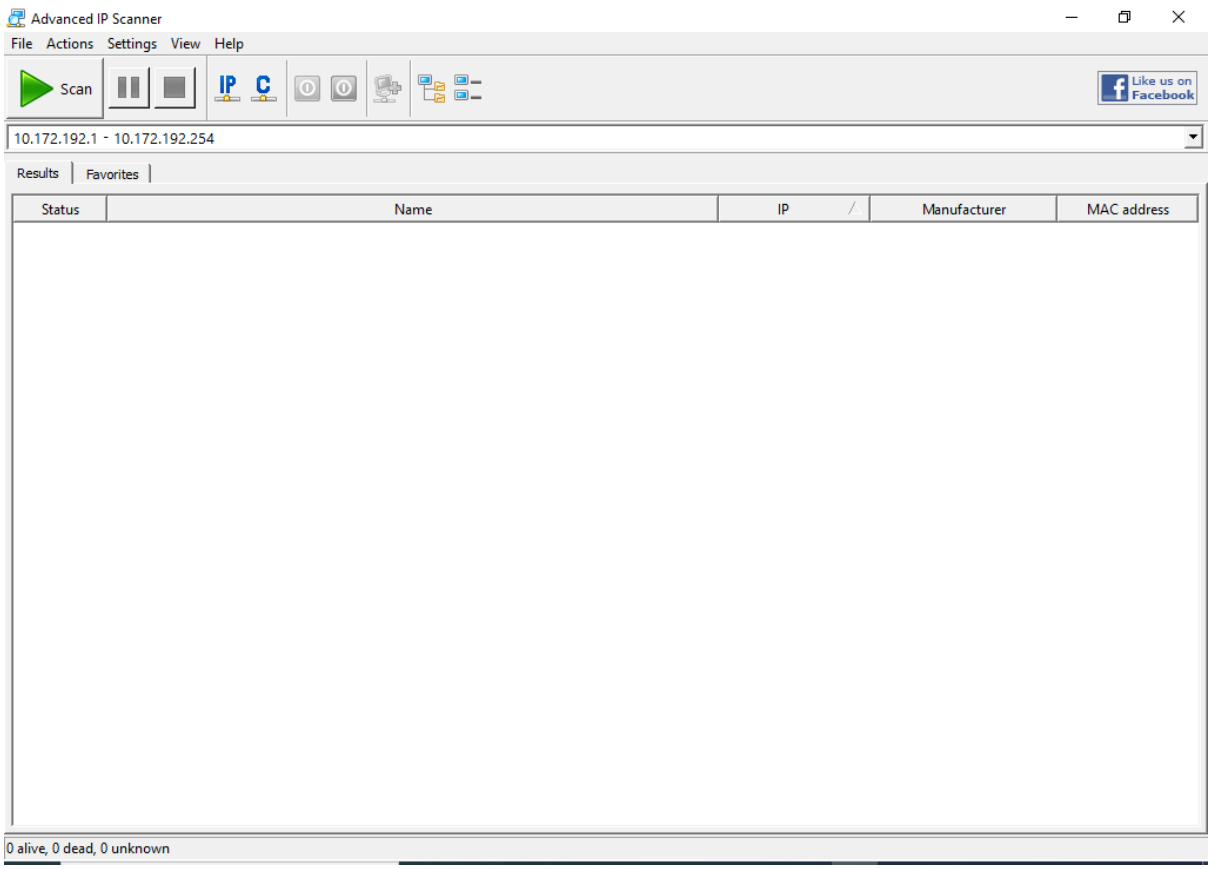
- Auto network discovery and layout
- Discovers any type or brand of device
- Device, Link monitoring, and notifications
- Includes SVG icons for devices, and supports custom icons and backgrounds
- Easy installation and usage
- Allows you to draw your own maps and add custom devices
- Supports SNMP, ICMP, DNS and TCP monitoring for devices that support it
- Individual Link usage monitoring and graphs
- Direct access to remote control tools for device management
- Supports remote Dude server and local client



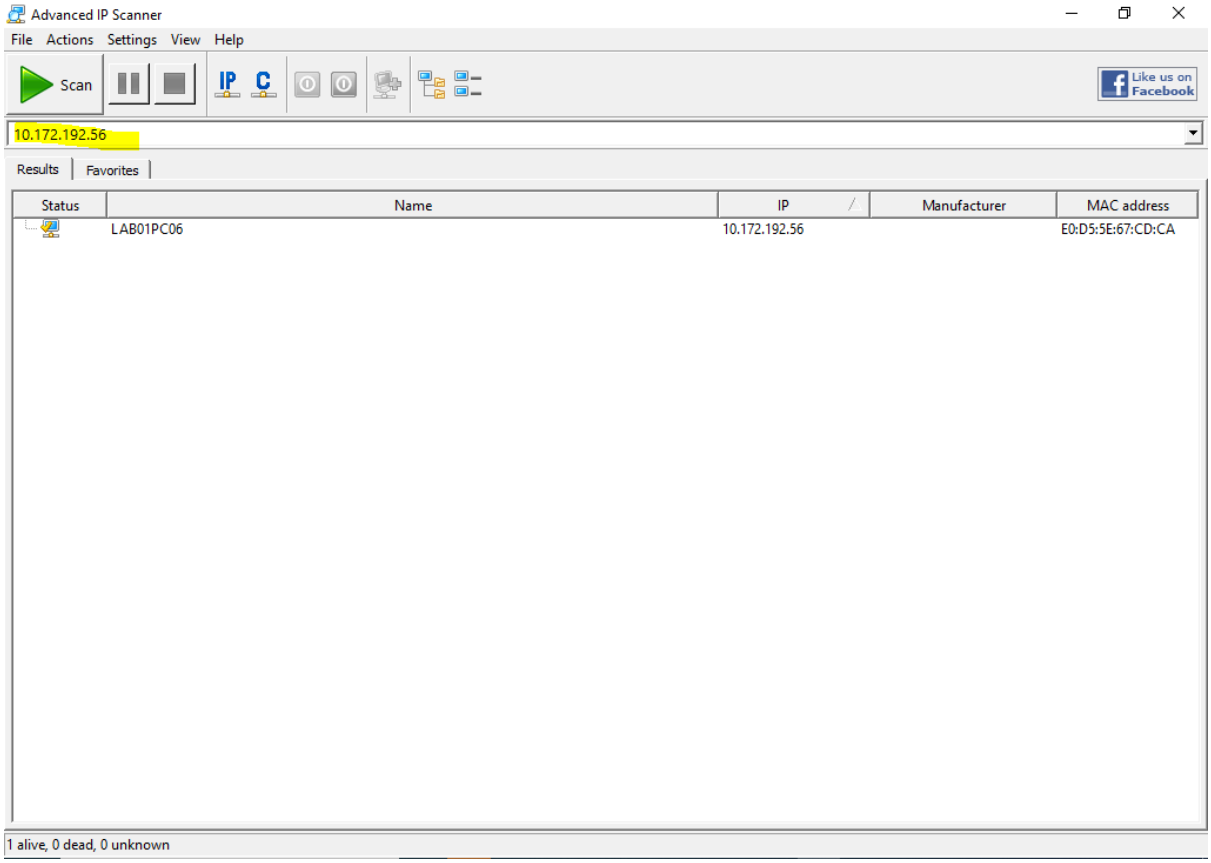

10.5.104.0/24 - Network Map
General
Polling
Outages
Appearance
Background
Export
Ok
Cancel
Apply
Notes
Name:
10.5.104.0/24
Default Zoom:
100%
Status:
partially down
Devices:
Partially Down - 1
Up - 16
Report Scan Status
csv
Network
Progress
Next S...
192.168.88.0/24
24
00:59:32
Auto Scan:


10.5.104.0/24 - Network Map
General
Polling
Outages
Appearance
Background
Export
Ok
Cancel
Apply
Notes
Remove Resolved
Status: all
Device: all
Service: all
Status
Time
Duration
Device
Service
active Dec/16 12:49:17 2d 04:39:25 gateway.lan dns
active Dec/16 12:49:17 2d 04:39:25 gateway.lan radius
active Dec/16 12:49:16 2d 04:39:26 gateway.lan router
active Dec/16 12:49:16 2d 04:39:26 gateway.lan mikrotik
active Dec/16 12:49:16 2d 04:39:26 gateway.lan switch
active Dec/16 12:49:07 2d 04:39:35 gateway.lan disk
active Dec/16 12:49:07 2d 04:39:35 gateway.lan cpu
resolved Dec/16 15:06:42 00:00:16 crs212.lan ssh
resolved Dec/16 15:06:42 00:00:16 crs212.lan http
resolved Dec/16 15:06:42 00:00:17 crs212.lan ftp
resolved Dec/16 15:06:41 00:00:17 crs212.lan ping
resolved Dec/16 15:03:57 00:00:32 crs212.lan ftp
resolved Dec/16 15:03:57 00:00:32 crs212.lan http
resolved Dec/16 15:03:57 00:00:31 crs212.lan ssh
resolved Dec/16 15:03:56 00:00:32 crs212.lan ping
resolved Dec/02 11:22:46 00:03:00 crs226.lan http
resolved Dec/02 11:22:46 00:03:00 crs226.lan ssh
resolved Dec/02 11:22:46 00:03:27 crs226.lan ping
resolved Dec/02 11:22:46 00:03:00 crs226.lan ftp
resolved Dec/02 11:22:34 00:03:27 nine.lan http
resolved Dec/02 11:22:34 00:03:27 nine.lan ping
resolved Dec/02 11:22:34 00:03:20 ppc.lan dns
resolved Dec/02 11:22:34 00:03:27 nine.lan telnet
resolved Dec/02 11:22:34 00:03:27 nine.lan ssh

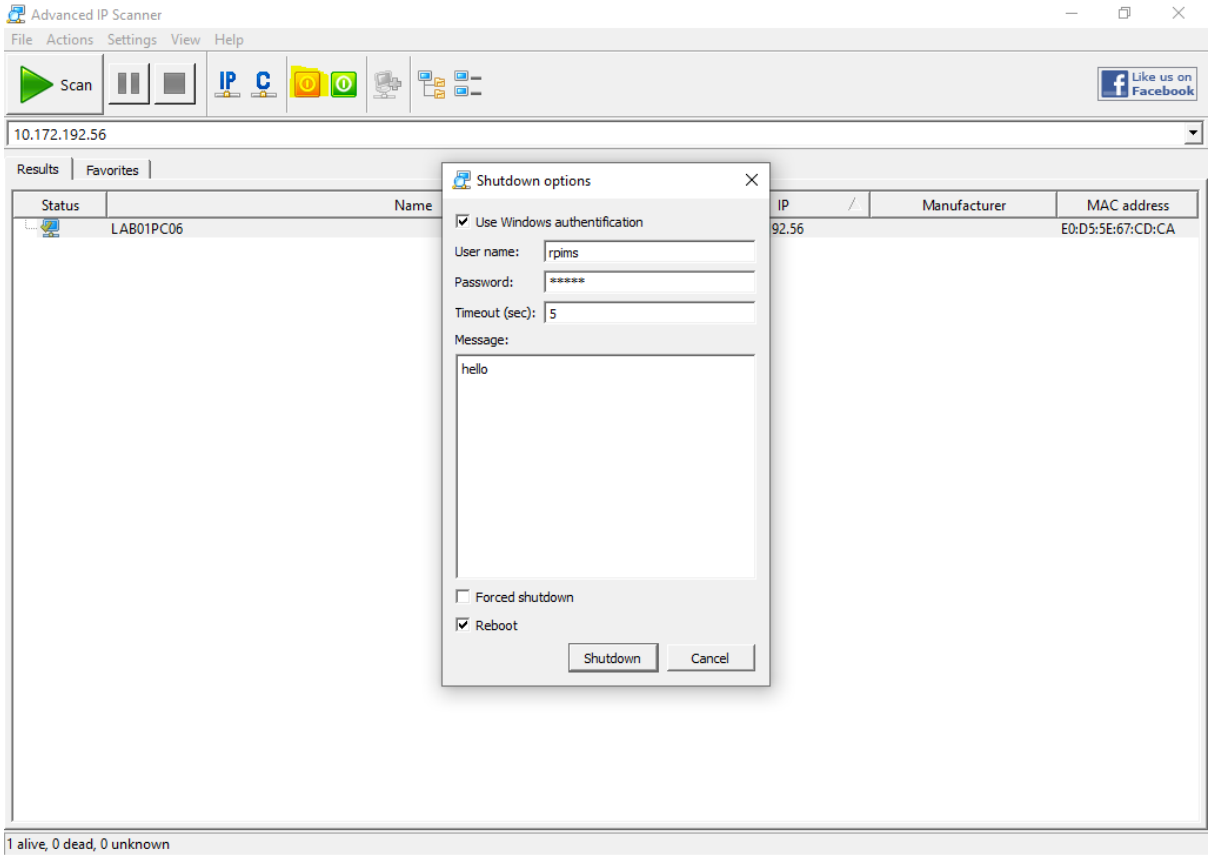
Advance ip scanner:



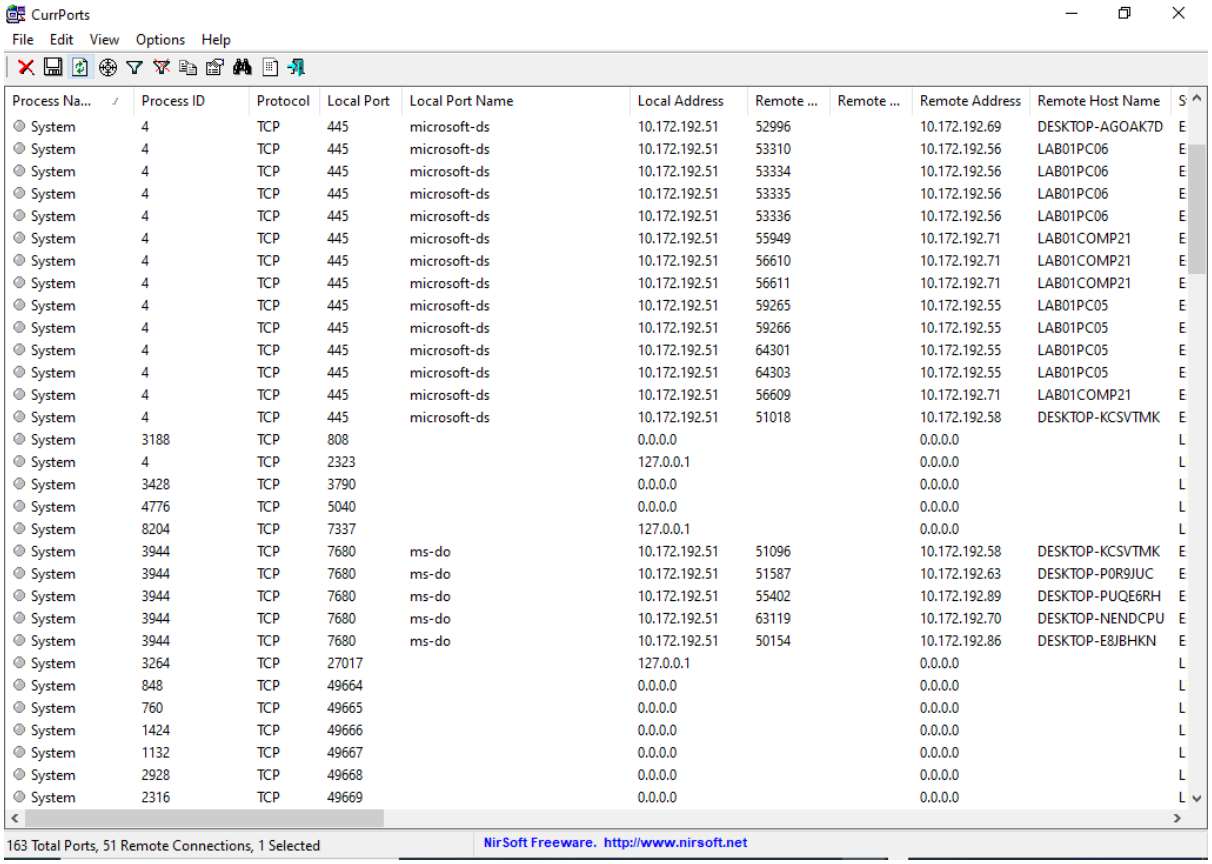
Insert ihte desired ip to be scan:



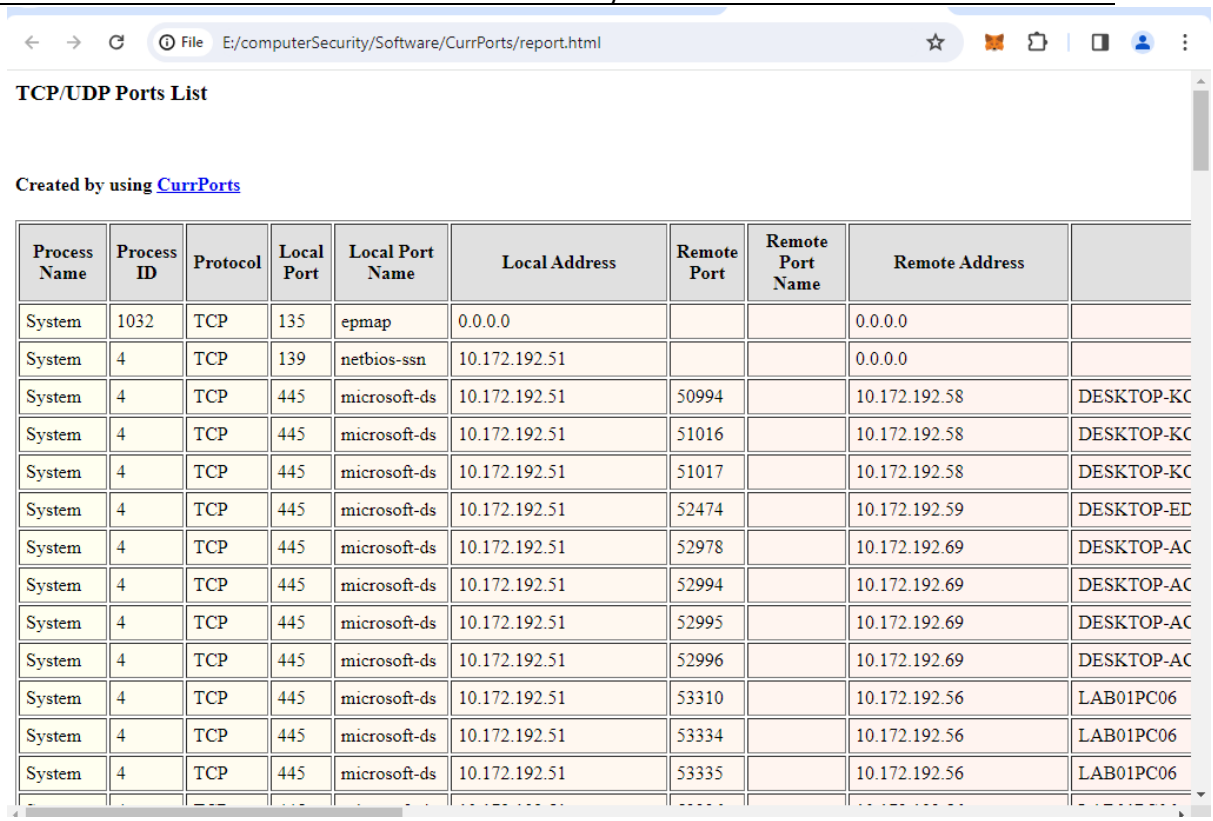
The clisk o the turnoff icon to shutdown the system:


Advanced IP Scanner
File Actions Settings View Help
Scan
Like us on Facebook
10.172.192.56
Results
Favorites
Status
Name
IP
Manufacturer
MAC address
LAB01PC06
92.56
E0:D5:5E:67:CD:CA
Shutdown options
Use Windows authentification
User name:
rpims
Password:
*****
Timeout (sec):
5
Message:
hello
Forced shutdown
Reboot
Shutdown
Cancel
1 alive, 0 dead, 0 unknown

CurrPorts:



Print the repot form _> view then HTML Report-All Items



File E:/computerSecurity/Software/CurrPorts/report.html

TCP/UDP Ports List

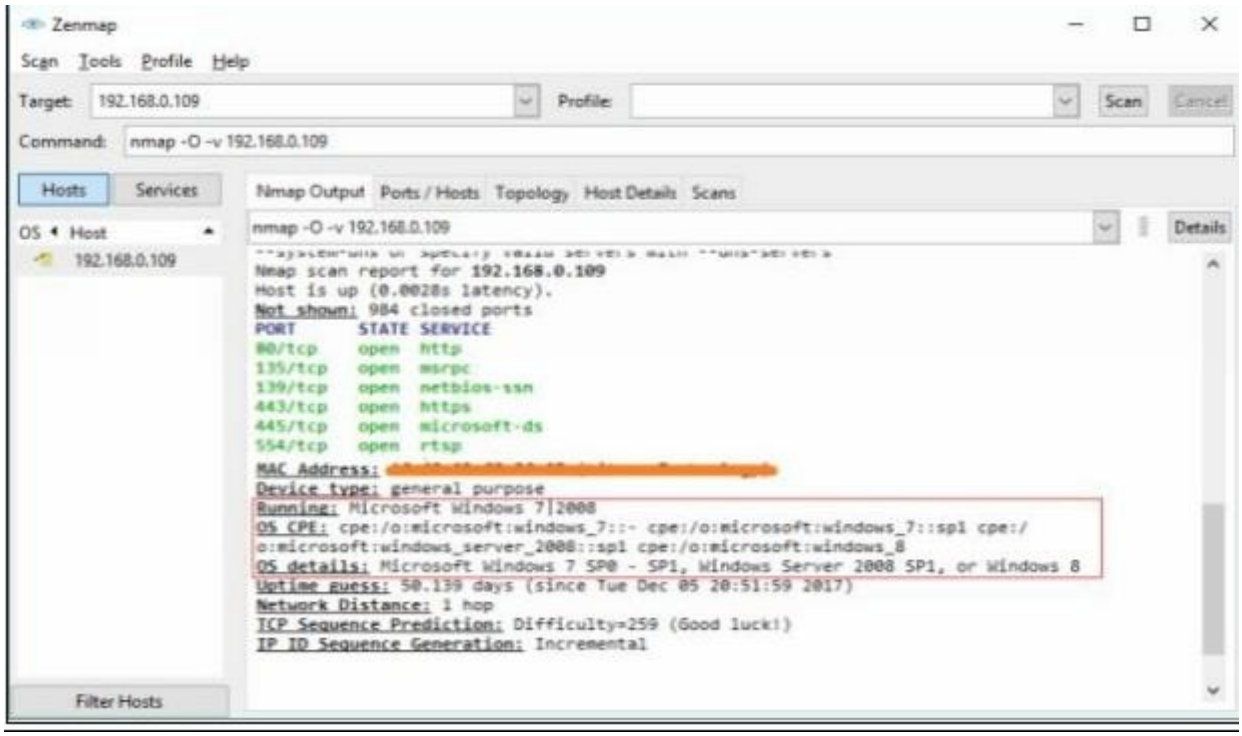
Created by using CurrPorts

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	
System	1032	TCP	135	epmap	0.0.0.0			0.0.0.0	
System	4	TCP	139	netbios-ssn	10.172.192.51			0.0.0.0	
System	4	TCP	445	microsoft-ds	10.172.192.51	50994		10.172.192.58	DESKTOP-KC
System	4	TCP	445	microsoft-ds	10.172.192.51	51016		10.172.192.58	DESKTOP-KC
System	4	TCP	445	microsoft-ds	10.172.192.51	51017		10.172.192.58	DESKTOP-KC
System	4	TCP	445	microsoft-ds	10.172.192.51	52474		10.172.192.59	DESKTOP-ED
System	4	TCP	445	microsoft-ds	10.172.192.51	52978		10.172.192.69	DESKTOP-AC
System	4	TCP	445	microsoft-ds	10.172.192.51	52994		10.172.192.69	DESKTOP-AC
System	4	TCP	445	microsoft-ds	10.172.192.51	52995		10.172.192.69	DESKTOP-AC
System	4	TCP	445	microsoft-ds	10.172.192.51	52996		10.172.192.69	DESKTOP-AC
System	4	TCP	445	microsoft-ds	10.172.192.51	53310		10.172.192.56	LAB01PC06
System	4	TCP	445	microsoft-ds	10.172.192.51	53334		10.172.192.56	LAB01PC06
System	4	TCP	445	microsoft-ds	10.172.192.51	53335		10.172.192.56	LAB01PC06

a. Perform Enumeration using the following tools:

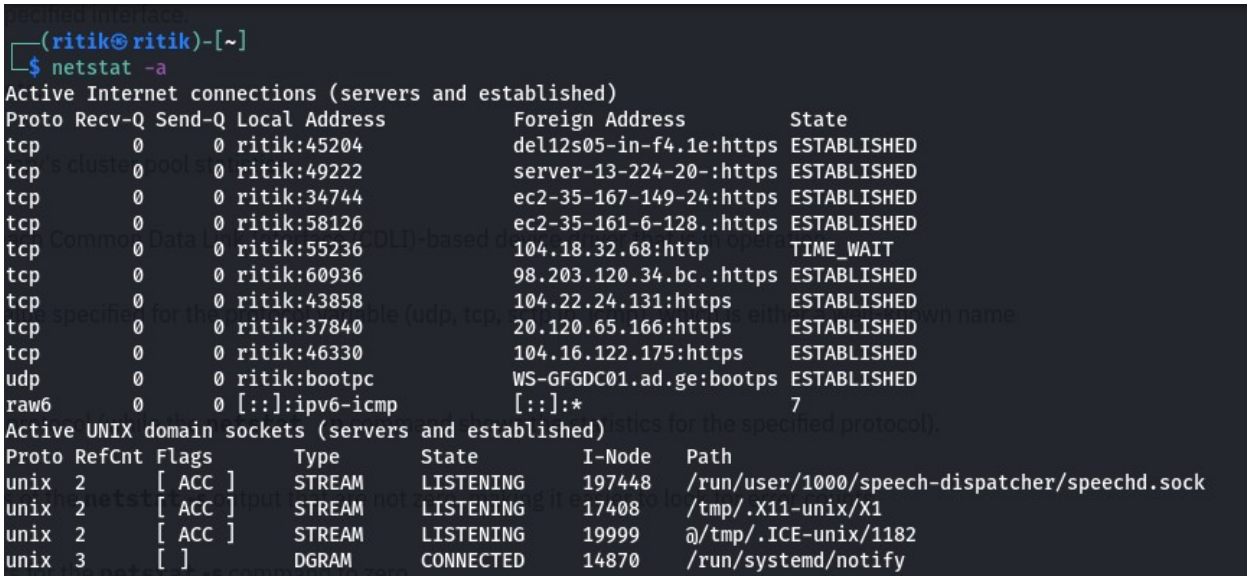
i. Nmap

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 bring someclues regarding nature of an operating system disclosing the type an OS. To perform OS detection with nmap perform the following: nmap -O<ip address>



ii. NetBIOS Enumeration Tool

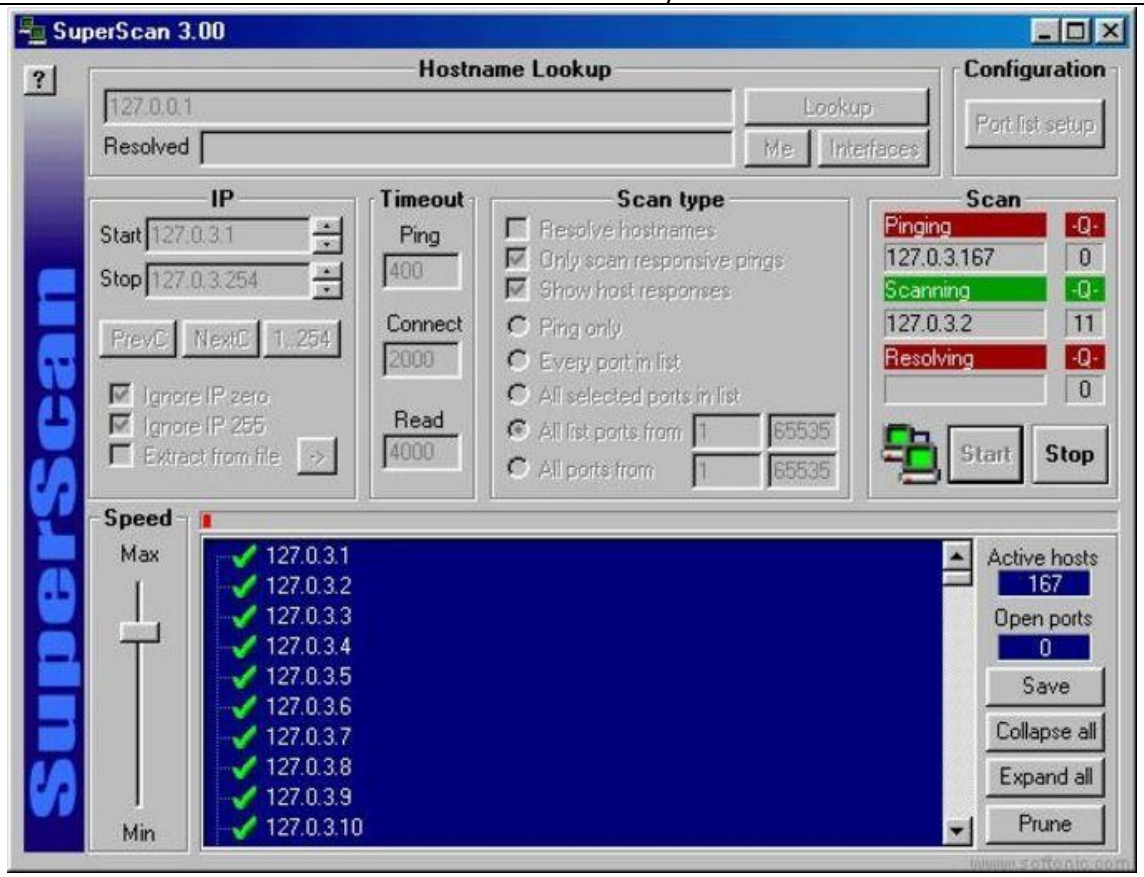
NetBIOS stands for Network Basic Input Output System. It Allows computer communicationover a LAN and allows them to share files and printers. NetBIOS names are used to identifynetwork devices over TCP/IP (Windows).



```
┌──(ritik㉿ritik)-[~]
└─$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ritik:45204             del12s05-in-f4.1e:https ESTABLISHED
tcp        0      0 ritik:49222             server-13-224-20-:https ESTABLISHED
tcp        0      0 ritik:34744             ec2-35-167-149-24:https ESTABLISHED
tcp        0      0 ritik:58126             ec2-35-161-6-128.:https ESTABLISHED
tcp        0      0 ritik:55236             104.18.32.68:http       TIME_WAIT
tcp        0      0 ritik:60936             98.203.120.34.bc.:https ESTABLISHED
tcp        0      0 ritik:43858             104.22.24.131:https     ESTABLISHED
tcp        0      0 ritik:37840             20.120.65.166:https     ESTABLISHED
tcp        0      0 ritik:46330             104.16.122.175:https    ESTABLISHED
udp        0      0 ritik:bootpc            WS-GFGDC01.ad.ge:bootps ESTABLISHED
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     197448   /run/user/1000/speech-dispatcher/speechd.sock
unix  2      [ ACC ]     STREAM     LISTENING     17408    /tmp/.X11-unix/X1
unix  2      [ ACC ]     STREAM     LISTENING     19999    @/tmp/.ICE-unix/1182
unix  3      [ ]         DGRAM      CONNECTED     14870    /run/systemd/notify
```

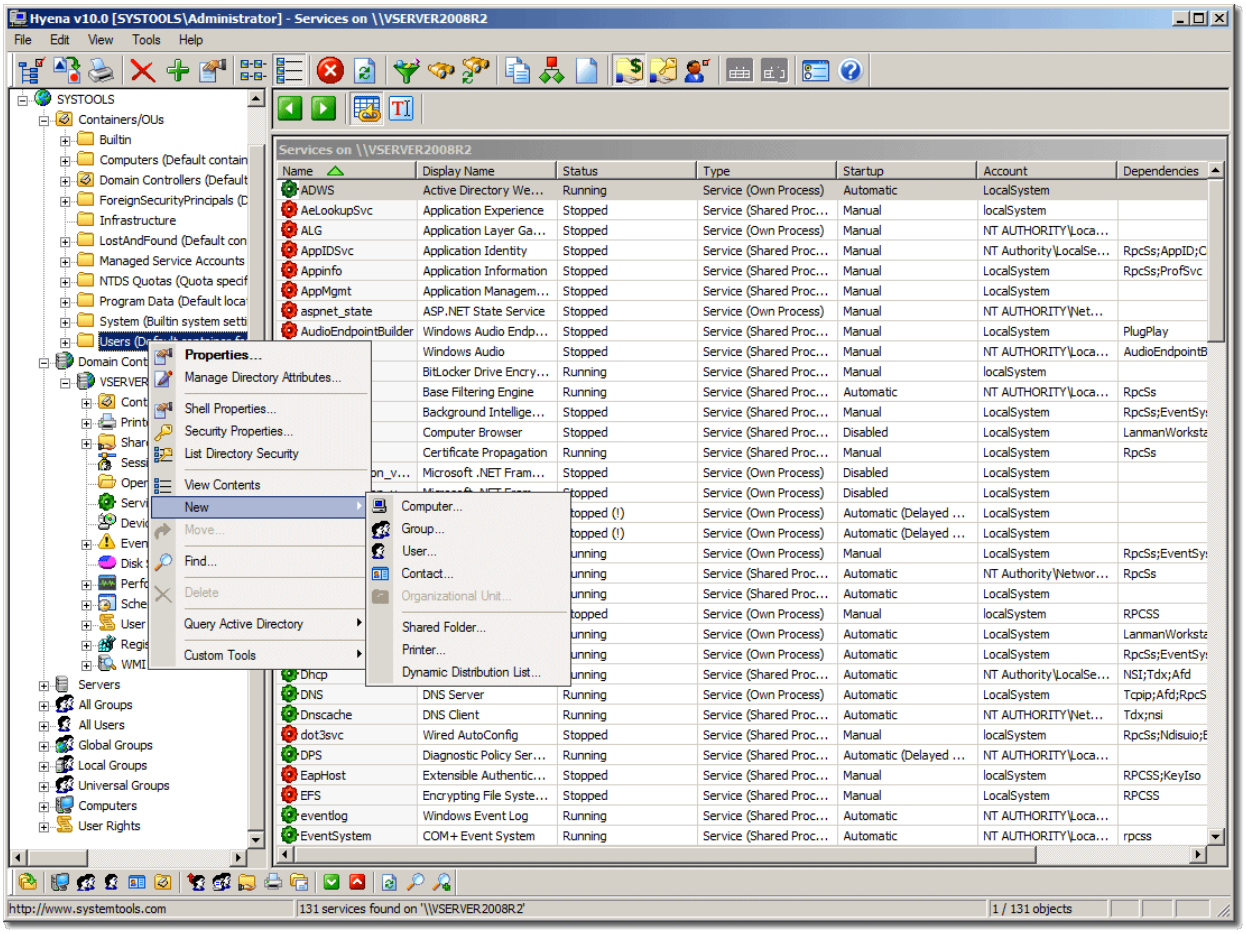
iii. SuperScan

SuperScan 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.


SuperScan 3.00
Hostname Lookup
127.0.0.1
Lookup
Resolved
Me
Interfaces
Configuration
Port list setup
IP
Start 127.0.3.1
Stop 127.0.3.254
PrevC
NextC
1..254
Ignore IP zero
Ignore IP 255
Extract from file
->
Timeout
Ping
400
Connect
2000
Read
4000
Scan type
Resolve hostnames
Only scan responsive pings
Show host responses
Ping only
Every port in list
All selected ports in list
All list ports from 1 65535
All ports from 1 65535
Scan
Pinging -Q-
127.0.3.167 0
Scanning -Q-
127.0.3.2 11
Resolving -Q-
0
Start
Stop
Speed
Max
Min
127.0.3.1
127.0.3.2
127.0.3.3
127.0.3.4
127.0.3.5
127.0.3.6
127.0.3.7
127.0.3.8
127.0.3.9
127.0.3.10
Active hosts
167
Open ports
0
Save
Collapse all
Expand all
Prune
SuperScan

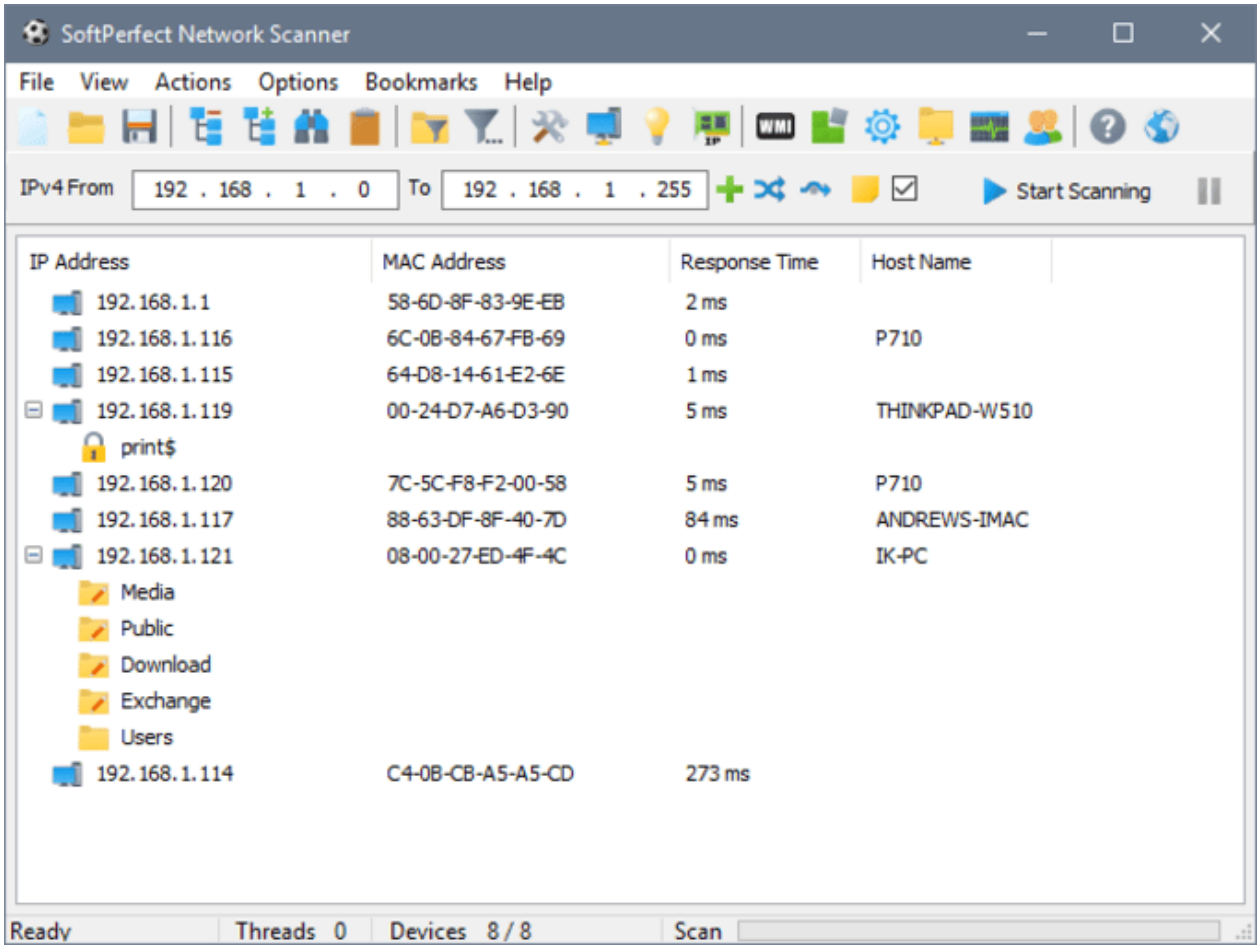
iv. Hyena

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



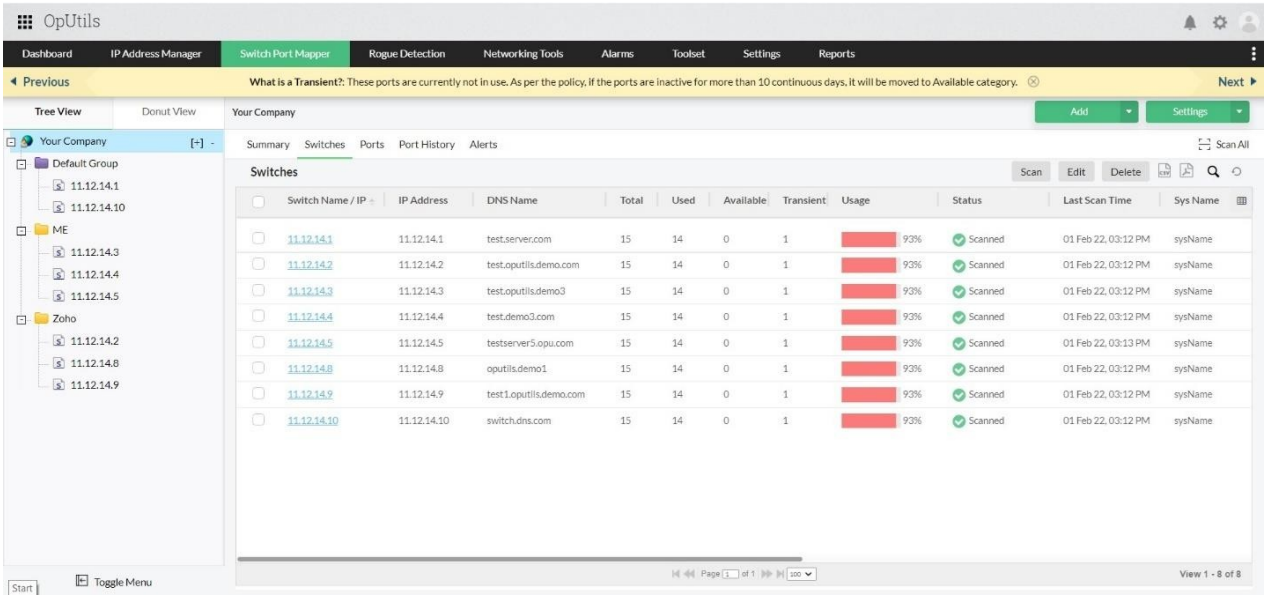
v. SoftPerfect Network Scanner Tool

SoftPerfect 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.



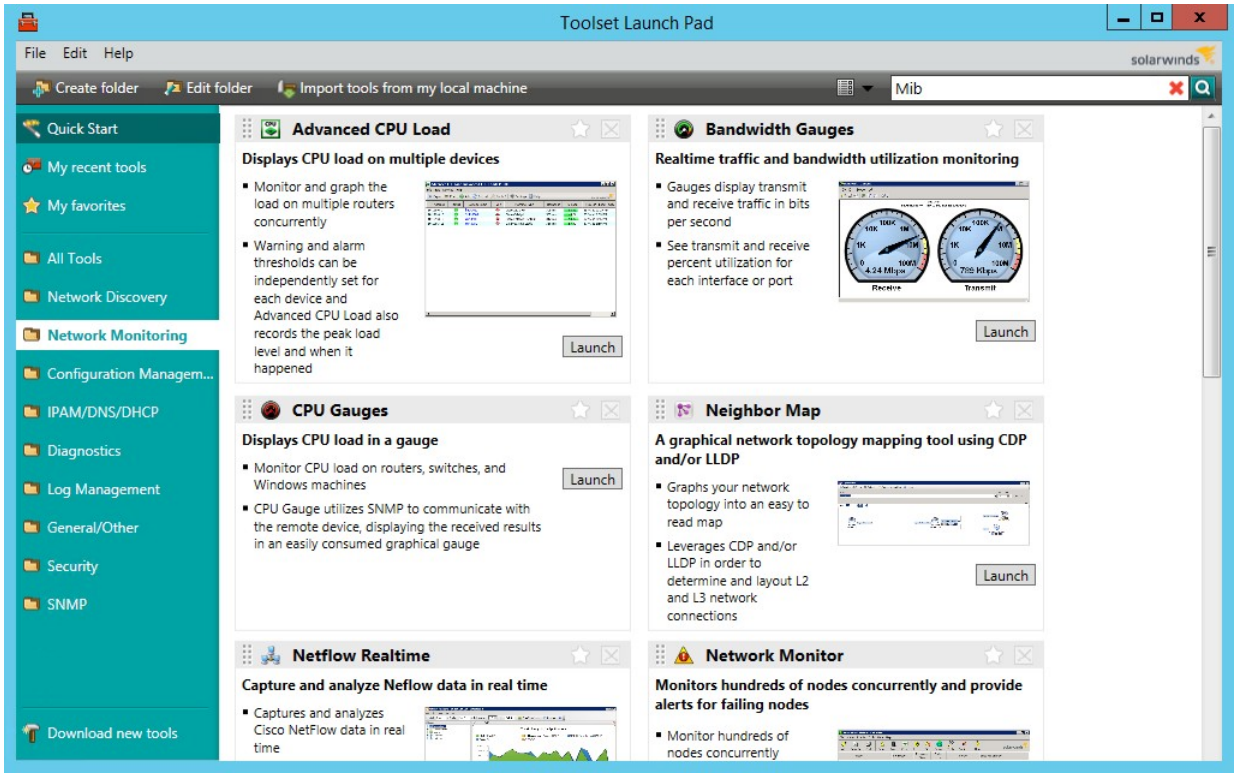
vi. OpUtils

OpUtils is **a IP address and Switch port management software that is geared towards helping engineers efficiently monitor, diagnose and troubleshoot IT resources**. OpUtilscomplements existing management tools by providing trouble shooting and real-time monitoring capabilities.



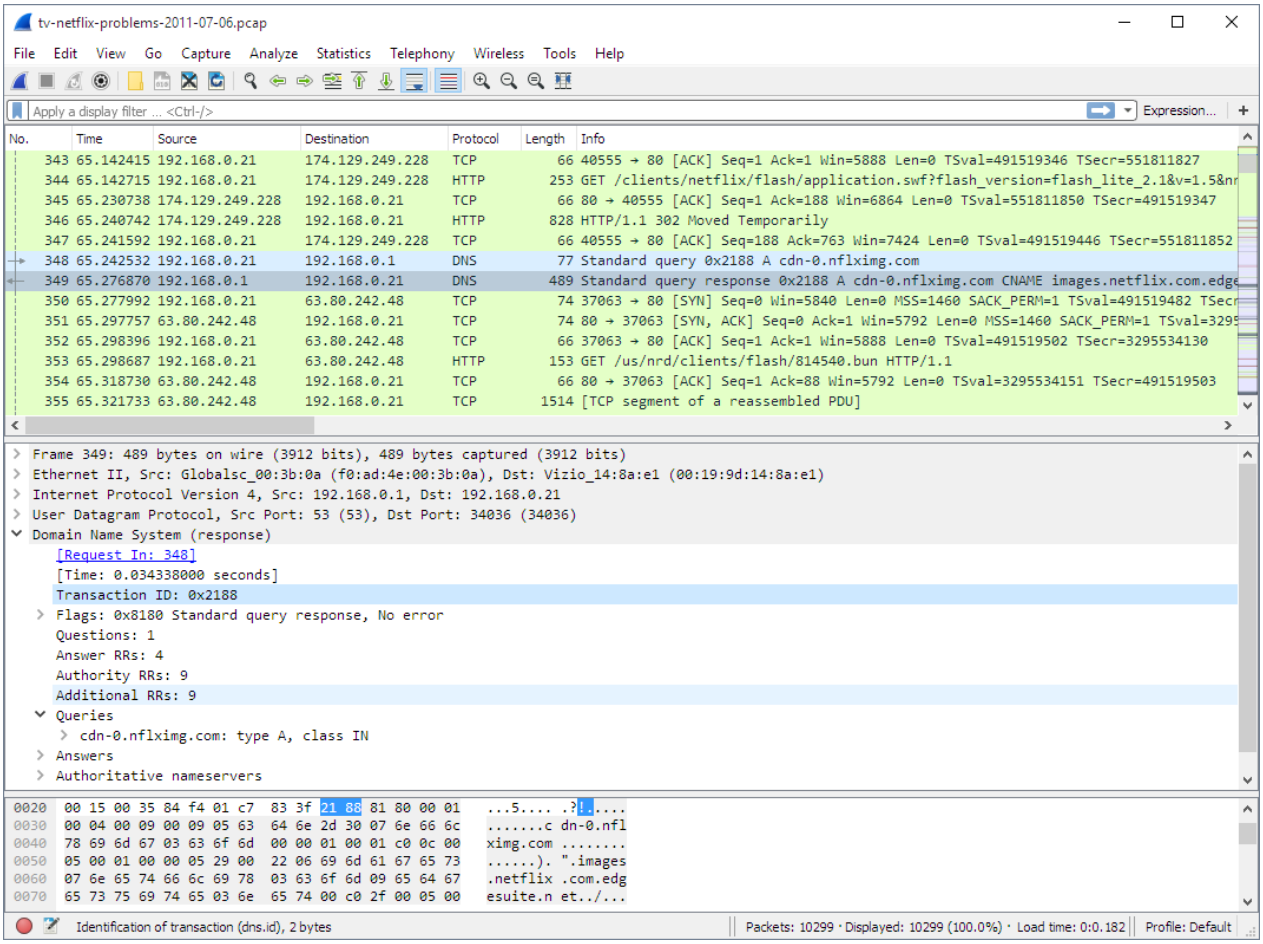
vii. SolarWinds Engineer's Toolset

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.



viii. Wireshark

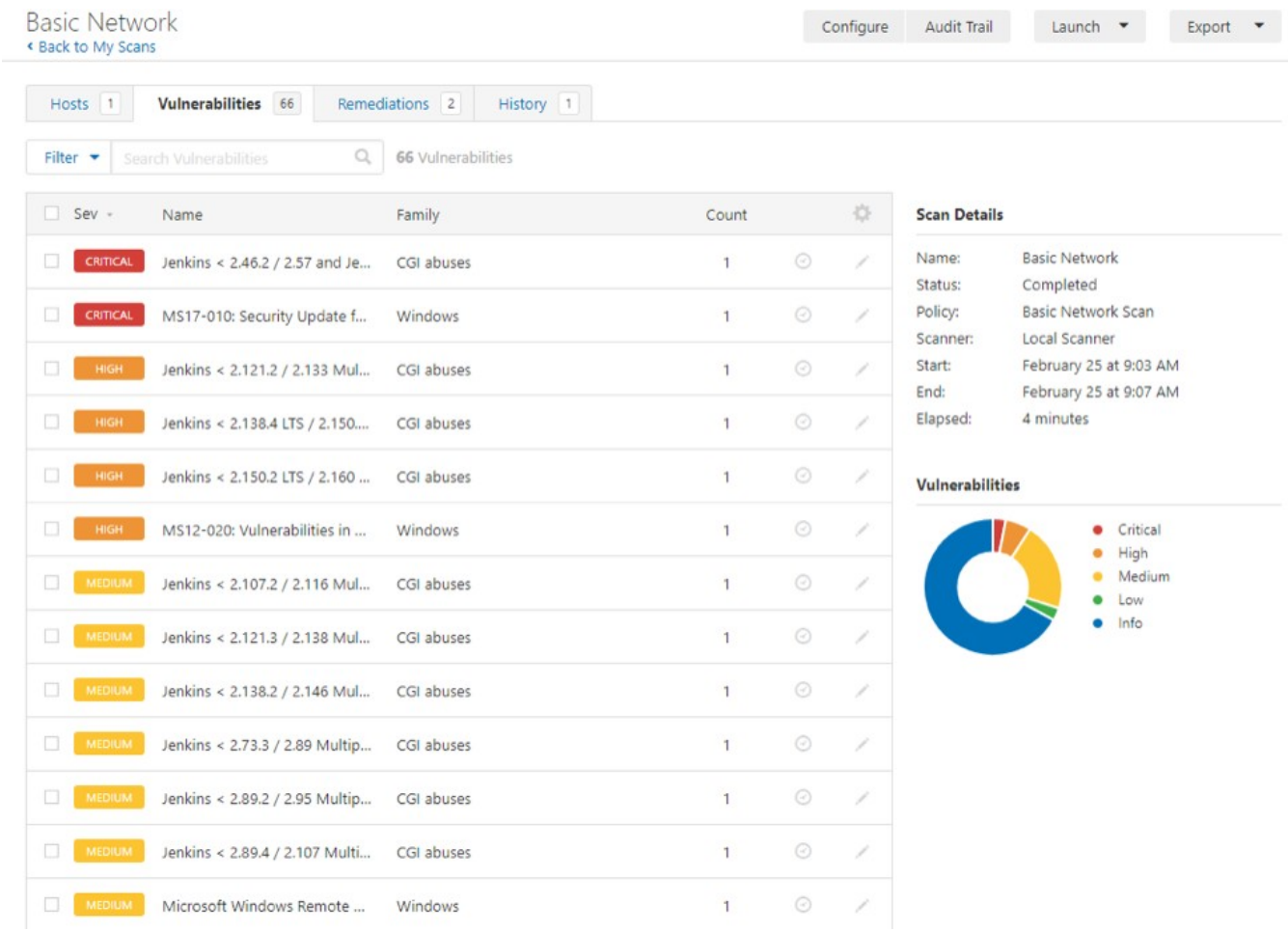
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally namedEthereal, the project was renamed Wireshark in May 2006 due to trademark issues



b. Perform the vulnerability analysis using the following tools:

i. Nessus

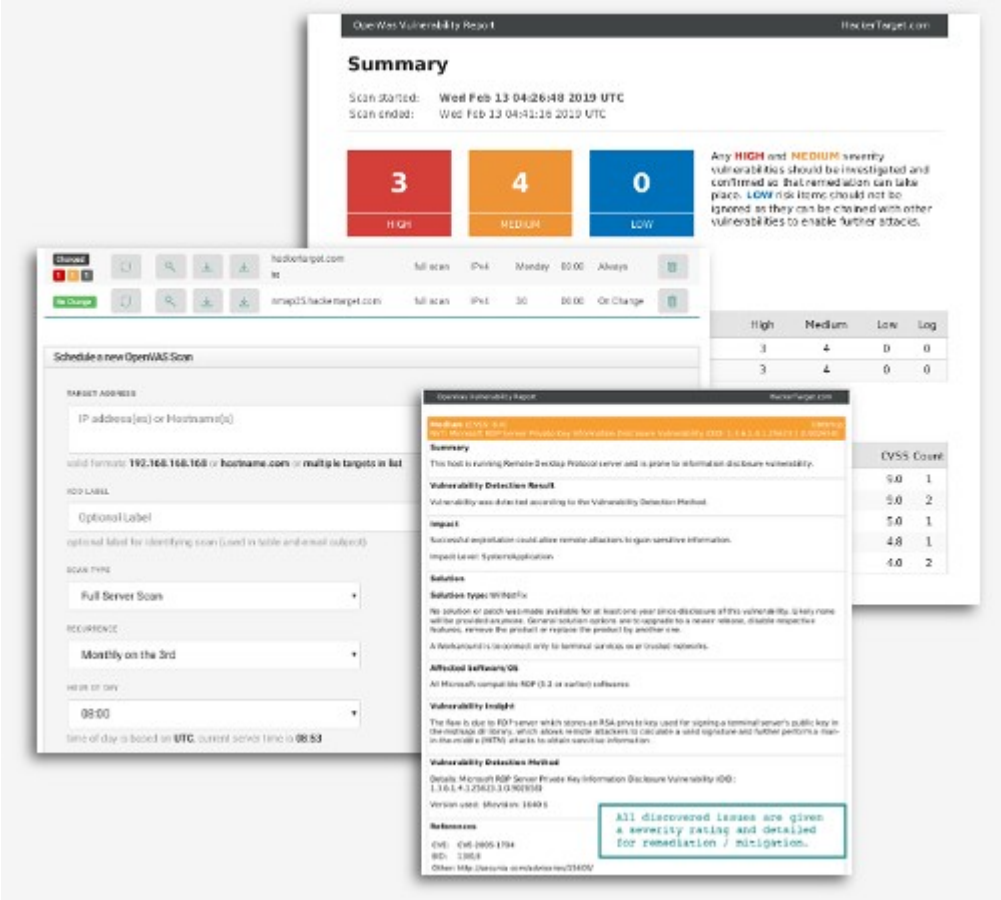
Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as-a-Service solution. Nessus is an open-source network vulnerability scanner that 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.



ii. OpenVas

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
The scanner obtains the tests for detecting vulnerabilities from a feed that has a long history anddaily updates.

OpenVAS has been developed and driven forward by the company Greenbone Networks since 2006. As part of the commercial vulnerability management product family Greenbone Enterprise Appliance, the scanner forms the Greenbone Community Edition together with other open-source modules.


Summary
Scan started: Wed Feb 13 04:26:48 2019 UTC
Scan ended: Wed Feb 13 04:41:16 2019 UTC
3
HIGH
4
MEDIUM
0
LOW
Any HIGH and MEDIUM severity vulnerabilities should be investigated and confirmed so that remediation can take place. LOW risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.
Schedule a new OpenVAS Scan
Full Server Scan
Monthly on the 3rd
08:00
All discovered issues are given a severity rating and detailed for remediation / mitigation.

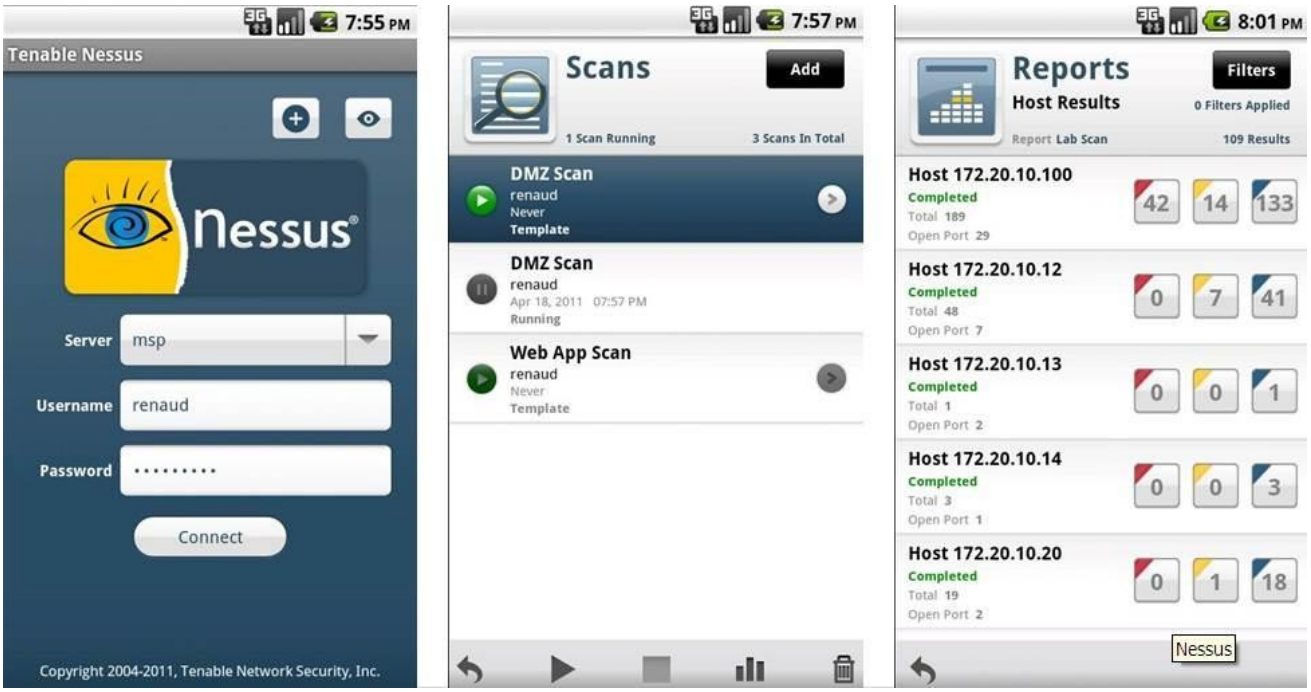
Practical No. 4

a. Perform mobile network scanning using NESSUS

Nessus has implemented new features to help users combat mobile threats. Network-based scanning is not the right approach to identify vulnerabilities on mobile devices, due in large part to the fact that most devices are in "sleep" mode and/or using a 3G/4G network. However, MDM (Mobile Device Management) technologies maintain information about the devices, including information about security vulnerabilities.

With Nessus Manager, the Nessus Mobile Devices plugin family allows you to obtain information from devices registered in a Mobile Device Manager (MDM) and from Active Directory servers that contain information from Microsoft Exchange Servers.

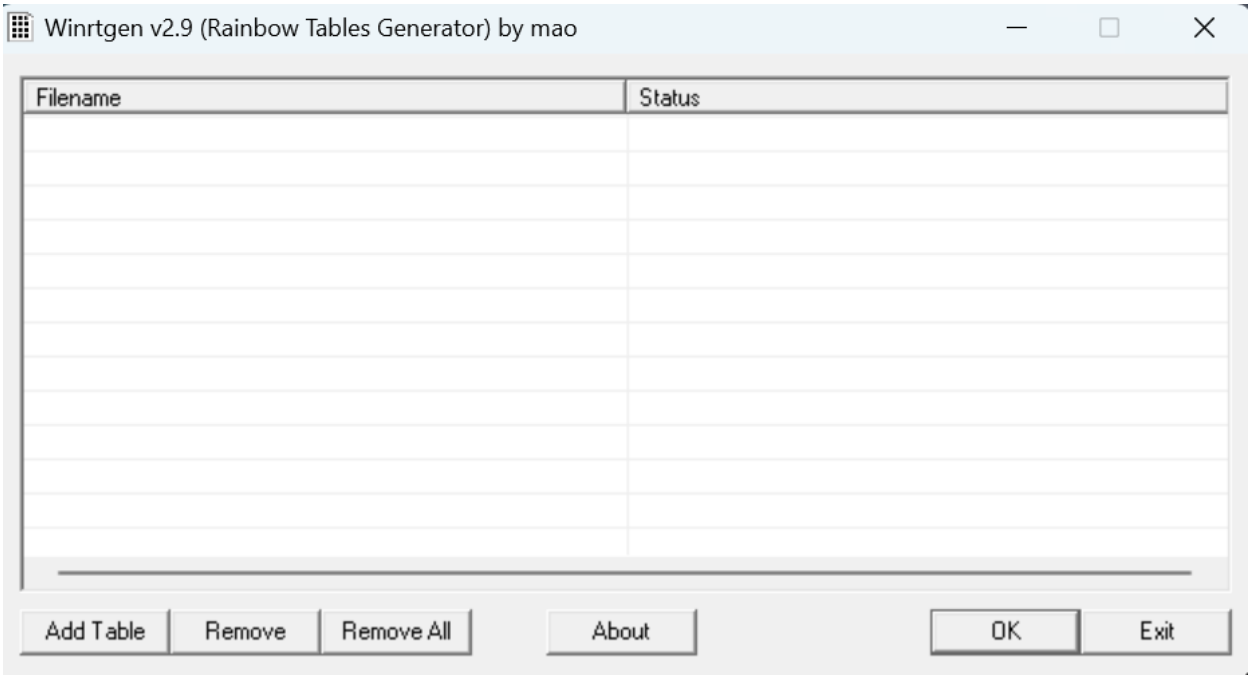
- To query for information, the Nessus scanner must be able to reach the Mobile DeviceMan-agement servers. Ensure no screening devices block traffic to these systems fromthe Nessus scanner. In addition, you must give Nessus administrative credentials (for example, domain administrator) to the Active Directory servers.
- To scan for mobile devices, you must configure Nessus with authentication information for the management server and the mobile plugins. Since Nessus authenticates directly tothe management servers, you do not need to configure a scan policy to scan specific hosts.
- For ActiveSync scans that access data from Microsoft Exchange servers, Nessus retrieves information from phones that have been updated in the last 365 days.



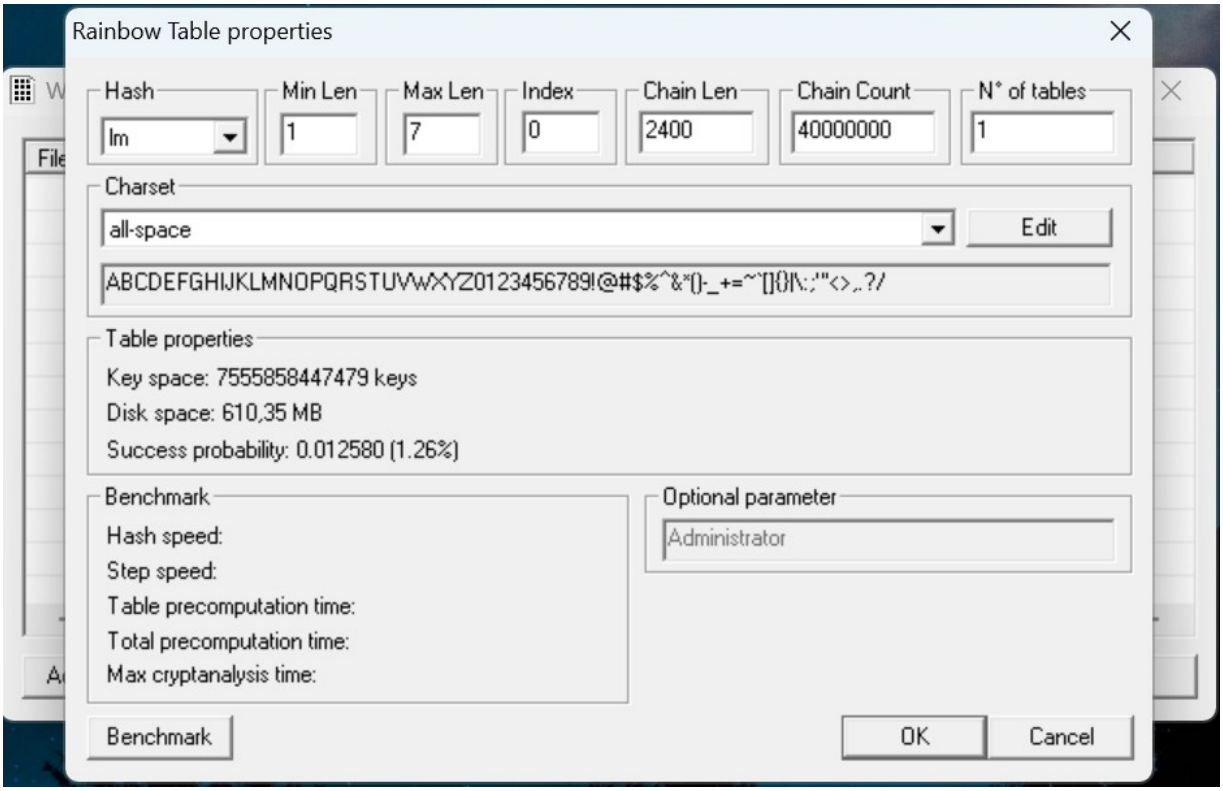
b. Perform the System Hacking using the following tools:

i. Winrtgen

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

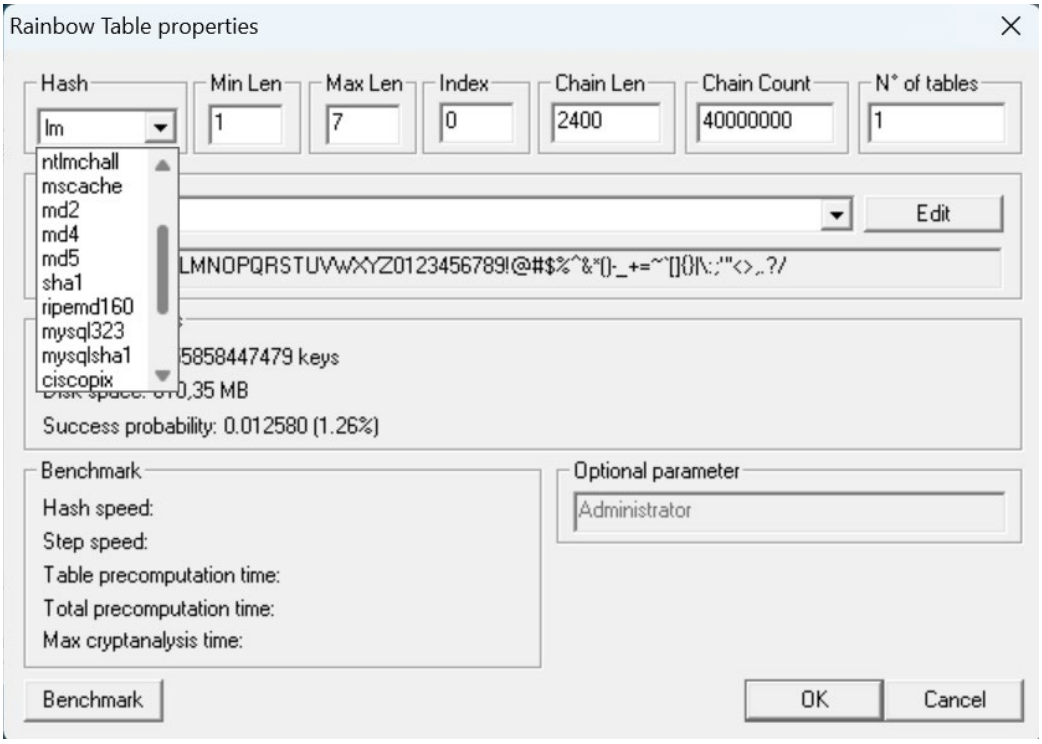


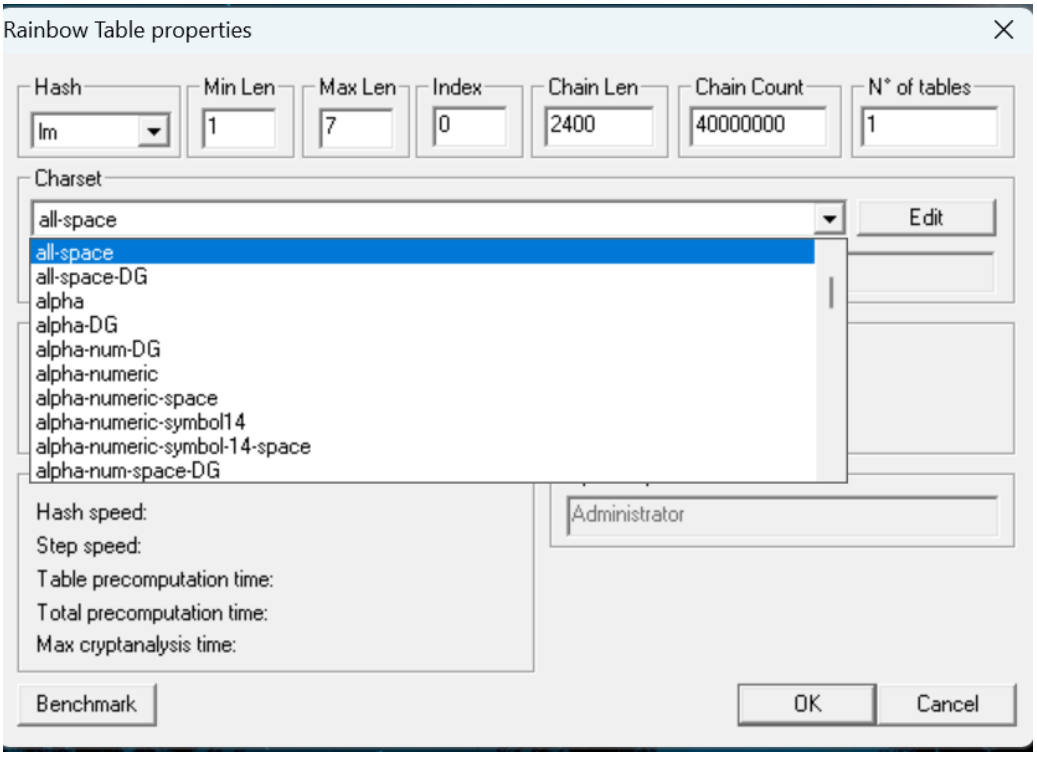
To generate rainbow tables first we will have to modify the properties of WinRTGen according to our need, and to do so Click on "Add Table". After this, a new box will appear named "Rainbow Table Properties"



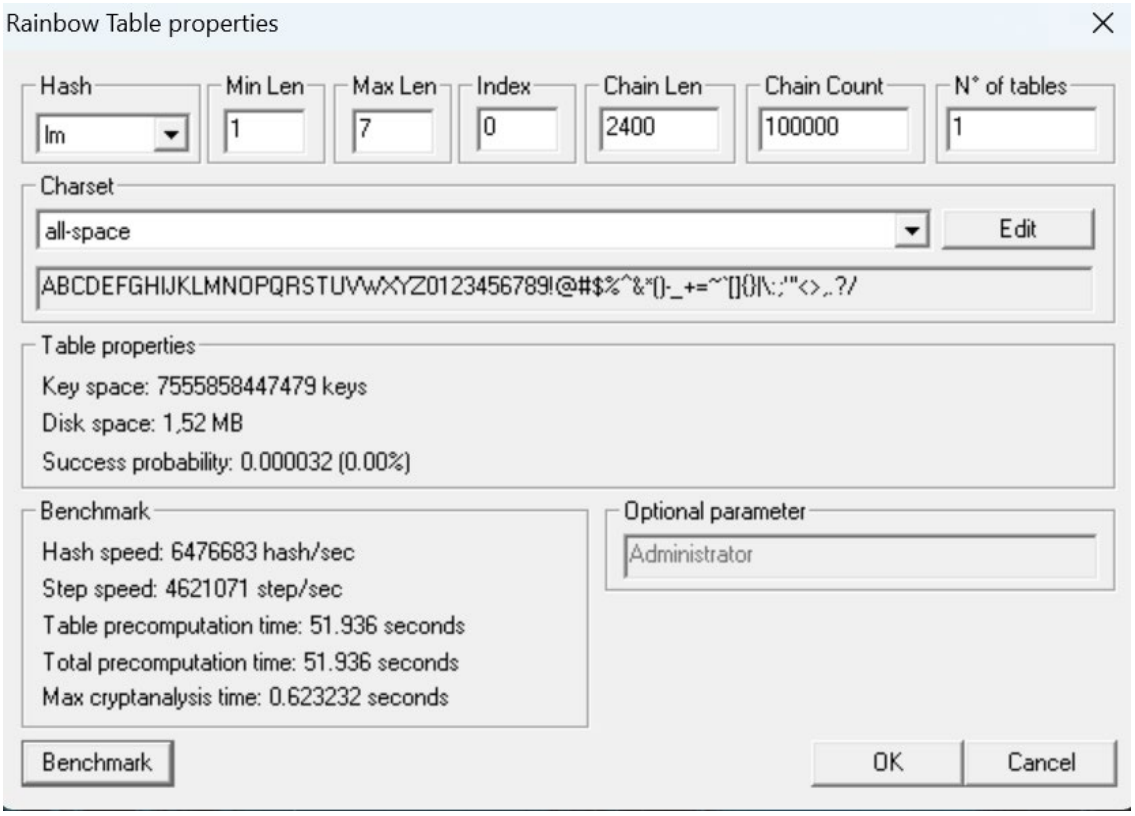
In the "**Rainbow Table Properties**" window we have the option to modify settings in order to generate rainbow tables according to our needs. The following properties can be modified:

- ☐ **Hash**: The type of encryption we want the rainbow table to be generated. For exampleMD5, MD4, SHA1, etc.

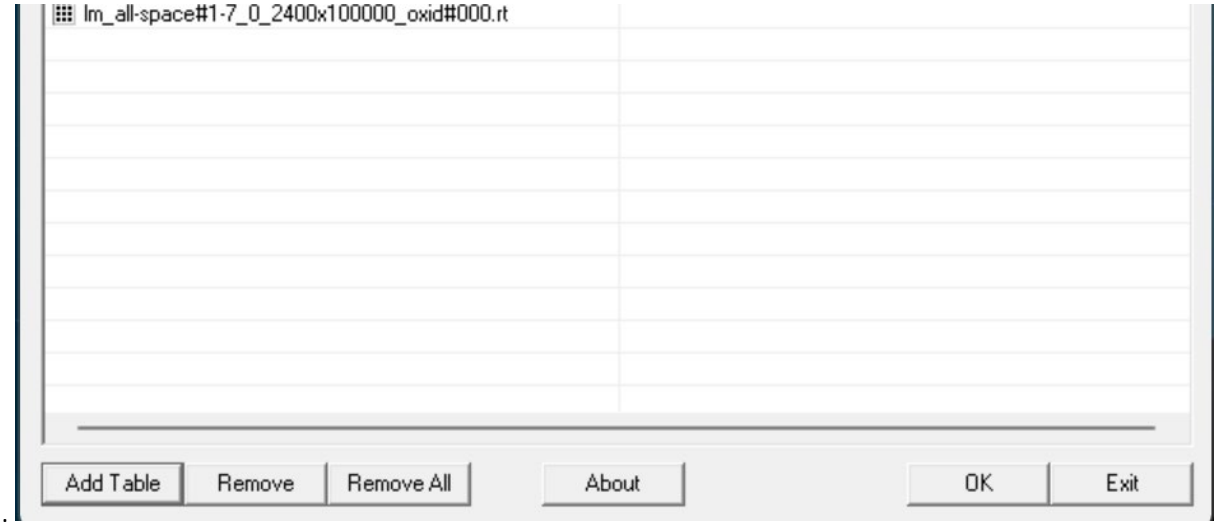




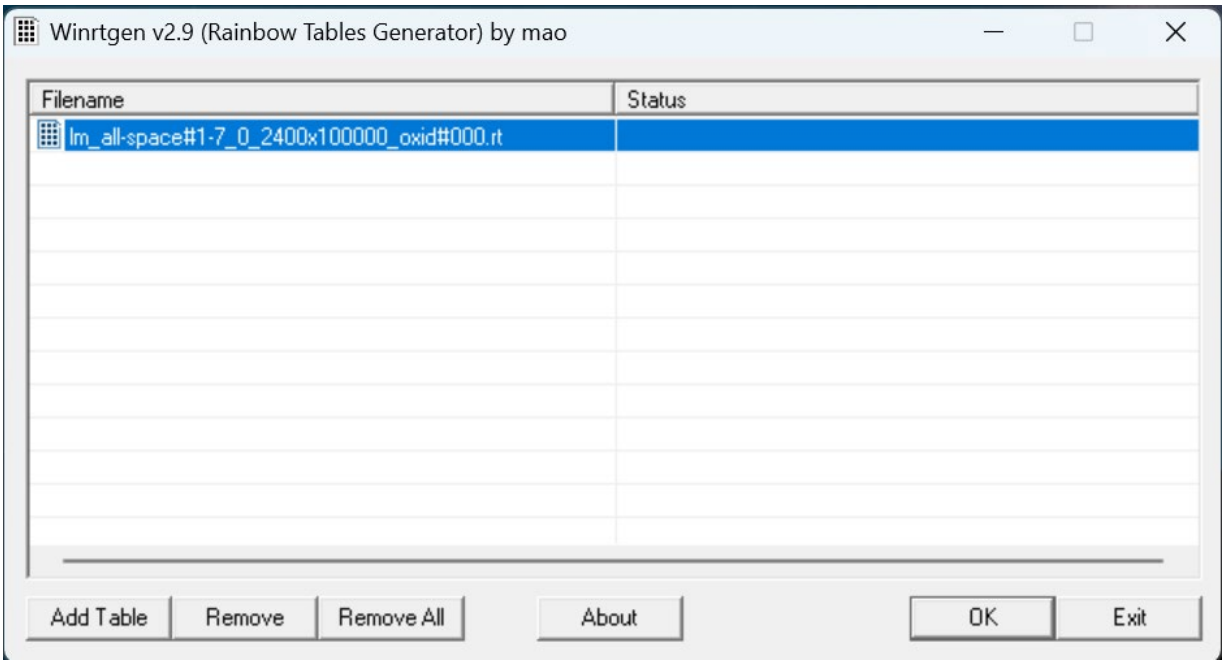
After assigning the values to the properties according to our needs click on “Benchmarks”. This will show the estimated time, Hash speed, Step speed, Table Pre-computing time, etc. that will be required to generate the Rainbow Table according to assigned properties.



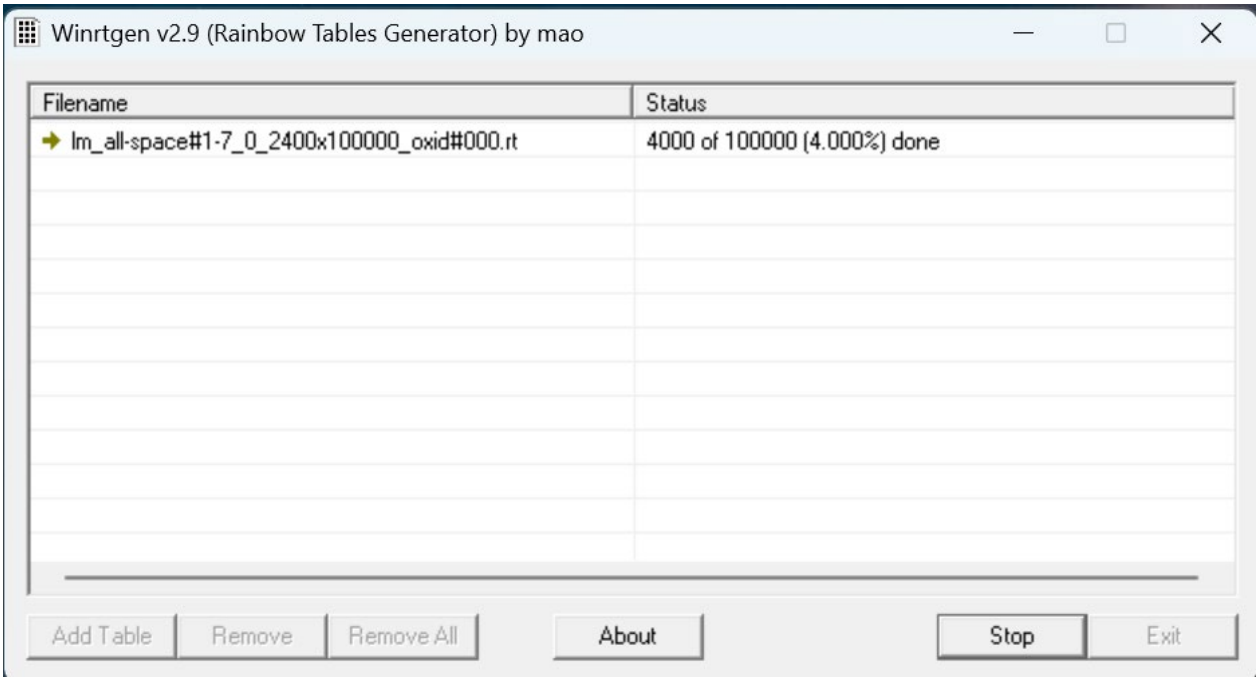
After “Benchmark” click on “Ok”. This will add the Rainbow Table to the queue in the main window of WinRTGen



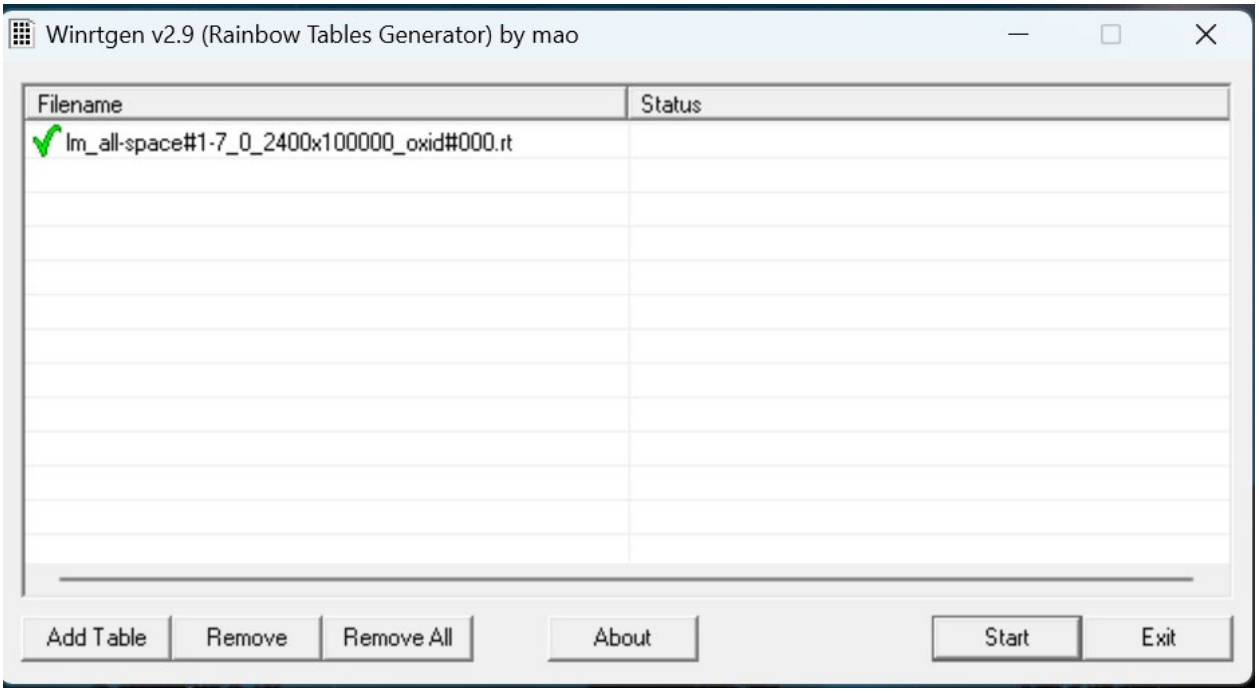
After this click on “Rainbow Table” You want to start processing and click “OK” .



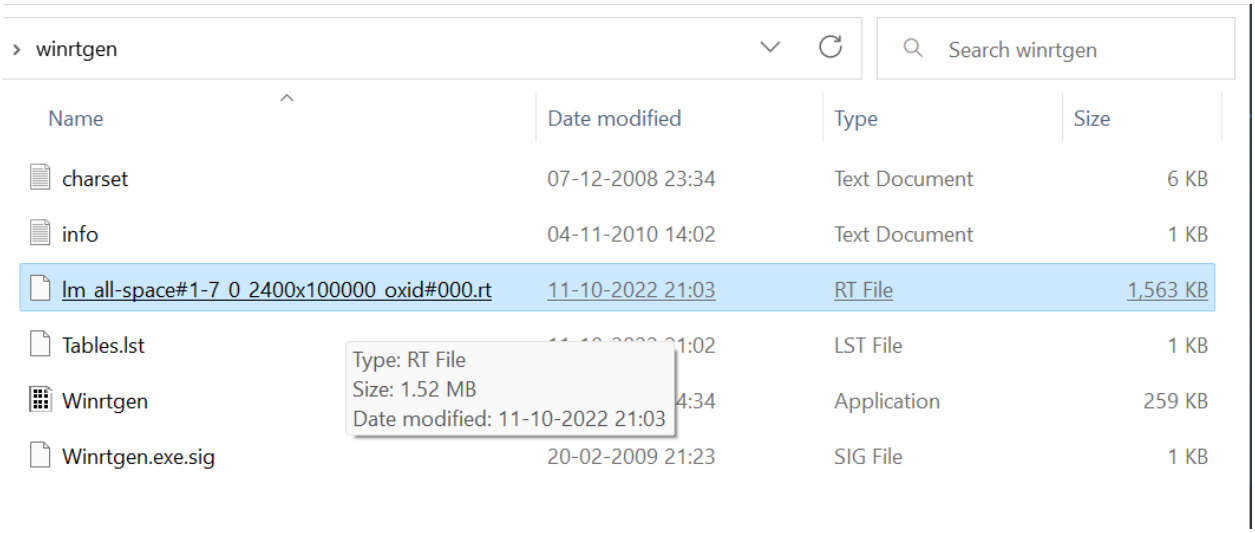
After clicking on ‘OK’ the WinRTGen” will start generating a rainbow table.



After completion, the window will appear as follows.



This table will be saved to your WinRTGen Directory.



ii. PWDump

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.

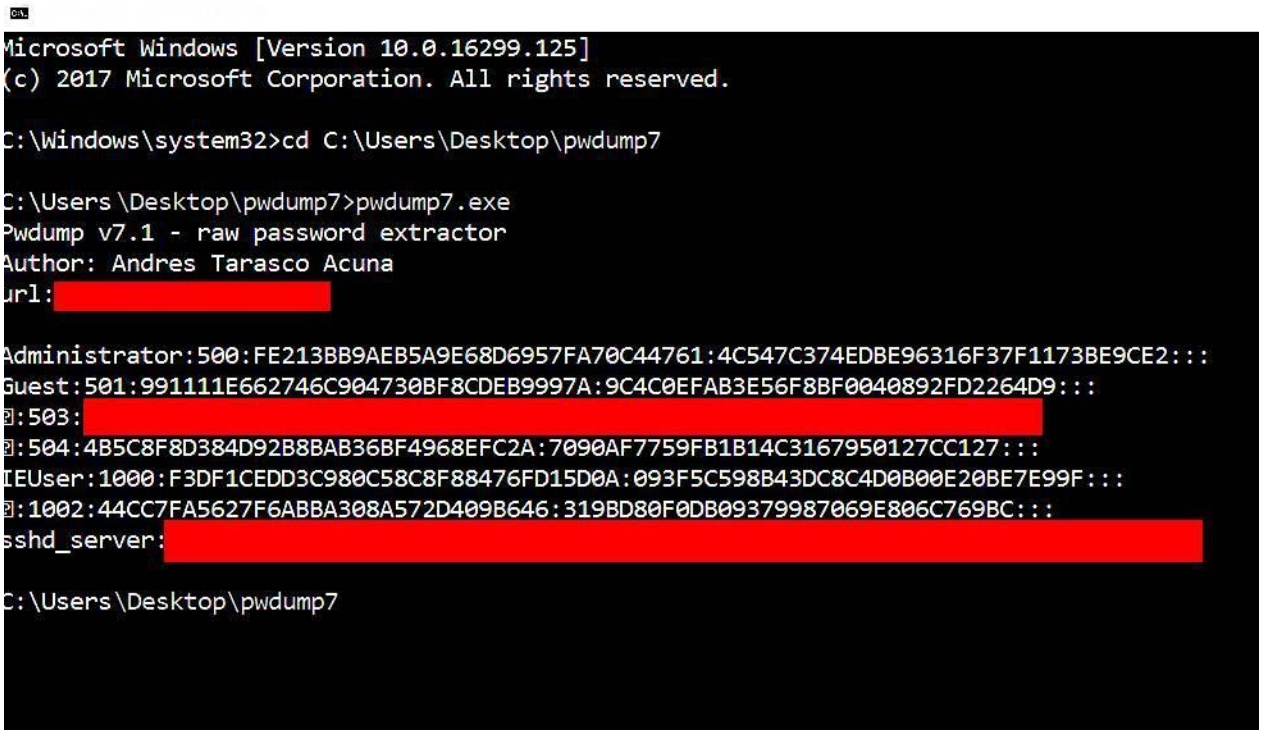
This utility was created by Tarasco. This utility dumps the system's SAM file's credentials after extracting it. Simply enter the following line on the command prompt after downloading to use this tool:

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



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 Windowsinstallation. This is made possible by the fact that Ophcrack itself contains a small

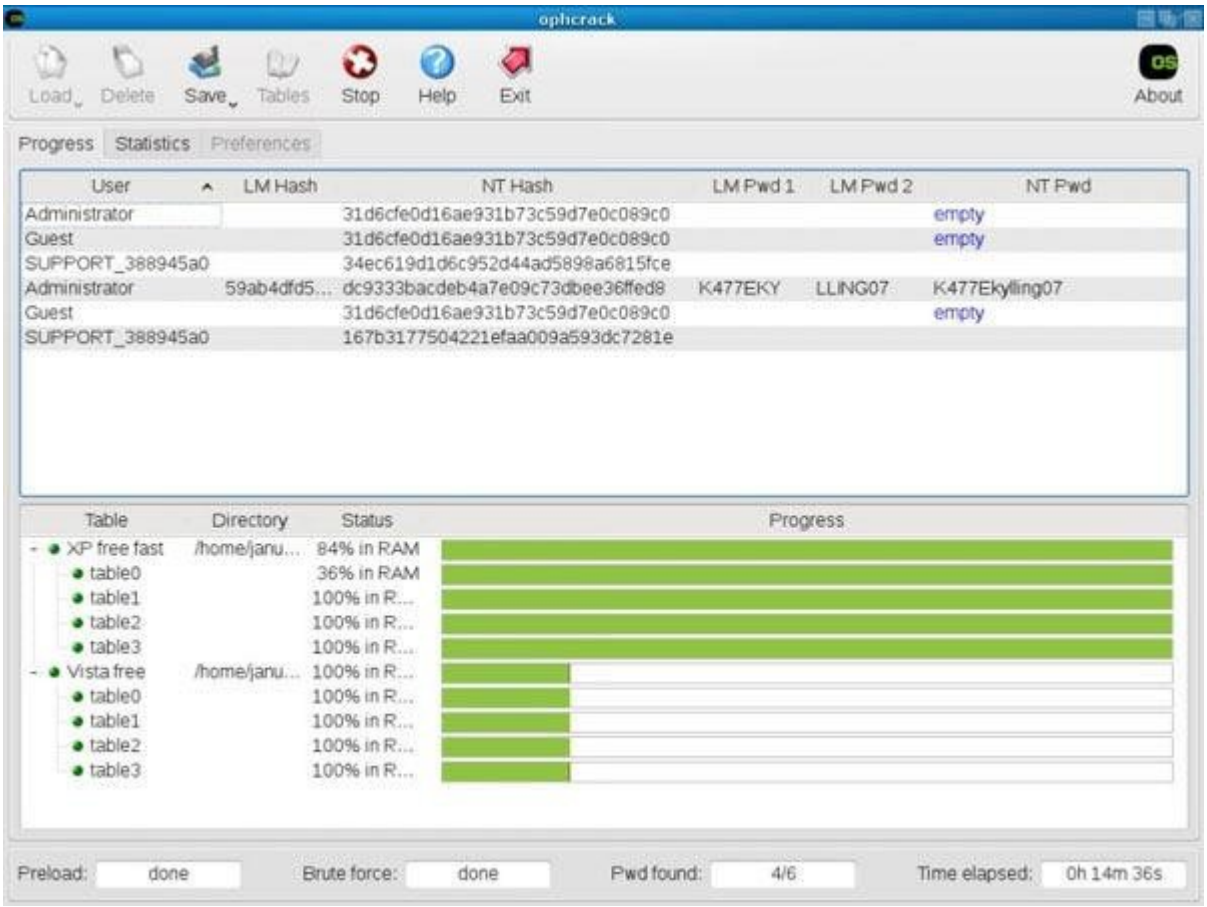
operatingsystem that can run independently of your Windows OS. In a few moments, you will see theOphcrack interface on your computer.

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.



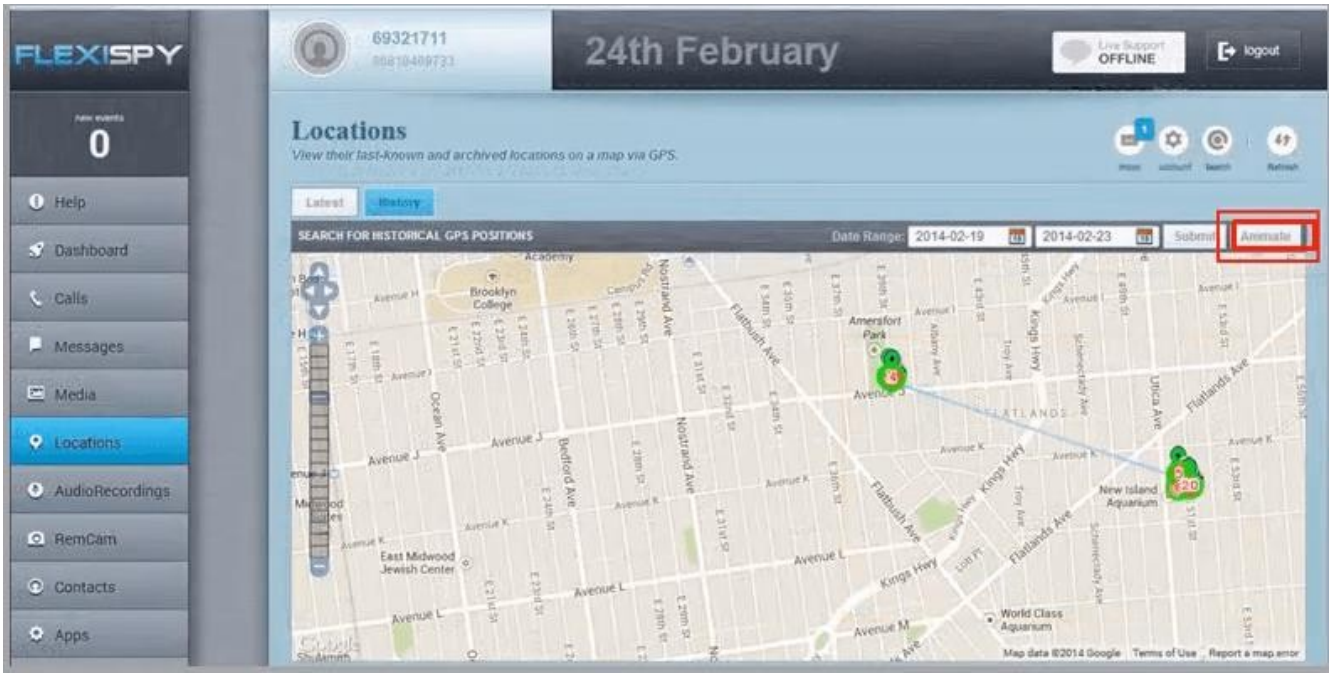
iv. Flexispy

FlexiSPY is a phone application which comes with an android keylogger for the phone as a feature. It will always appear in the list whenever one is speaking about the world's best spy phone applications. This app comes with everything you expect when looking for a monitoring system for your phone.

It will help you record phone calls, capture SMS, WhatsApp messages, even capture keystrokes, allow you to read emails, read Facebook messages.

The app will as well track the device and you know what, from where you are you can turn on its

recorder and record conversations without the owner noticing.



v. 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. Anotherform 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 witha 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 fromthe 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.

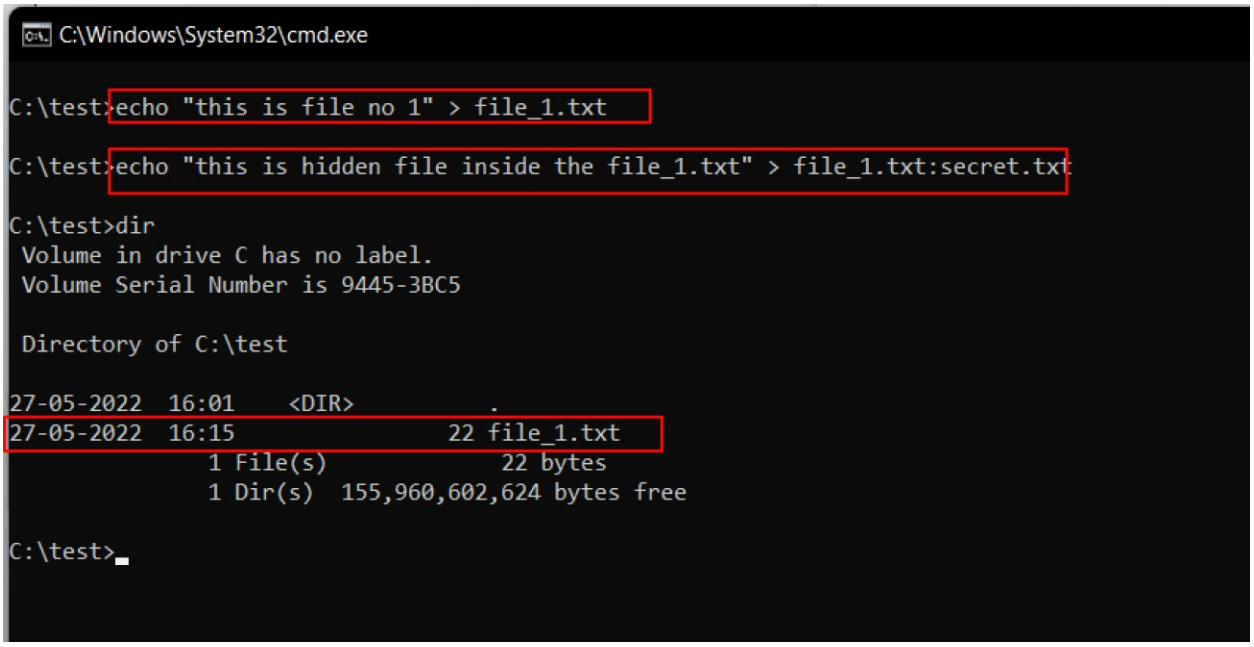
Creation of NTFS streams:

When the user reads or writes a file, their only manipulation in the main data stream by default. The following is the syntax of ADSs

filename.extension:alternativeNmae

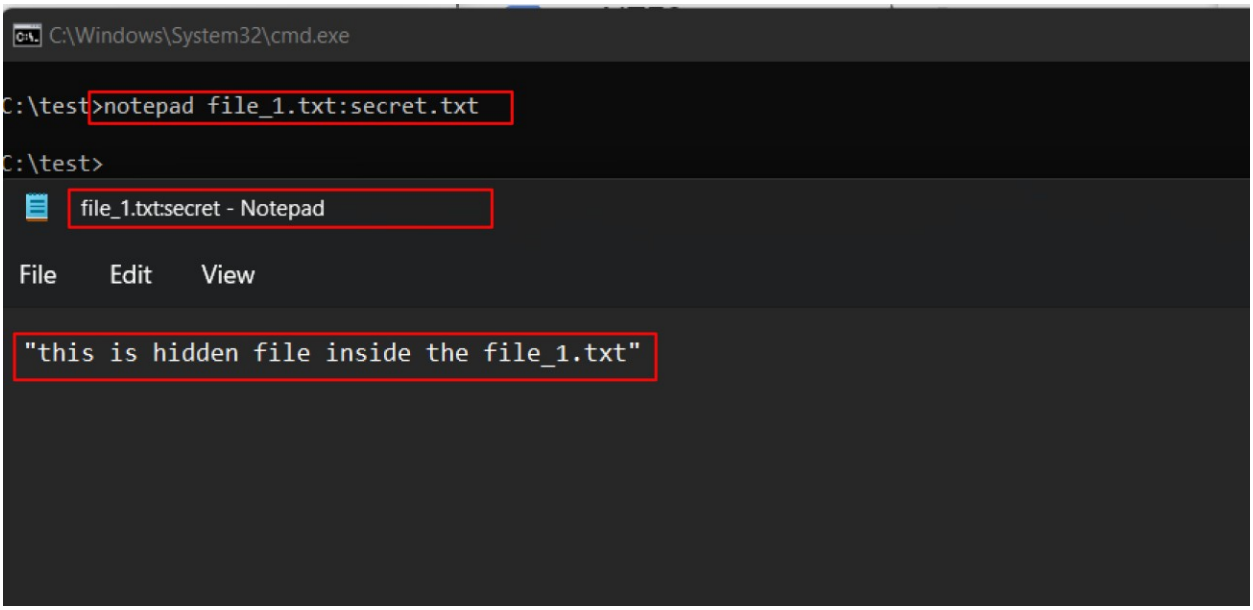
Open the terminal and type the following command to create a file named file_1.txt. echo "this is file no 1" > file_1.txt

Now, type the following command to write to the stream named secret.txt. echo "this is a hidden file inside the file_1.txt" > file_1.txt:secret.txt



We've just created a stream named secret.txt that is associated with file_1.txt and when you look at the file_1.txtyou will only find the data present in file_1.txt. And also stream willnot be shown in the directory as well.

The following command can be used to view or modify the stream hidden in file_1.txt notepad file_1.txt:secret.txt


C:\Windows\System32\cmd.exe
C:\test>notepad file_1.txt:secret.txt
C:\test>
file_1.txt:secret - Notepad
File Edit View
"this is hidden file inside the file_1.txt"

Note: Notepad is a stream-compliant application. Never use alternative streams to store sensitiveinformation.

Hiding Trojan.exe in note.txt file stream:

The following command has used the copy the trojan.exe into a note.txt(stream)

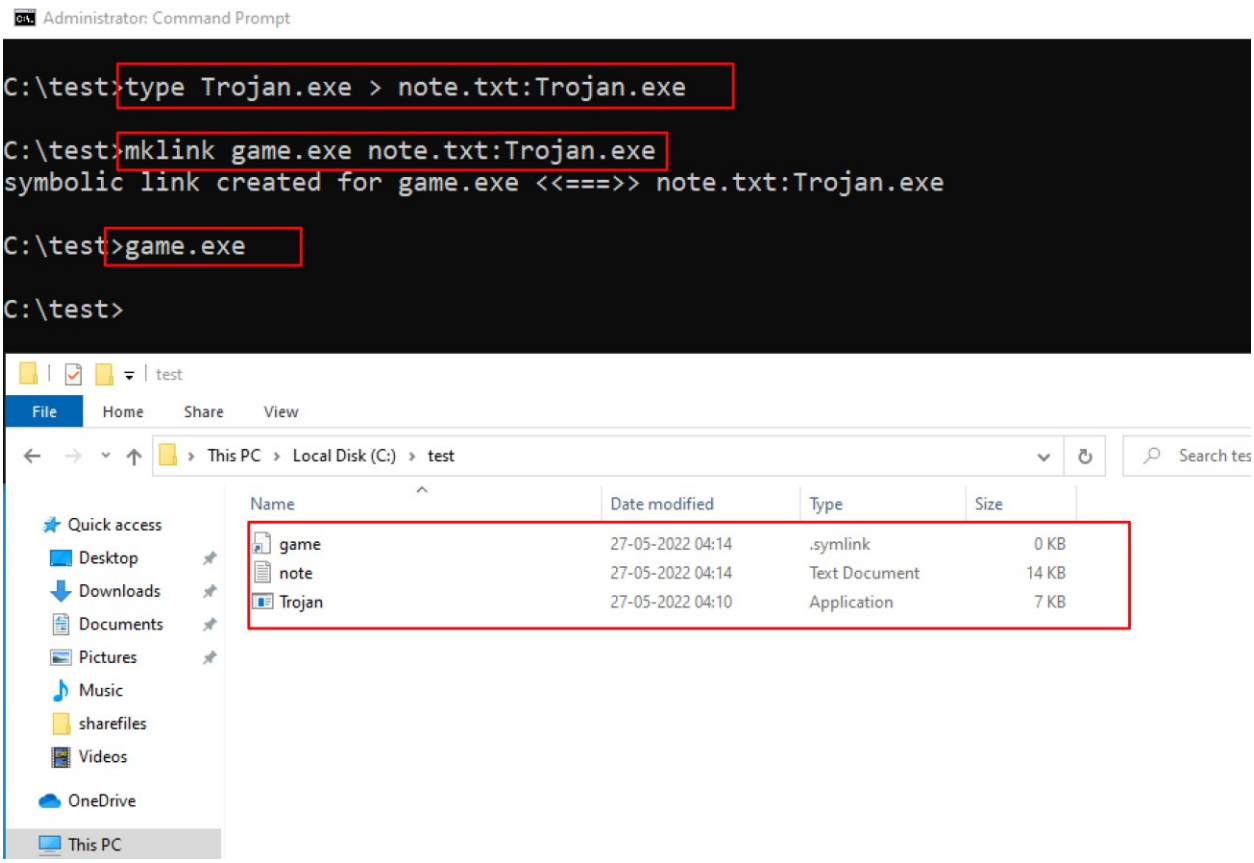
C:\test>type Trojan.exe > note.txt:Trojan.exe

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 fromthe stream. The following command is used to create a shortcut in the stream.

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

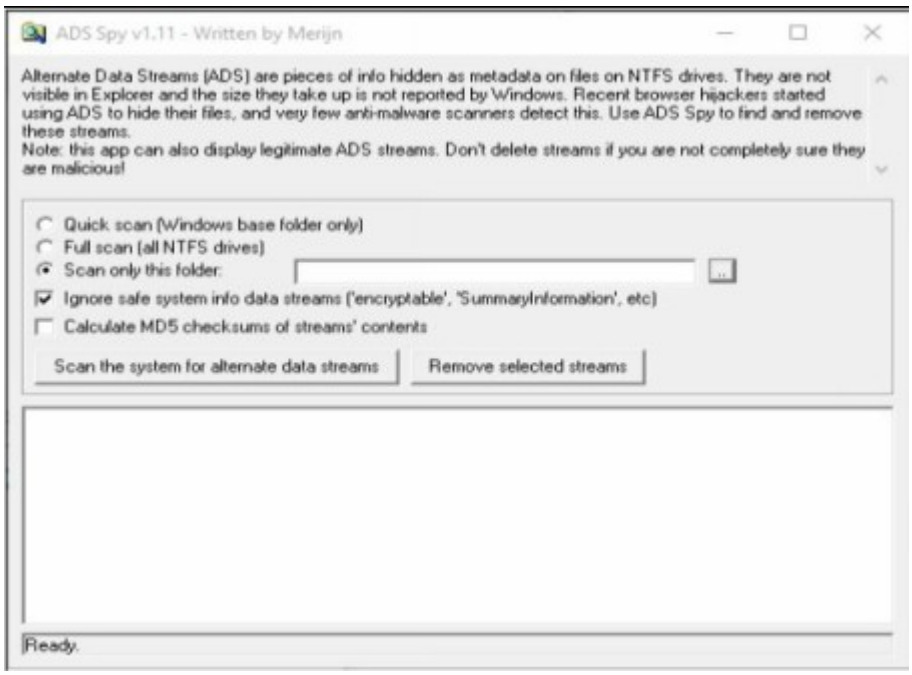
Type game.exe to run the trojan that is hidden behind the note.txt. Here, game.exeis the shortcut created to launch trojan.exe.



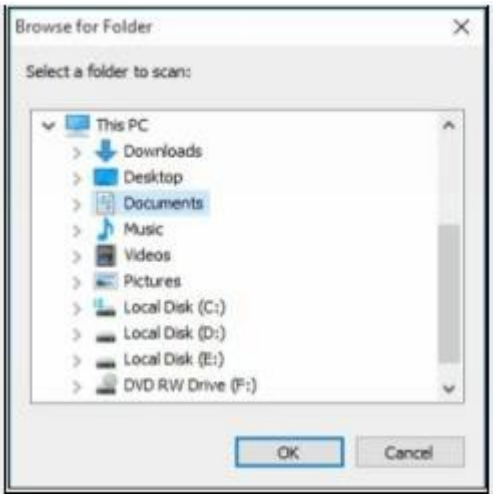
vi. ADS Spy

AdSpy 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

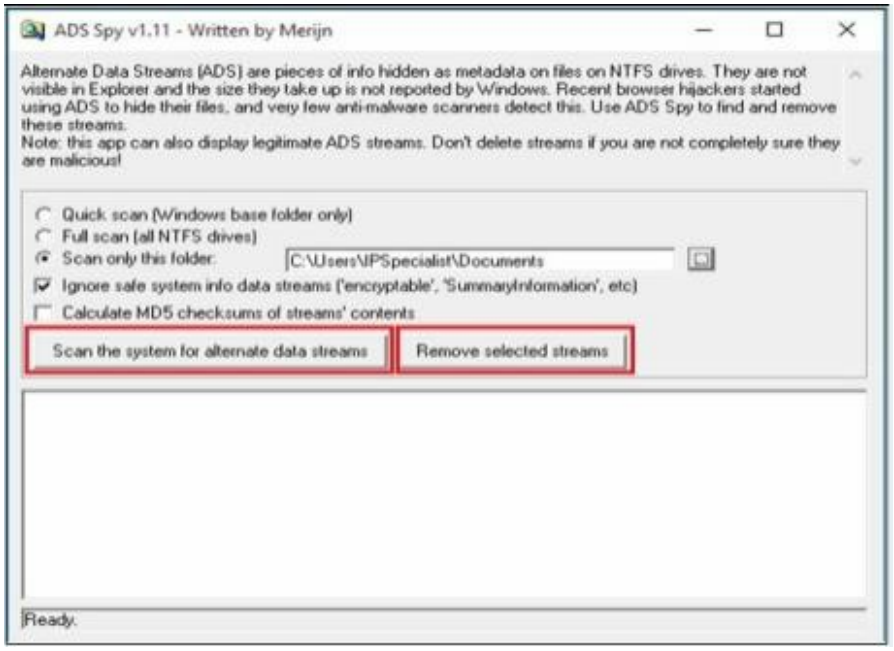


As we store the file in the Document folder, Selecting Document folder to scan particular folder only.



Select an Option, if you want to scan for ADS, click "Scan the system for ADS"/ or click

removes button to remove the file



As shown in the figure below, ADS Spy has detected the Testfile.txt:hidden.txt file from the directory.

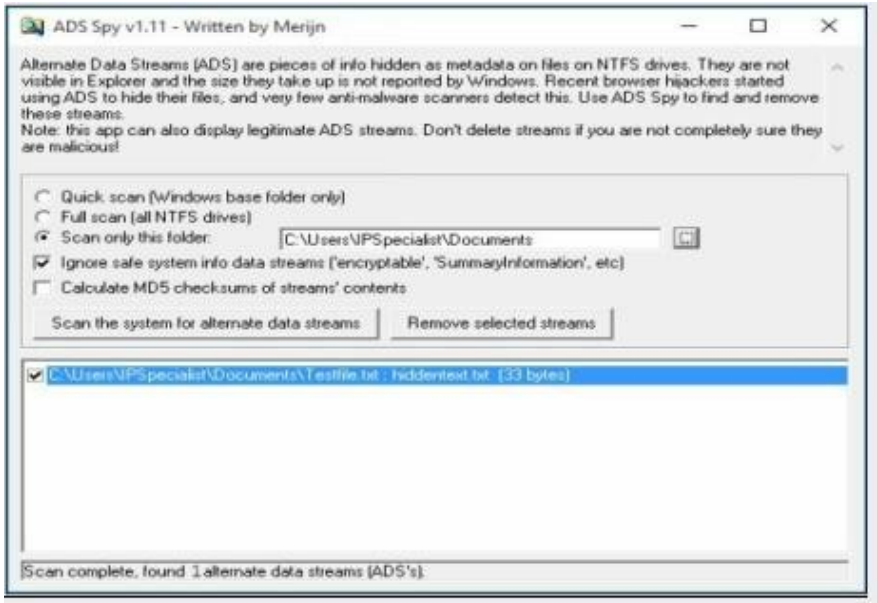
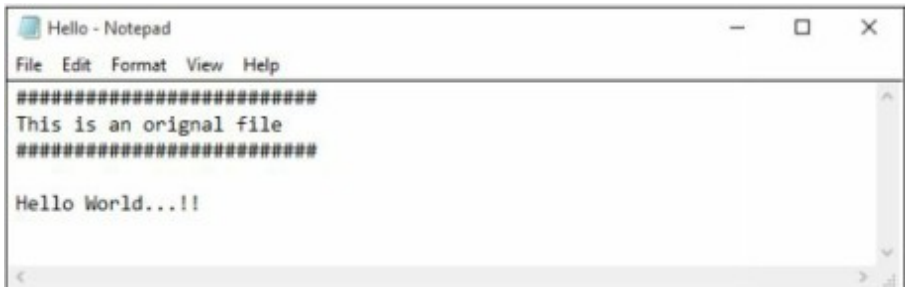


Figure 6-50 ADS Detection

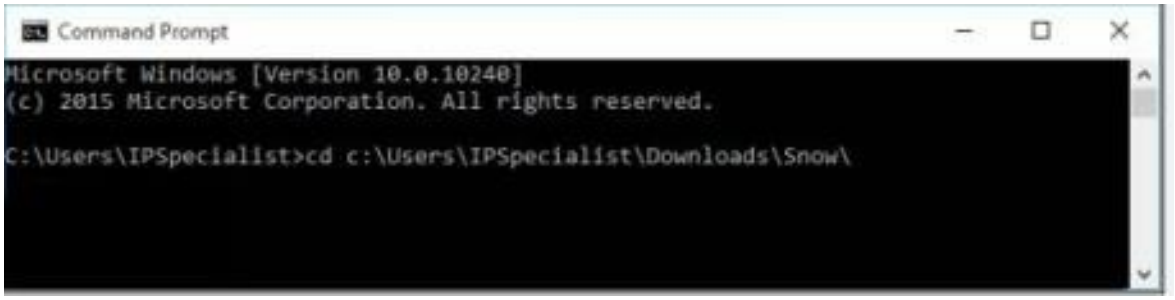
vii. Snow

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



Go to Command Prompt

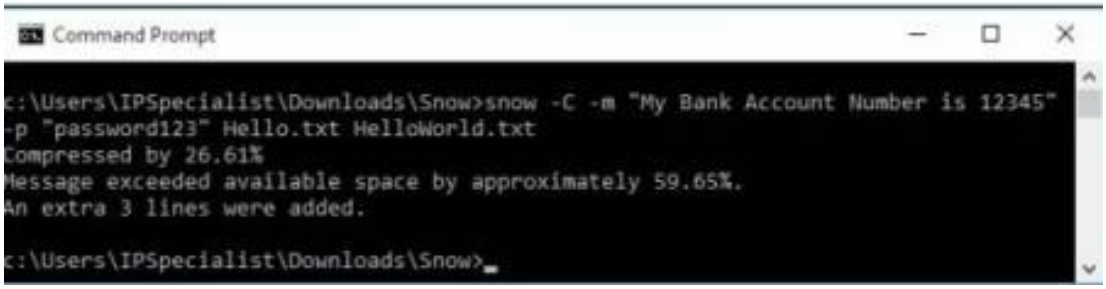
Change the directory to run Snow tool



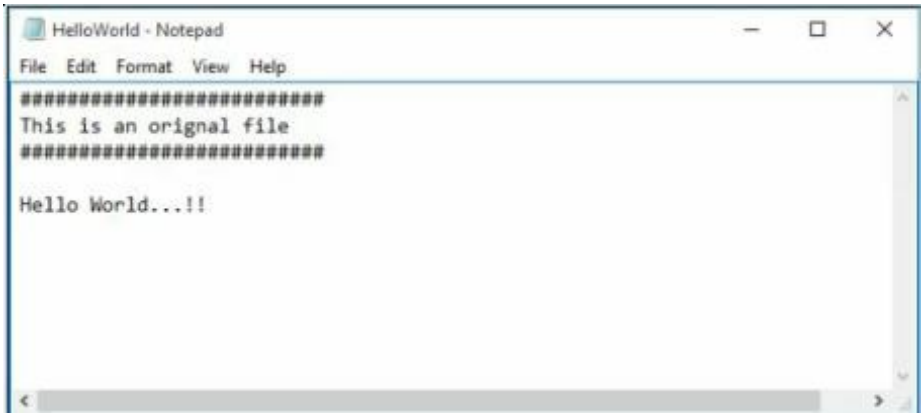
Type the command

Snow –C –m “text to be hide” –p “password” <Sourcefile> <Destinationfile>

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



Go to the directory; you will a new file HelloWorld.txt. Open the File

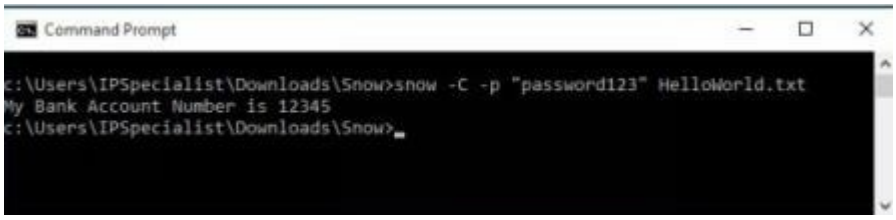


New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command

Snow –C –p “password123” HelloWorld.txt

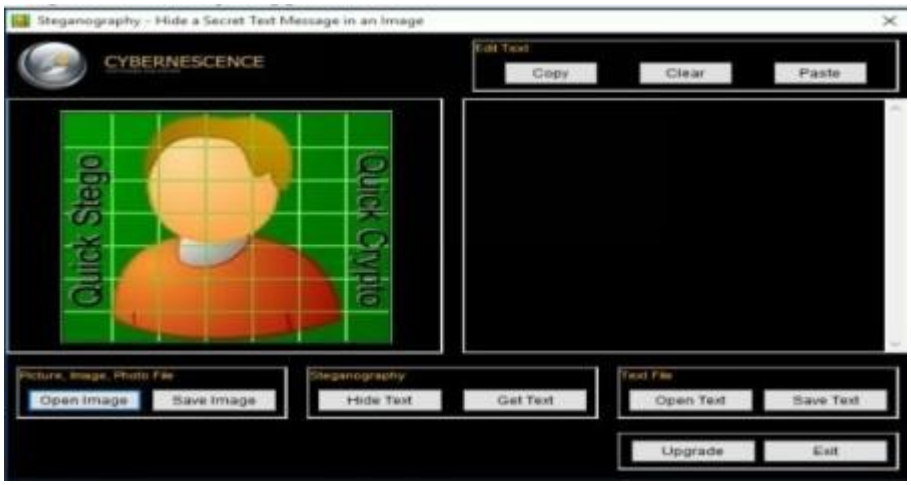


As shown in the above figure, File decrypted, showing hidden information encrypted in the previous section.

viii. 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

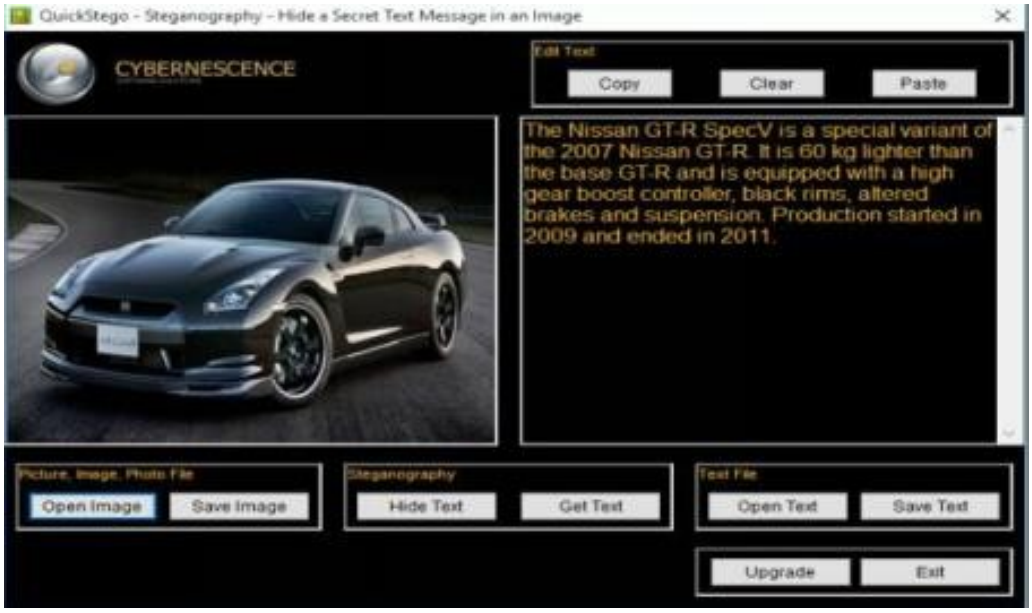
4. Click Hide Text Button

5. Save Image

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

Recovering Data from Image Steganography using QuickStego

1. Open QuickStego
2. Click Get Text



3. Open and Compare Both Images

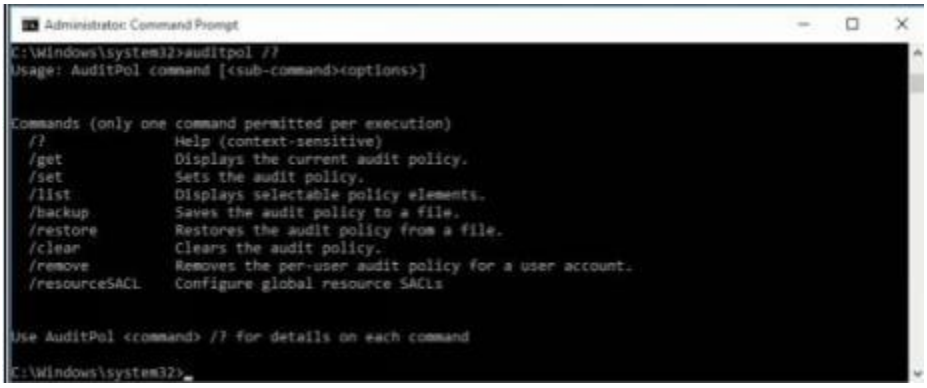
Left Image is without Hidden Text; Right Image is with hidden text

ix. Clearing Audit Policies

Enabling and Clearing Audit Policies

To check command's available option Enter

C:\Windows\system32> **auditpol /?**

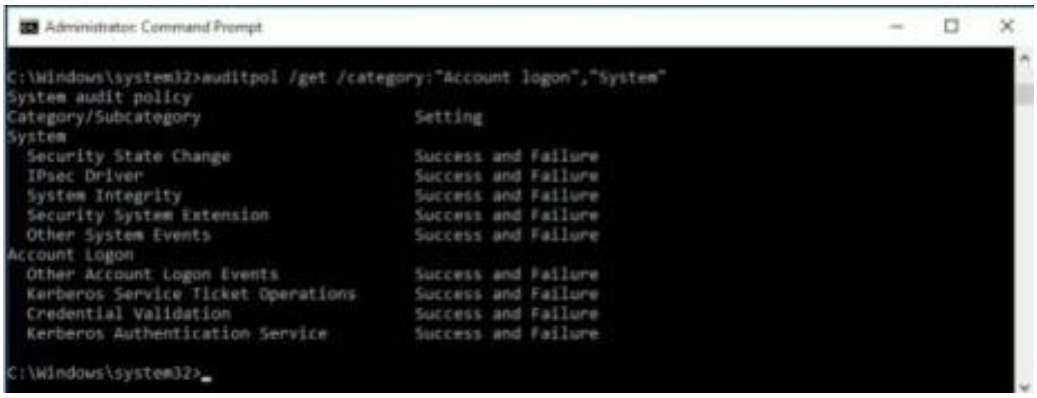

Administrator: Command Prompt
C:\Windows\system32>auditpol /?
Usage: AuditPol command [<sub-command><options>]
Commands (only one command permitted per execution)
/? Help (context-sensitive)
/get Displays the current audit policy.
/set Sets the audit policy.
/list Displays selectable policy elements.
/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**

To check Auditing is enabled, enter the command

C:\Windows\system32>**auditpol logon","System"/get /category:"Account**



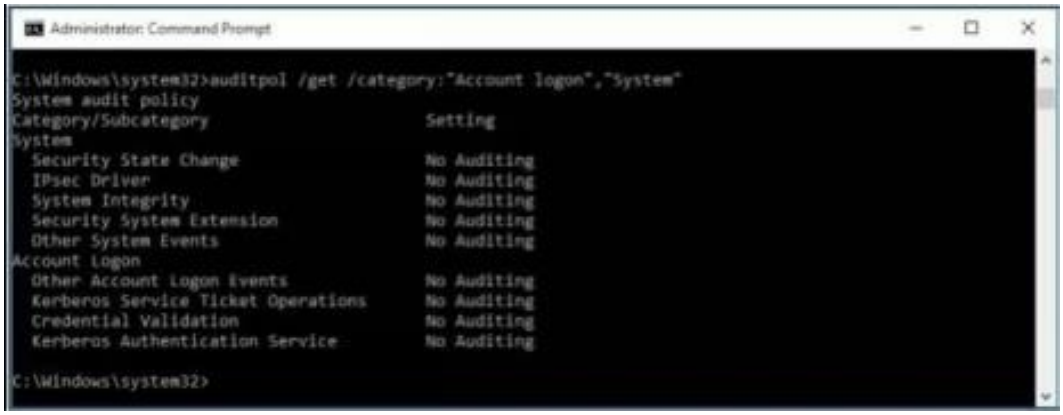
To clear Audit Policies, Enter the following command

C:\Windows\system32>**auditpol /clear**

Are you sure (Press N to cancel or any other key to continue)?**Y**

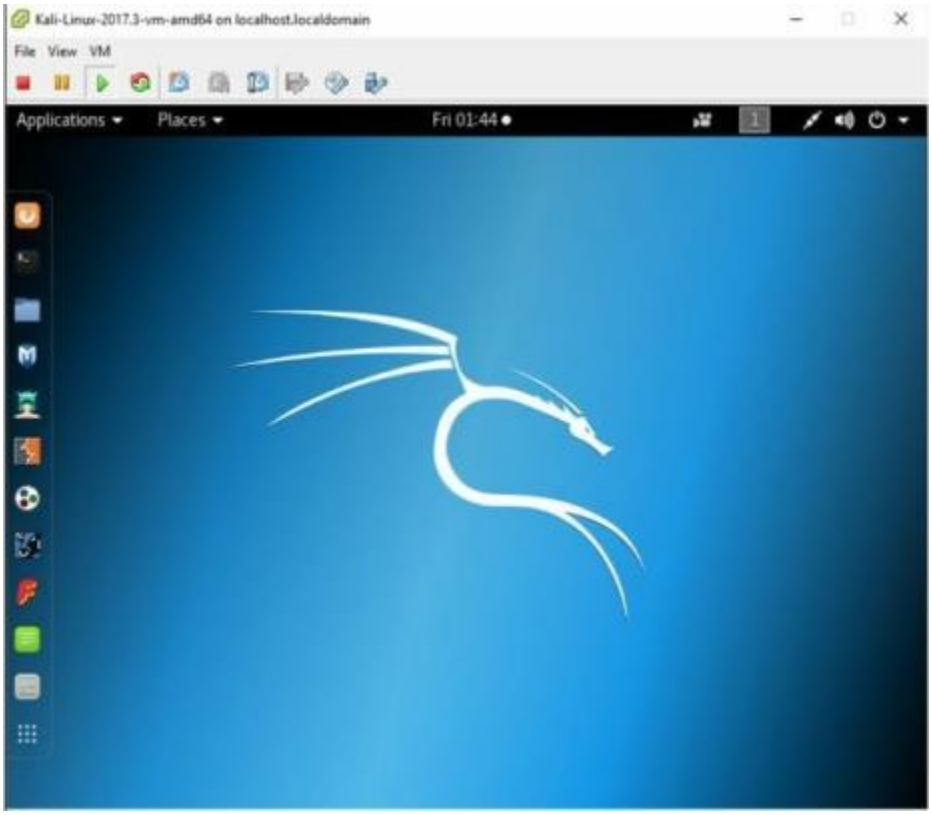
To check Auditing, enter the command

C:\Windows\system32>**auditpol /get /category:"Account logon","System"**

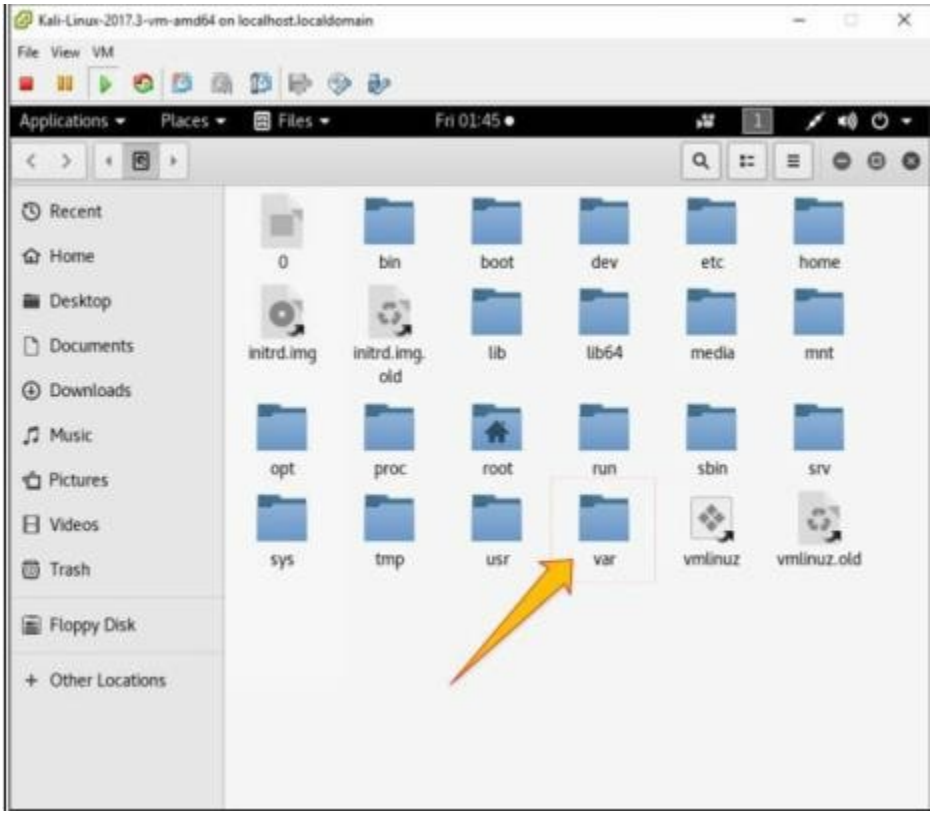


x. Clearing Logs

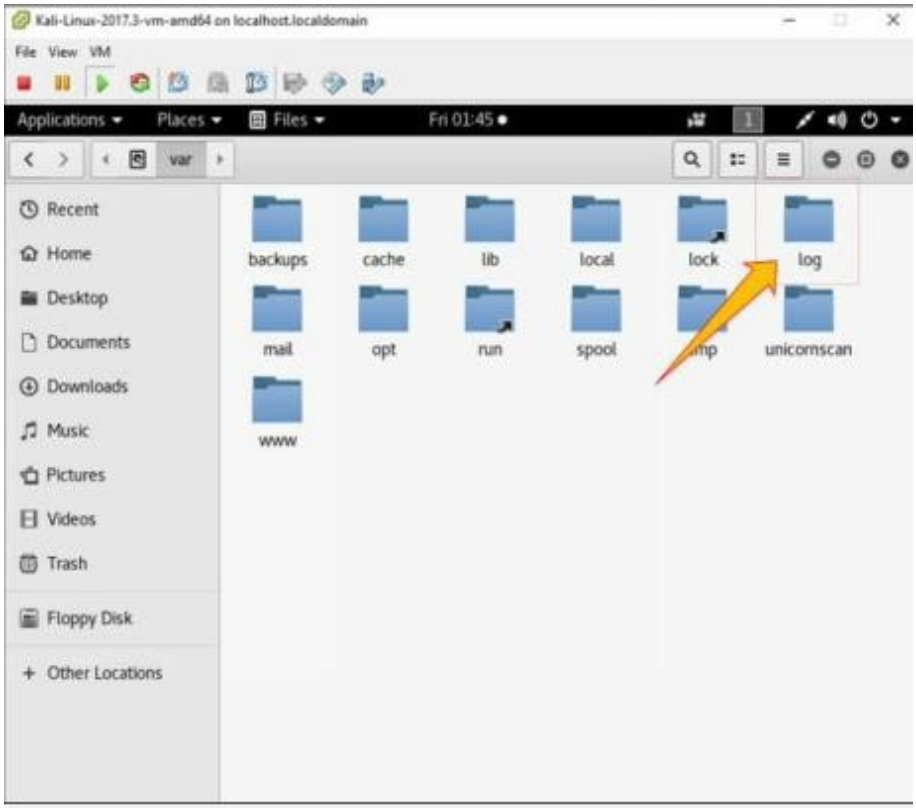
1. Go to Kali Linux Machine



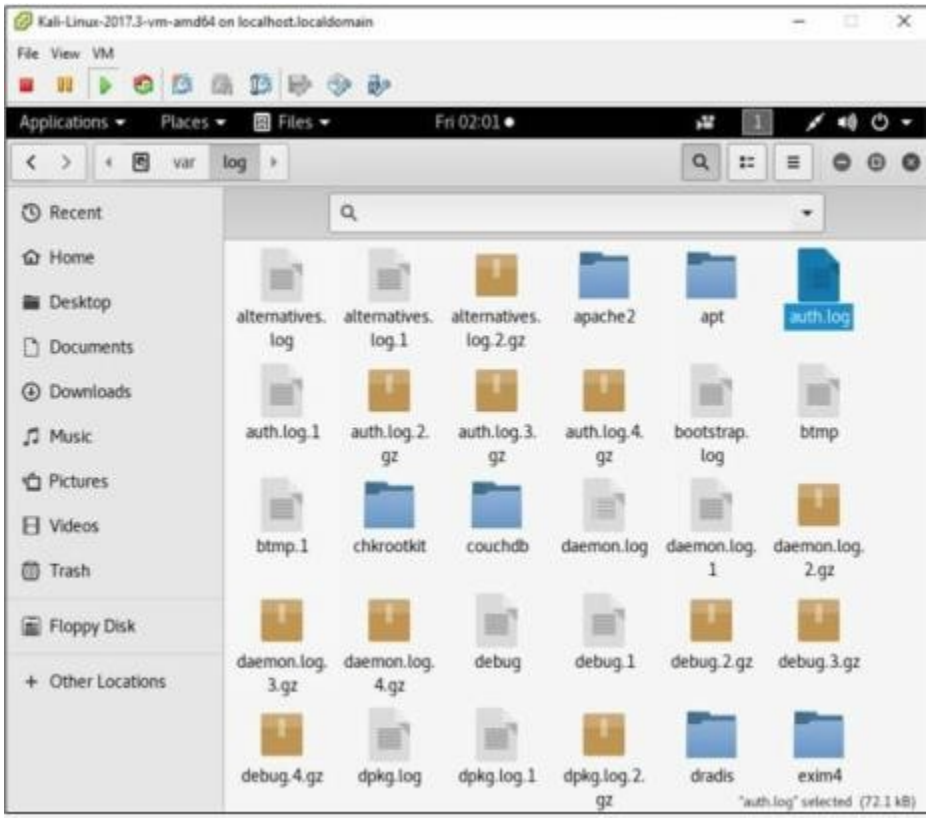
2. Open the /var directory:



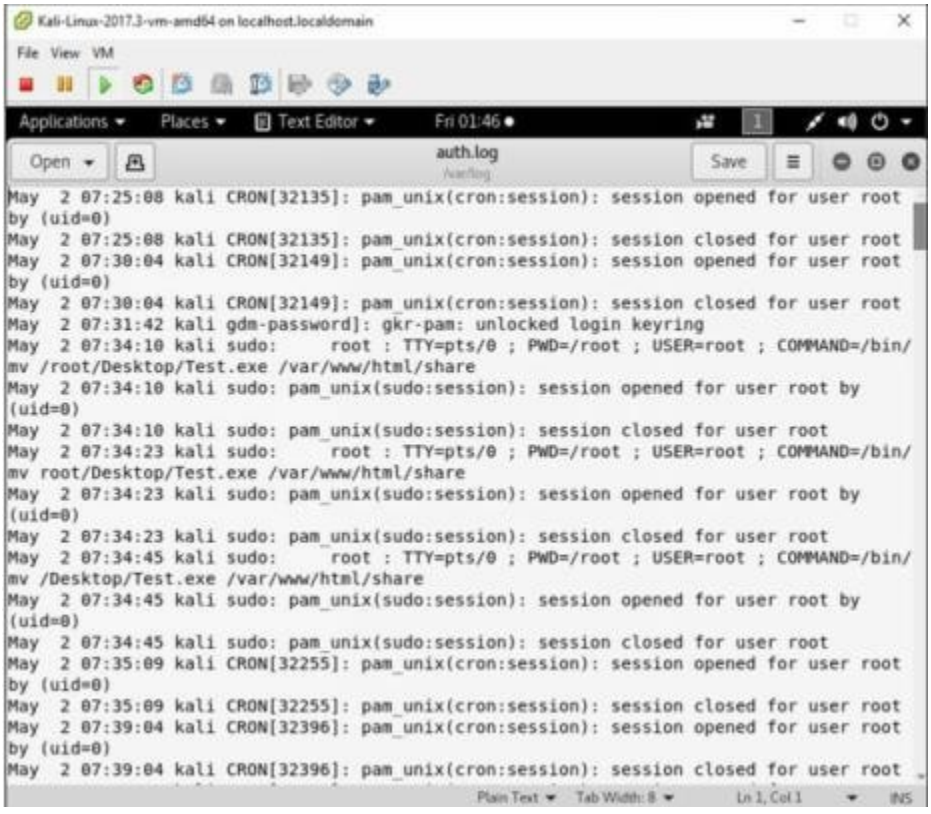
3. Go to **Logs** folder:


Kali-Linux-2017.3-vm-amd64 on localhost.localdomain
File View VM
Applications Places Files Fri 01:45
var
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Other Locations
backups
cache
lib
local
lock
log
mail
opt
run
spool
unicornscan
www

4. Select any log file:



5. Open any log file; you can delete

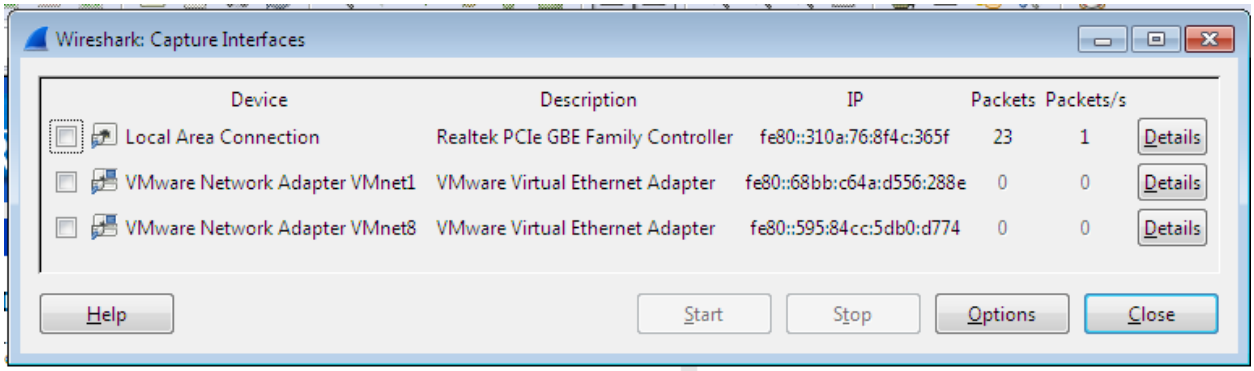


Practical No. 5

a. Use wireshark to sniff the network.

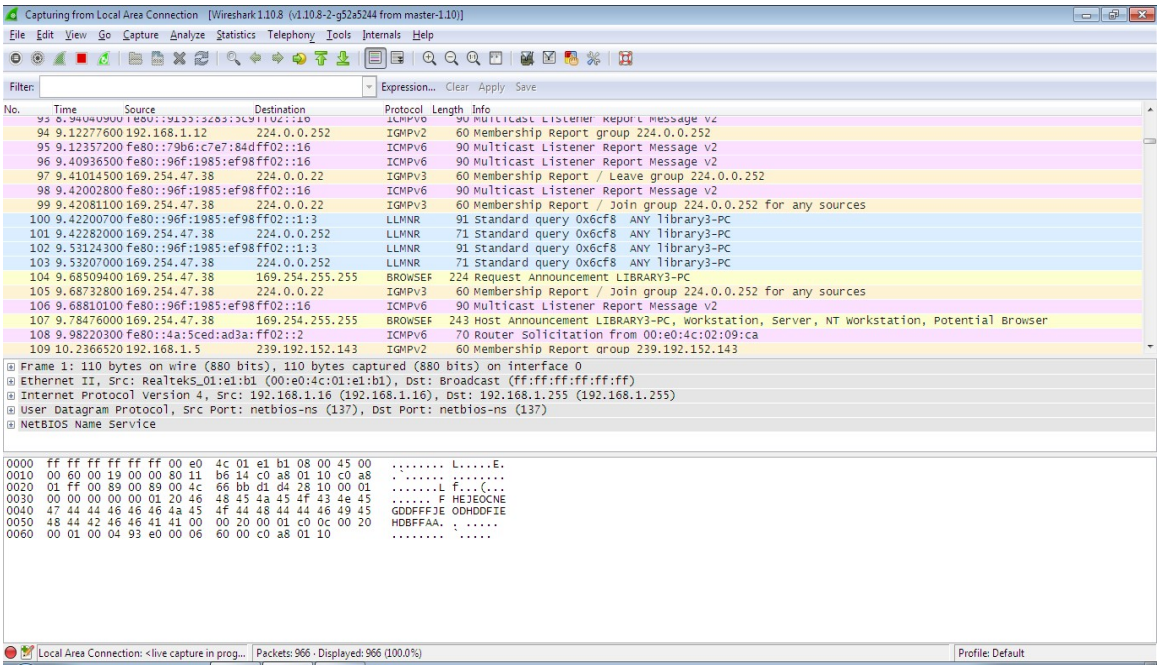
Wireshark is a GUI-based packet capture program. As noted, it comes with some command-line programs. There are a lot of advantages to using Wireshark. First, it gives us a way to view the packets easily, moving around the complete capture. Unlike with tcpdump and tshark, we see theentire network stack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

- Start Wireshark. Under the "Capture" header, select the "Interface List" option; orclick on the "Interfaces" button on the toolbar:
  This will bring up a list of network interfaces that Wireshark is able to capturepackets from:



List of available capture interfaces

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


Capturing from Local Area Connection [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
94 9.12277600 192.168.1.12 224.0.0.252 IGMPv2 60 Membership Report group 224.0.0.252
95 9.12357200 fe80::79b6:c7e7:84d ff02::16 ICMPv6 90 Multicast Listener Report Message v2
96 9.40936500 fe80::96f:1985:ef98 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
97 9.41014500 169.254.47.38 224.0.0.22 IGMPv3 60 Membership Report / Leave group 224.0.0.252
98 9.42002800 fe80::96f:1985:ef98 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
99 9.42081100 169.254.47.38 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.252 for any sources
100 9.42200700 fe80::96f:1985:ef98 ff02::1:3 LLMNR 91 Standard query 0x6cf8 ANY library3-PC
101 9.42282000 169.254.47.38 224.0.0.252 LLMNR 71 Standard query 0x6cf8 ANY library3-PC
102 9.53124300 fe80::96f:1985:ef98 ff02::1:3 LLMNR 91 Standard query 0x6cf8 ANY library3-PC
103 9.53207000 169.254.47.38 224.0.0.252 LLMNR 71 Standard query 0x6cf8 ANY library3-PC
104 9.68509400 169.254.47.38 169.254.255.255 BROWSER 224 Request Announcement LIBRARY3-PC
105 9.68732800 169.254.47.38 224.0.0.22 IGMPv3 60 Membership Report / Join group 224.0.0.252 for any sources
106 9.68810100 fe80::96f:1985:ef98 ff02::16 ICMPv6 90 Multicast Listener Report Message v2
107 9.78476000 169.254.47.38 169.254.255.255 BROWSER 243 Host Announcement LIBRARY3-PC, Workstation, Server, NT Workstation, Potential Browser
108 9.98220300 fe80::4a:5ced:ad3a: ff02::2 ICMPv6 70 Router Solicitation from 00:e0:4c:02:09:ca
109 10.2366520 192.168.1.5 239.192.152.143 IGMPv2 60 Membership Report group 239.192.152.143
Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
Ethernet II, Src: Realtek_01:e1:b1 (00:e0:4c:01:e1:b1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.1.16 (192.168.1.16), Dst: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
NetBIOS Name Service
0000 ff ff ff ff ff ff 00 e0 4c 01 e1 b1 08 00 45 00 .... L.....E.
0010 00 60 00 19 00 00 80 11 b6 14 c0 a8 01 10 c0 a8 .`...... ....
0020 01 ff 00 89 00 89 00 4c 66 bb d1 d4 28 10 00 01 .... f...(...
0030 00 00 00 00 00 01 20 46 48 45 4a 45 4f 43 4e 45 ...... F HEJEOCNE
0040 47 44 44 46 46 46 4a 45 4f 44 48 44 44 46 49 45 GDDFFFJE ODHDDFIE
0050 48 44 42 46 46 41 41 00 00 20 00 01 c0 0c 00 20 HDBFFAA. . .....
0060 00 01 00 04 93 e0 00 06 60 00 c0 a8 01 10 .... `.....
Local Area Connection: <live capture in prog...
Packets: 966 · Displayed: 966 (100.0%)
Profile: Default

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

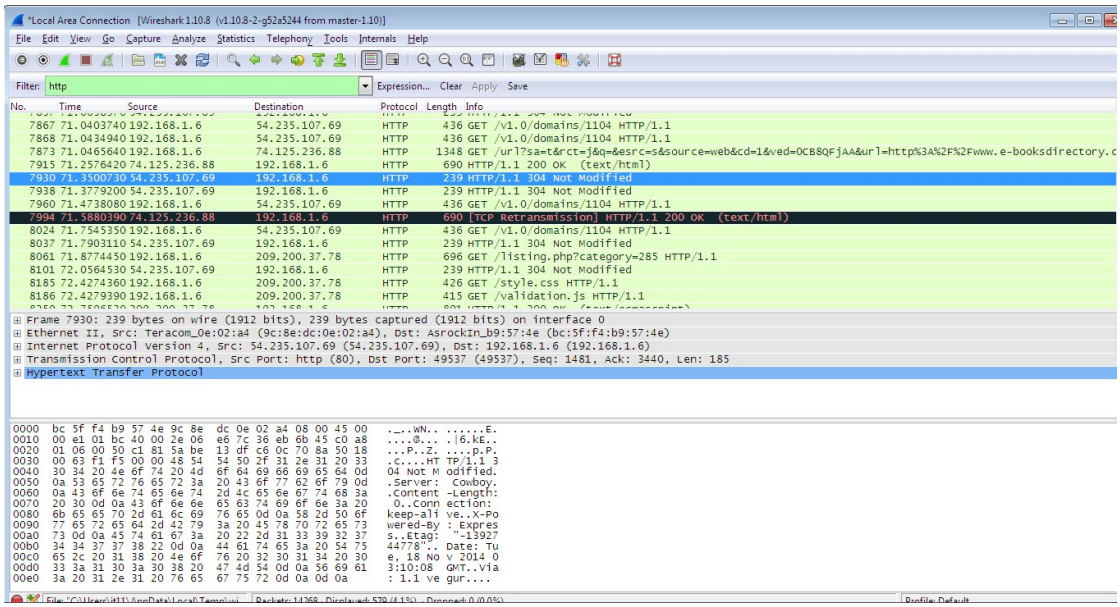
Capturing network traffic for a couple minutes could include traffic on many different protocols such as ARP, TCP, UDP, DNS, HTTP, etc.

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:

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 willnow list only captured packets related to HTTP traffic:


*Local Area Connection [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
7867 71.0403740 192.168.1.6 54.235.107.69 HTTP 436 GET /v1.0/domains/1104 HTTP/1.1
7868 71.0434940 192.168.1.6 54.235.107.69 HTTP 436 GET /v1.0/domains/1104 HTTP/1.1
7873 71.0465640 192.168.1.6 74.125.236.88 HTTP 1348 GET /url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.e-booksdirectory.c
7915 71.2576420 74.125.236.88 192.168.1.6 HTTP 690 HTTP/1.1 200 OK (text/html)
7930 71.3500730 54.235.107.69 192.168.1.6 HTTP 239 HTTP/1.1 304 Not Modified
7938 71.3779200 54.235.107.69 192.168.1.6 HTTP 239 HTTP/1.1 304 Not Modified
7960 71.4738080 192.168.1.6 54.235.107.69 HTTP 436 GET /v1.0/domains/1104 HTTP/1.1
7994 71.5880390 74.125.236.88 192.168.1.6 HTTP 690 [TCP Retransmission] HTTP/1.1 200 OK (text/html)
8024 71.7545350 192.168.1.6 54.235.107.69 HTTP 436 GET /v1.0/domains/1104 HTTP/1.1
8037 71.7903110 54.235.107.69 192.168.1.6 HTTP 239 HTTP/1.1 304 Not Modified
8061 71.8774450 192.168.1.6 209.200.37.78 HTTP 696 GET /listing.php?category=285 HTTP/1.1
8101 72.0564530 54.235.107.69 192.168.1.6 HTTP 239 HTTP/1.1 304 Not Modified
8185 72.4274360 192.168.1.6 209.200.37.78 HTTP 426 GET /style.css HTTP/1.1
8186 72.4279390 192.168.1.6 209.200.37.78 HTTP 415 GET /validation.js HTTP/1.1
Frame 7930: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface 0
Ethernet II, Src: Teracom_0e:02:a4 (9c:8e:dc:0e:02:a4), Dst: AsrockIn_b9:57:4e (bc:5f:f4:b9:57:4e)
Internet Protocol Version 4, Src: 54.235.107.69 (54.235.107.69), Dst: 192.168.1.6 (192.168.1.6)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49537 (49537), Seq: 1481, Ack: 3440, Len: 185
Hypertext Transfer Protocol
0000 bc 5f f4 b9 57 4e 9c 8e dc 0e 02 a4 08 00 45 00 ._..WN.. ......E.
0010 00 e1 01 bc 40 00 2e 06 e6 7c 36 eb 6b 45 c0 a8 ....@... .|6.kE..
0020 01 06 00 50 c1 81 5a be 13 df c6 0c 70 8a 50 18 ...P..Z. ....p.P.
0030 00 63 f1 f5 00 00 48 54 54 50 2f 31 2e 31 20 33 .c....HT TP/1.1 3
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not M odified.
0050 0a 53 65 72 76 65 72 3a 20 43 6f 77 62 6f 79 0d .Server: Cowboy.
0060 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a .Content -Length:
0070 20 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 0..Conn ection:
0080 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 58 2d 50 6f keep-ali ve..X-Po
0090 77 65 72 65 64 2d 42 79 3a 20 45 78 70 72 65 73 wered-By : Expres
00a0 73 0d 0a 45 74 61 67 3a 20 22 2d 31 33 39 32 37 s..Etag: "-13927
00b0 34 34 37 37 38 22 0d 0a 44 61 74 65 3a 20 54 75 44778"..Date: Tu
00c0 65 2c 20 31 38 20 4e 6f 76 20 32 30 31 34 20 30 e, 18 No v 2014 0
00d0 33 3a 31 30 3a 30 38 20 47 4d 54 0d 0a 56 69 61 3:10:08 GMT..Via
00e0 3a 20 31 2e 31 20 76 65 67 75 72 0d 0a 0d 0a : 1.1 ve gur....

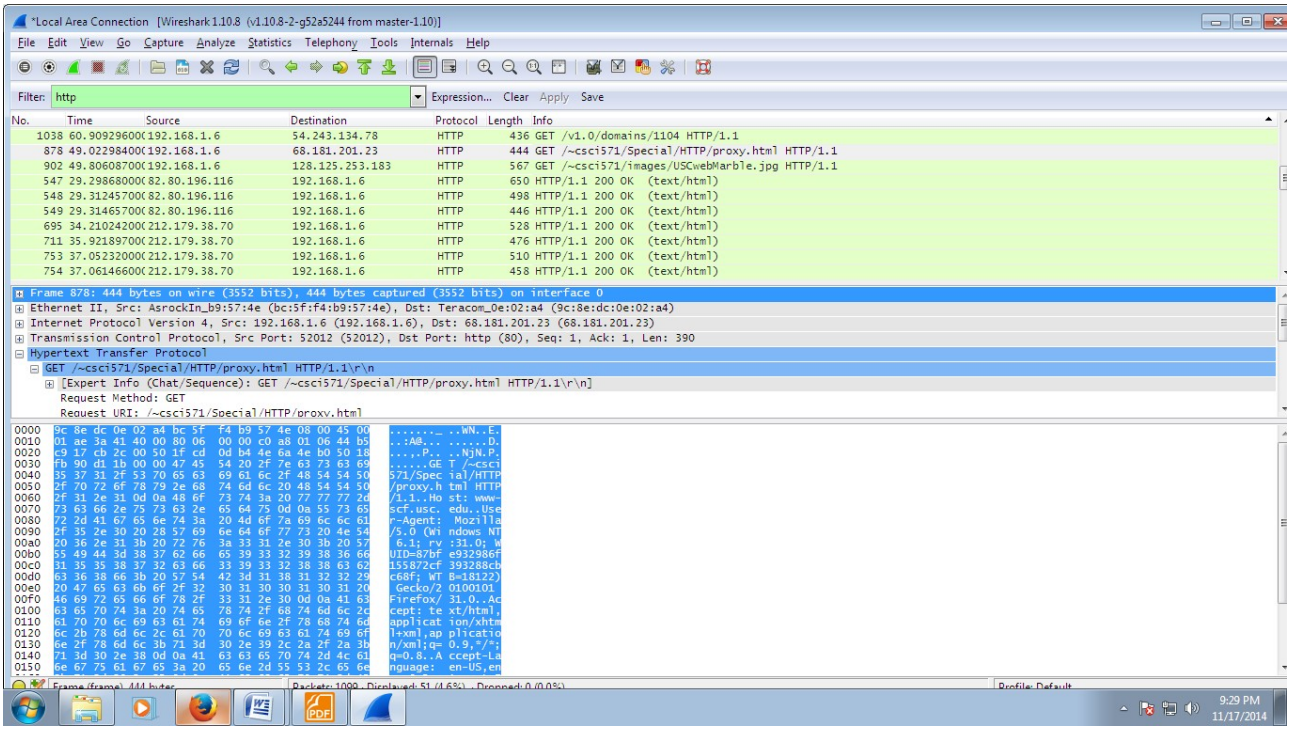
Examining HTTP Traffic

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://www-scf.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. Selectthis 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
    - etc

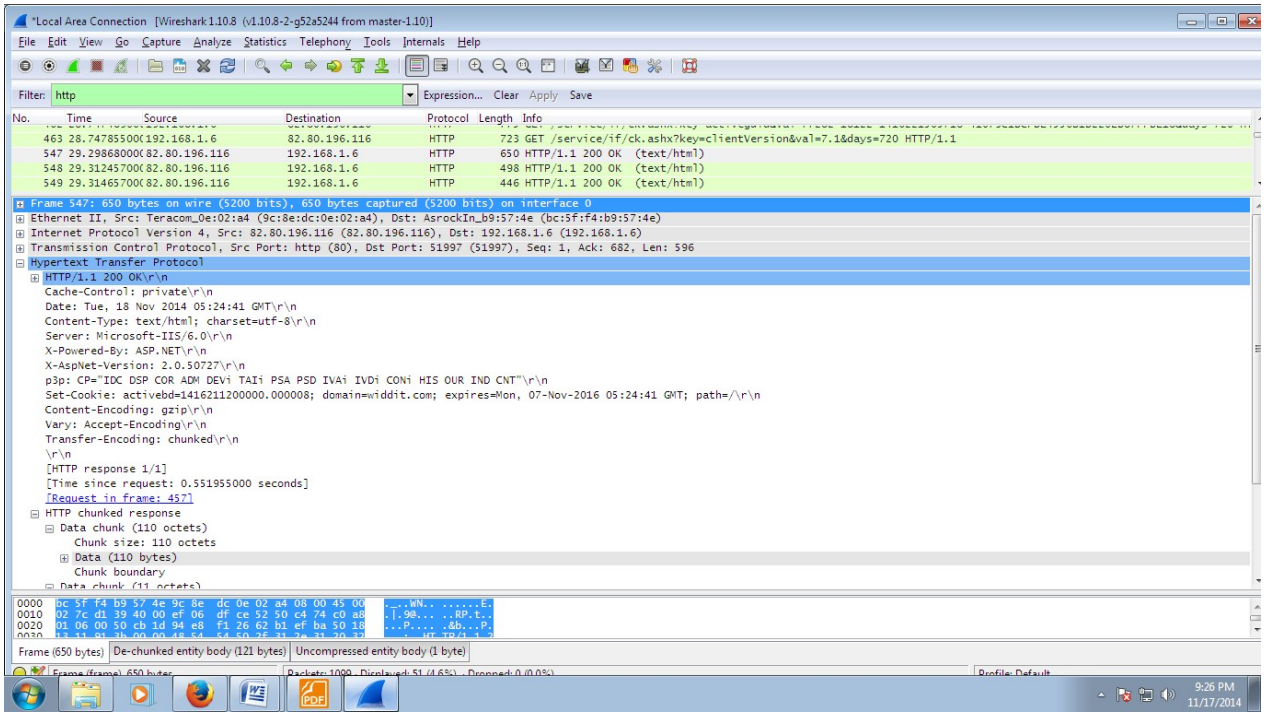


Take a look at the HTTP response to the above request.

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 therequested web page.

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

- Cache-Control
- Content-Type
- Server
- Etc



Details of incoming HTTP response corresponding to proxy.html

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 appreciatethe ability to hand enter a new MAC address.

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 SMACmain 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 A

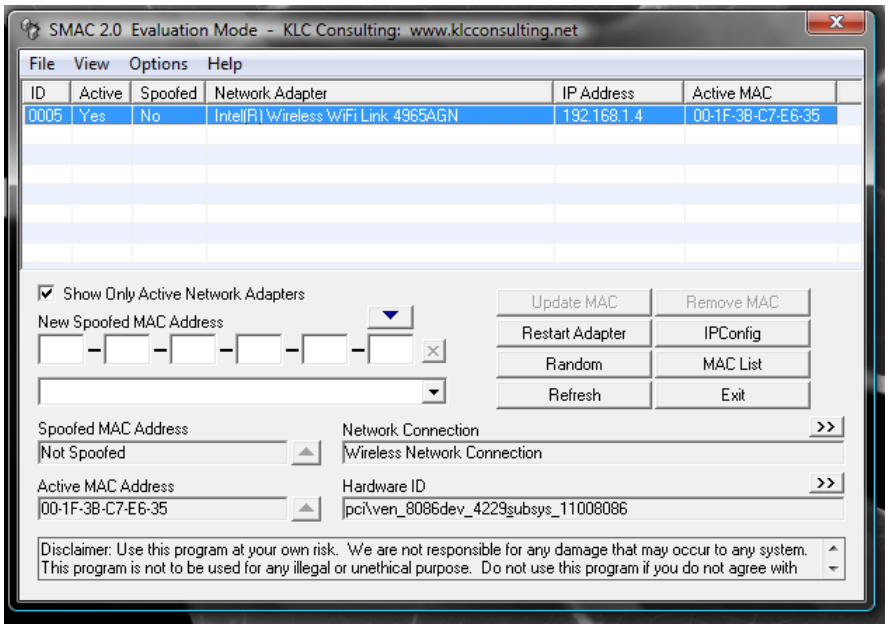
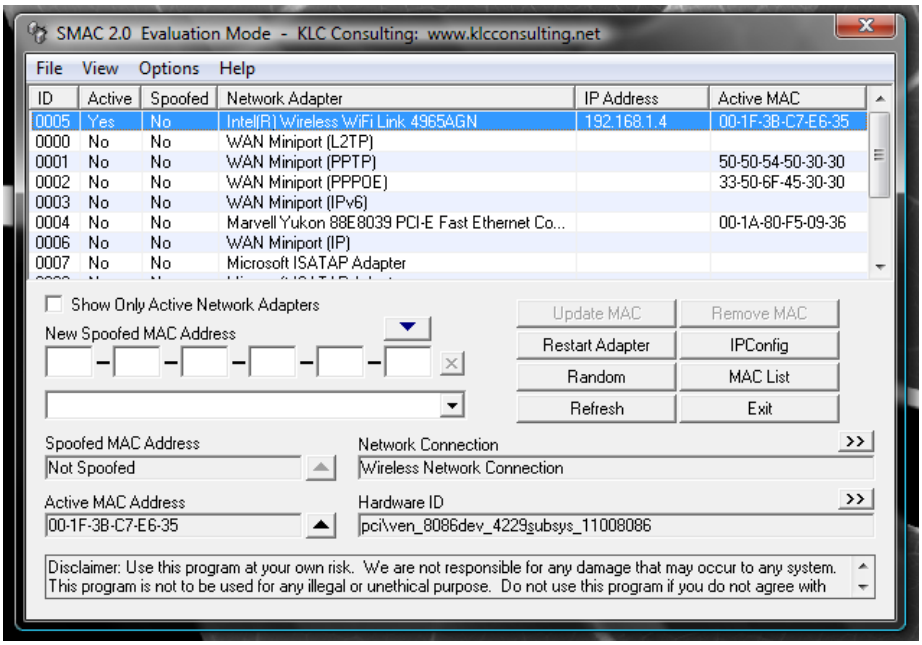


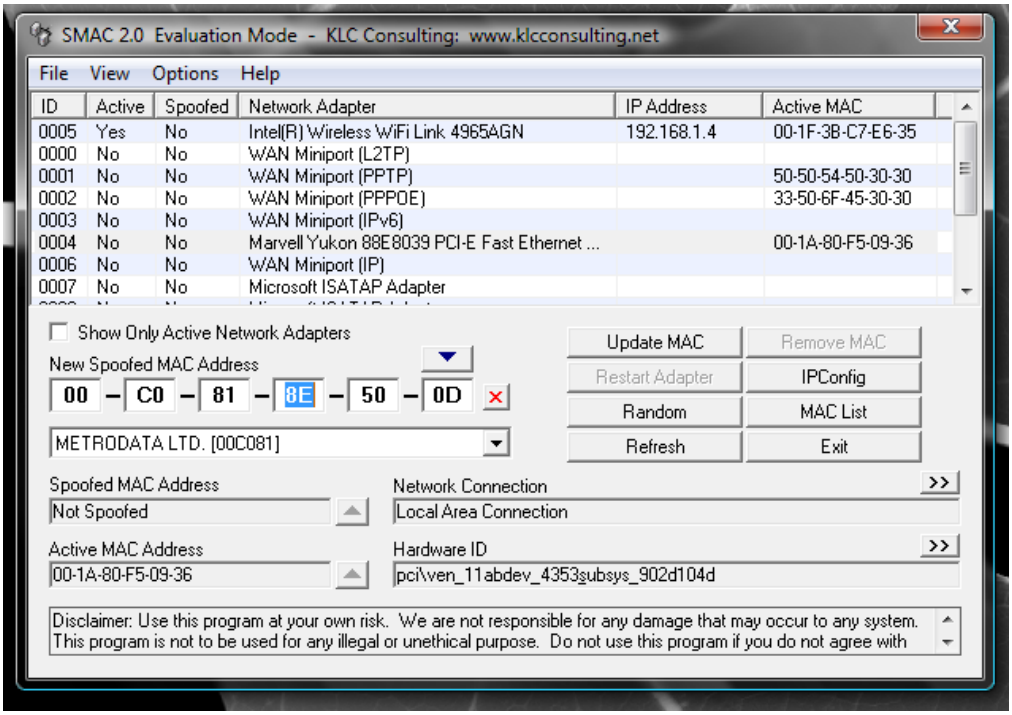
Figure B



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 **FigureC**, the new, random MAC address is displayed in the New Spoofed MAC Address section.

Figure C



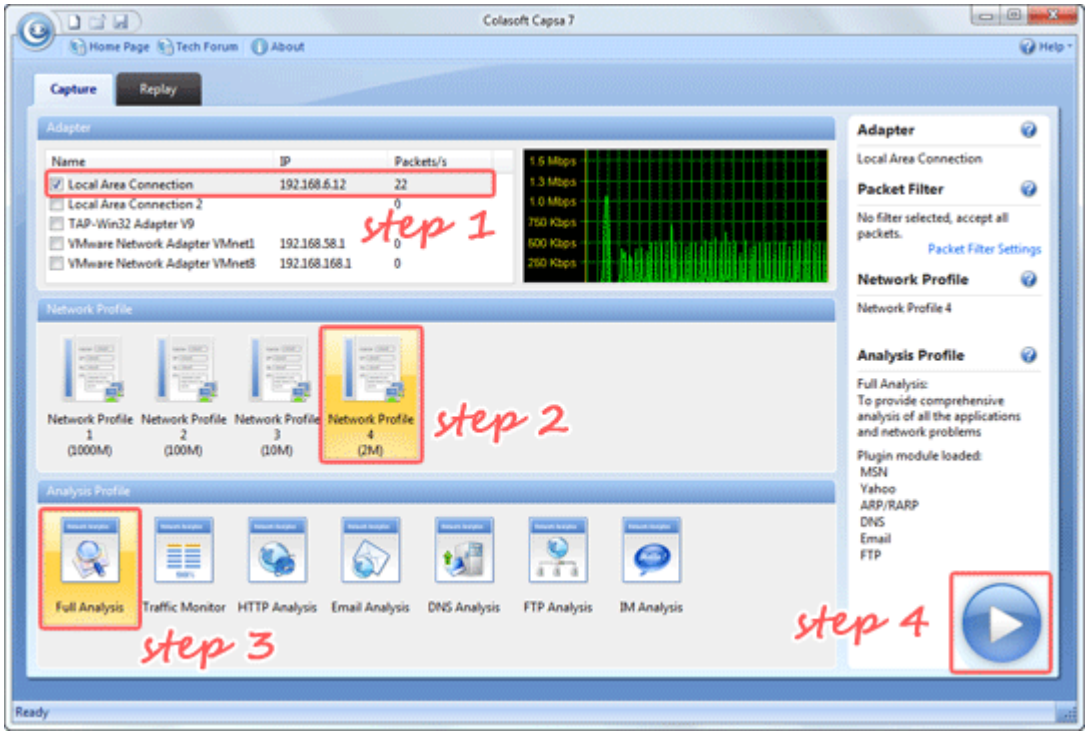
The address listed will correspond to a manufacturer list that you can choose from.

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).

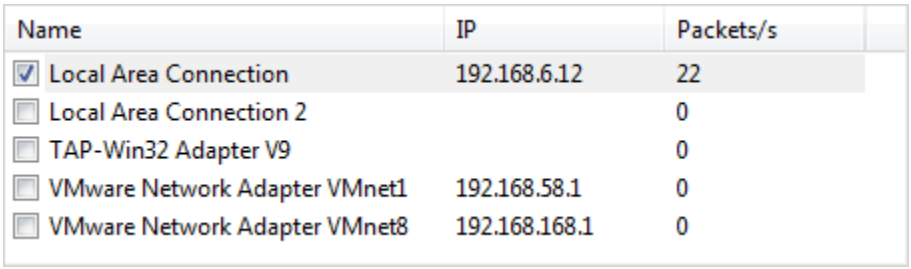
Once you have your address, select the Options menu and make sure Automatically Restart Adapter is checked. Once that is checked, hit the Update MAC Address button and the new MAC address will be applied.

c. Use Caspa Network Analyser.

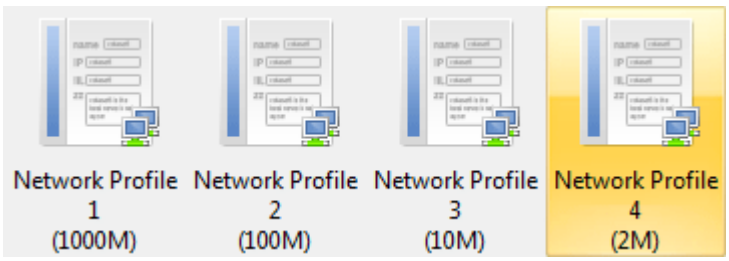
When we correctly deployed Capsa, we cannot wait to start our first capture right away. Capsa7's new Start Page guides us start an accurate capture mission step by step:



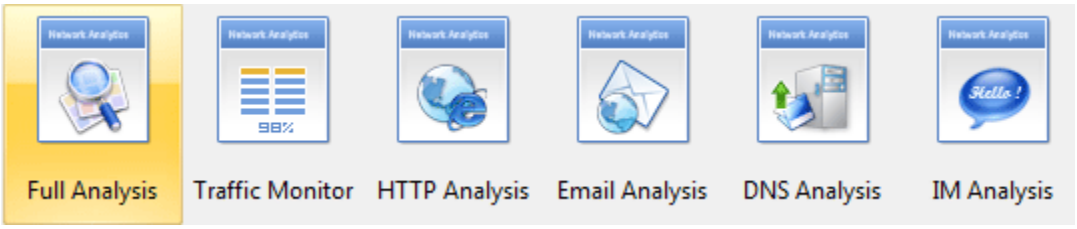
1. Double-click  icon on the desktop.
2. In the Start Page, select your NICs (multiple selections available) in the Capture panel first.



3. Select any Network Profile in the Network Profile panel.



4. Select Full Analysis in the Analysis Profile panel.



5. Click the big Run button to start a capture right away.

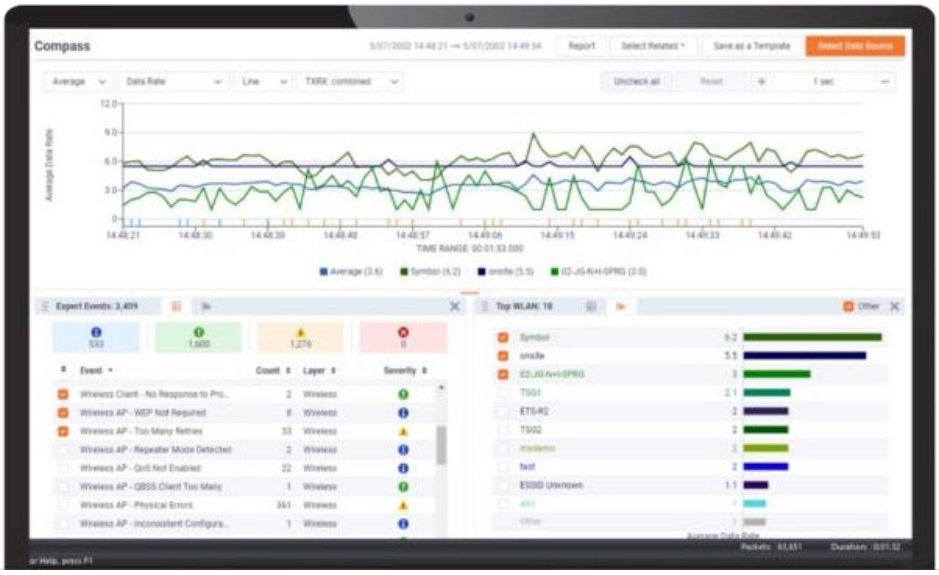
This is the common procedure to start a capture, which helps us get accurate and useful analysisdata: Select NIC -> Select Network Profile -> Select Analysis Profile -> Run.

d. Use Omnipeek Network Analyzer.

Omnipeek is a high-performance network protocol analyzer, capable of decoding thousands ofprotocols for fast network troubleshooting and diagnostics, anywhere network issues happen.

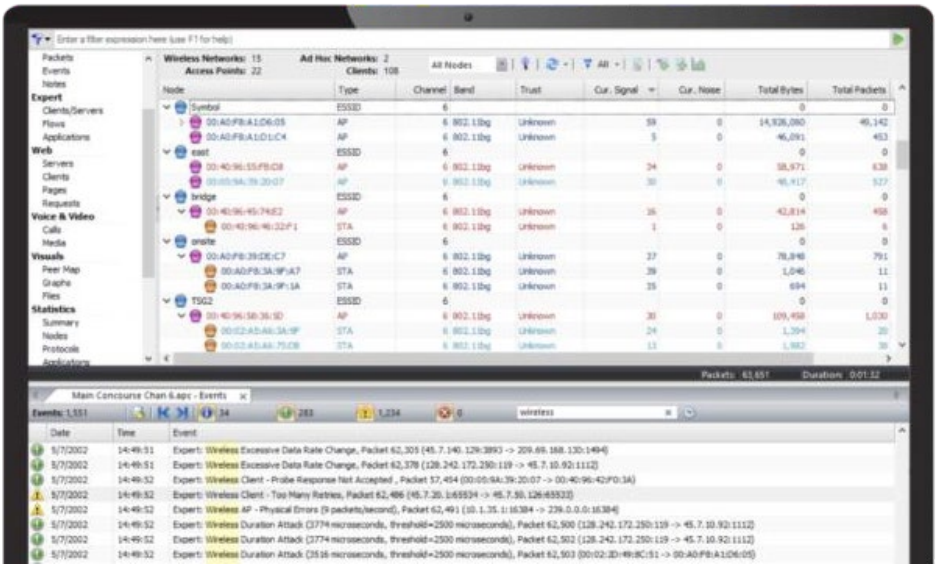
Real-Time Network Protocol Analyzer

Omnipeek provides real-time analysis for every type of network segment – 1/10/40/100 Gigabit, 802.11, and voice and video over IP – and for every level of network traffic.


Compass
Report
Select Related
Save as a Template
Select Data Source
Average
Data Rate
Line
TXRX: combined
Uncheck all
Reset
1 sec
Average Data Rate
12.0
9.0
6.0
3.0
0
14:48:21
14:48:30
14:48:39
14:48:48
14:48:57
14:49:06
14:49:15
14:49:24
14:49:33
14:49:42
14:49:51
TIME RANGE: 00:01:33.000
Average (3.6)
Symbol (6.2)
onsite (5.5)
Expert Events: 3,409
Top WLAN: 18
Other
533
1,600
1,276
0
Event
Count
Layer
Severity
Wireless Client - No Response to Pro...
Wireless AP - WEP Not Required
Wireless AP - Too Many Retries
Wireless AP - Repeater Mode Detected
Wireless AP - QoS Not Enabled
Wireless AP - QBSS Client Too Many
Wireless AP - Physical Errors
Wireless AP - Inconsistent Configura...
Symbol
onsite
TSG1
ETS-R2
TSG2
test
ESSID Unknown
Average Data Rate
Packets: 43,851
Duration: 0:01:32
or Help, press F1

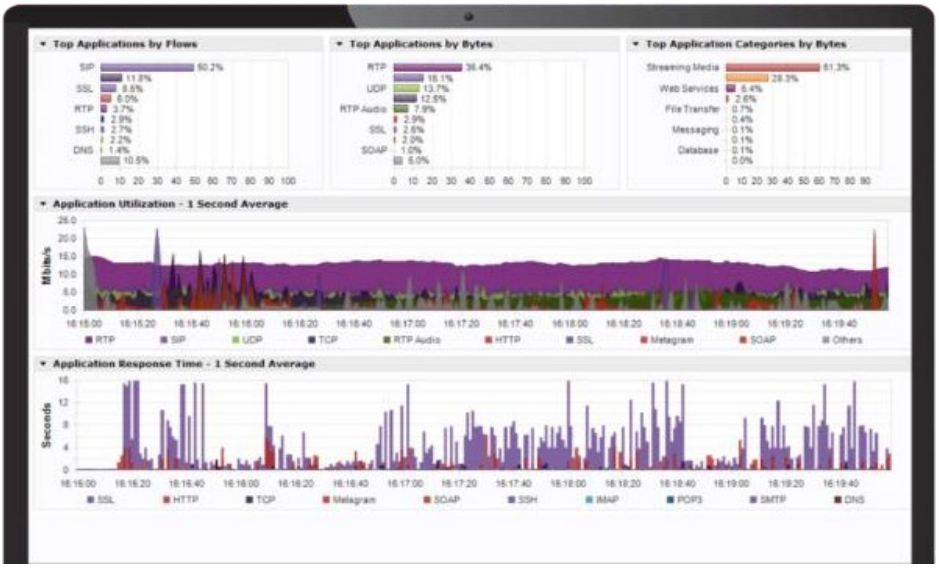
Intuitive Graphic Displays and Visualization

Omnipeek delivers intuitive visualization and effective forensics for faster resolution of network and application performance issues and security investigations.



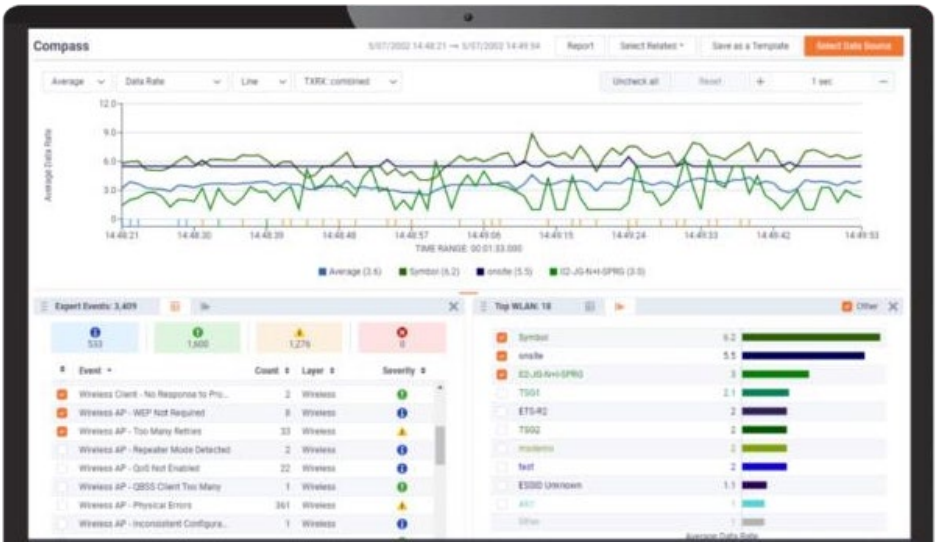
Best-In-Class Network Analysis Workflow

Widely recognized as the best network analysis workflow in the industry, we make it easy to drill down to a single packet – all from a single pane of glass.



WiFi Troubleshooting

The Omnipeek WiFi adaptor is a USB-connected WLAN device designed for wireless packet capture. The 802.11ac adapter supports 802.11ac capture up to 2 transmit/receive streams (866Mbps wireless traffic) and supports 20MHz, 40MHz, and 80MHz channel operation.



Monitor Distributed Networks Remotely

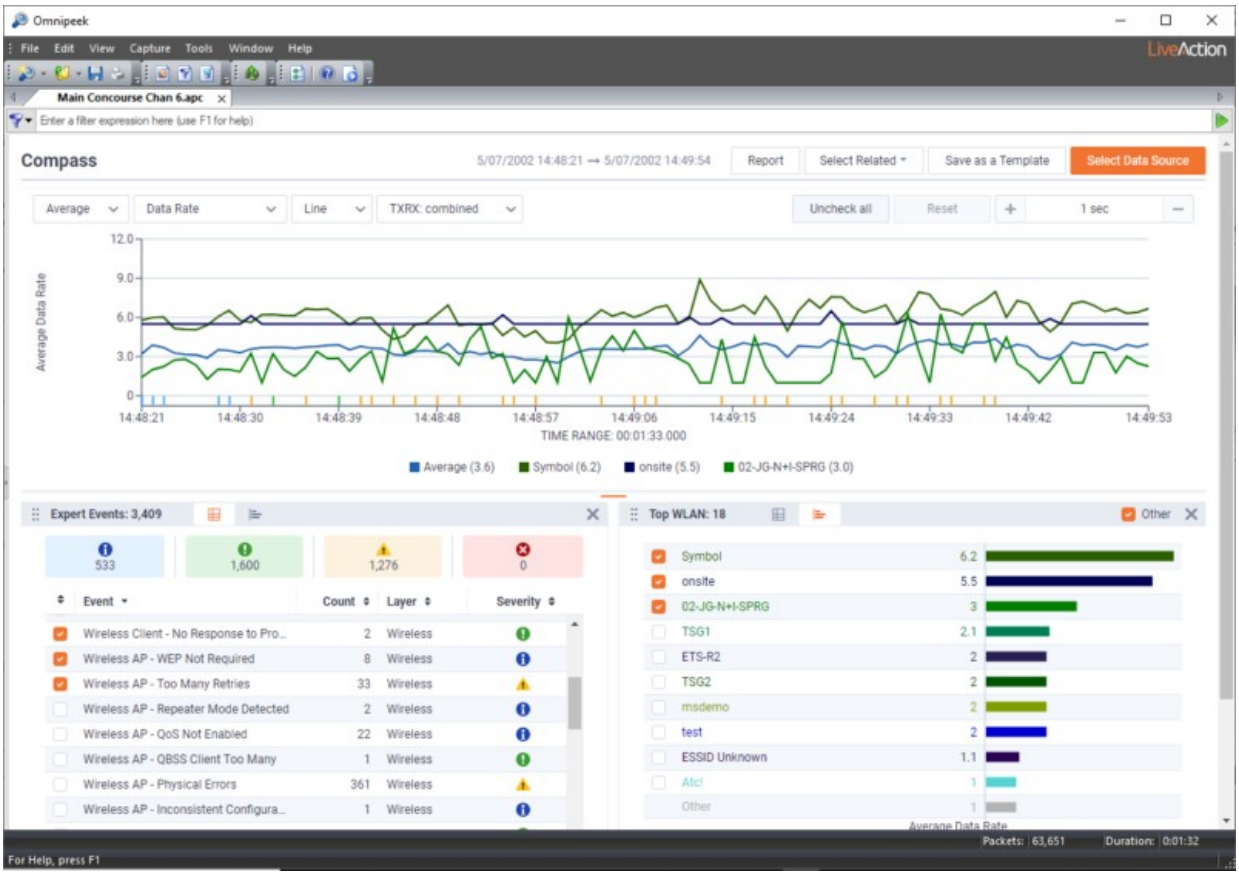
Integrating with LiveCapture, Omnipeek extends network monitoring and visibility for troubleshooting application-level issues at remote sites and branches, WAN links, and data centers.

Voice and Video Monitoring and Troubleshooting

Monitor and troubleshoot voice and video over IP traffic in real-time with high-level multi-media summary statistics, call playback, and comprehensive signaling and media analyses.

Simplify Troubleshooting Remote Devices

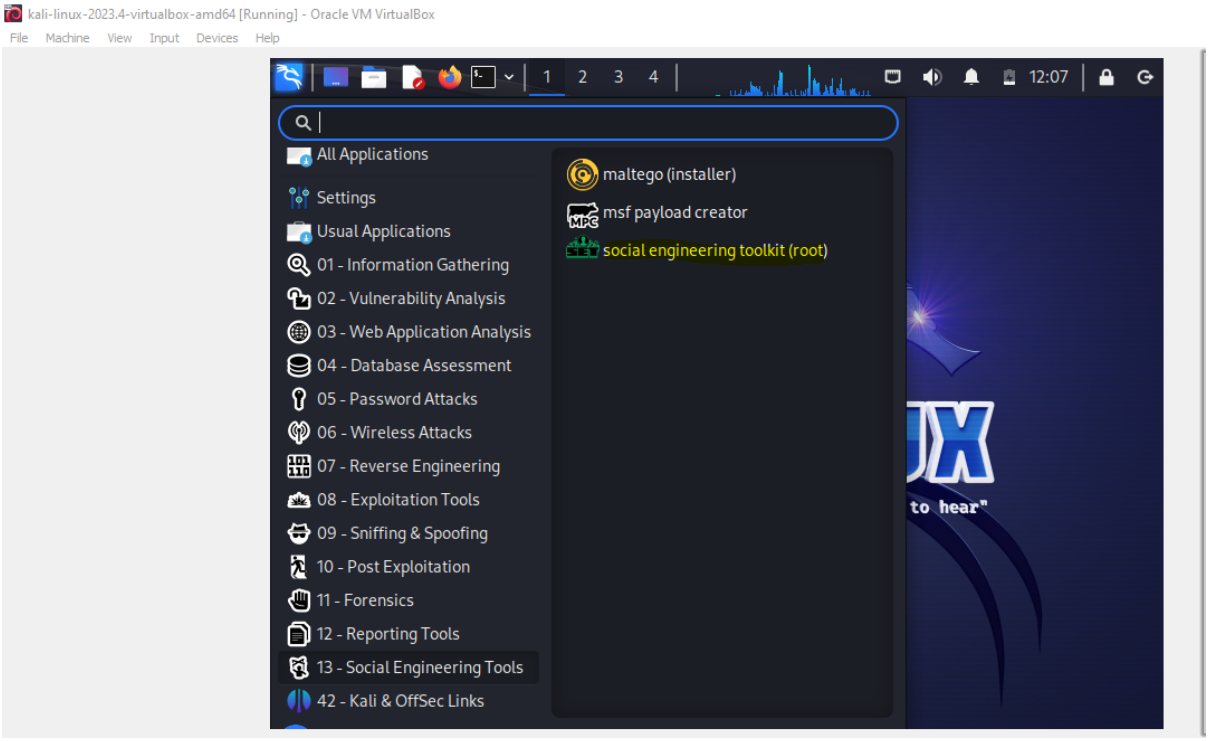
Easily troubleshoot end-user devices remotely and securely with encrypted files, avoiding the need to travel to a user's location.



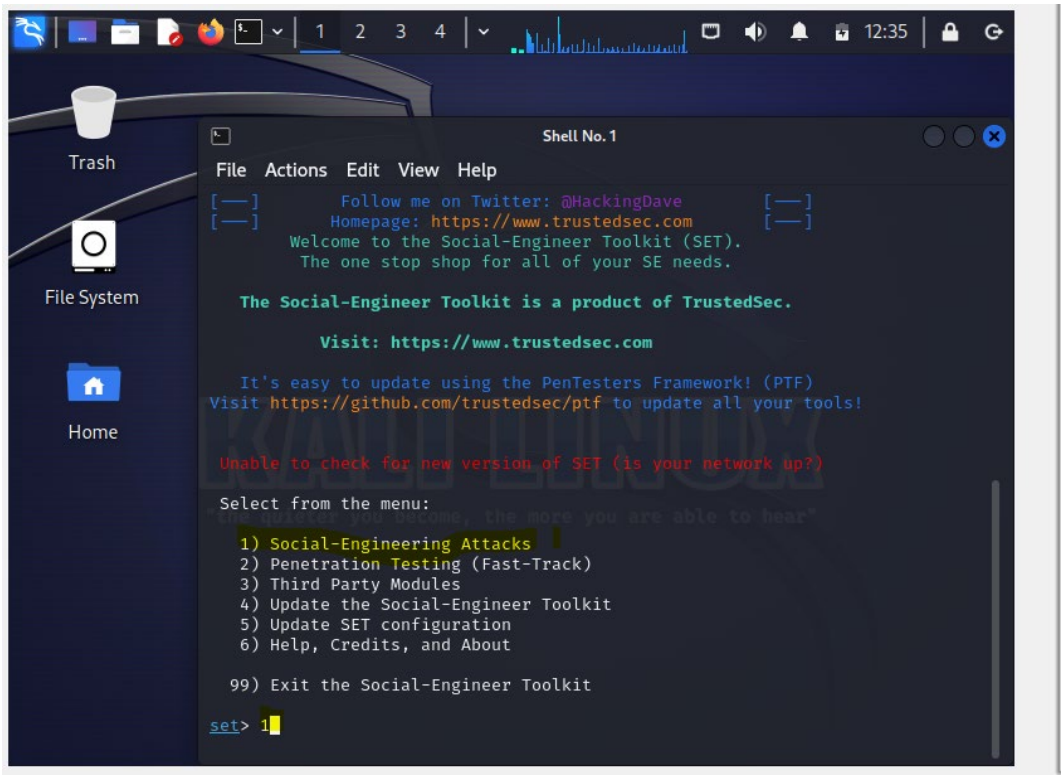
Section III A.

a. **Aim:** Use Social Engineering Toolkit on Kali Linux.

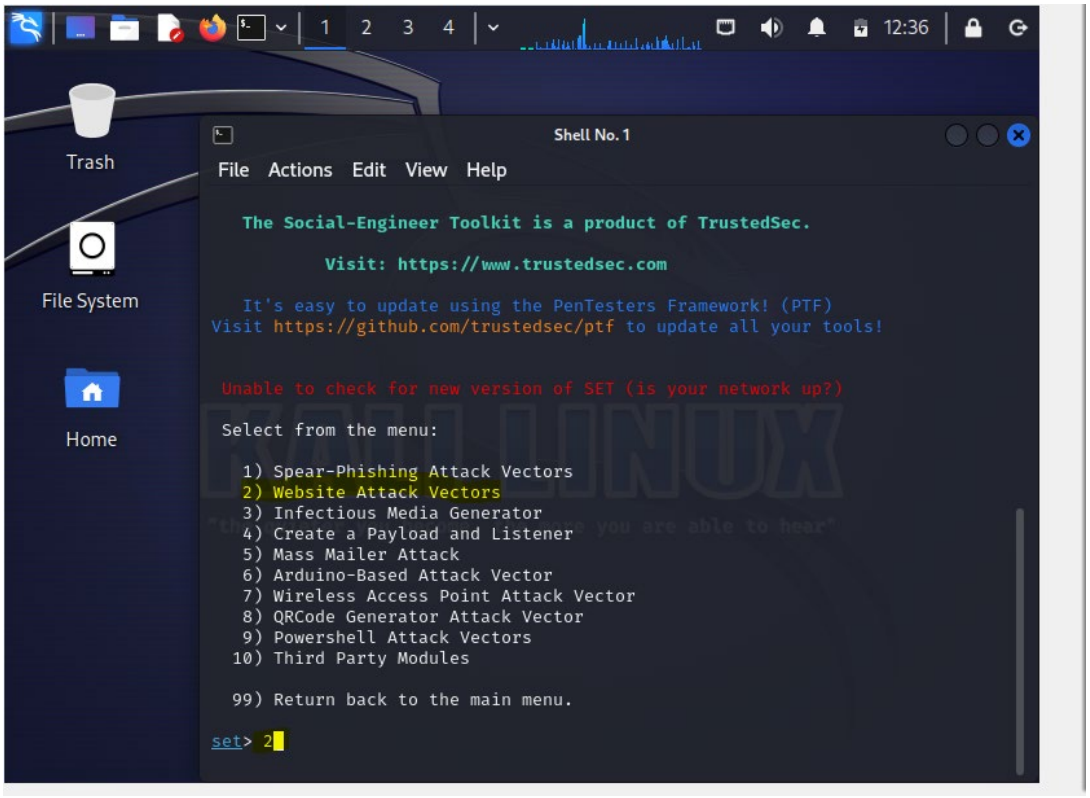
Step 1: Select social engineering toolkit in the Kali Linux.



Step 2: Select option 1. Social engineering attack



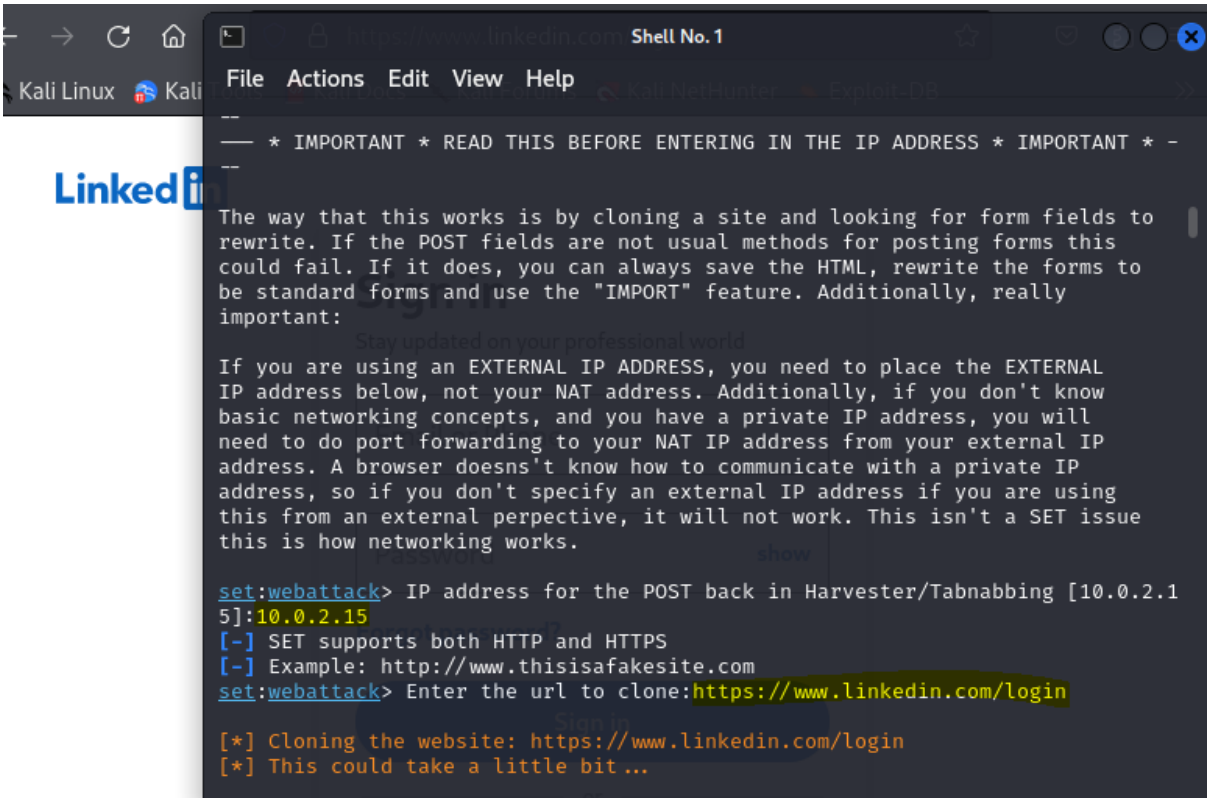
Step 3: Select option 3, website attack vectors



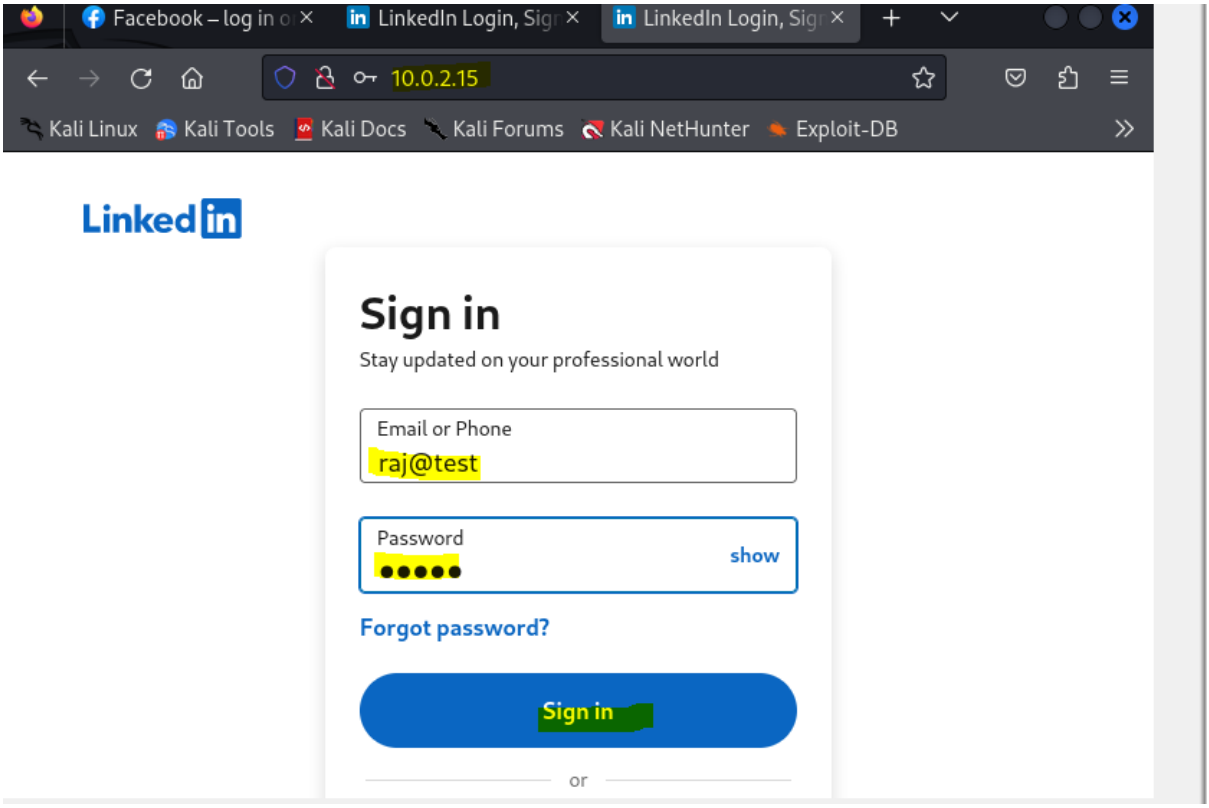
Step 4: Select Credential Harvester attack method

Step4: Select option 2 Site cloner.

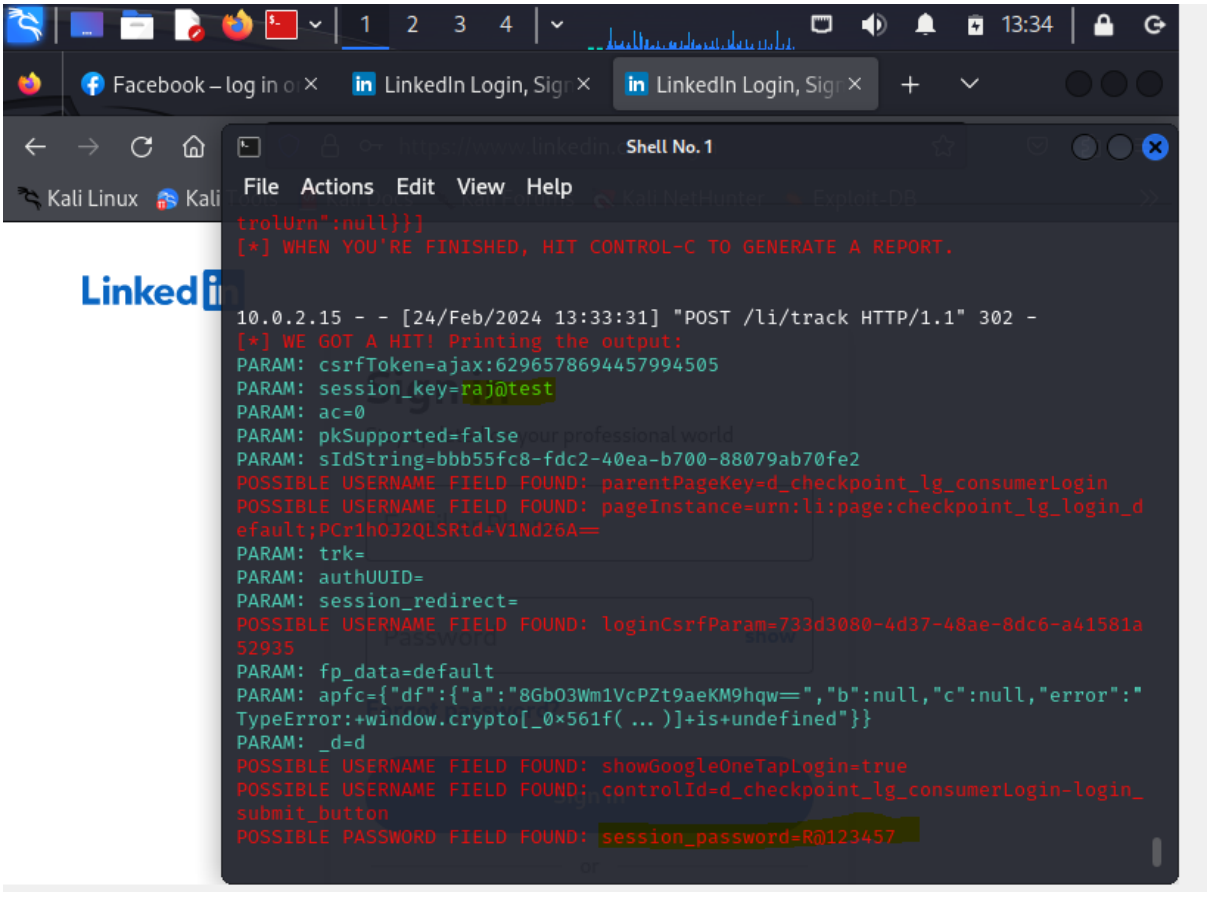
Step 5: Enter IP of the local server and URL of the attacking site



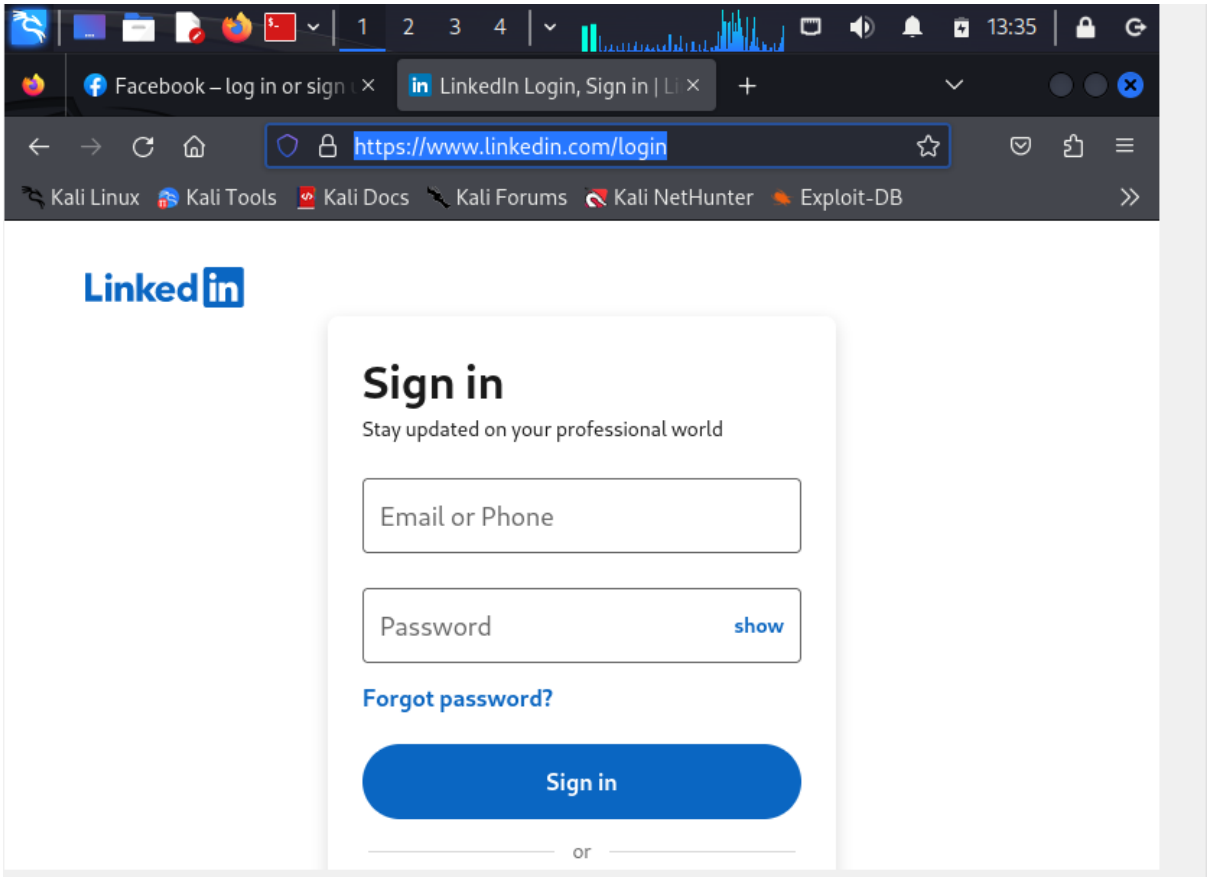
Step 6: now enter the ip in the browser, you will find clone website:



Step 7: You can see in the terminal the user id and password is being displayed.



Step 8: Post the attack user is redirected to the original site:

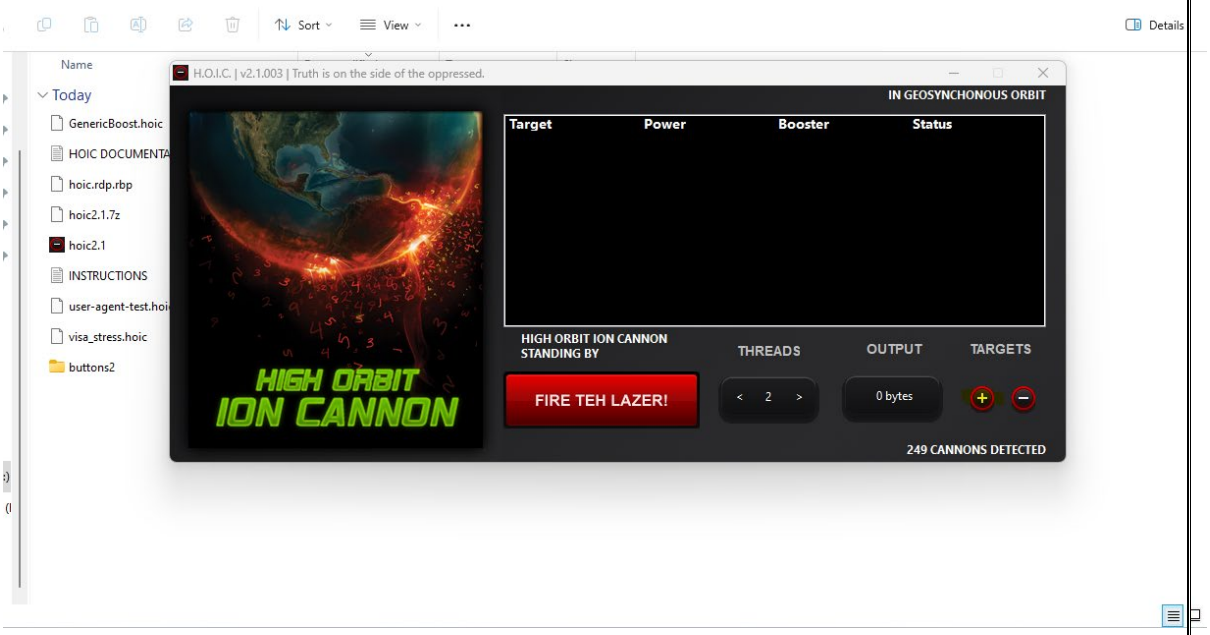

1 2 3 4
13:35
Facebook – log in or sign
LinkedIn Login, Sign in |
https://www.linkedin.com/login
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Linked in
Sign in
Stay updated on your professional world
Email or Phone
Password
show
Forgot password?
Sign in
or

Section III A.

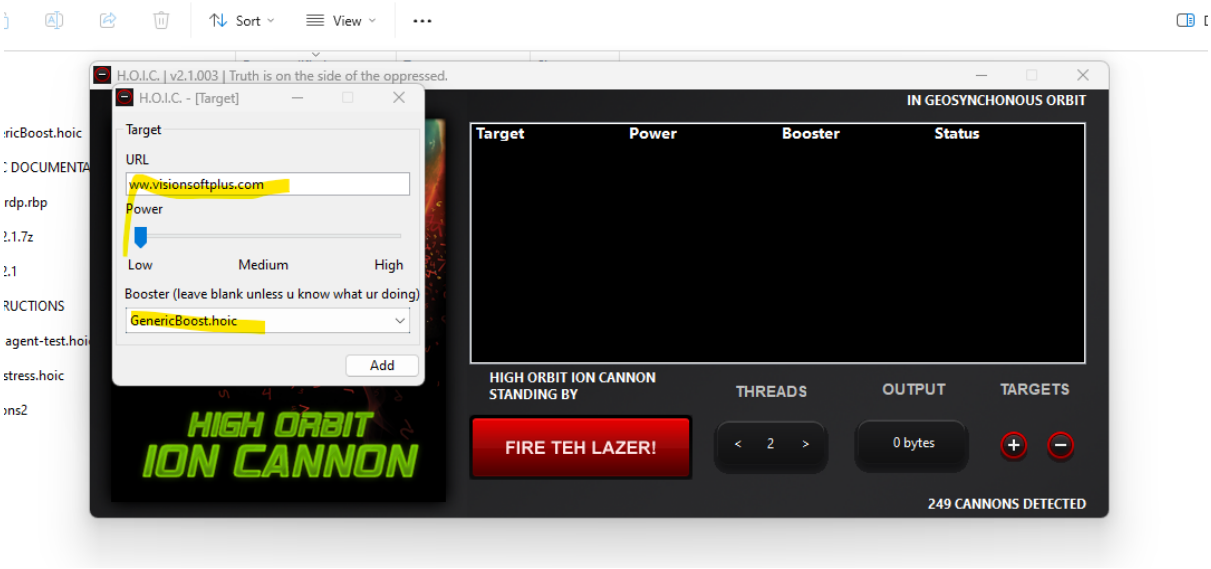
b. Aim: Perform the DDOS attack using the following tools

I. HOIC

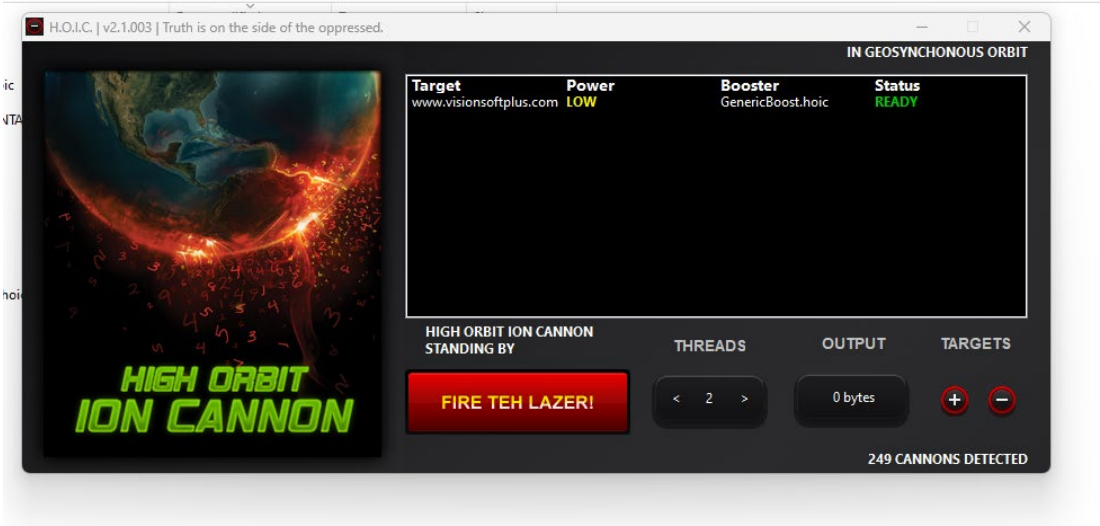
Step 1. Open hoic2.1.exe, once it open click on the "+" button



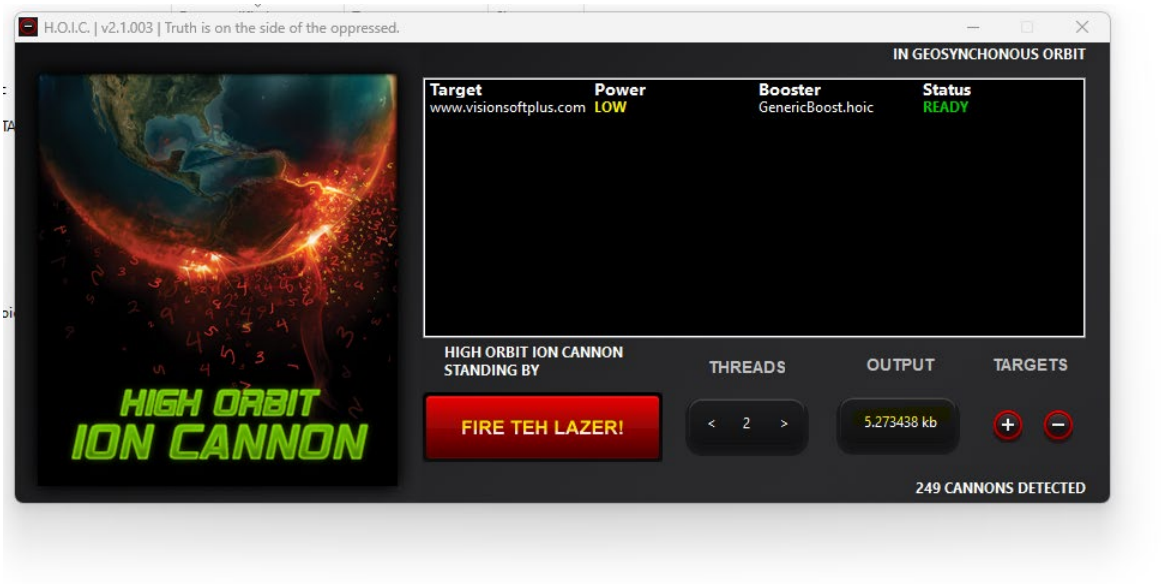
Step2: enter the url you want to attack, then click on add button.



Step 3: Click on fire button to attack



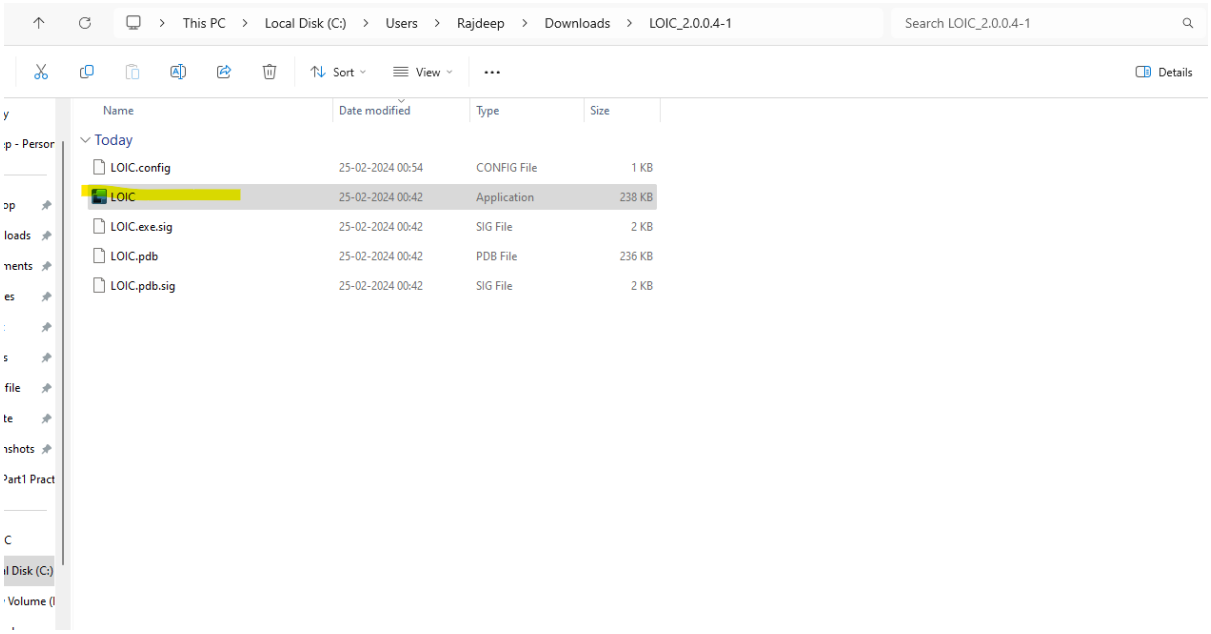
Step 4: you can see the attack is carried on and check the same on wire shark also



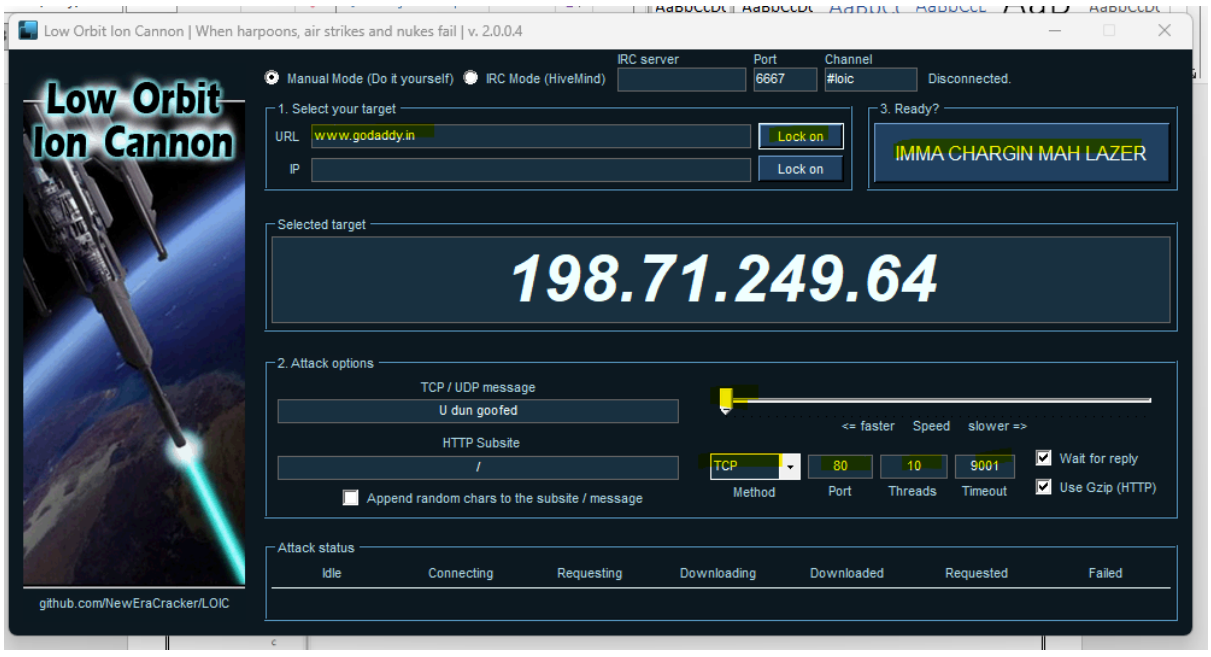
Step 5: To stop the attack again click on the Fire button.

II. LOIC

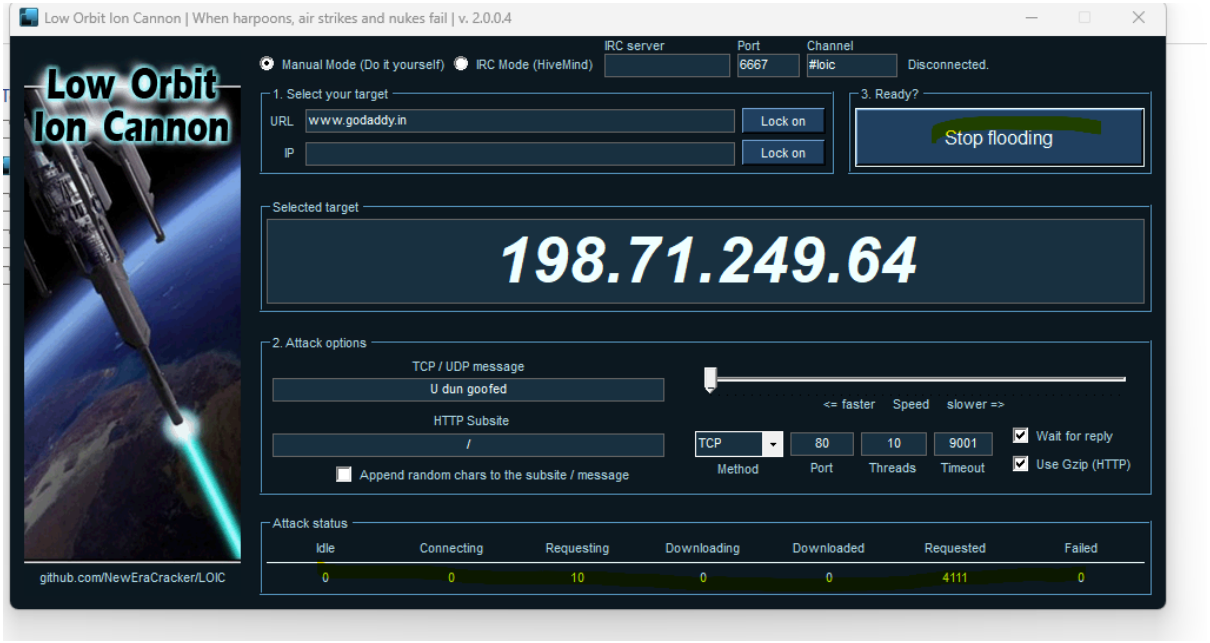
Step 1. Click on the loic.exe:



Step 2. Enter the URL click on Lock On button, change the parameter Like speed, method, number of thread, timeout. And the click on IMMA Chargin button.



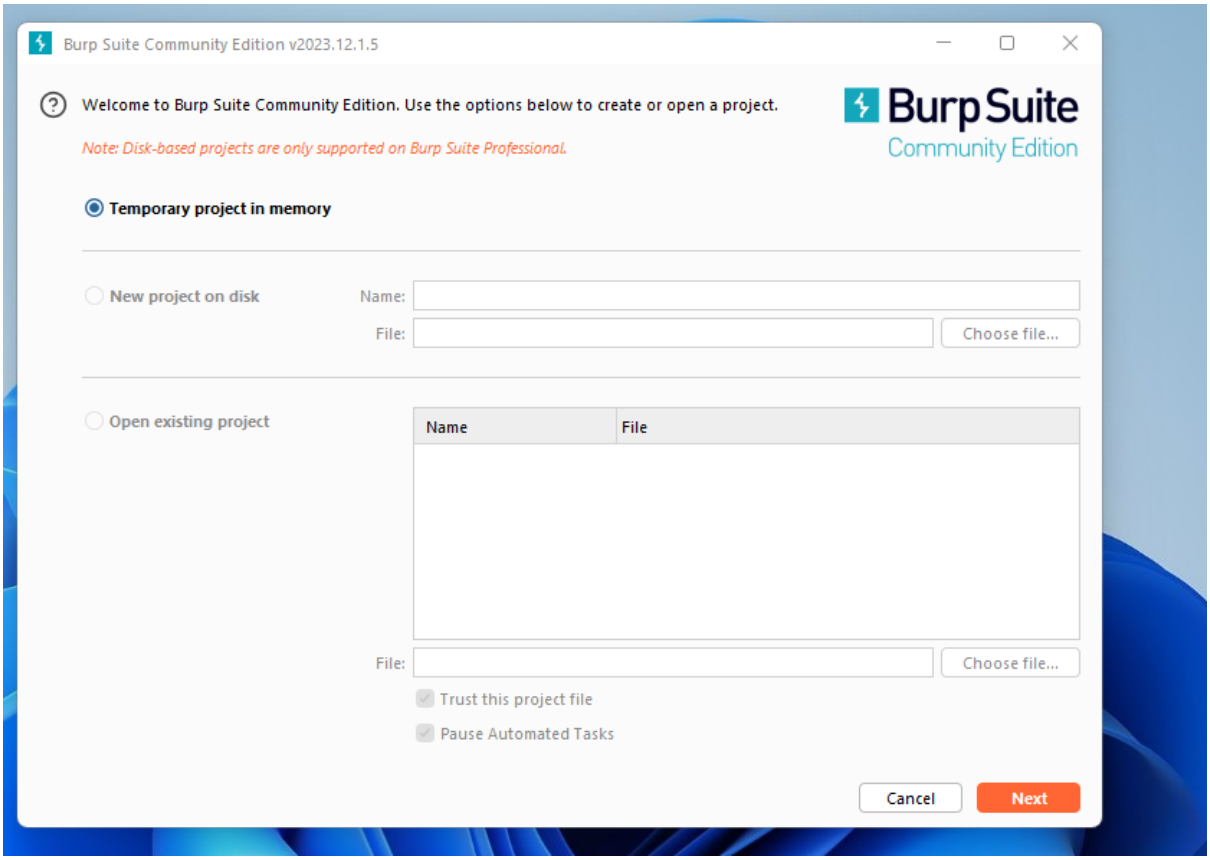
Step 3: You can see the number of requests getting hit. Click on Stop button to stop the DDOS attack.



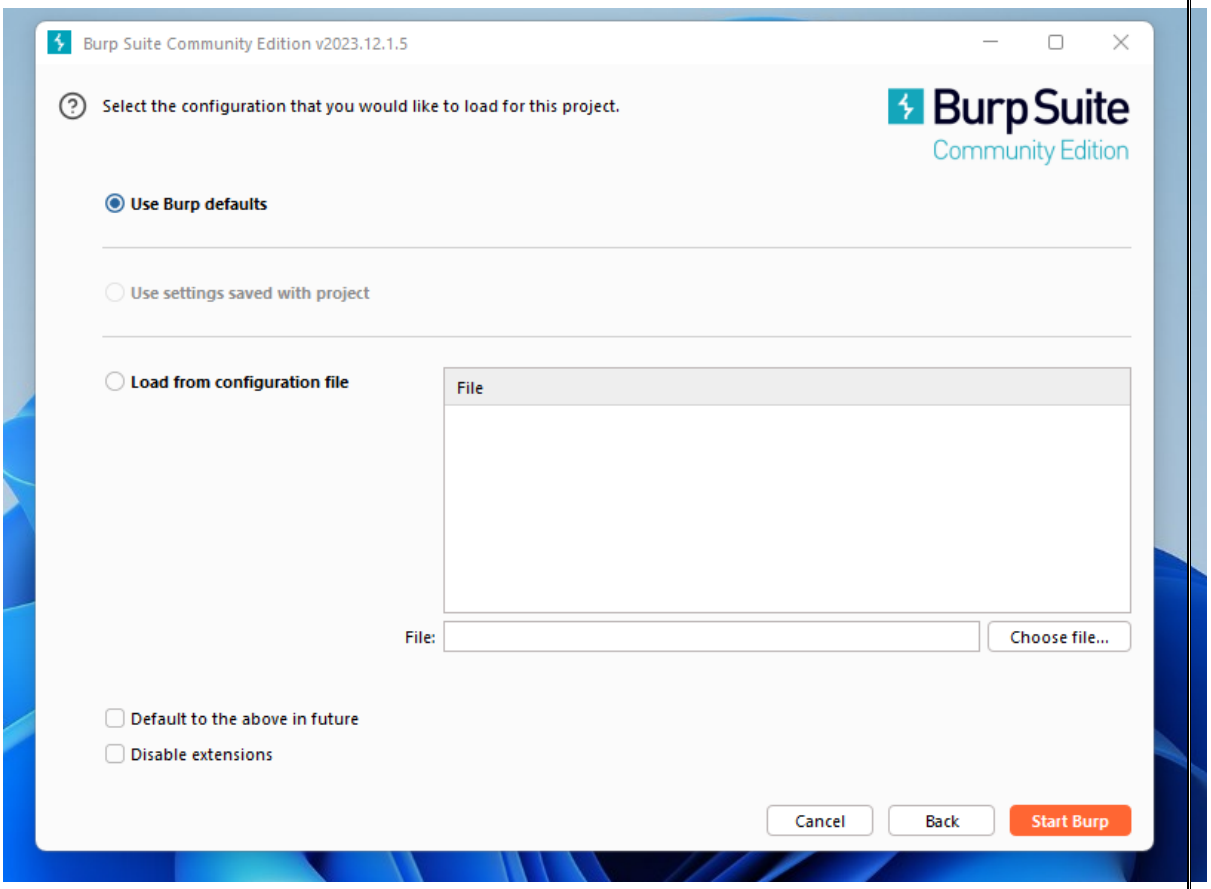
C. Aim: Using Burp Suite to inspect and modify traffic between the browser and target application

Application name : Burp tool

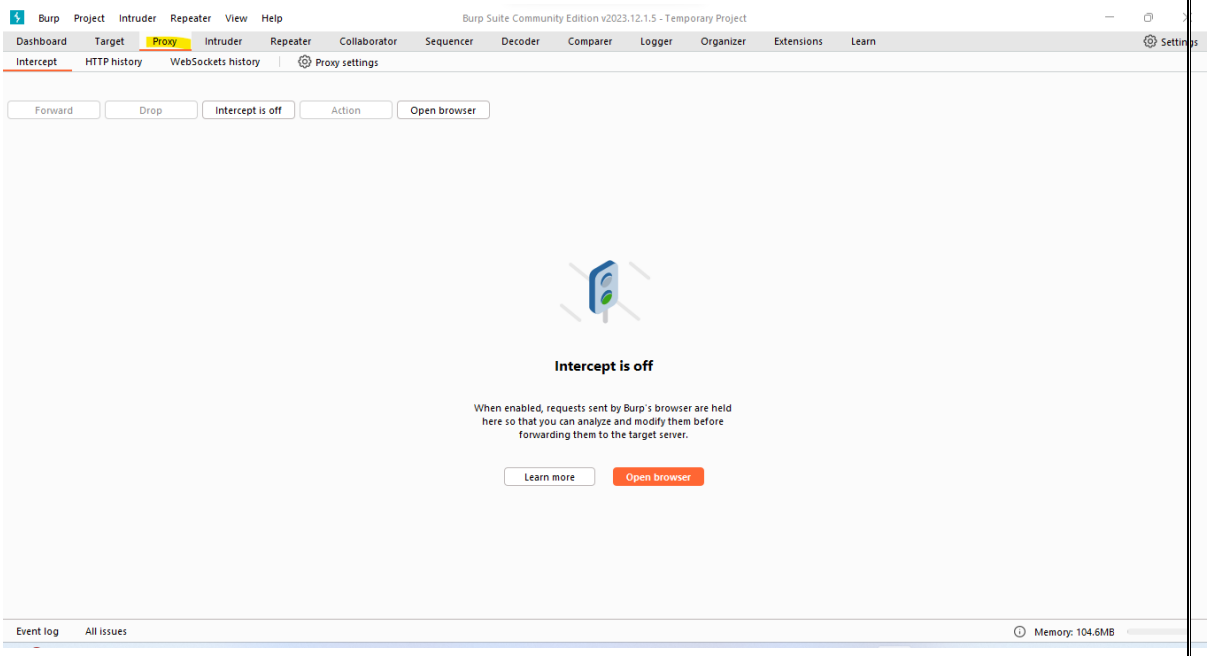
1. Open Burp Tool: Click on next



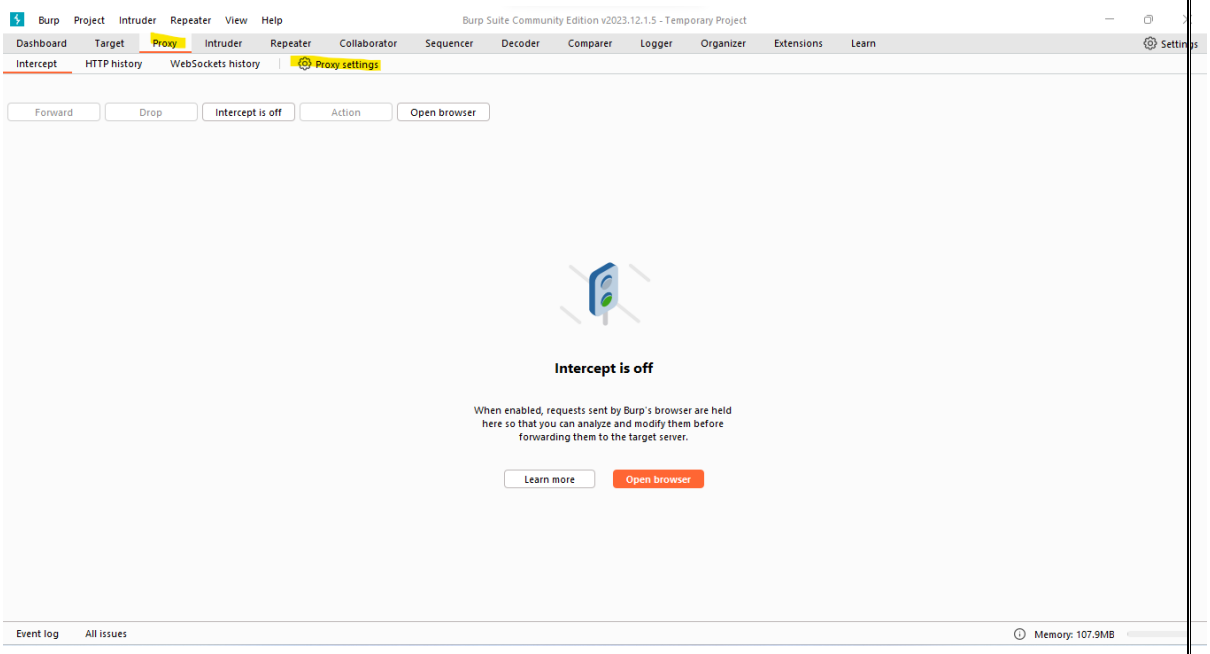
2. Click on start Burp



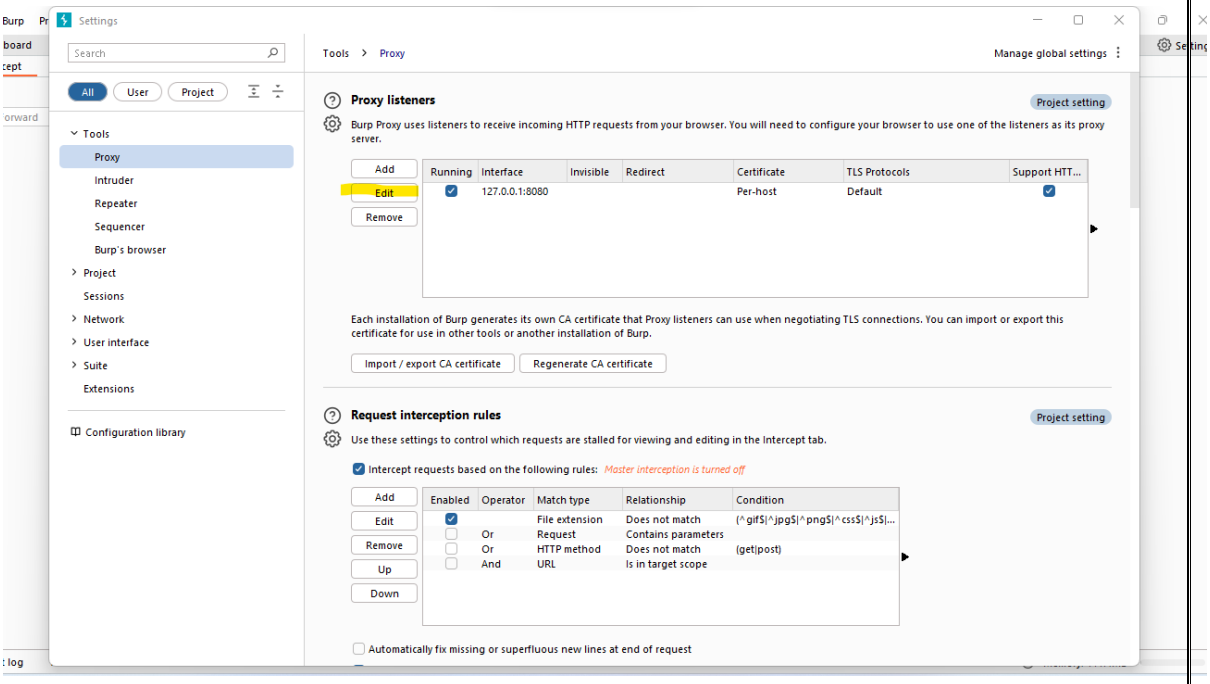
3. Select Proxy in the tab:



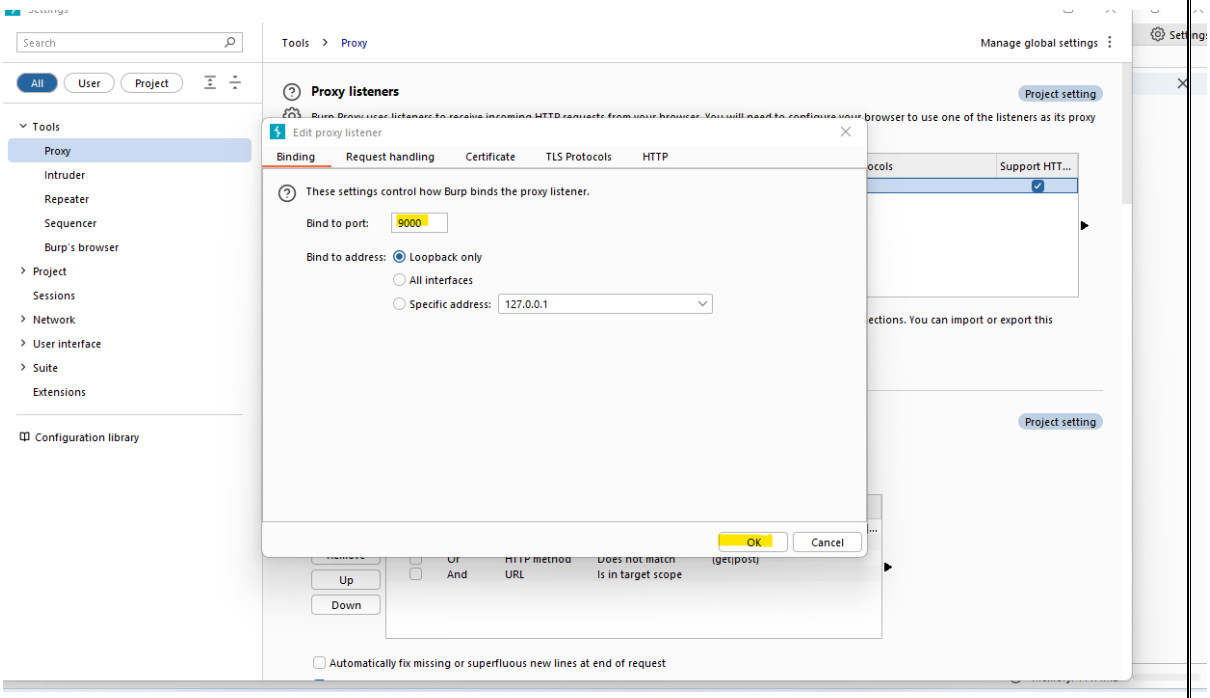
4. Go to proxy setting:



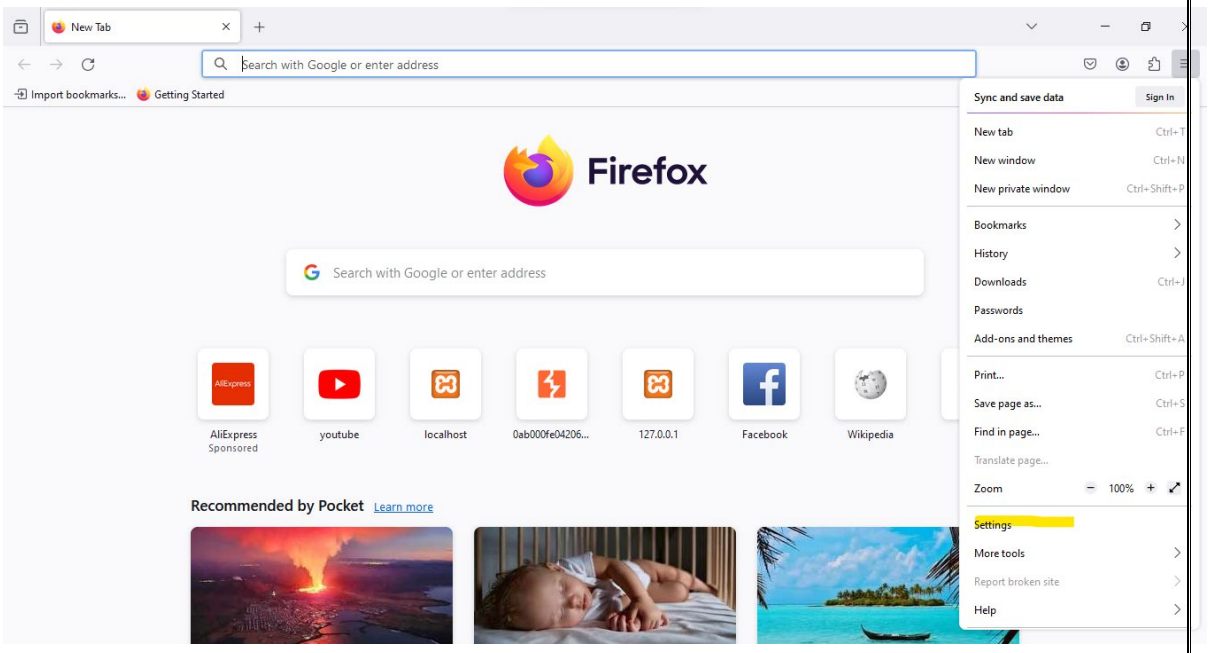
5. Click on Edit:



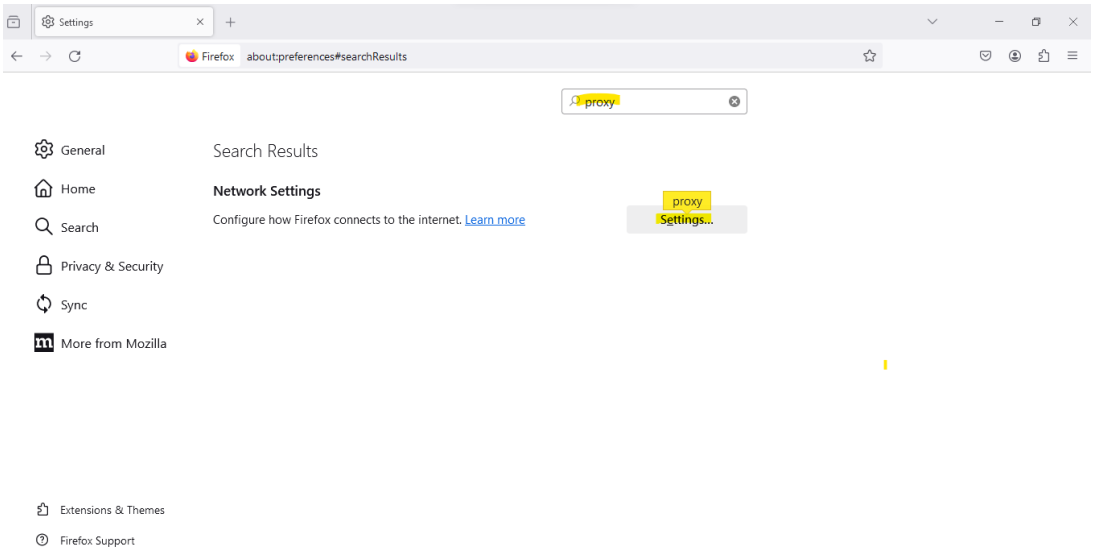
6. Change the port number in our case its change from 8080 to 9000. And then click on OK.



9. Now go to the firefox browser: goto settings or preference depending on the version:



10. Search for proxy in the search bar and then click on setting:



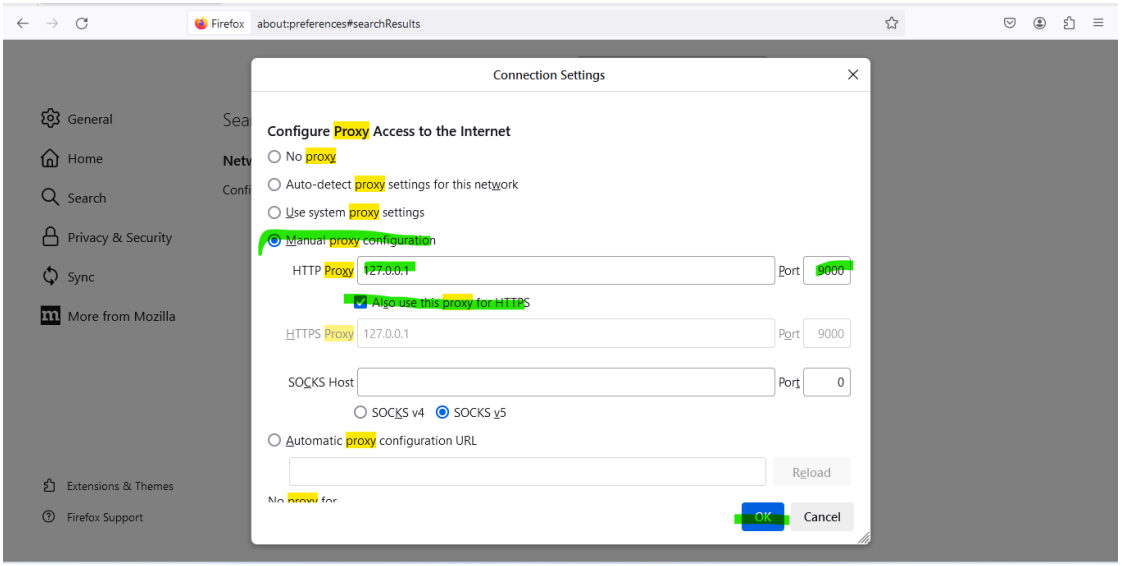
11. Now do the following steps:

a. select manual

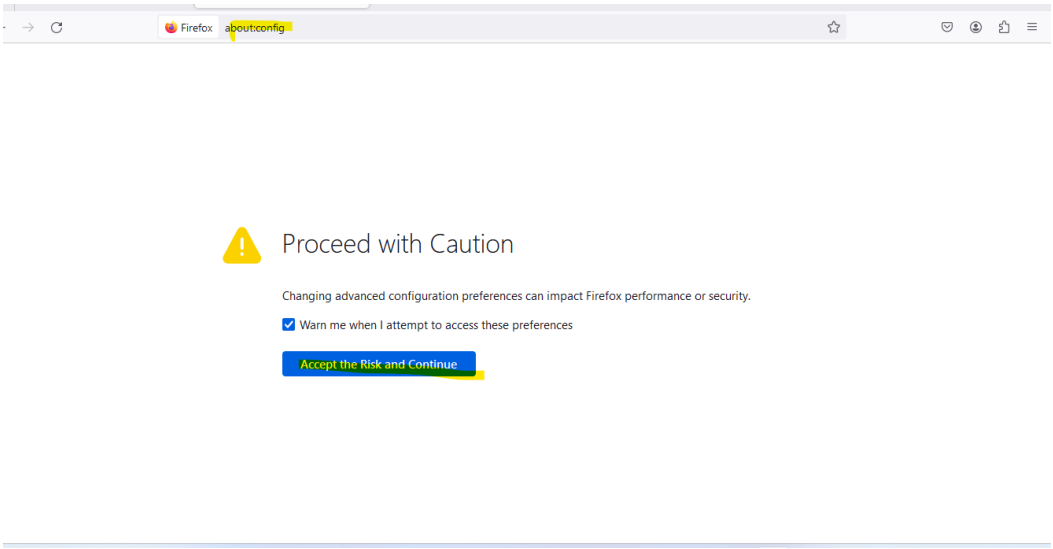
b. Enter ip as 127.0.0.1 and port as 9000.

c. select option also use this proxy for HTTPS

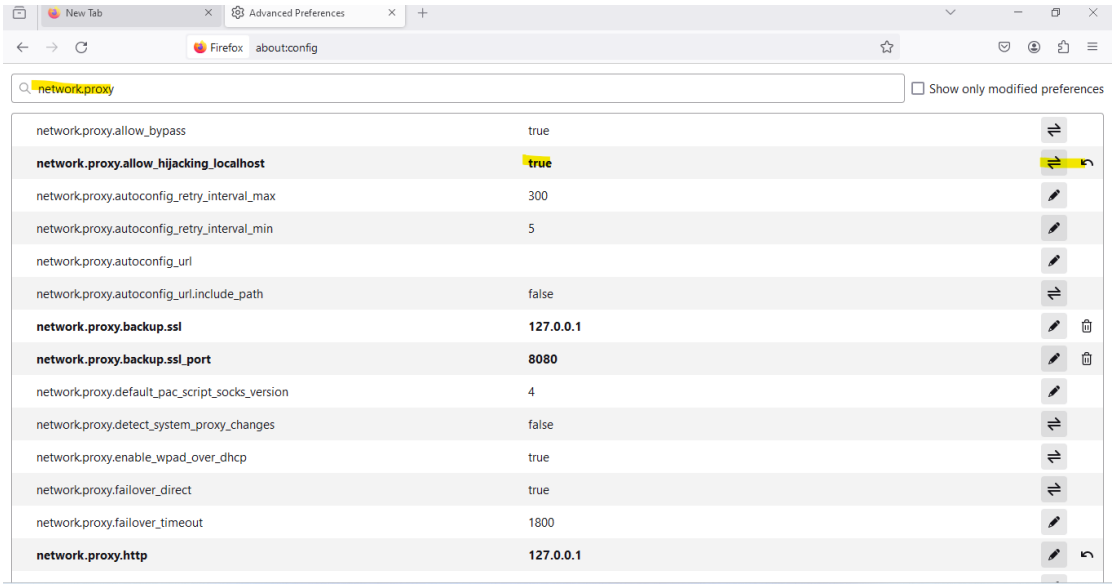
d. click on ok



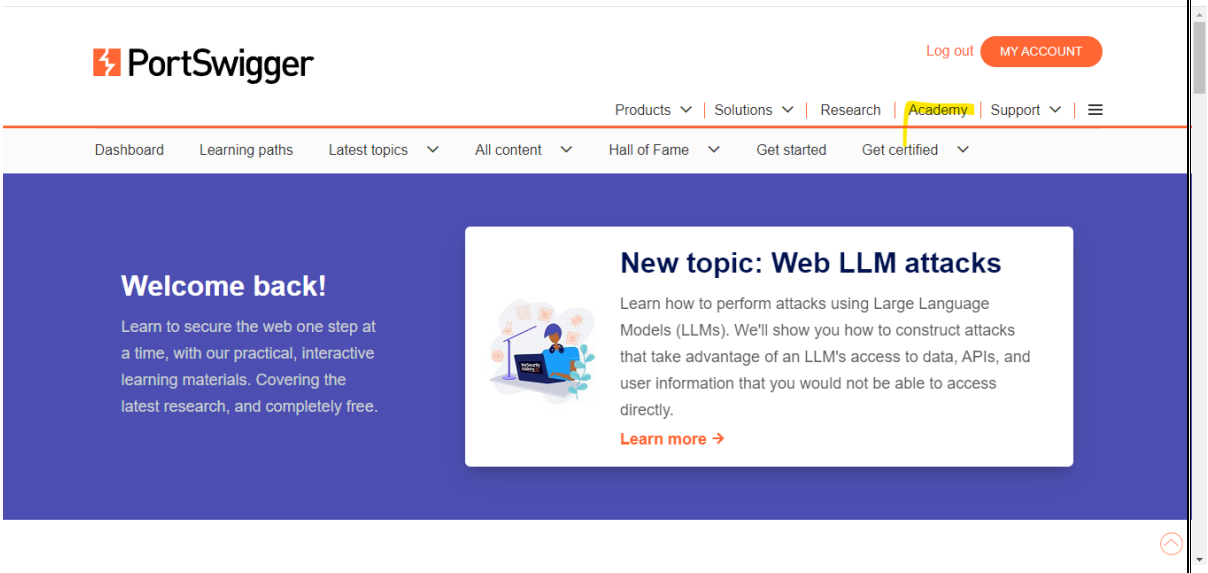
12. Now go to firefox search bar and type “about:config”. In the screen click on “Accept the Risk and Continue”.



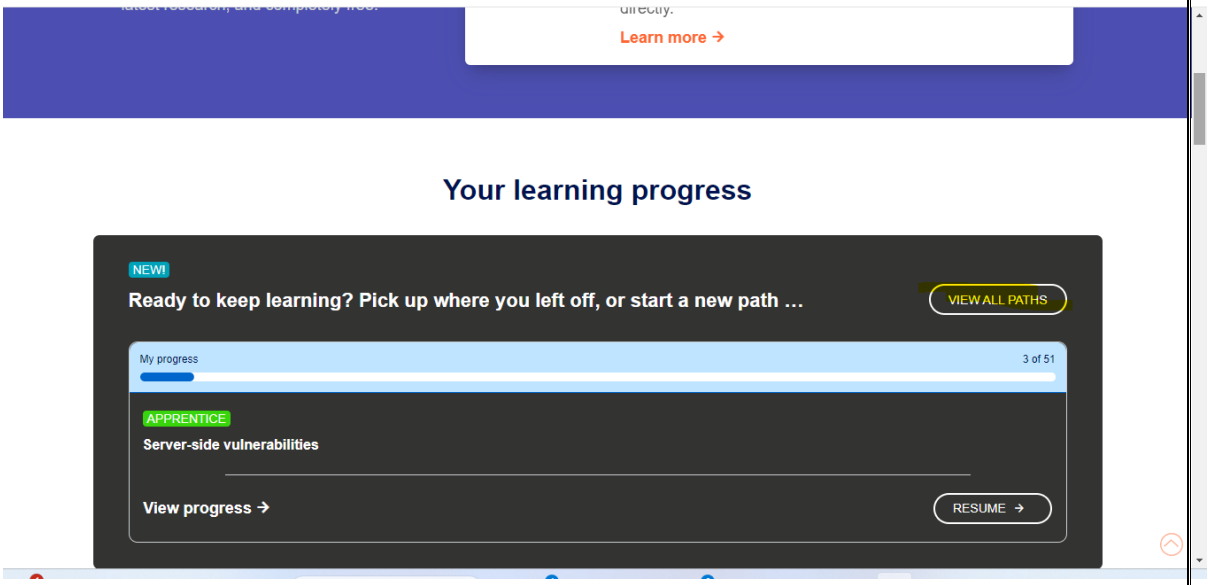
13. Enter: “network.proxy” and select the option as per the image below, click on the right side button to make the value true:



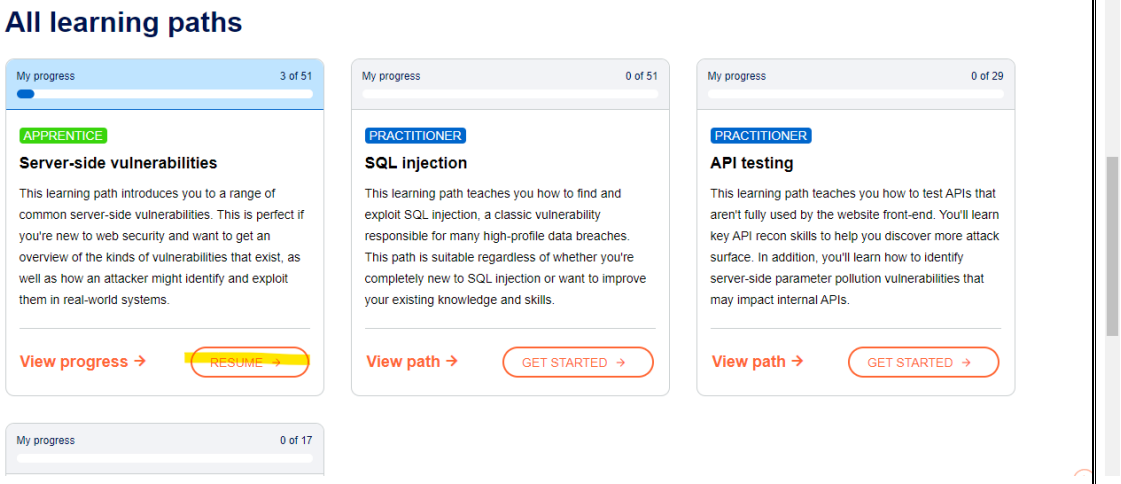
14. go to web security academy, login and select academy go to:



15. scroll dow click on all path button:

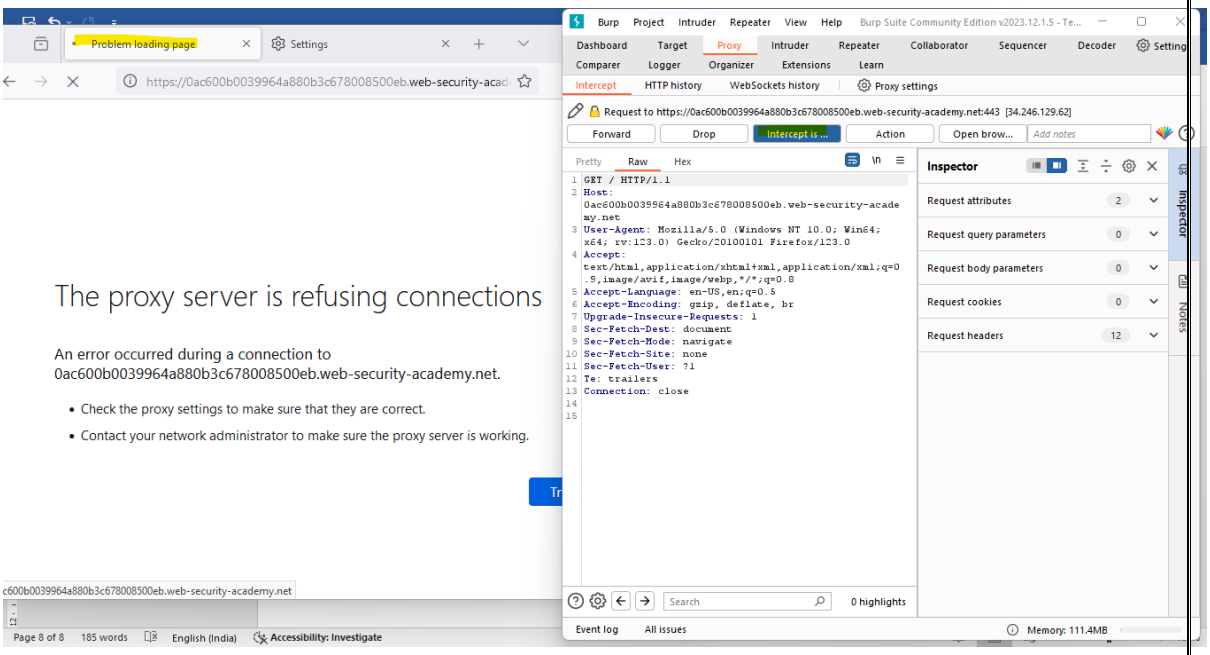


15. click on button “resume” on server side validation section:

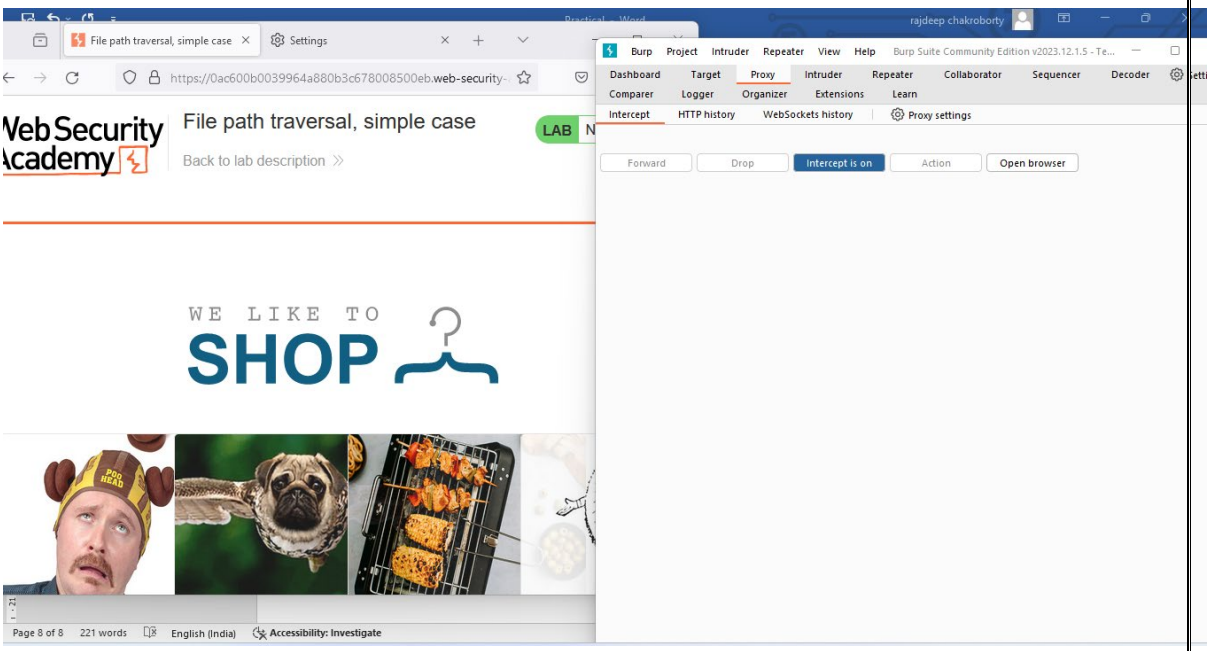


16. click on access Lab:

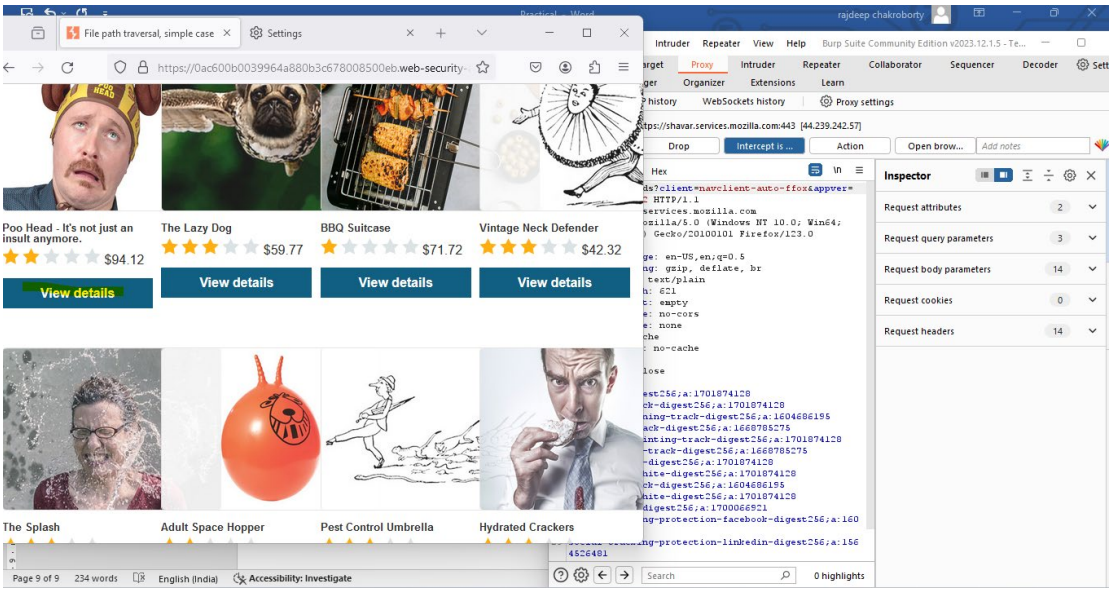
17. Once the lab is open click on start the interception on in the burp tool.
Note in he browser you will find page is not loading.



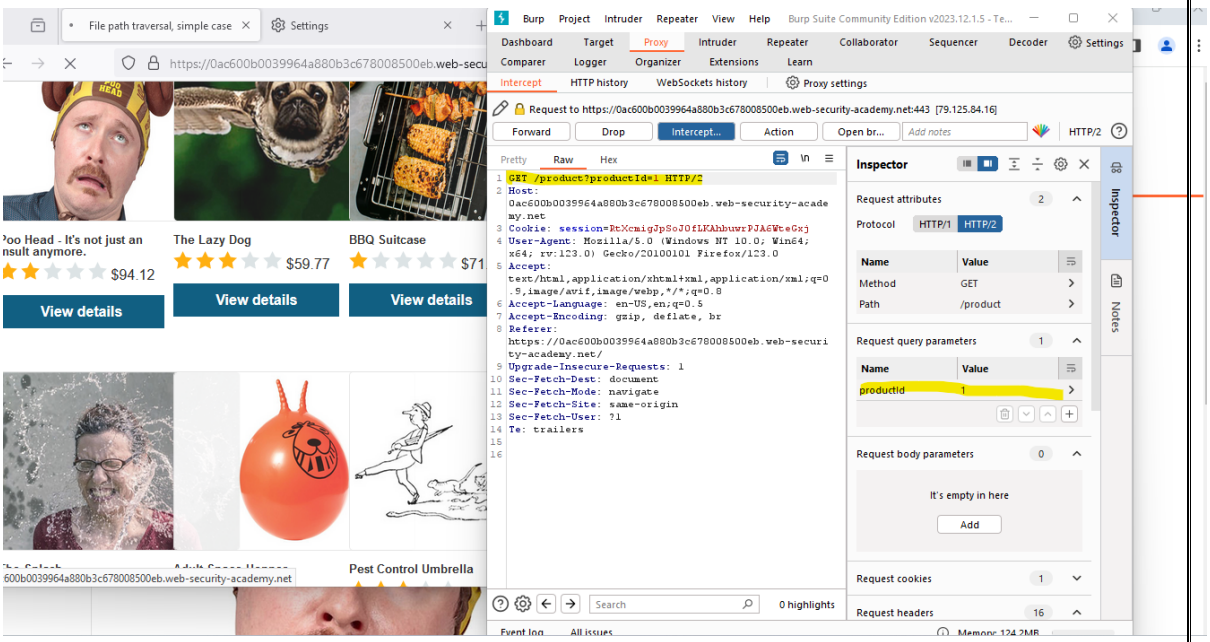
18. To load the field click on forward button.
Note you will have to click multiple time to load the entire page.



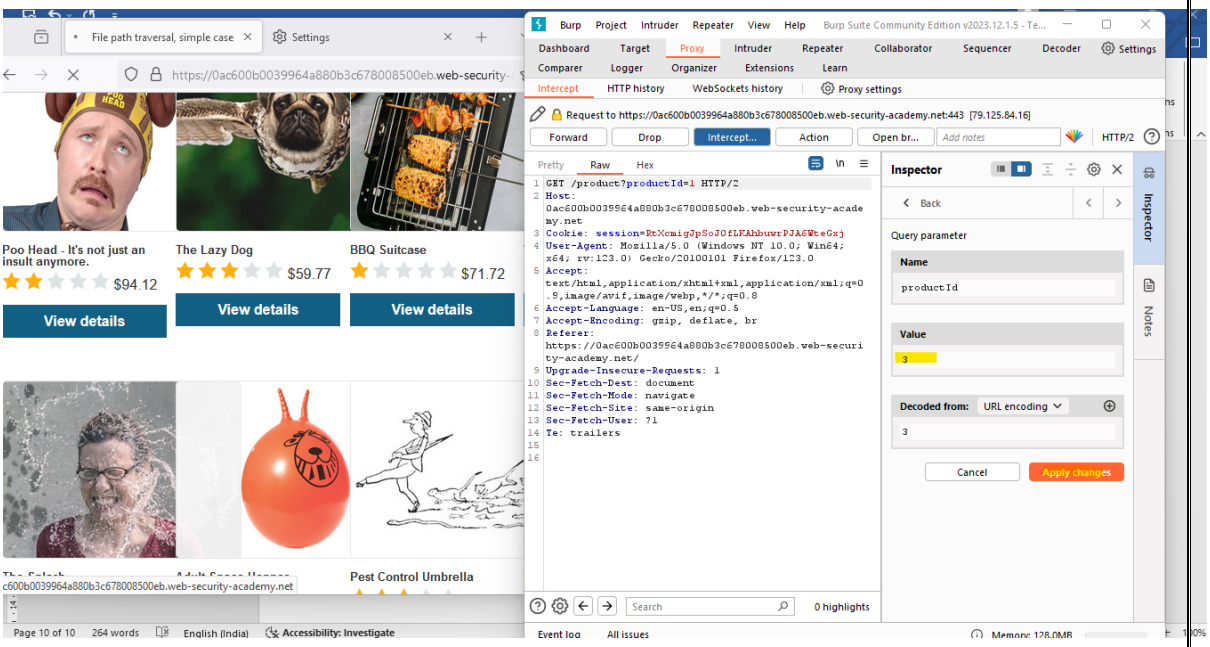
19. click on the first grid view details button:



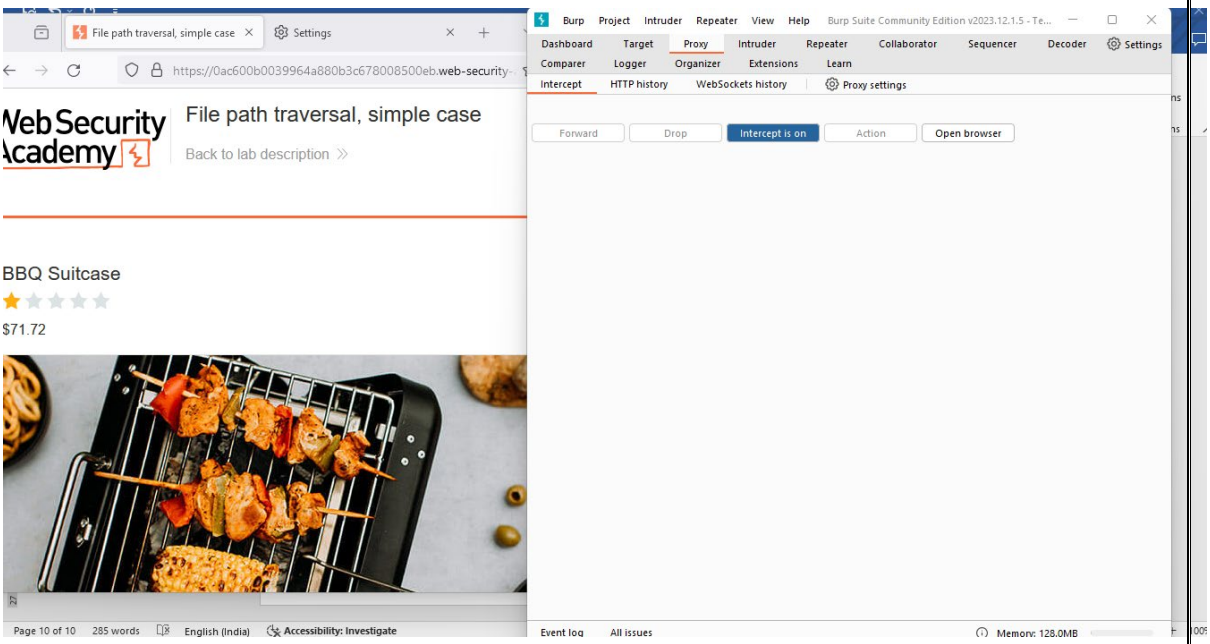
20. Click forward on the burb application, go to request query parameter:



21. change the value of the productid to 3. Click on apply changes:



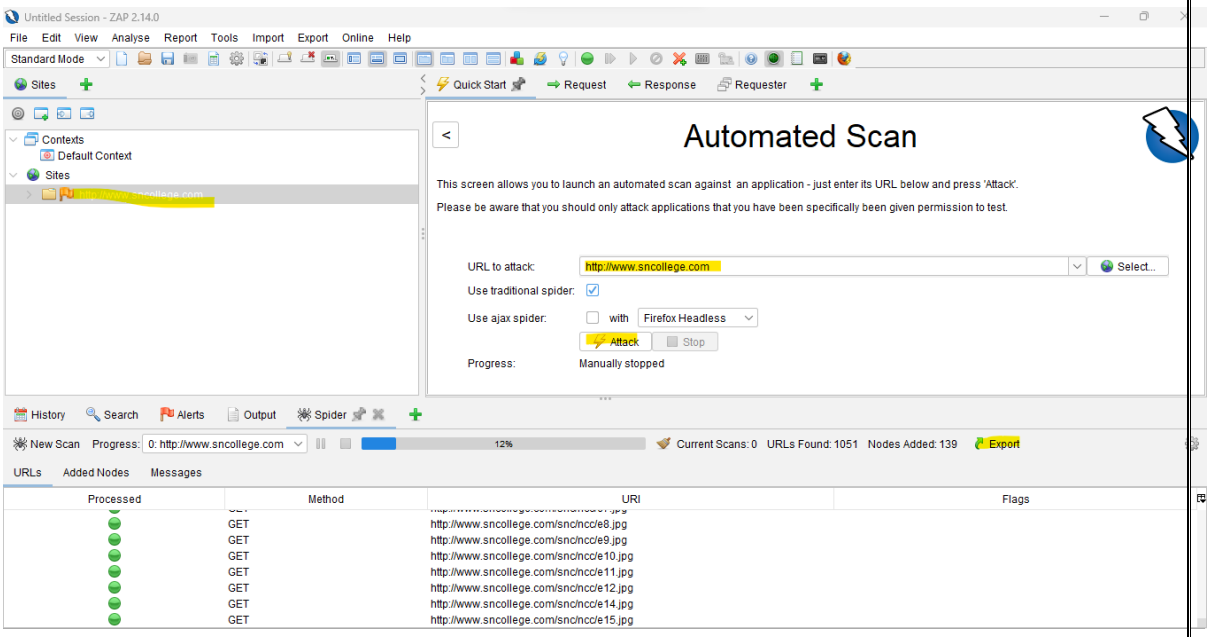
4. Then click on forward you will observe, page for item 3 will open instead of 1.


File path traversal, simple case
Settings
https://0ac600b0039964a880b3c678008500eb.web-security-
Web Security Academy
File path traversal, simple case
Back to lab description
BBQ Suitcase
$71.72
Page 10 of 10
285 words
English (India)
Accessibility: Investigate
Burp
Project
Intruder
Repeater
View
Help
Burp Suite Community Edition v2023.12.1.5 - Te...
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Settings
Comparer
Logger
Organizer
Extensions
Learn
Intercept
HTTP history
WebSockets history
Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Event log
All issues
Memory: 128.0MB

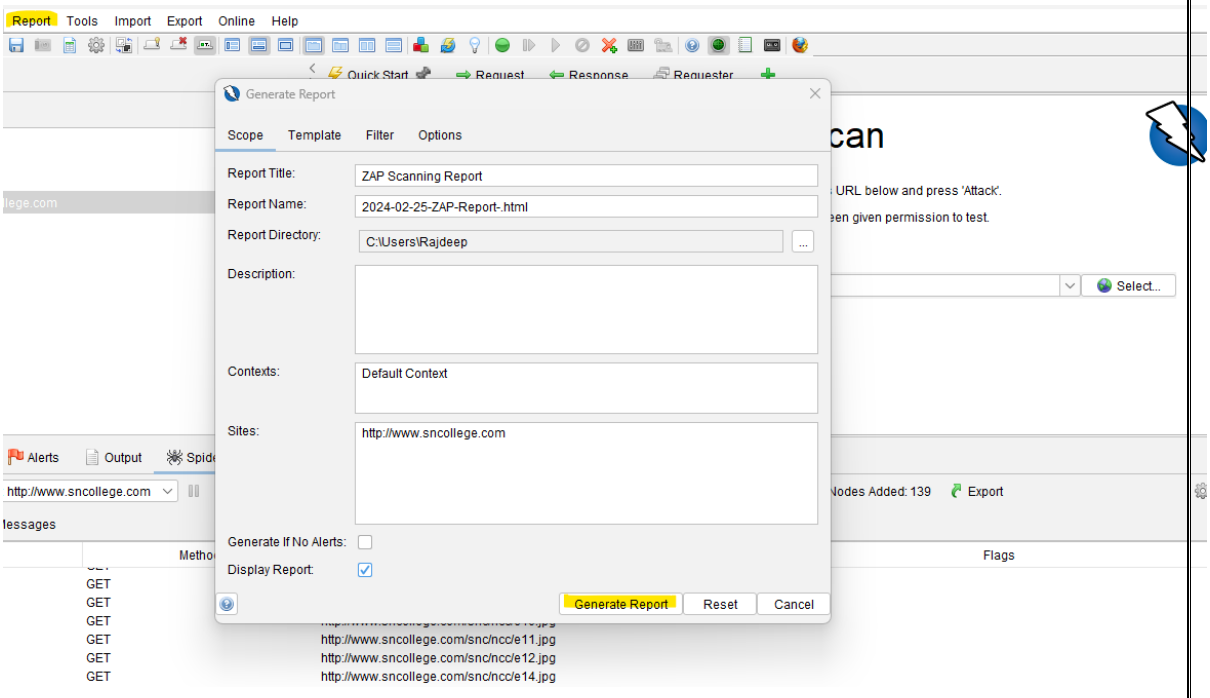
Section 3 B.

a. a. Perform Web App Scanning using OWASP Zed Proxy.

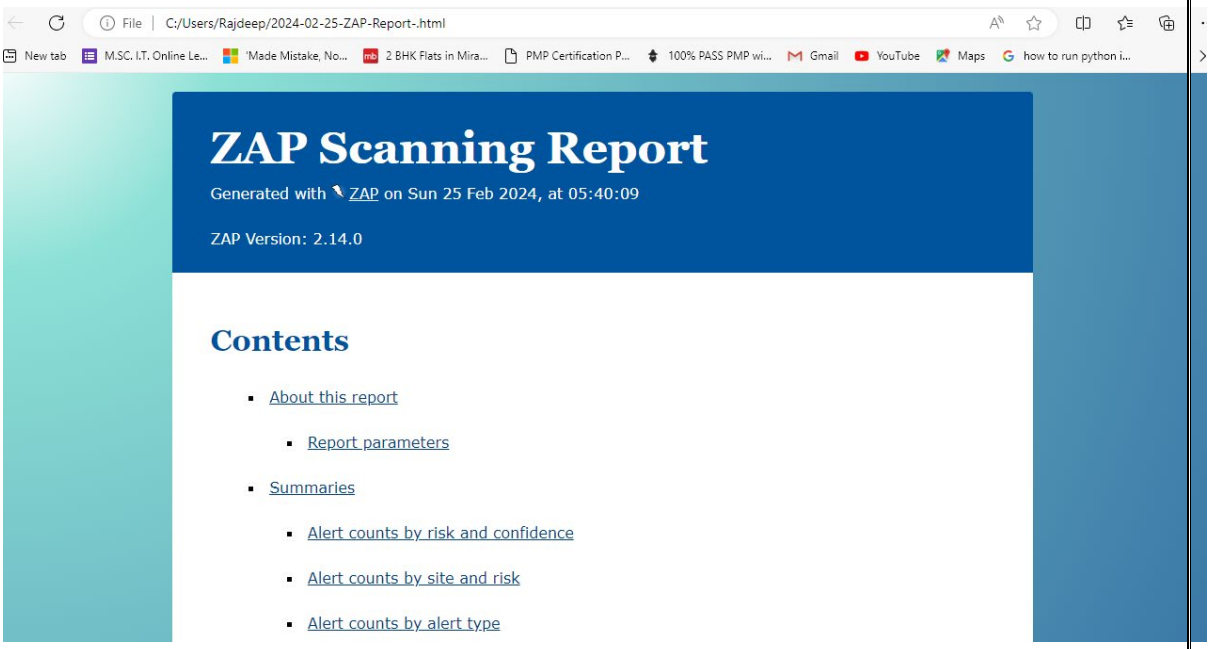
Step 1. Open Zed Proxy, click on quick start enter he URL and click on attack.



Step 2: go to report generate report, click on generate report:



Step 3: Output:



Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	1 (14.3%)
Content Security Policy (CSP) Header Not Set	Medium	127 (1,814.3%)
Missing Anti-clickjacking Header	Medium	122 (1,742.9%)
Cross-Domain JavaScript Source File Inclusion	Low	6 (85.7%)
X-Content-Type-Options Header Missing	Low	135 (1,928.6%)
Information Disclosure - Suspicious Comments	Informational	16 (228.6%)
Modern Web Application	Informational	127 (1,814.3%)
Total		7

Risk=Medium, Confidence=High (1)

http://www.sncollege.com (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET http://www.sncollege.com

Risk=Medium, Confidence=Medium (1)

http://www.sncollege.com (1)

Missing Anti-clickjacking Header (1)

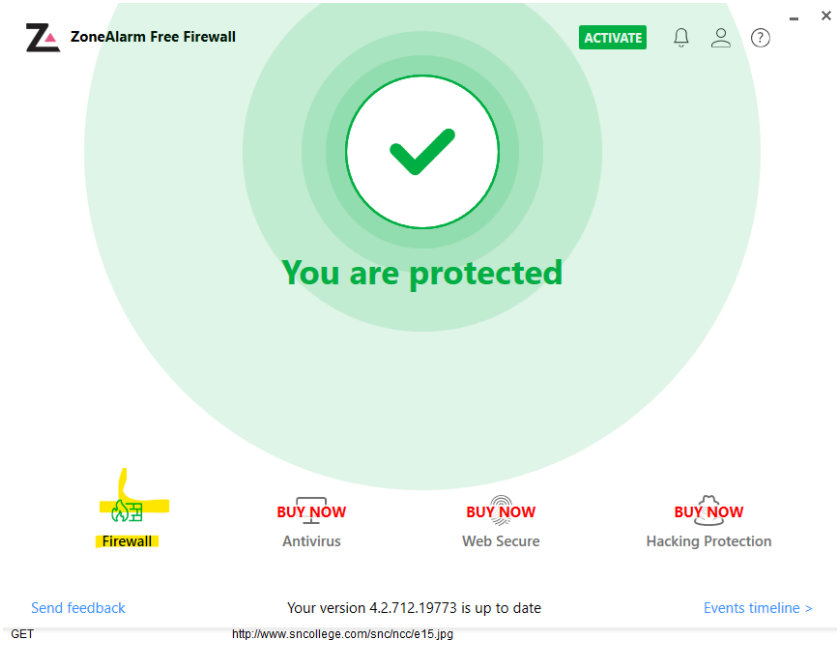
▶ GET http://www.sncollege.com

Risk=Medium, Confidence=Low (1)

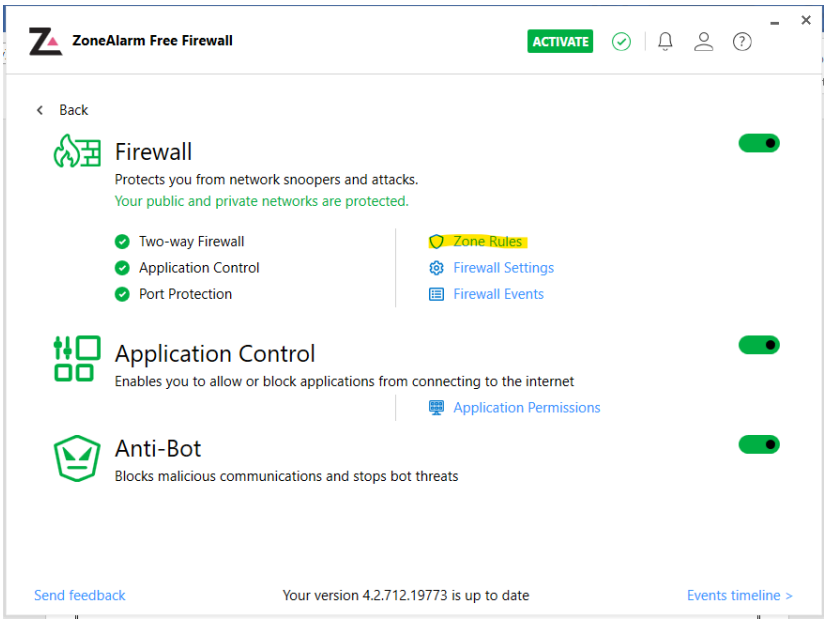
C: Demonstrate the use of the following firewalls

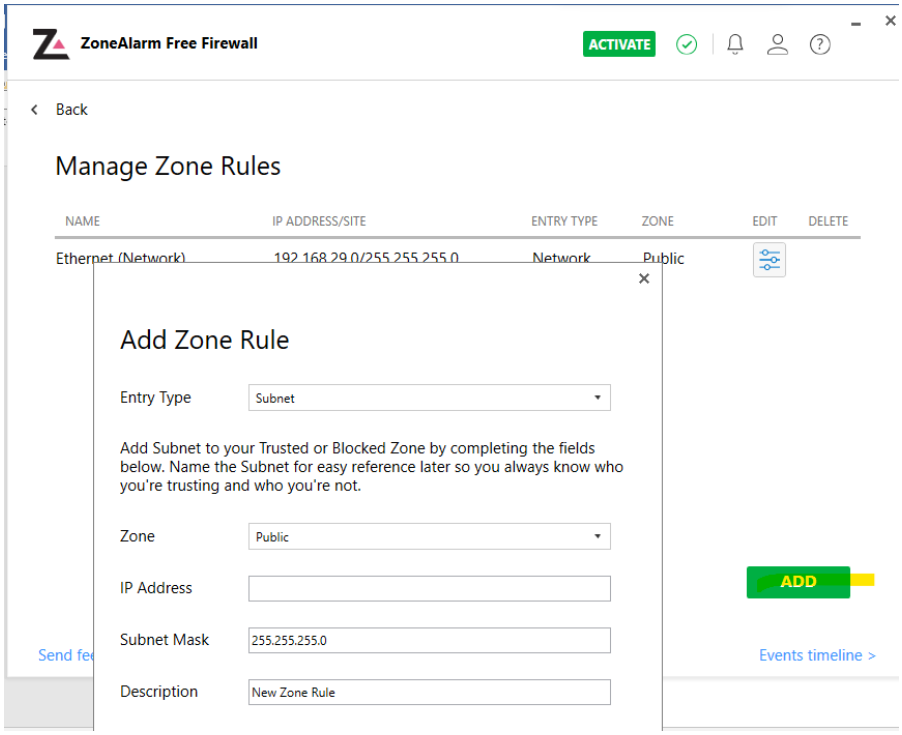
i. AIM: Zonealarm and analyse using Firewall Analyzer.

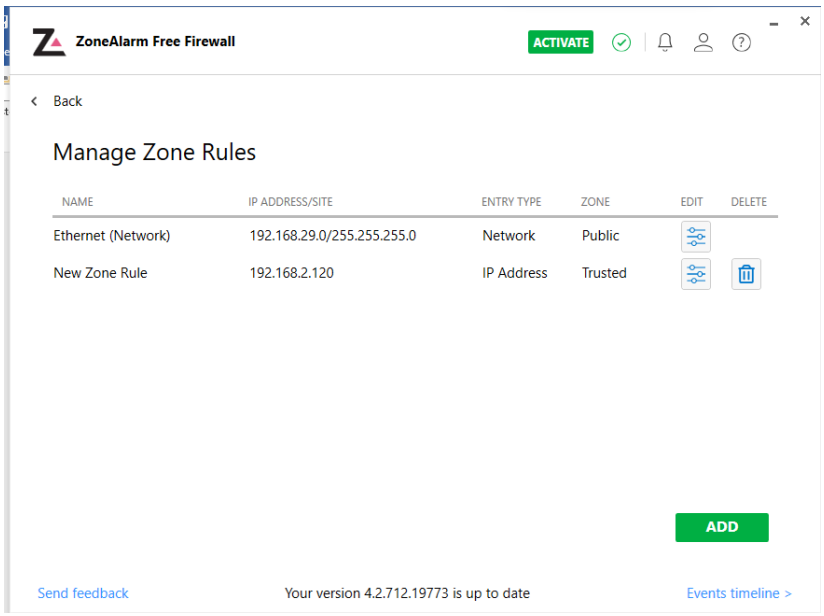
Step1: Open zone alarm, click on firewall:



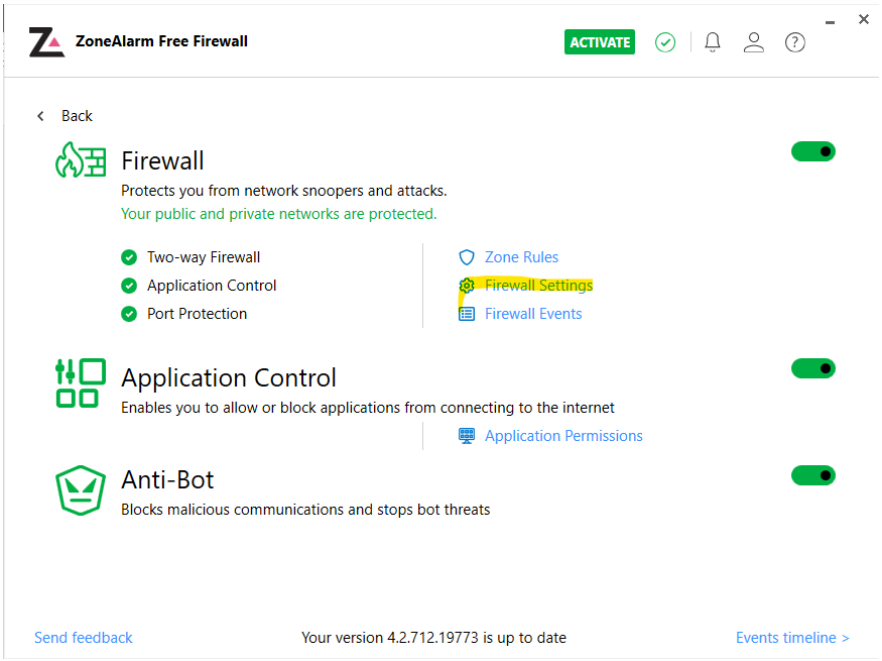
Step 2: Select Zone Rule: You can add/update new rule:

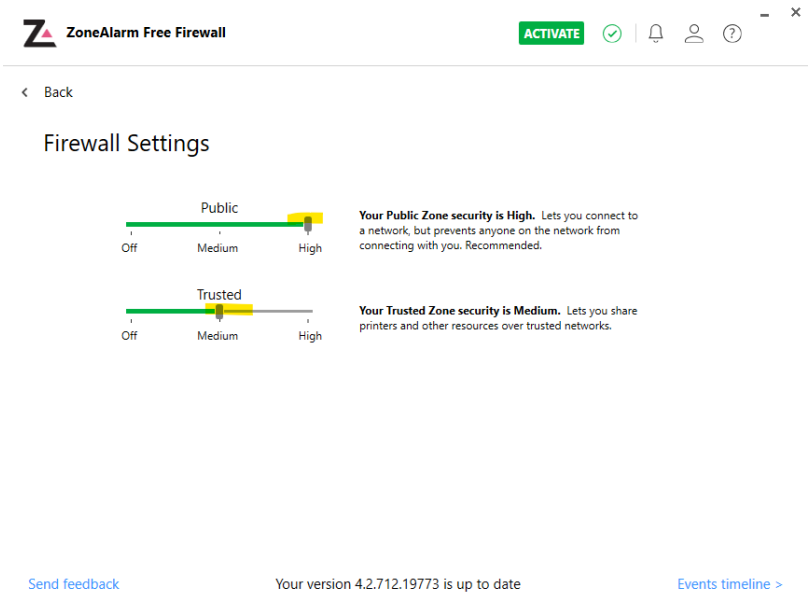






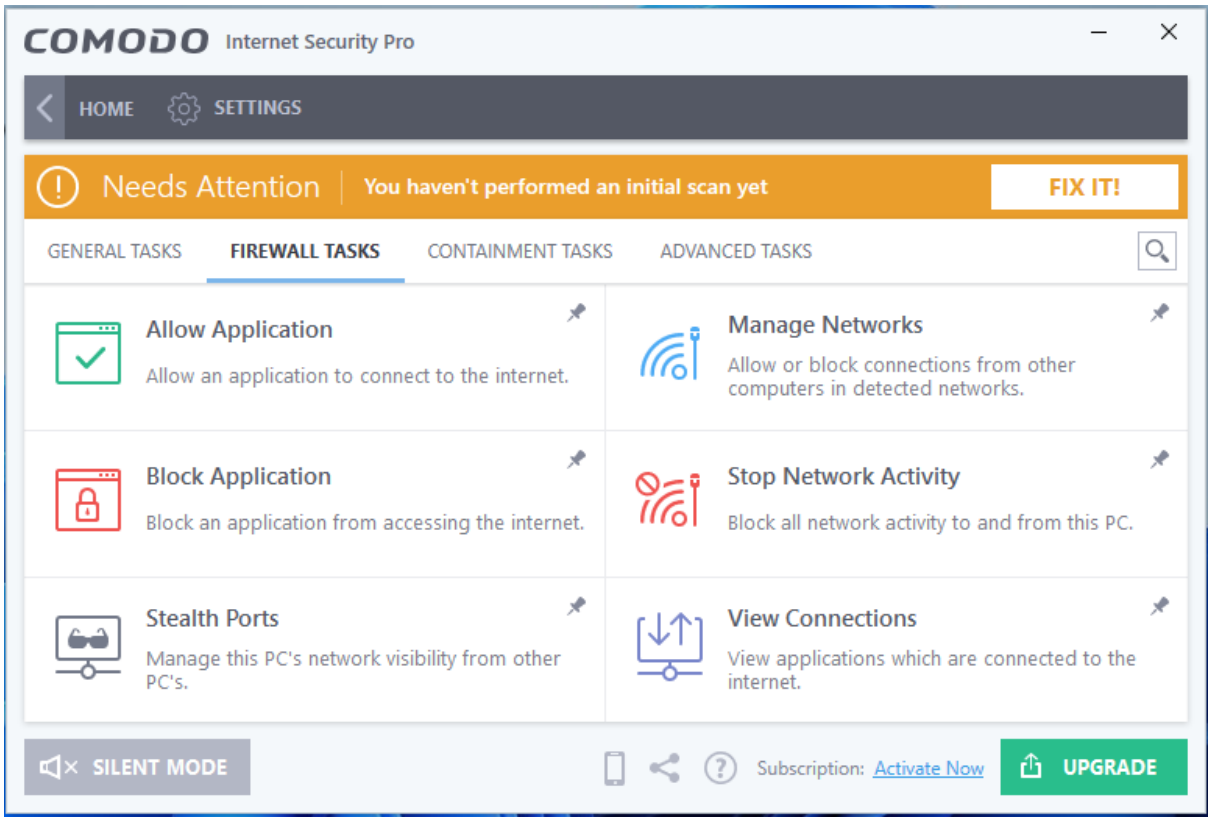
Step 3: You can select Firewall setting:


ZoneAlarm Free Firewall
ACTIVATE
Back
Firewall
Protects you from network snoopers and attacks.
Your public and private networks are protected.
Two-way Firewall
Application Control
Port Protection
Zone Rules
Firewall Settings
Firewall Events
Application Control
Enables you to allow or block applications from connecting to the internet
Application Permissions
Anti-Bot
Blocks malicious communications and stops bot threats
Send feedback
Your version 4.2.712.19773 is up to date
Events timeline >


ZoneAlarm Free Firewall
ACTIVATE
Back
Firewall Settings
Public
Off
Medium
High
Your Public Zone security is High. Lets you connect to a network, but prevents anyone on the network from connecting with you. Recommended.
Trusted
Off
Medium
High
Your Trusted Zone security is Medium. Lets you share printers and other resources over trusted networks.
Send feedback
Your version 4.2.712.19773 is up to date
Events timeline >

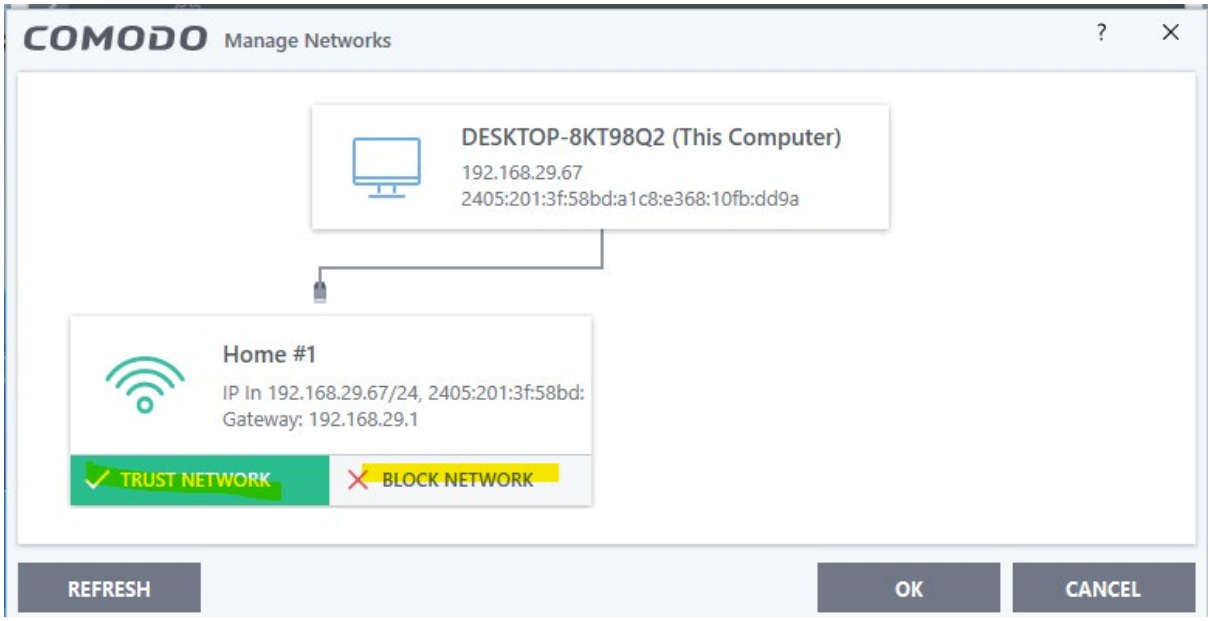
II Comodo Firewall:

Step 1: Open comodo-> go to firewall.

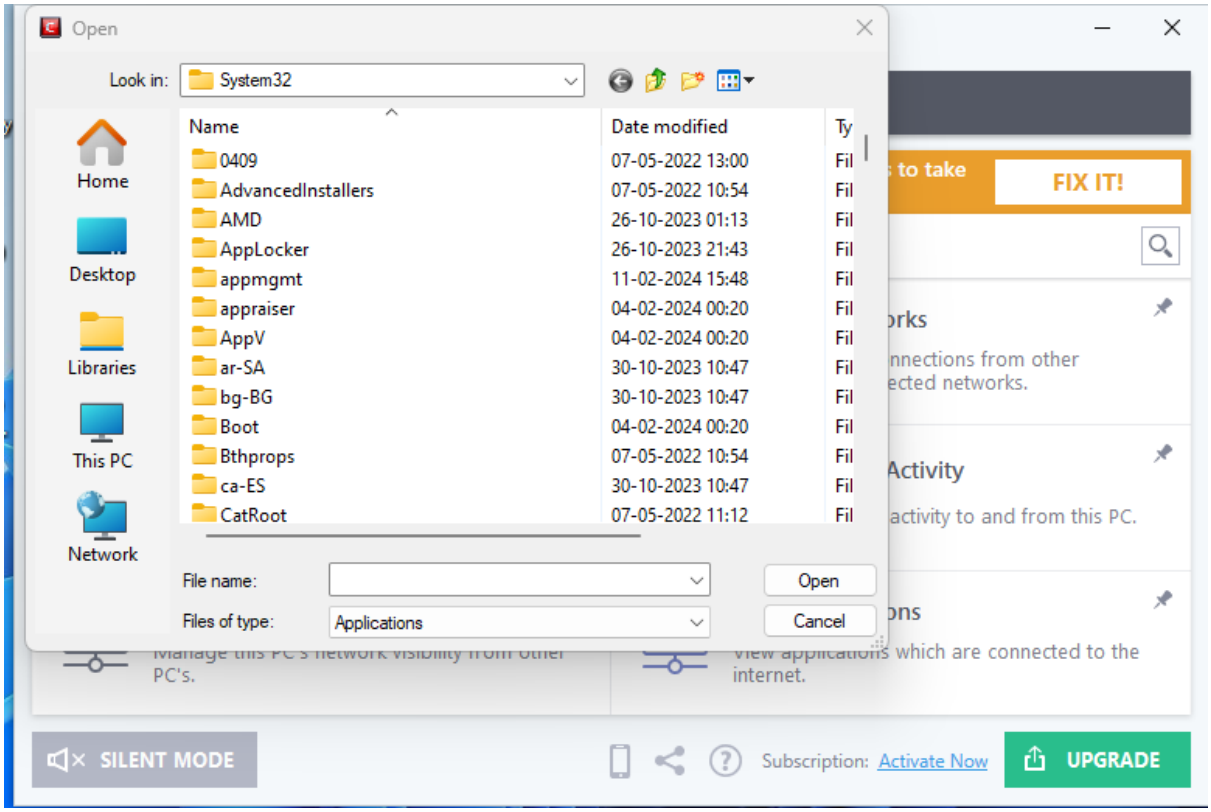


Step 2 : You can select and perform different Network activity like

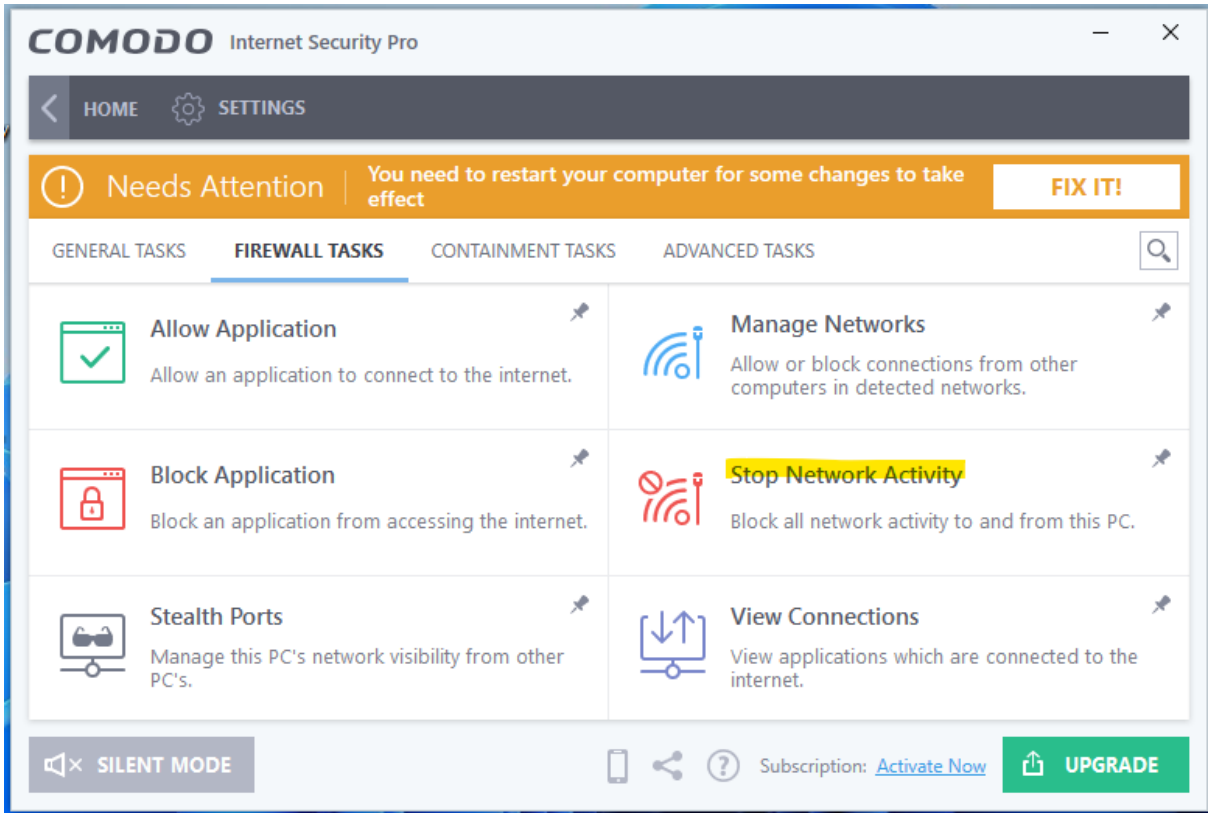
a. Manage network: Like trust or block any network:



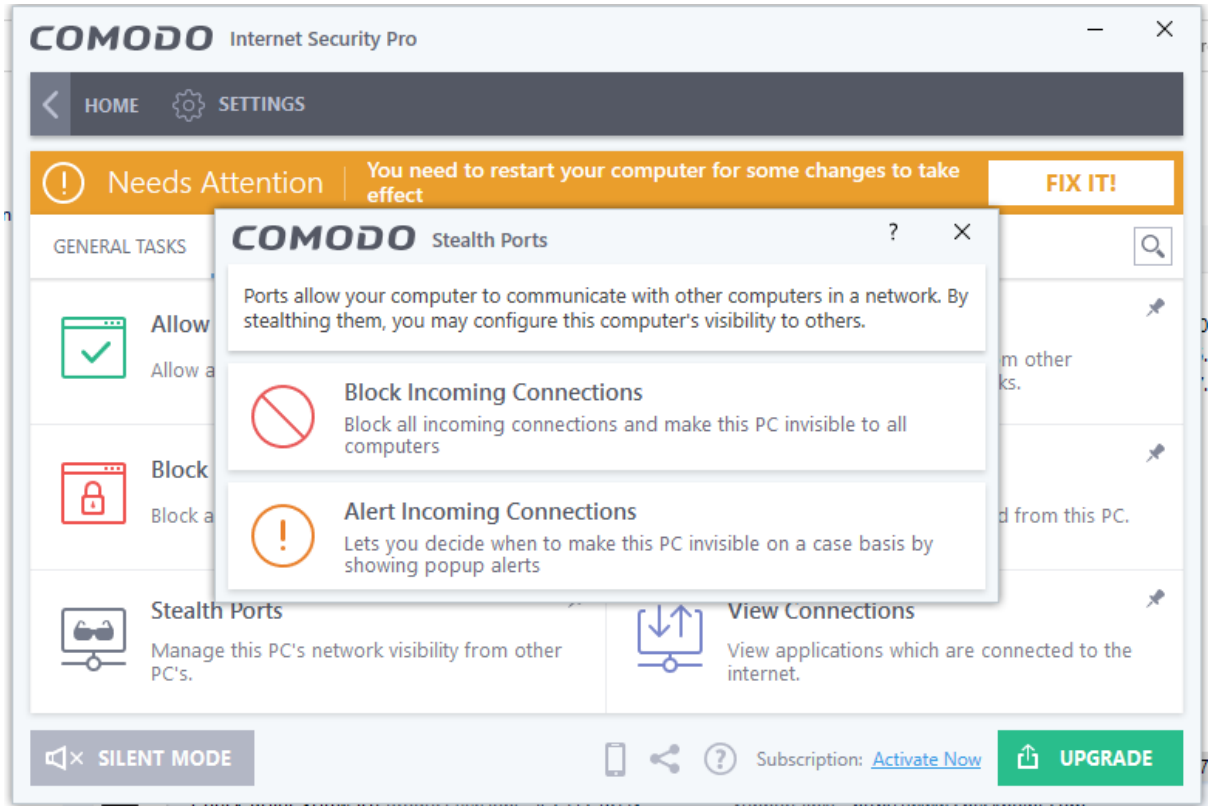
B. allow or block any application by selecting application path:



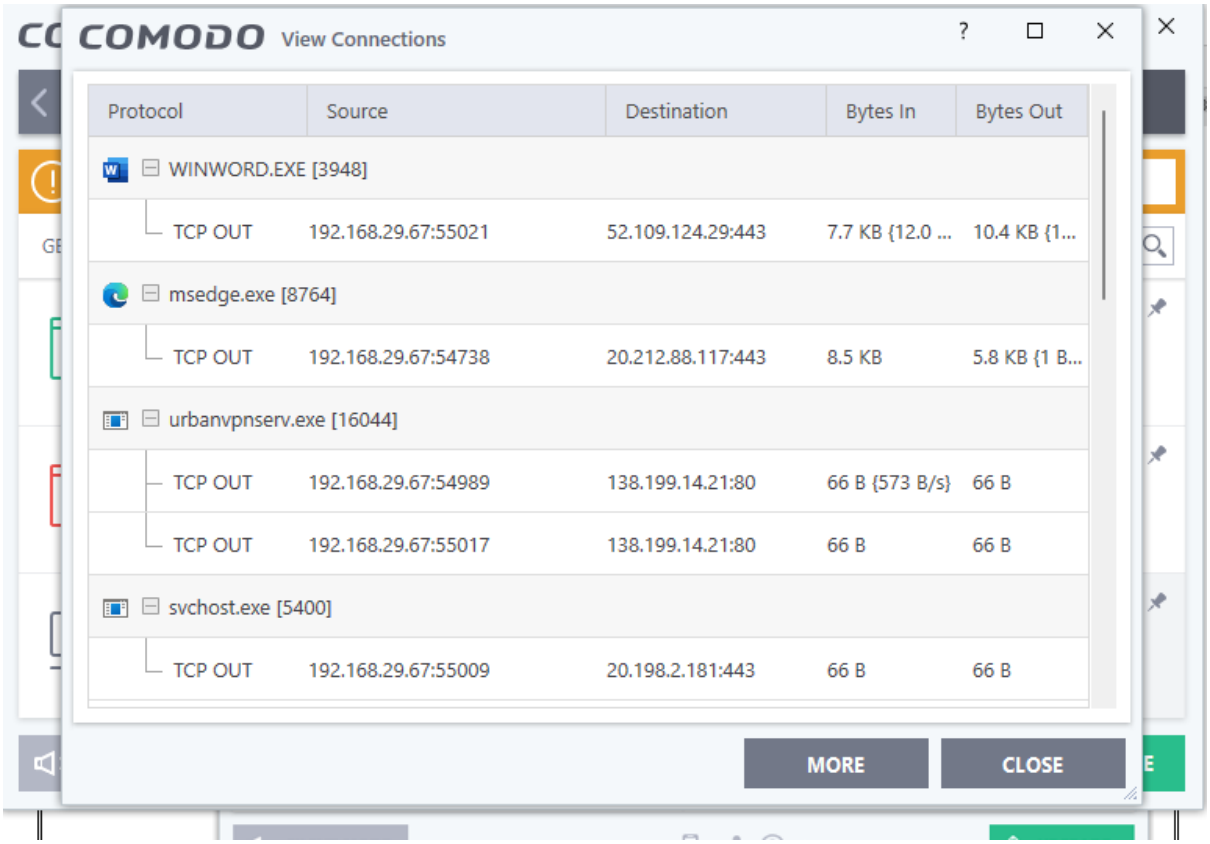
c. Allow or block network traffic in our machine:



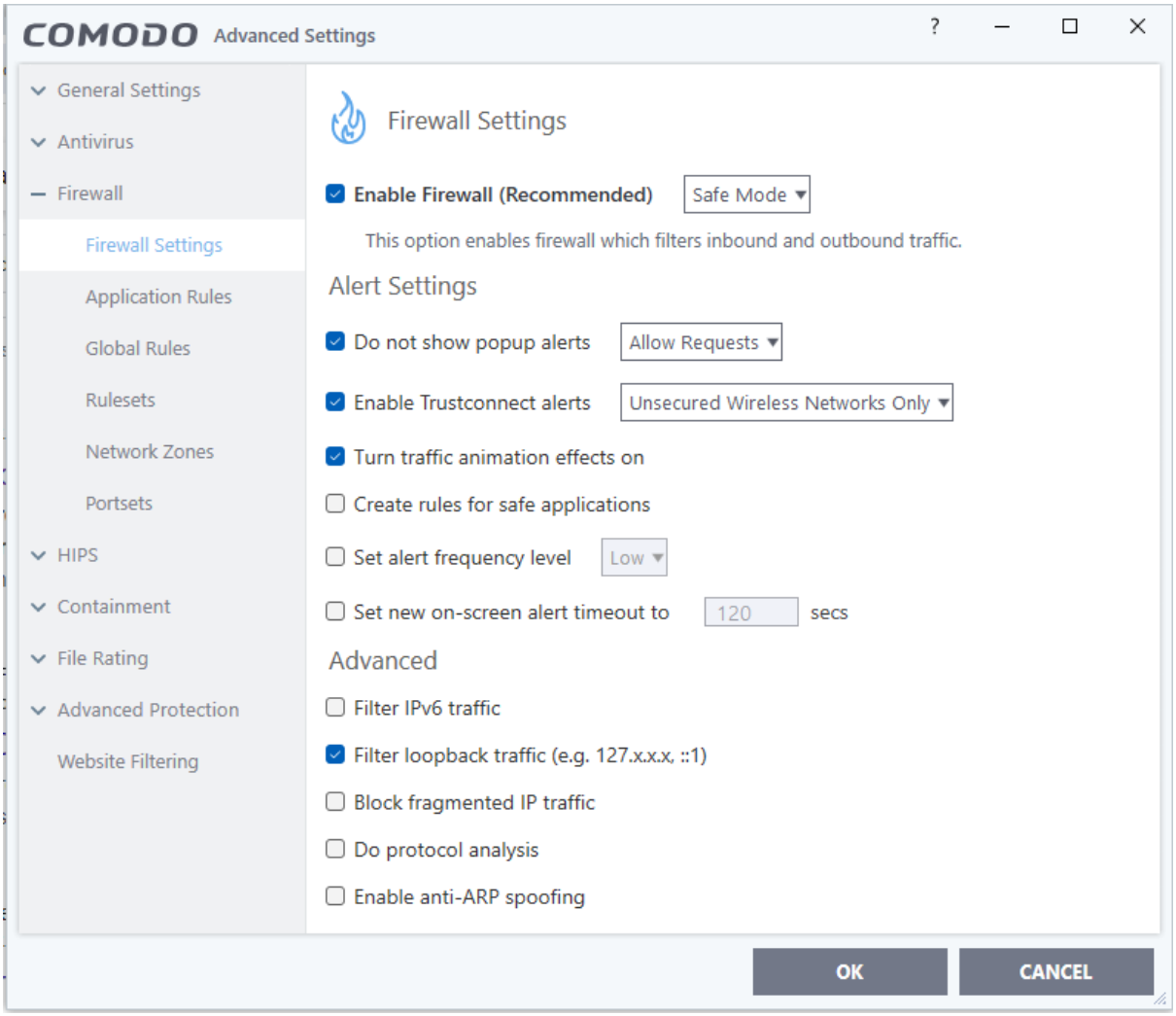
d. Sealth mode: allow or block on incoming network:

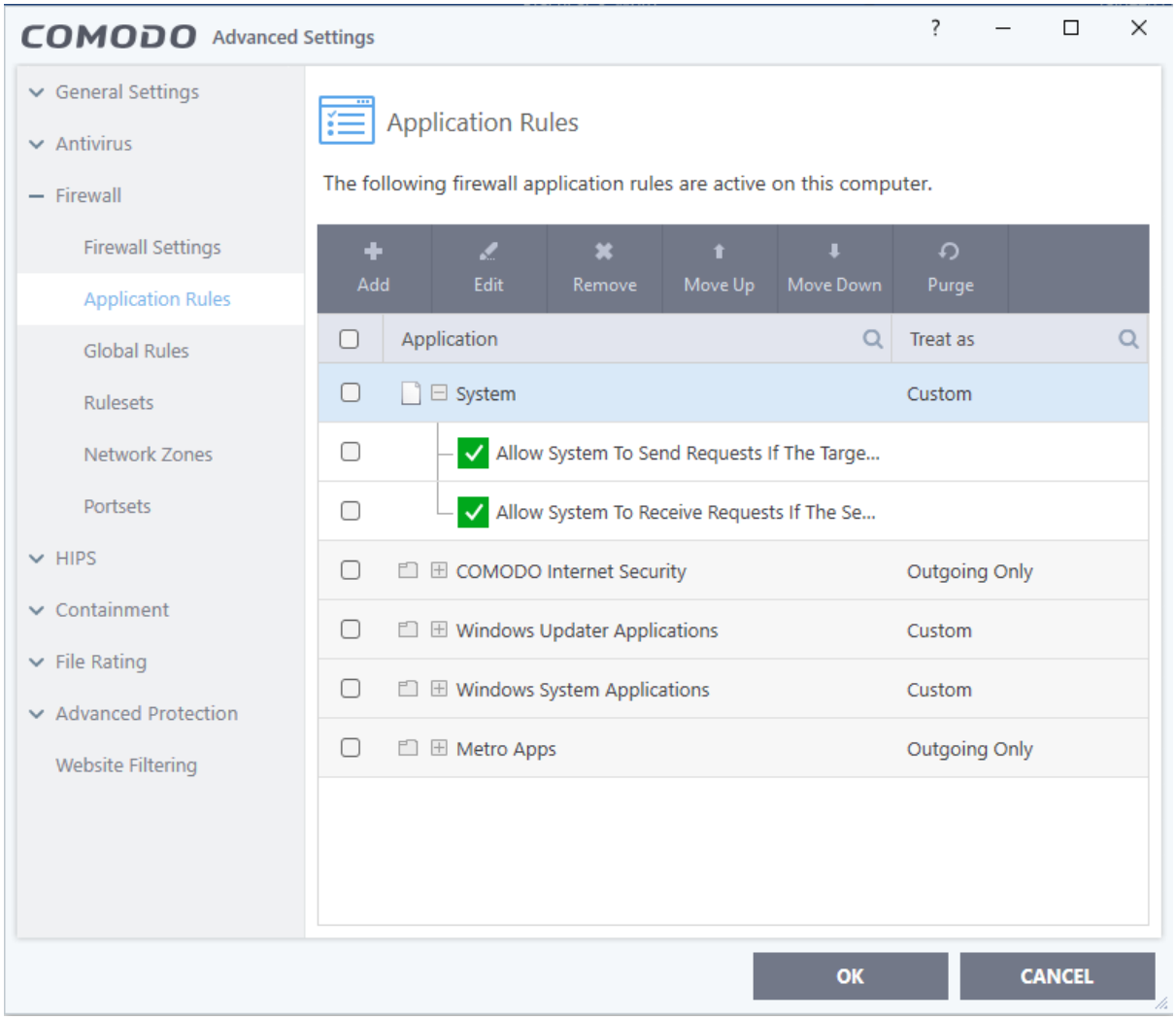


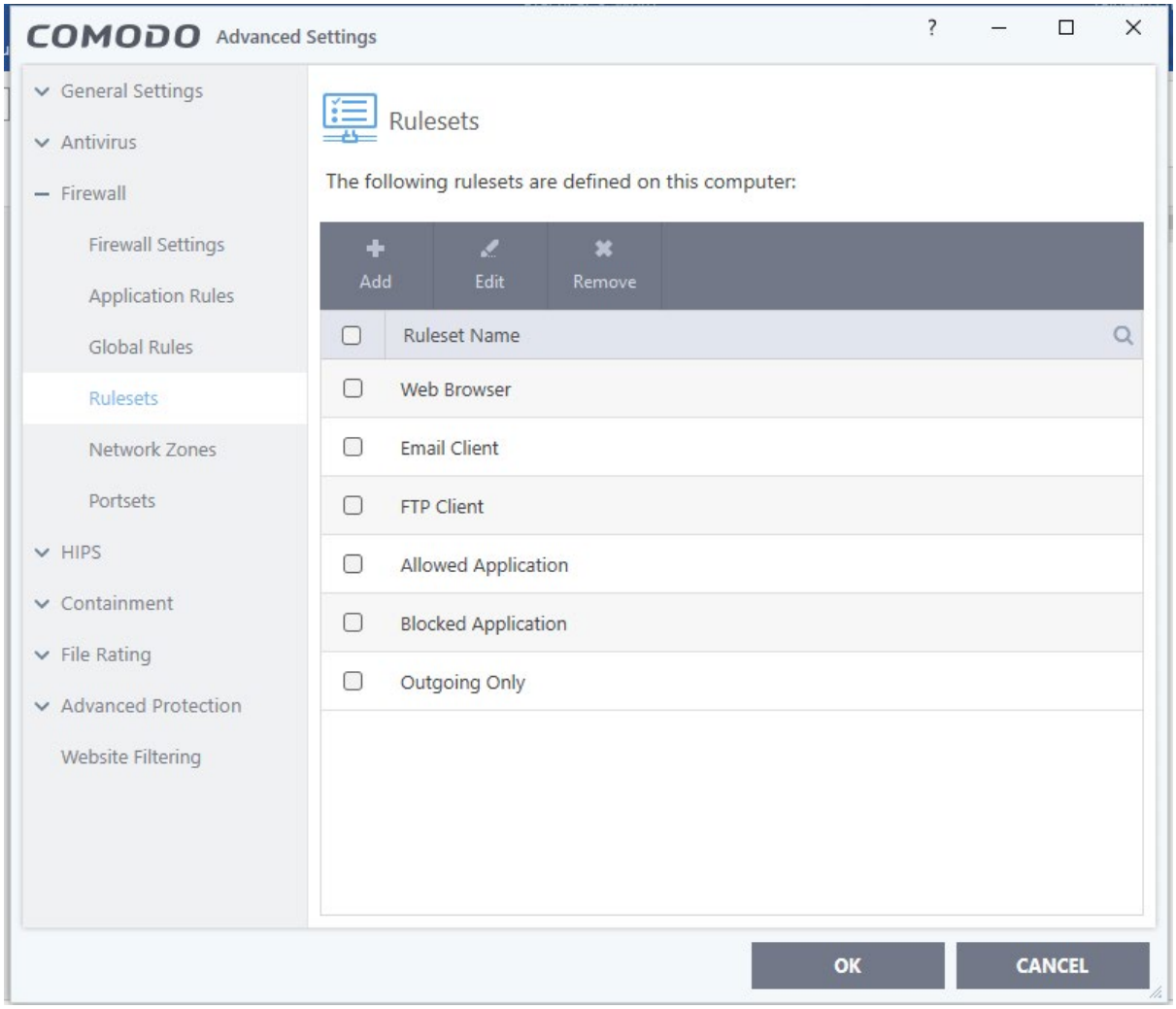
e. View Connection: View all the connection in the network:

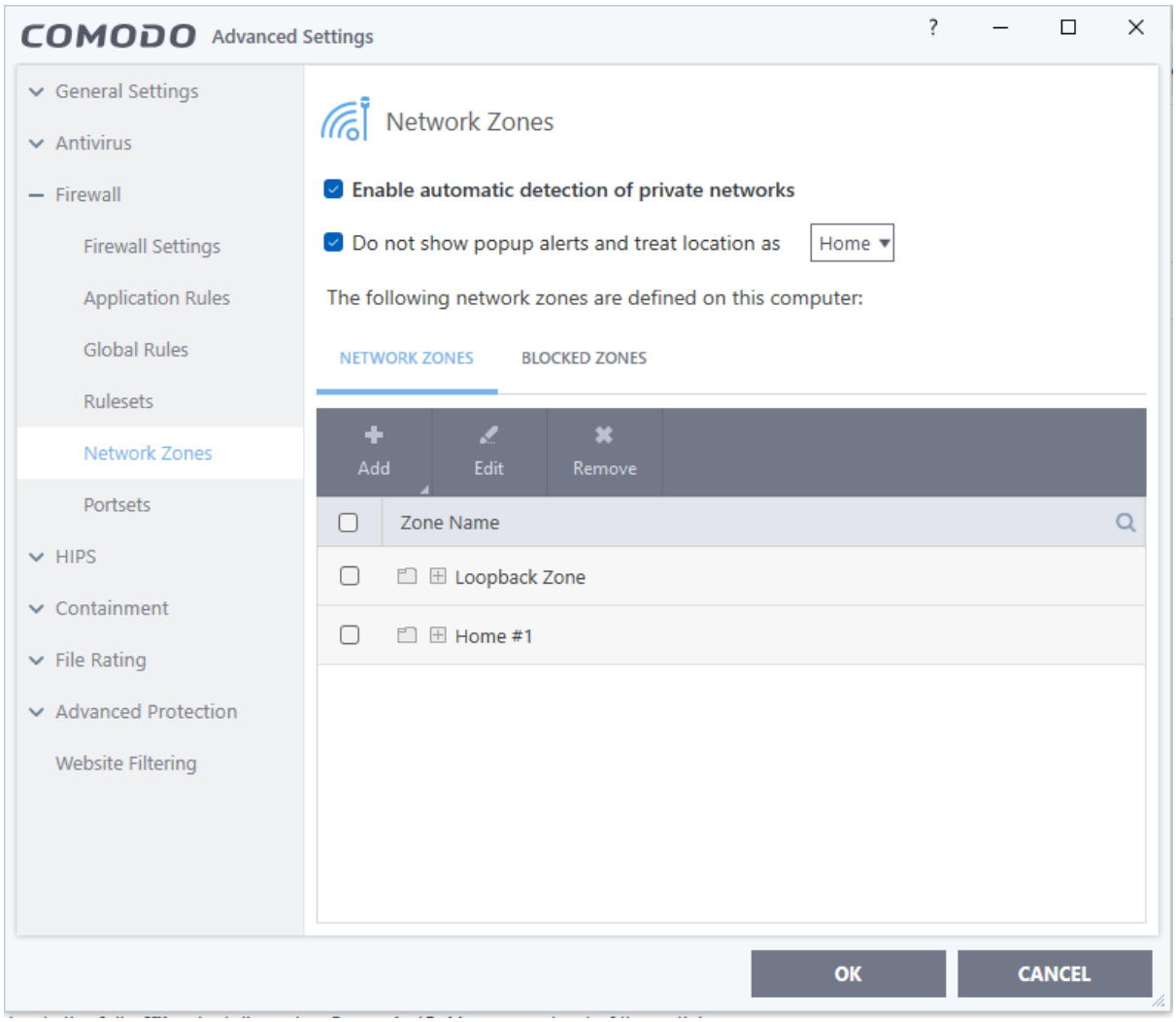


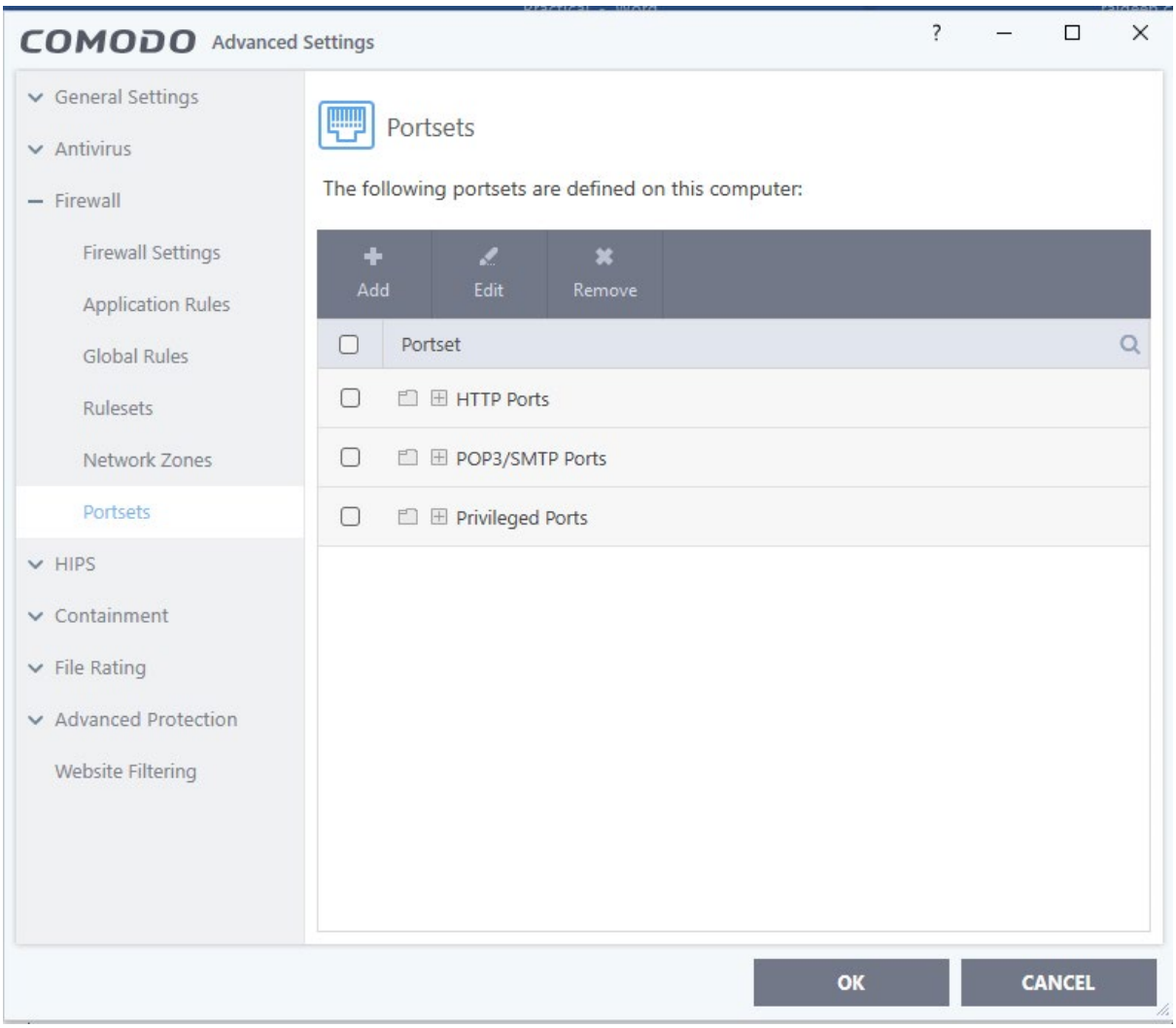
Step 3: Go to firewall setting:


COMODO Advanced Settings
General Settings
Antivirus
Firewall
Firewall Settings
Application Rules
Global Rules
Rulesets
Network Zones
Portsets
HIPS
Containment
File Rating
Advanced Protection
Website Filtering
Firewall Settings
Enable Firewall (Recommended)
Safe Mode
This option enables firewall which filters inbound and outbound traffic.
Alert Settings
Do not show popup alerts
Allow Requests
Enable Trustconnect alerts
Unsecured Wireless Networks Only
Turn traffic animation effects on
Create rules for safe applications
Set alert frequency level
Low
Set new on-screen alert timeout to
120
secs
Advanced
Filter IPv6 traffic
Filter loopback traffic (e.g. 127.x.x.x, ::1)
Block fragmented IP traffic
Do protocol analysis
Enable anti-ARP spoofing
OK
CANCEL


COMODO Advanced Settings
General Settings
Antivirus
Firewall
Firewall Settings
Application Rules
Global Rules
Rulesets
Network Zones
Portsets
HIPS
Containment
File Rating
Advanced Protection
Website Filtering
Application Rules
The following firewall application rules are active on this computer.
Add
Edit
Remove
Move Up
Move Down
Purge
Application
Treat as
System
Custom
Allow System To Send Requests If The Targe...
Allow System To Receive Requests If The Se...
COMODO Internet Security
Outgoing Only
Windows Updater Applications
Custom
Windows System Applications
Custom
Metro Apps
Outgoing Only
OK
CANCEL

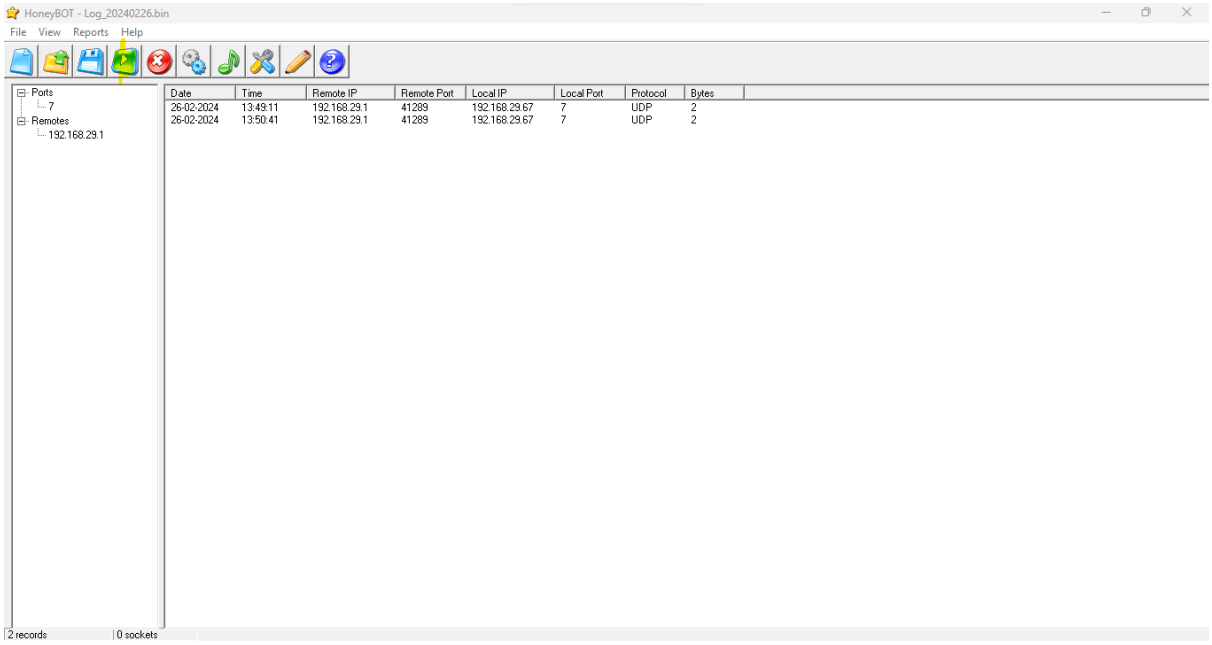

COMODO Advanced Settings
General Settings
Antivirus
Firewall
Firewall Settings
Application Rules
Global Rules
Rulesets
Network Zones
Portsets
HIPS
Containment
File Rating
Advanced Protection
Website Filtering
Rulesets
The following rulesets are defined on this computer:
Add
Edit
Remove
Ruleset Name
Web Browser
Email Client
FTP Client
Allowed Application
Blocked Application
Outgoing Only
OK
CANCEL


COMODO Advanced Settings
General Settings
Antivirus
Firewall
Firewall Settings
Application Rules
Global Rules
Rulesets
Network Zones
Portsets
HIPS
Containment
File Rating
Advanced Protection
Website Filtering
Network Zones
Enable automatic detection of private networks
Do not show popup alerts and treat location as
Home
The following network zones are defined on this computer:
NETWORK ZONES
BLOCKED ZONES
Add
Edit
Remove
Zone Name
Loopback Zone
Home #1
OK
CANCEL

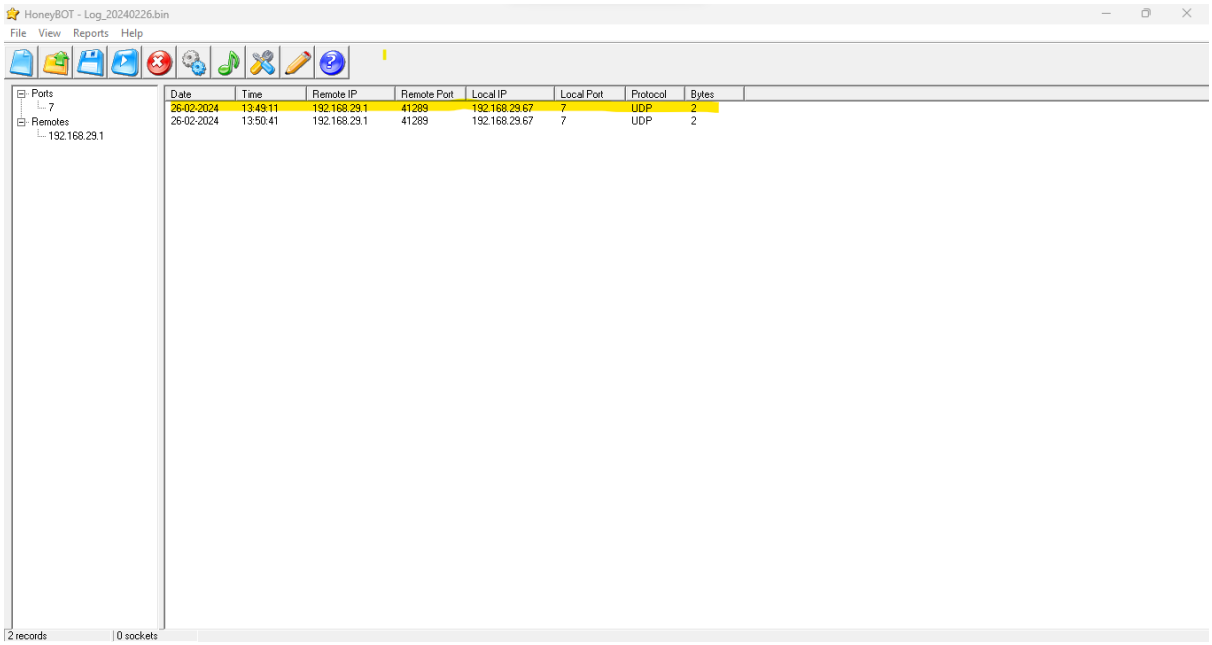

COMODO Advanced Settings
General Settings
Antivirus
Firewall
Firewall Settings
Application Rules
Global Rules
Rulesets
Network Zones
Portsets
HIPS
Containment
File Rating
Advanced Protection
Website Filtering
Portsets
The following portsets are defined on this computer:
Add
Edit
Remove
Portset
HTTP Ports
POP3/SMTP Ports
Privileged Ports
OK
CANCEL

d. Aim: Use HoneyBOT to capture malicious network traffic.

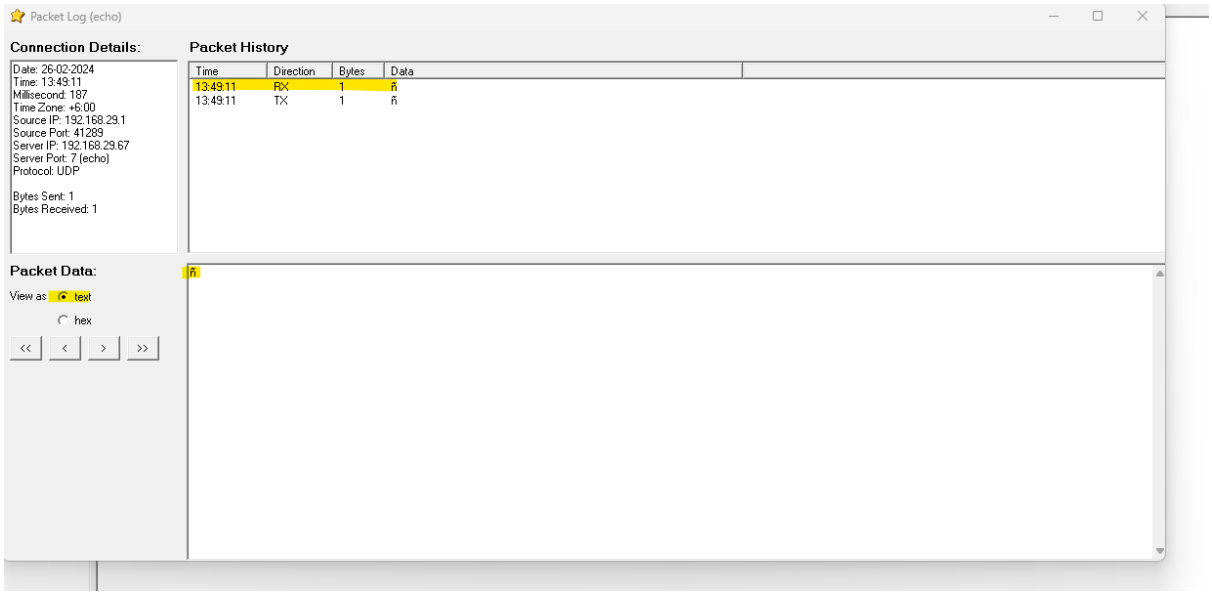
1. Open HoneyBot click on start icon.



Step 2 :Double click on any one of the ip list:



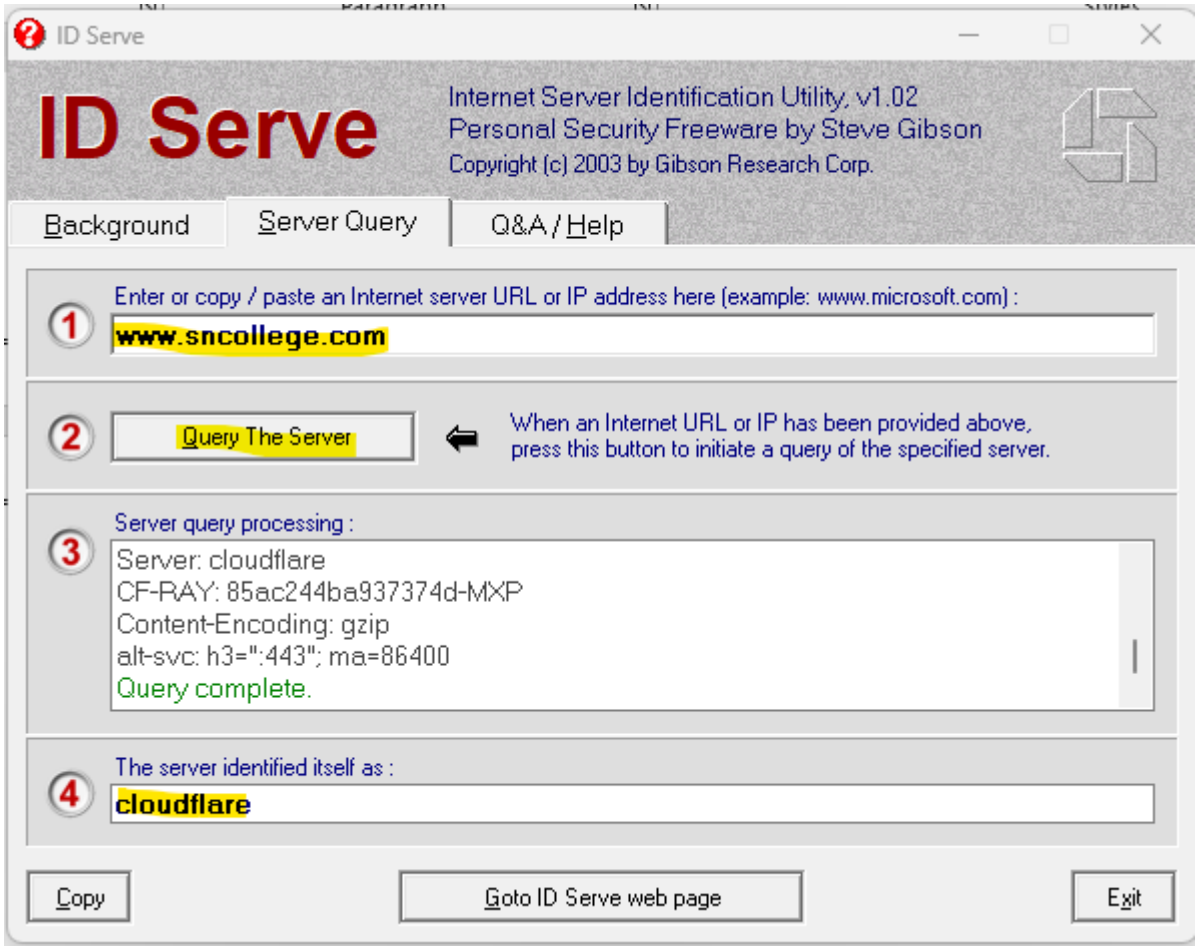
Step 3: Select any of the packet , then select from the option of text or hex format to see the output.


Packet Log (echo)
Connection Details:
Date: 26-02-2024
Time: 13:49:11
Millisecond: 187
Time Zone: +6:00
Source IP: 192.168.29.1
Source Port: 41289
Server IP: 192.168.29.67
Server Port: 7 (echo)
Protocol: UDP
Bytes Sent: 1
Bytes Received: 1
Packet History
Time
Direction
Bytes
Data
13:49:11
RX
1
ñ
13:49:11
TX
1
ñ
Packet Data:
View as:
text
hex
<<
<
>
>>
ñ

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

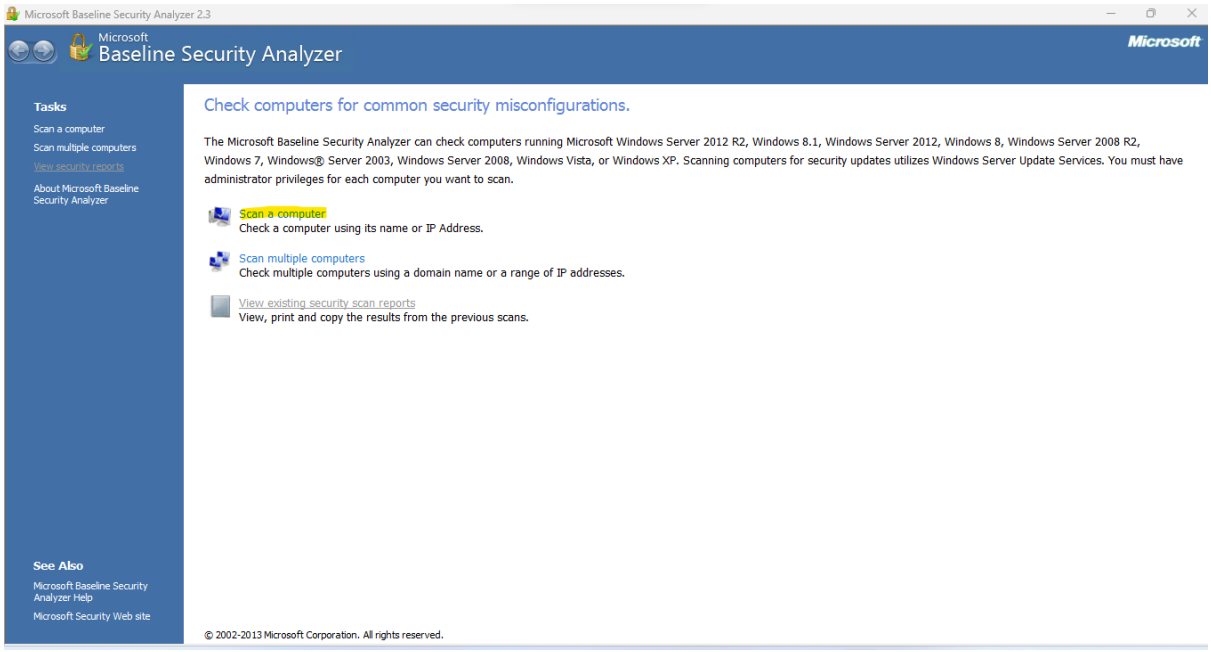
1. ID Server

Step 1. Open ID server. Click on "**Query the Server**" button and you will get the server details.

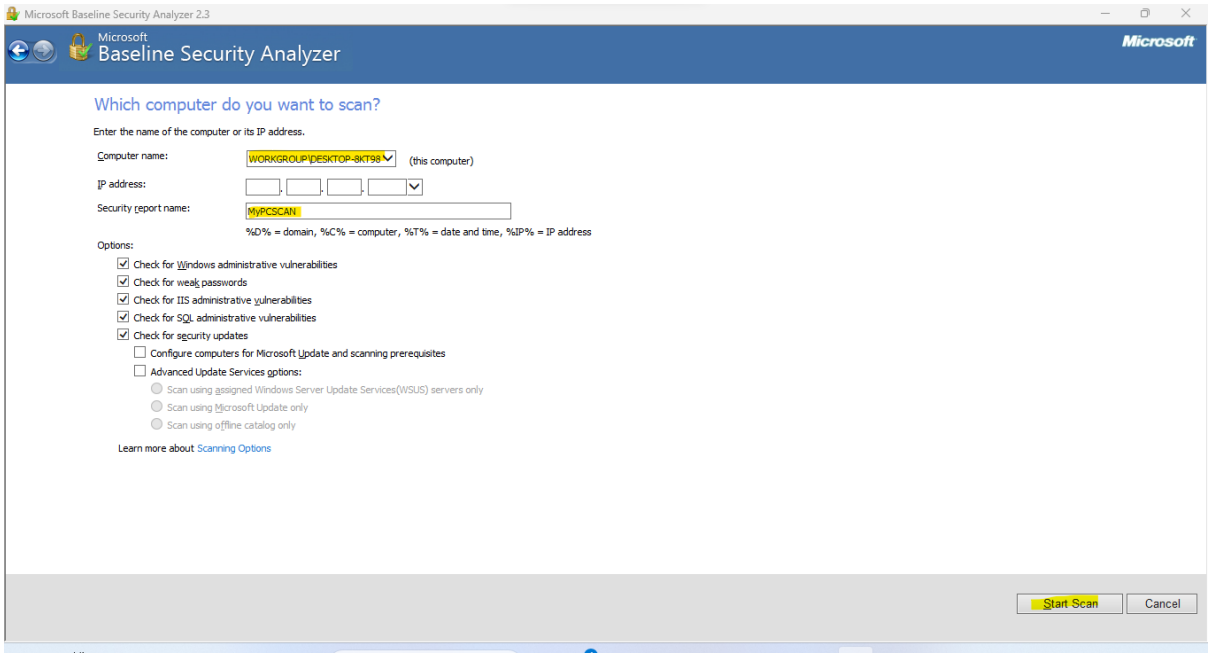


ii. **Aim:** Microsoft Baseline Security Analyzer

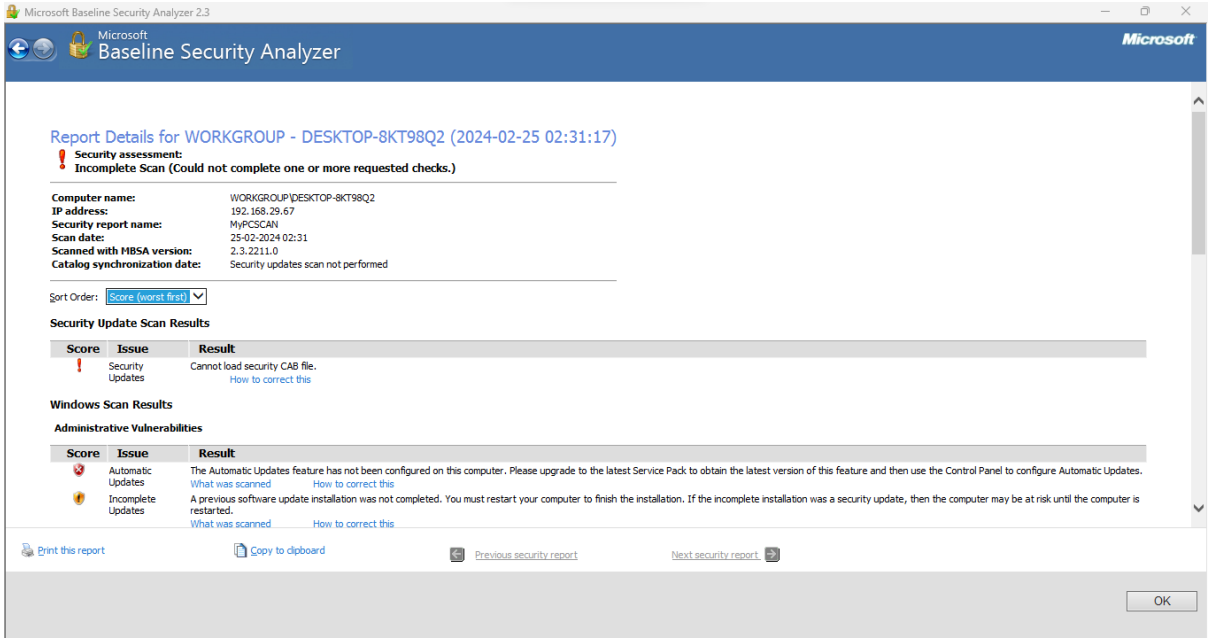
Step 1. Open Microsoft Baseline Security application and click on scan a computer:



Step 2: Scan the computer or any computer in the network by providing IP, and giving report name. then click on start scan button:

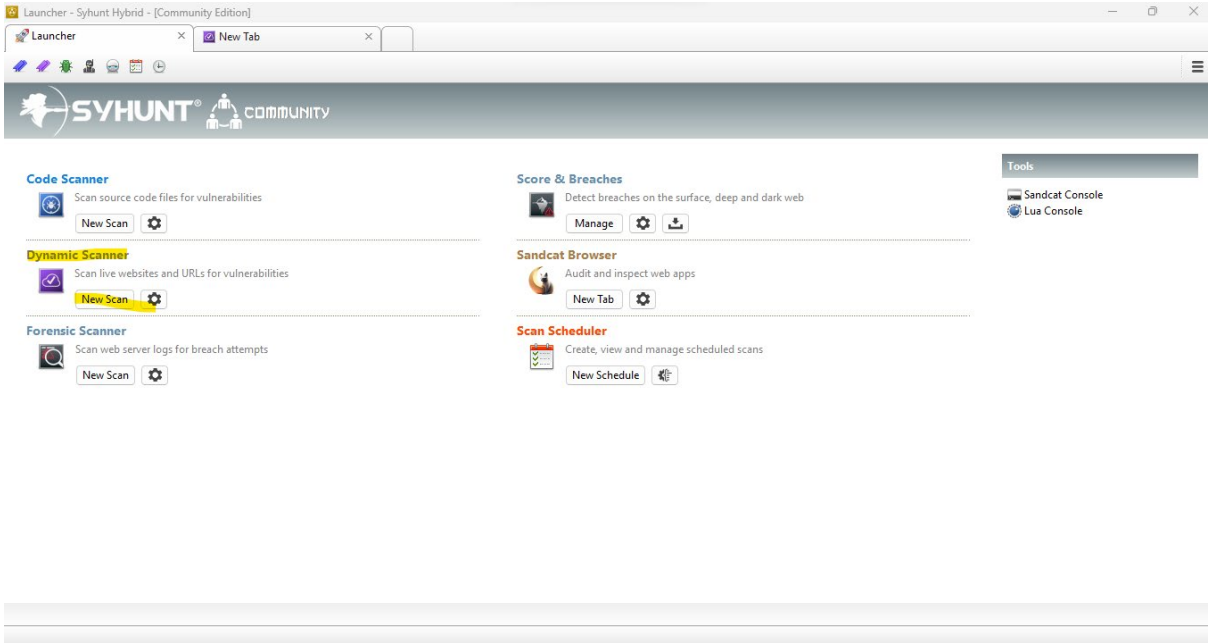


Output: You will get Report for the Scan:

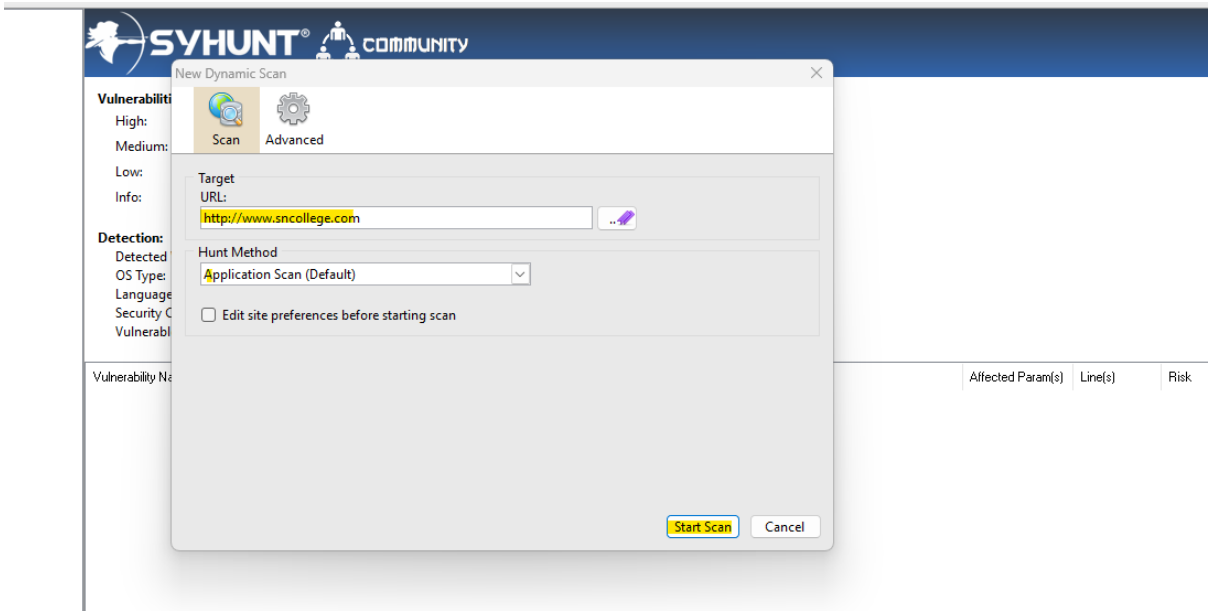


III. Syhunt Hybri

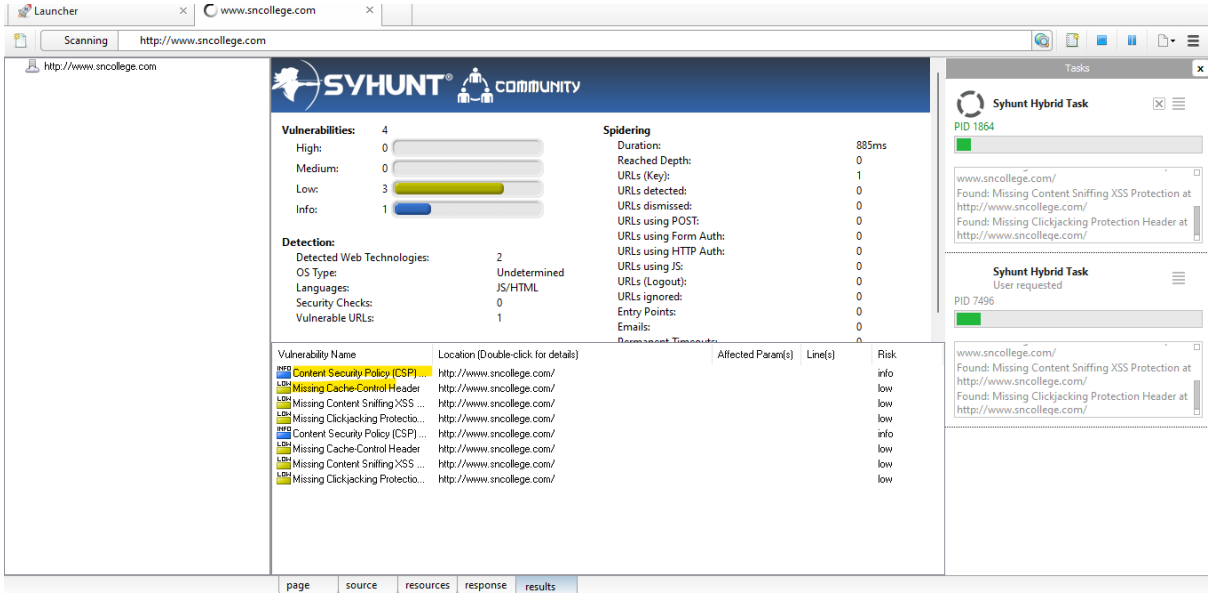
Step 1: Open Syhunt hunt Appliation -> go to Dynamic Scanner,



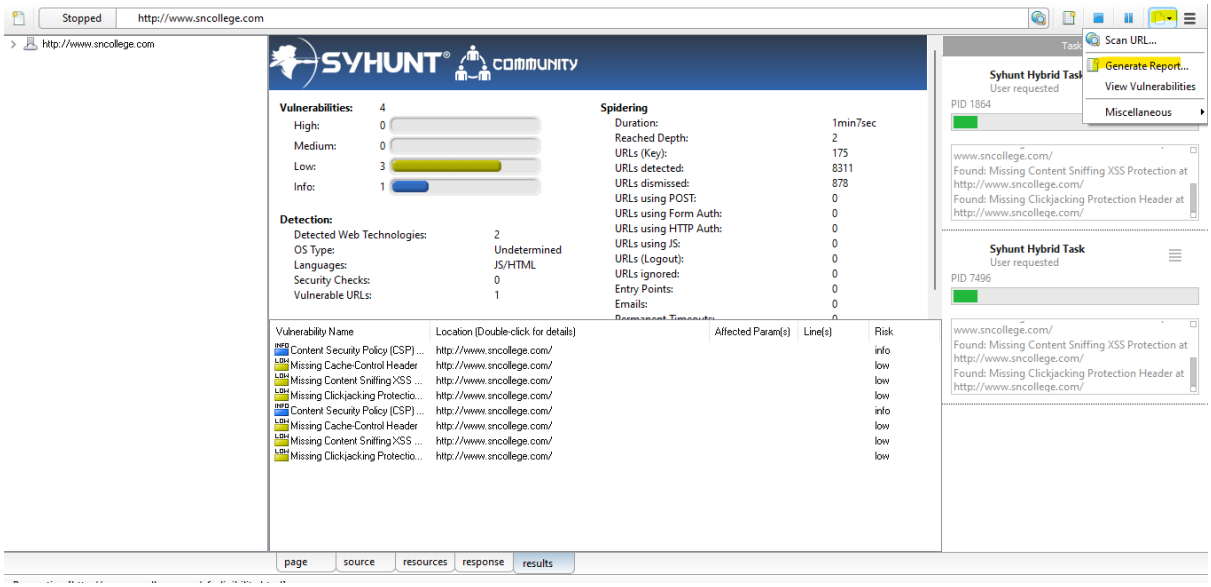
Step 2: Insert URL you need to scan and click on “Start” button:



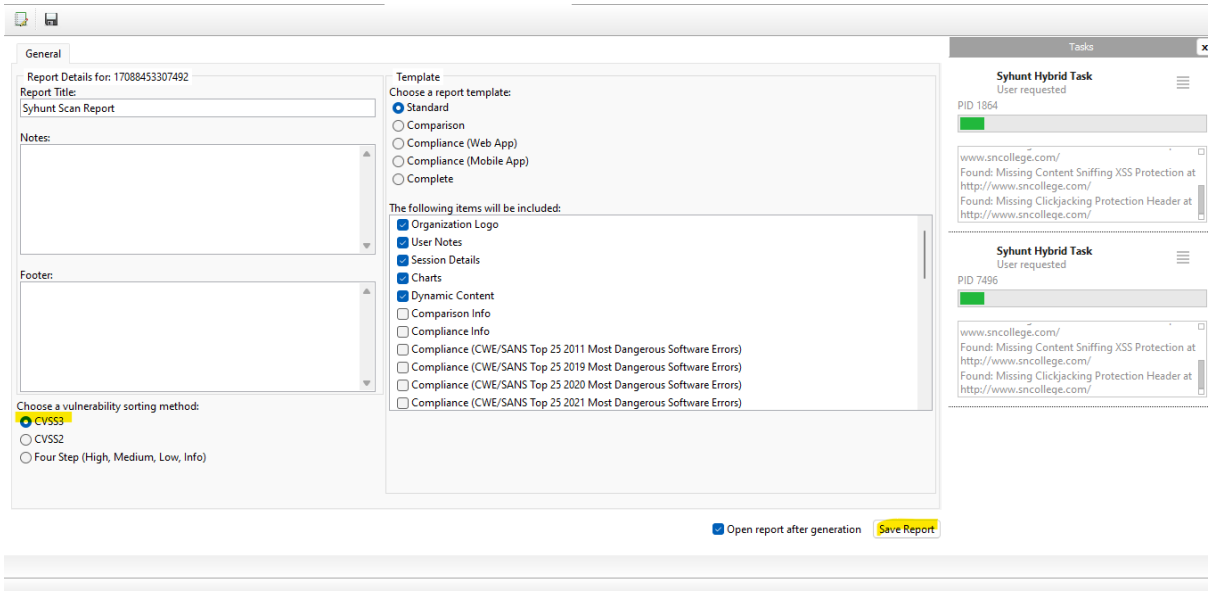
Step 3: Scanning in progress can be seen:



Step 4: Generate report by clicking on “generate Report” button:



Step 5: Select the format or repot and click on Save:



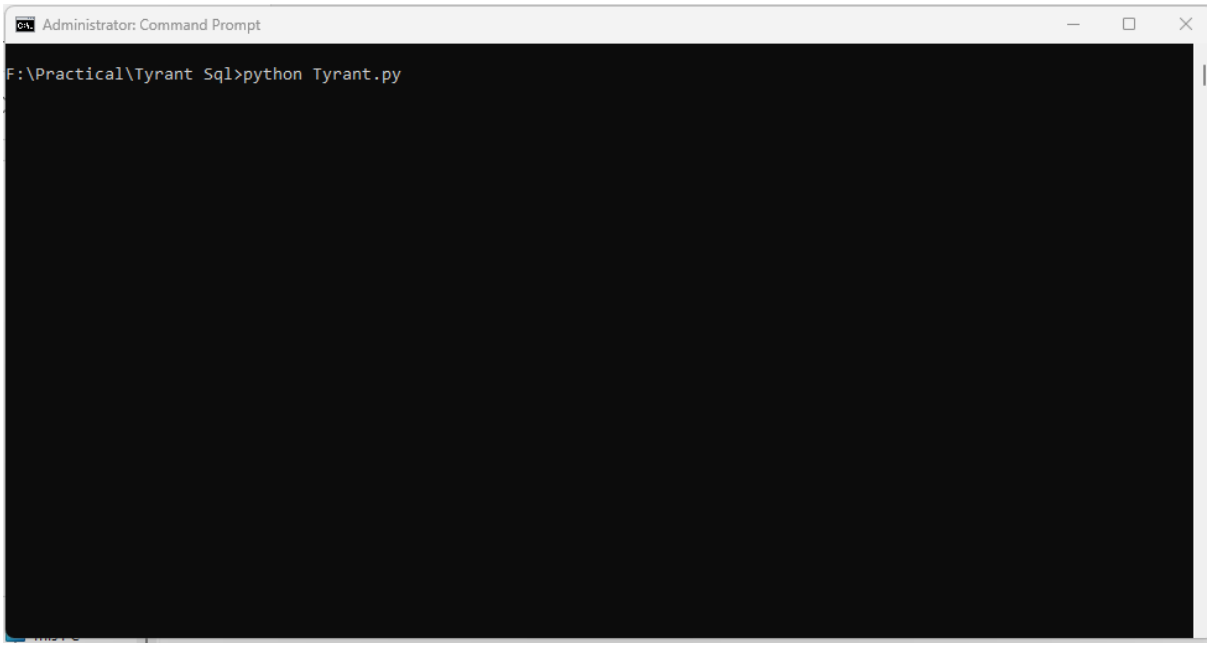
Section 3 B

a. Tyrant SQL
   Tyrant SQL is a Havij based cross-platform. It's Sqlmap's gui version.
   Follow the below process to run the Tyrant SQL :
   Step 1. Install below software and package:

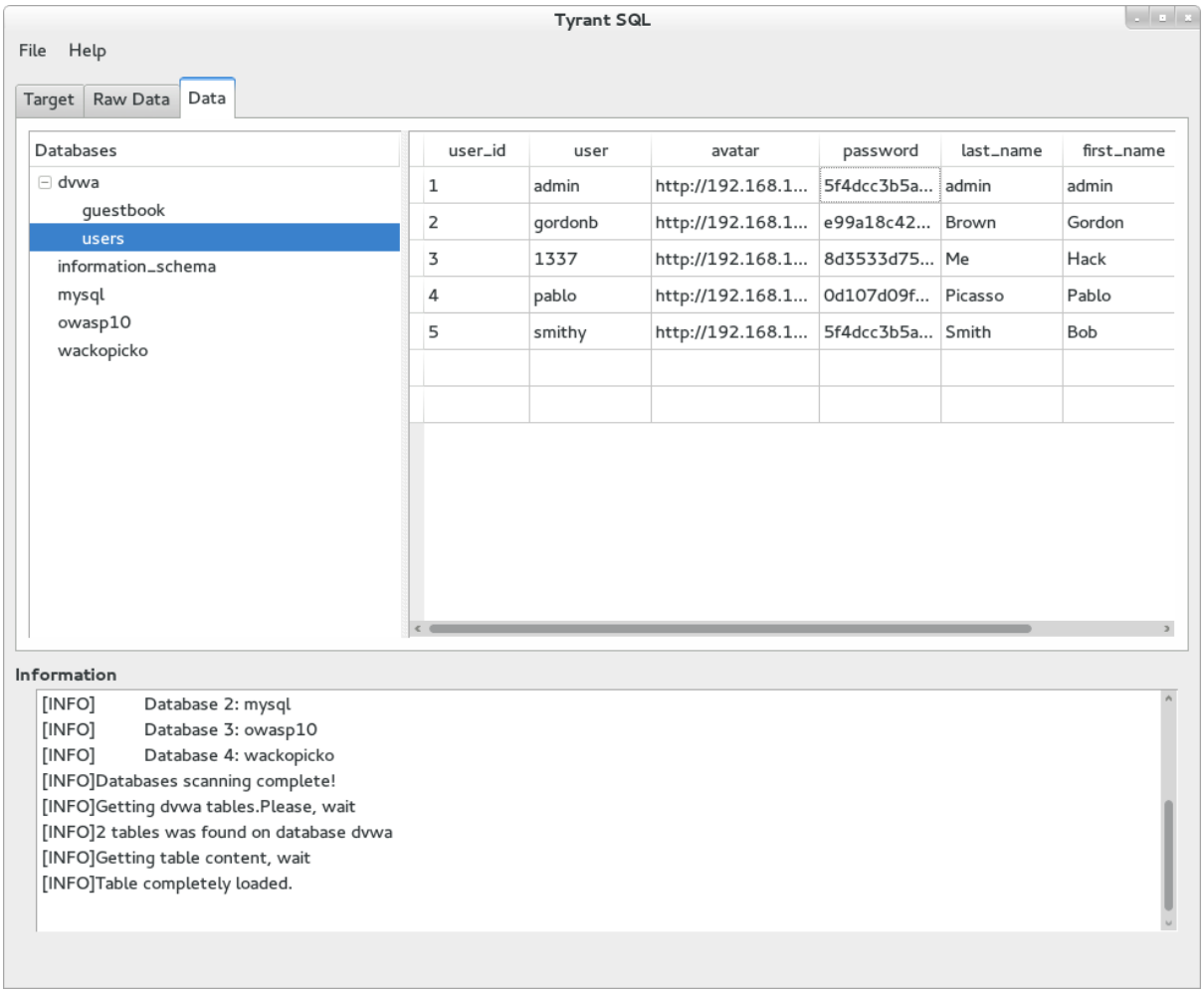
->Python 2.7 Site: http://www.python.org/download/releases/2.7.5/

->PySide 1.2.0 Site: http://qt-project.org/wiki/Category:LanguageBindings::PySide::Downloads

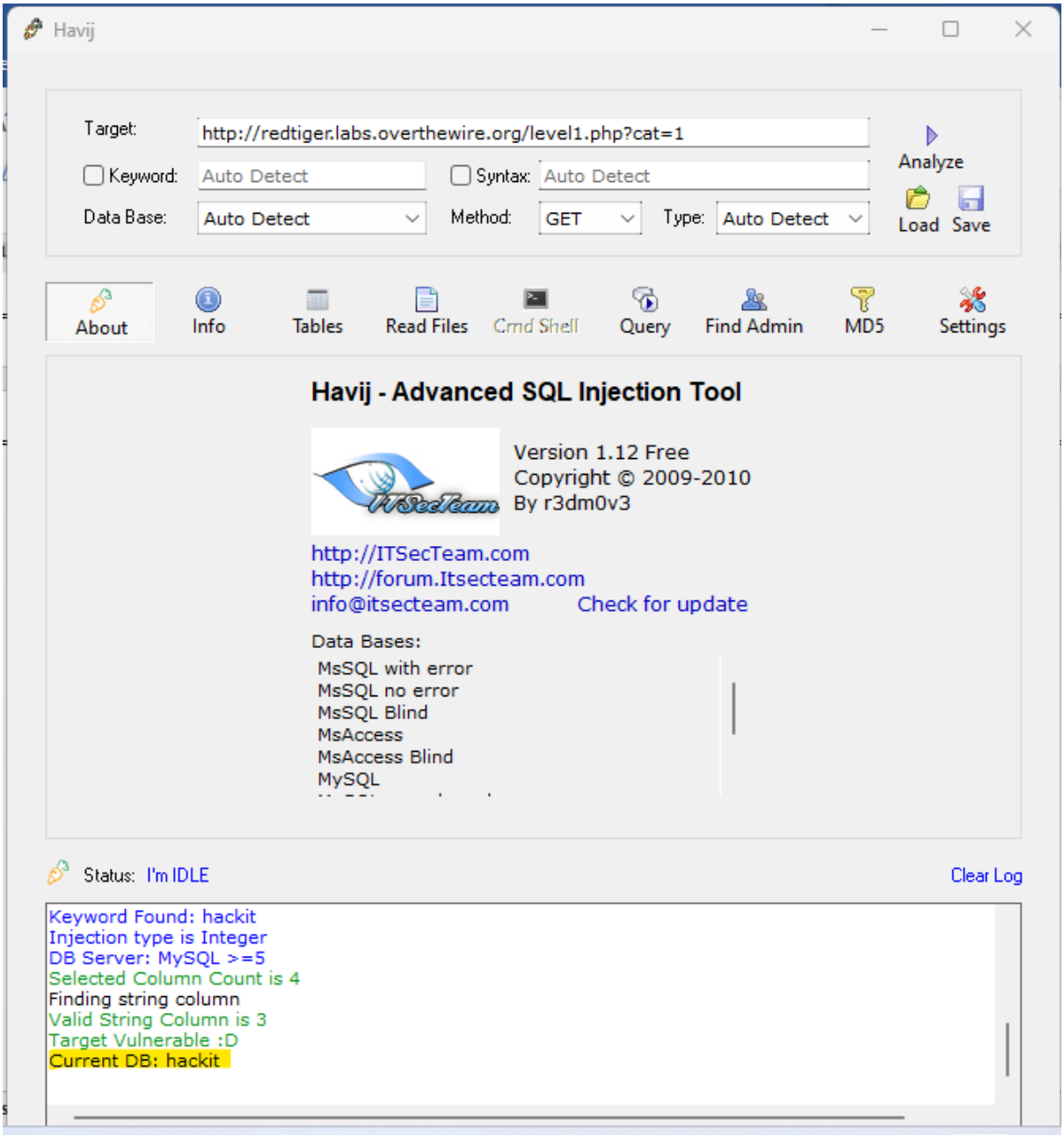
   Step 2: Run the file from command prompt



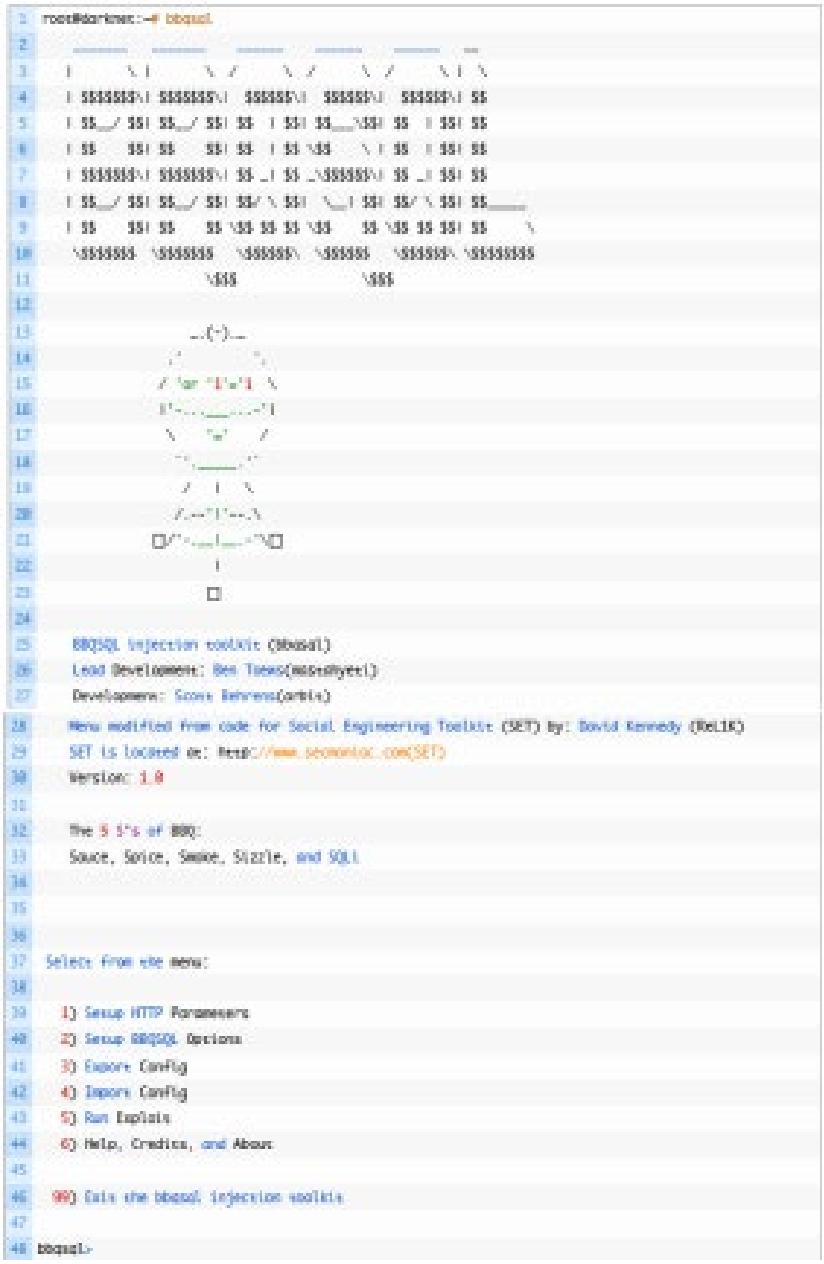
Step 3: Use the vulnerable URL in target :
Example: http://redtiger.labs.overthewire.org/level1.php?cat=1



b. Havij : Open the Havij Application, in the target add any of the vulnerabilities site. We will be using below venerable URL:
http://redtiger.labs.overthewire.org/level1.php?cat=1


Havij
Target:
http://redtiger.labs.overthewire.org/level1.php?cat=1
Analyze
Keyword:
Auto Detect
Syntax:
Auto Detect
Data Base:
Auto Detect
Method:
GET
Type:
Auto Detect
Load
Save
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Havij - Advanced SQL Injection Tool
Version 1.12 Free
Copyright © 2009-2010
By r3dm0v3
http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com
Check for update
Data Bases:
MsSQL with error
MsSQL no error
MsSQL Blind
MsAccess
MsAccess Blind
MySQL
Status: I'm IDLE
Clear Log
Keyword Found: hackit
Injection type is Integer
DB Server: MySQL >=5
Selected Column Count is 4
Finding string column
Valid String Column is 3
Target Vulnerable :D
Current DB: hackit

c. BBQSQL



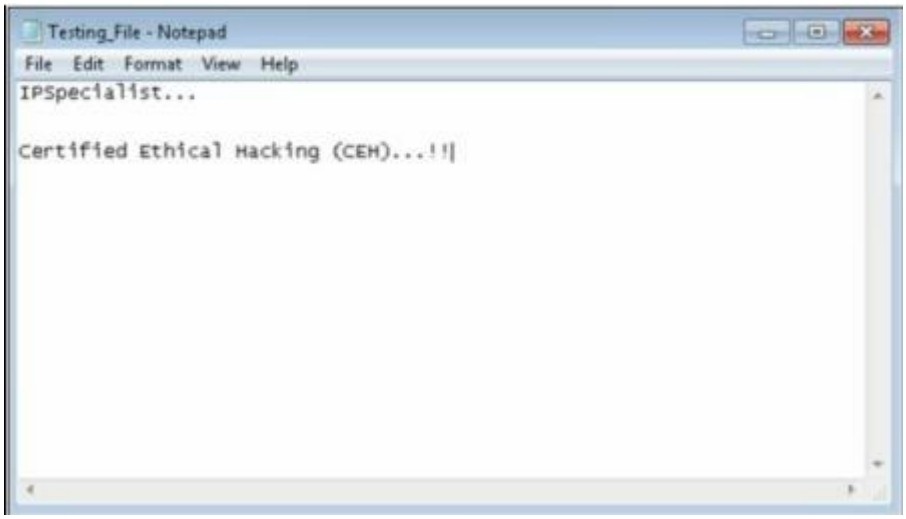
Aim: Use the following tools for cryptography.

i. HashCalc

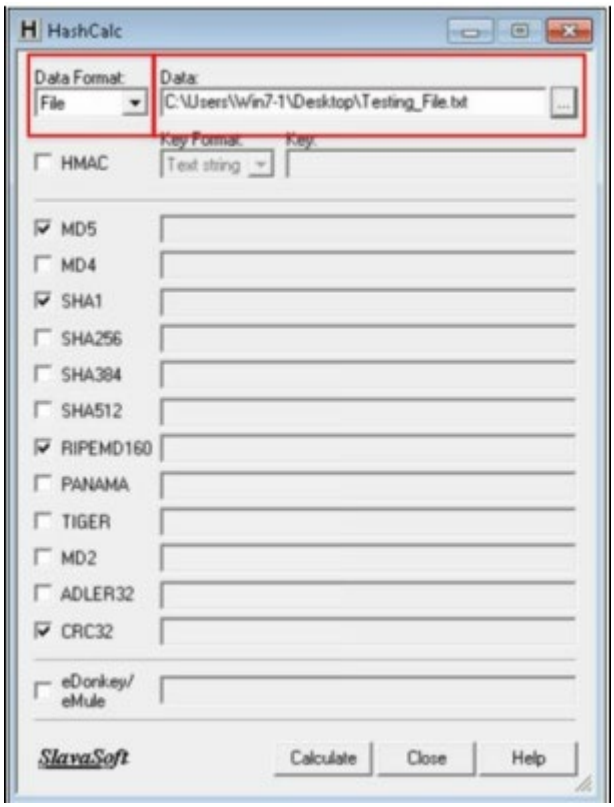
Calculating MD5 value using HashCalc

1. Open HashCalc tool

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

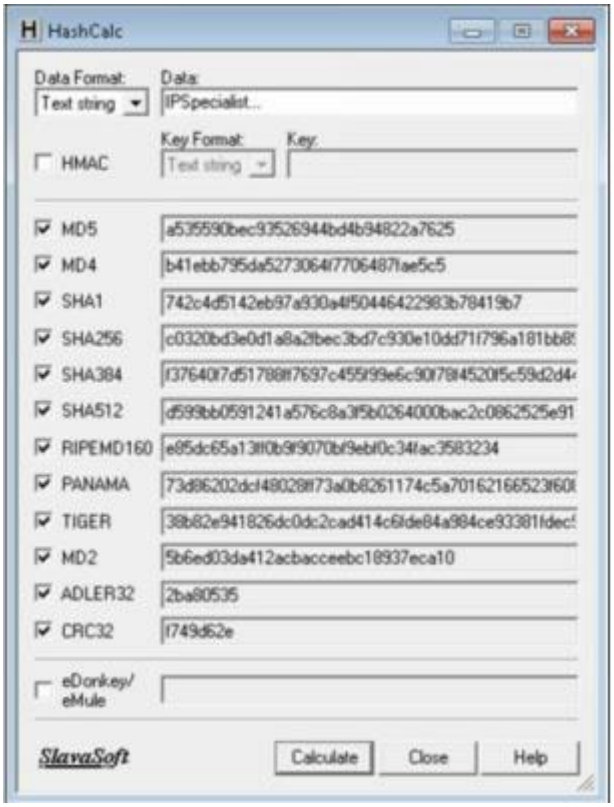


3. Select Data Format as “File” and upload your file



4. Select Hashing Algorithm and Click Calculate

5. Now Select the Data Format to "Text String" and Type "IPSpecialist…" into Data filed and calculated MD5.



MD5 Calculated for the text string "IPSpecialist..." is "a535590bec93526944bd4b94822a7625"

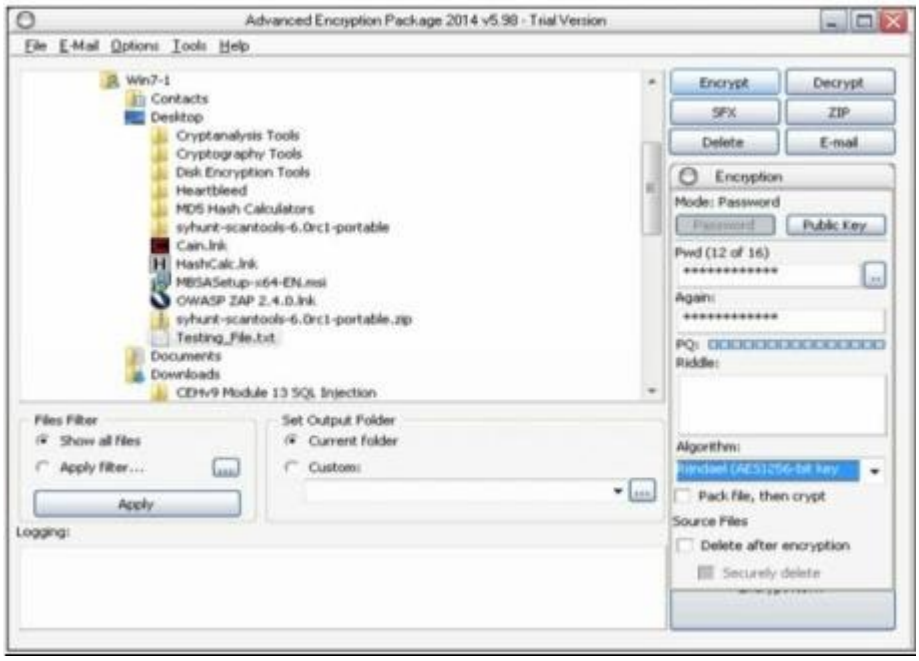
6. Now, let's see how MD5 value is changed from minor change.

Just lowering the case of single alphabet changes entire hashing value. MD5 Calculated for the text string "IPspecialist..." "997bd71ad0158de71f6e97a57261b9a7"

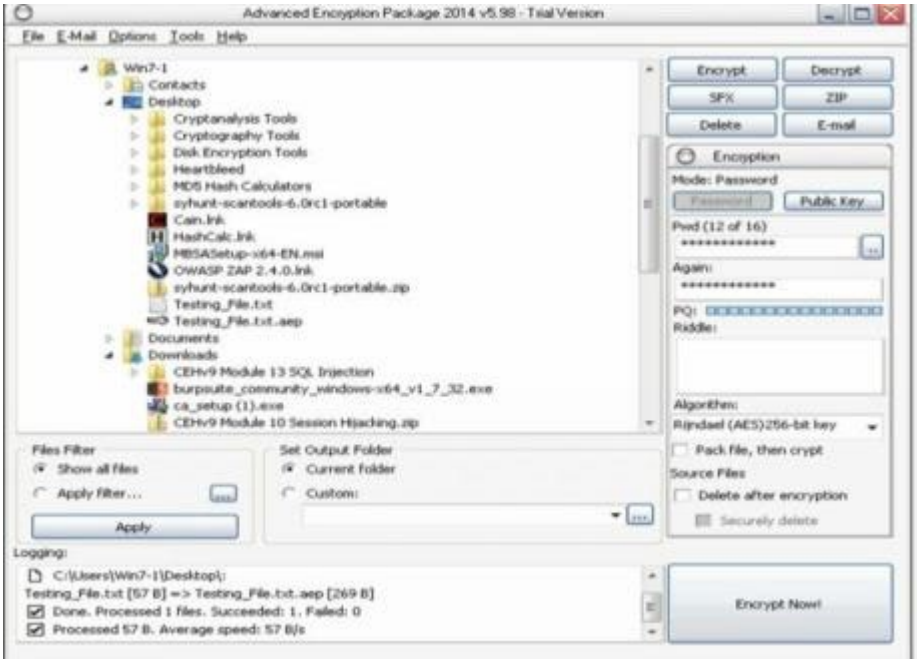
ii. Advanced Encryption Package

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.

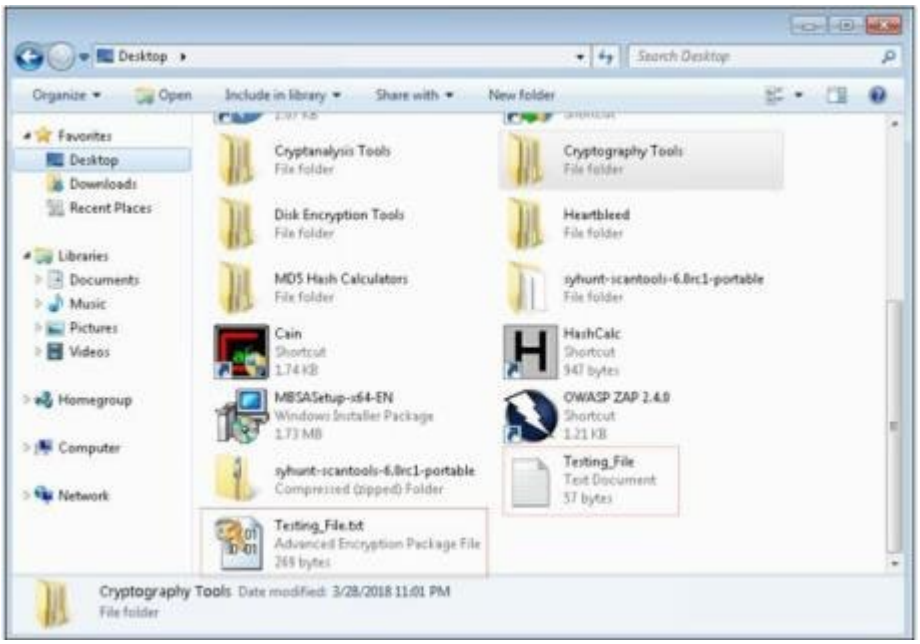
2. Select the File you want to Encrypt.
3. Set password
4. Select Algorithm



5. Click Encrypt



7. Compare both Files



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

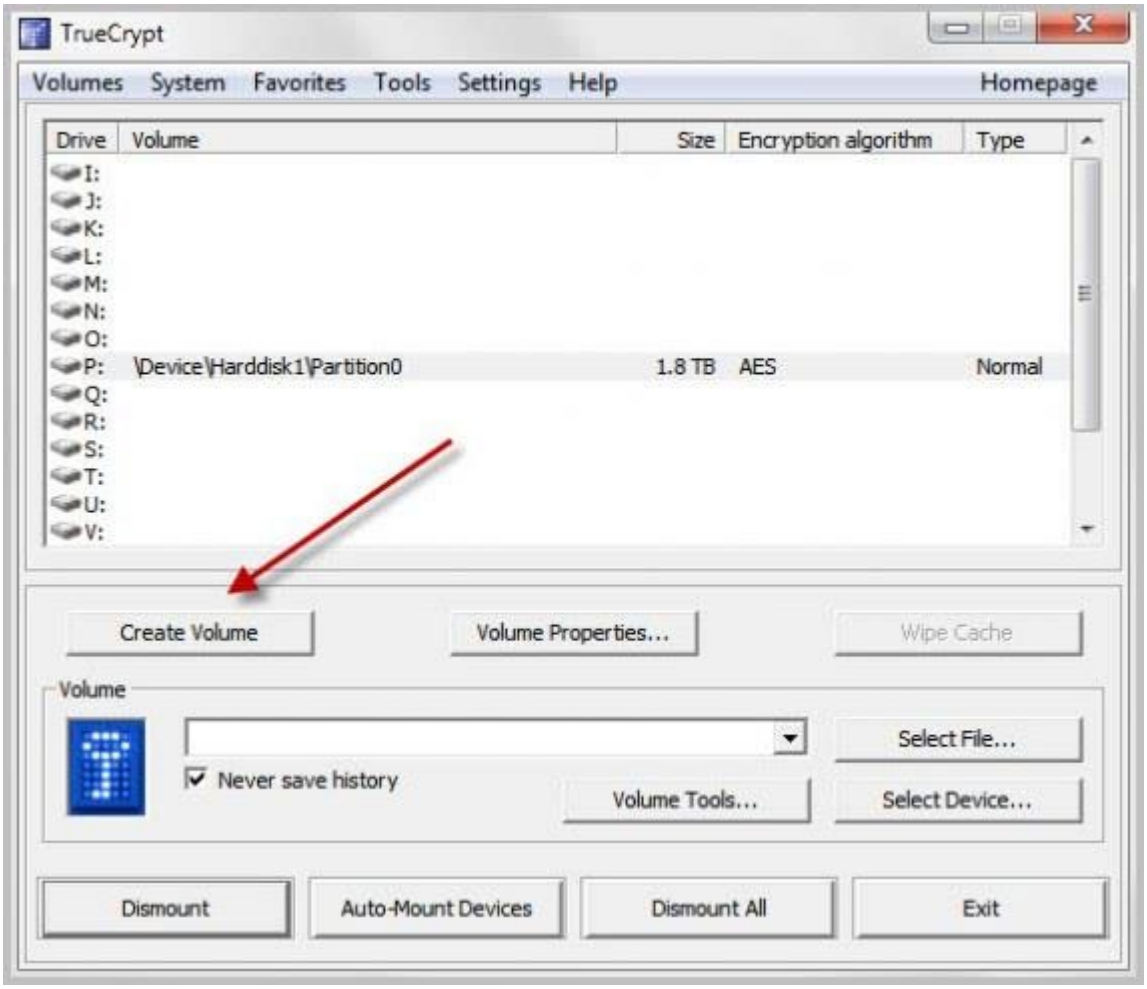
8. Enter password

9. File Successfully decrypted.

\

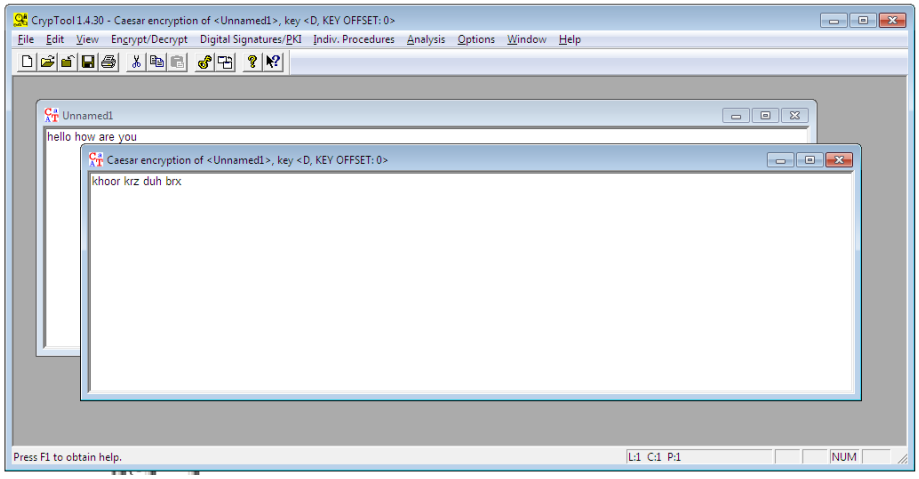
TrueCrypt:

TrueCrypt is the tool to protect your data.



iv. CrypTool

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


CrypTool 1.4.30 - Caesar encryption of <Unnamed1>, key <D, KEY OFFSET: 0>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Unnamed1
hello how are you
Caesar encryption of <Unnamed1>, key <D, KEY OFFSET: 0>
khoor krz duh brx
Press F1 to obtain help.
L:1 C:1 P:1
NUM