

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 ssldump
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”

The screenshot shows the recon-ng interface running in a terminal window titled "Shell No. 1". The window has a dark background with a watermark of the word "PRACTISEC" and the URL "www.practise.com". The terminal window contains the following text:

```
File Actions Edit View Help
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.

[recon-ng][default] > marketplace search
+-----+
| Updated | D | K | Path | Version | Status
+-----+
| discovery/info_disclosure/cache_snoop | 1.1 | not instal
led | 2020-10-13 | | |
| discovery/info_disclosure/interesting_files | 1.2 | not instal
led | 2021-10-04 | | |
| exploitation/injection/command_injector | 1.0 | not instal
led | 2019-06-24 | | |
| exploitation/injection/xpath_bruter | 1.2 | not instal
led | 2019-10-08 | | |
| import/csv_file | 1.1 | not instal
```

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

File Actions Edit View Help

led 2019-06-24 *			
reporting/csv	1.0	not instal	
led 2019-06-24			
reporting/html	1.0	not instal	
led 2019-06-24			
reporting/json	1.0	not instal	
led 2019-06-24			
reporting/list	1.0	not instal	
led 2019-06-24			
reporting/proxifier	1.0	not instal	
led 2019-06-24			
reporting/pushpin	1.0	not instal	
led 2019-06-24 *			
reporting/xlsx	1.0	not instal	
led 2019-06-24			
reporting/xml	1.1	not instal	
led 2019-06-24			

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

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

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.

```
Shell No. 1

File Actions Edit View Help
| reporting/proxifier | 1.0 | not instal
led | 2019-06-24 | | |
| reporting/pushpin | 1.0 | not instal
led | 2019-06-24 | * |
| reporting/xlsx | 1.0 | not instal
led | 2019-06-24 | | |
| reporting/xml | 1.1 | not instal
led | 2019-06-24 | | |
+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

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

Step 6: Use command run to execute the scan.

The screenshot shows a terminal window titled "Shell No. 1". The terminal displays the following command-line session:

```
[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>

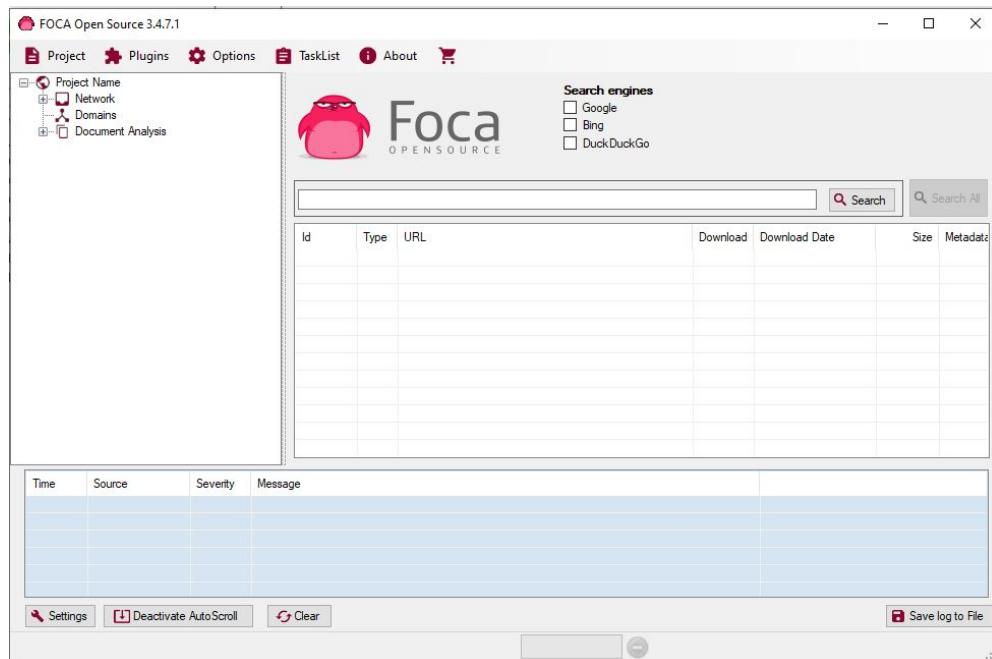
[recon-ng][default][hackertarget] > options set SOURCE tesla.com
SOURCE => tesla.com
[recon-ng][default][hackertarget] > run

_____
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
```

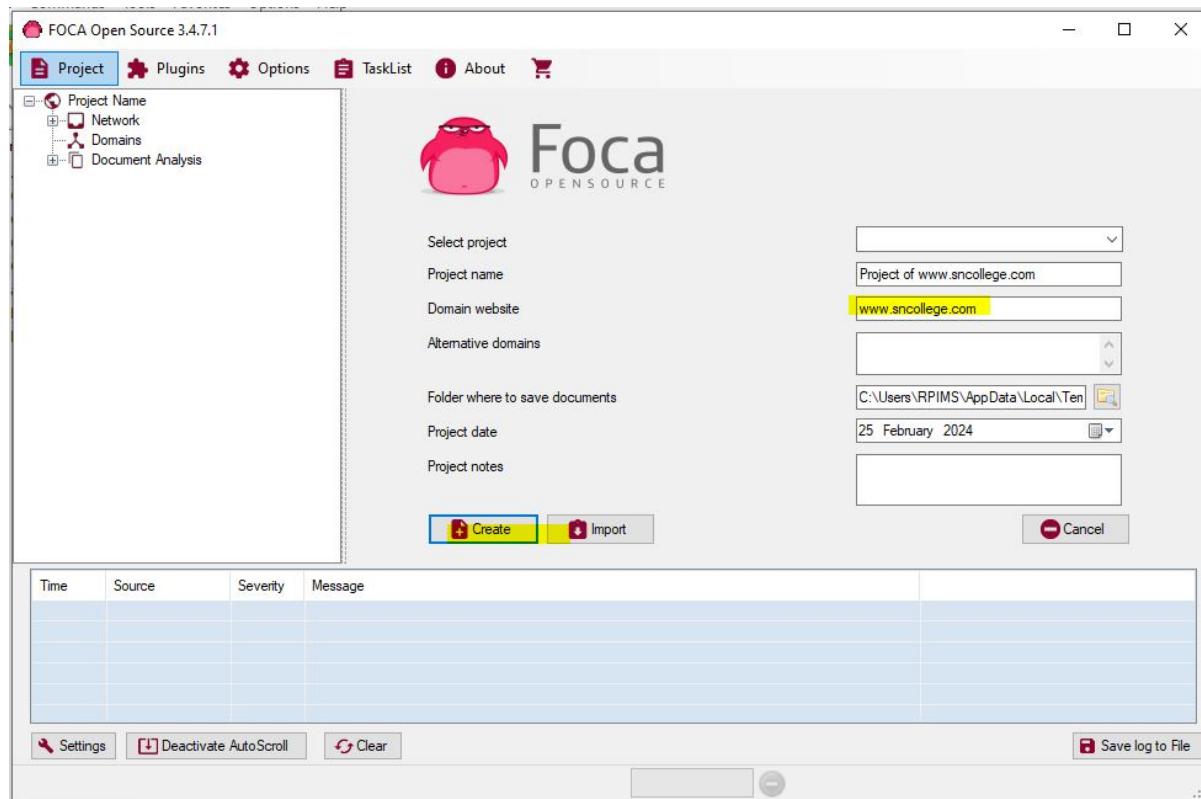
Practical 2:

Aim:- Use of FOCA Tools.

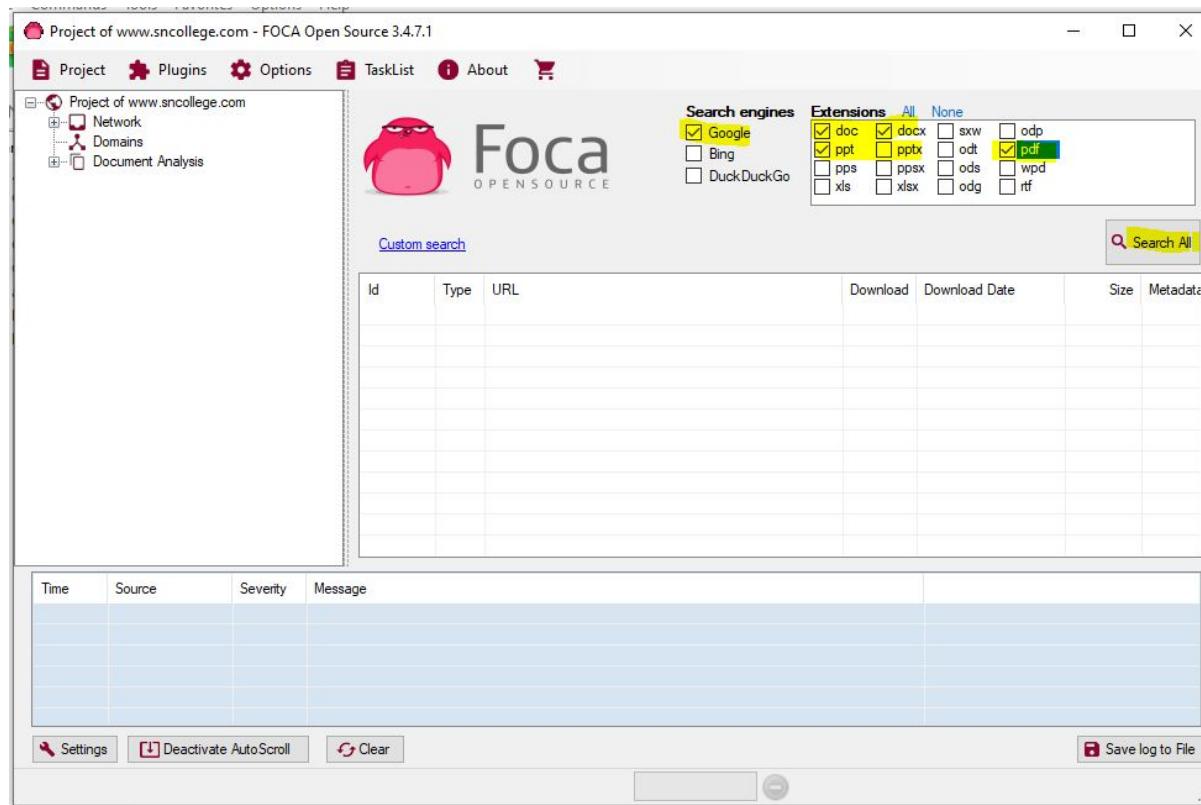
Step 1: Open FOCA Tool, goto project -> select new project.



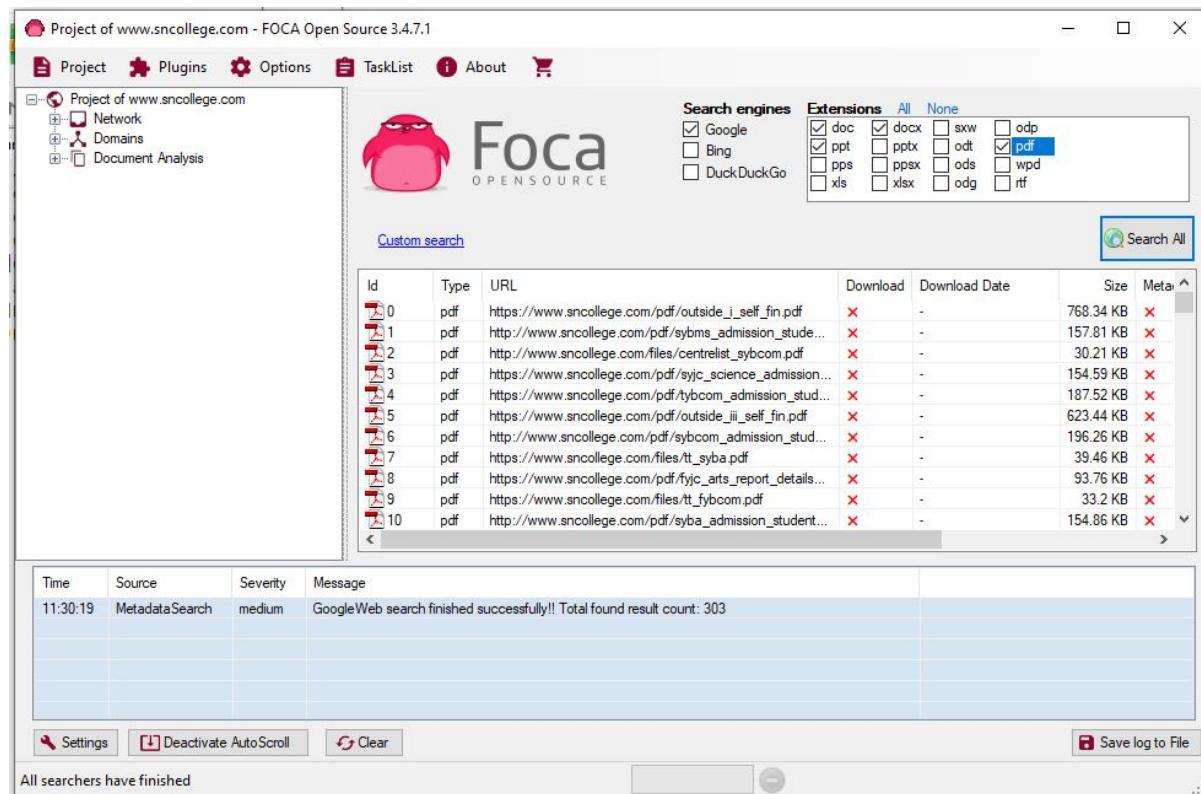
Step 2: Enter the URL then click the “Create” button.



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.

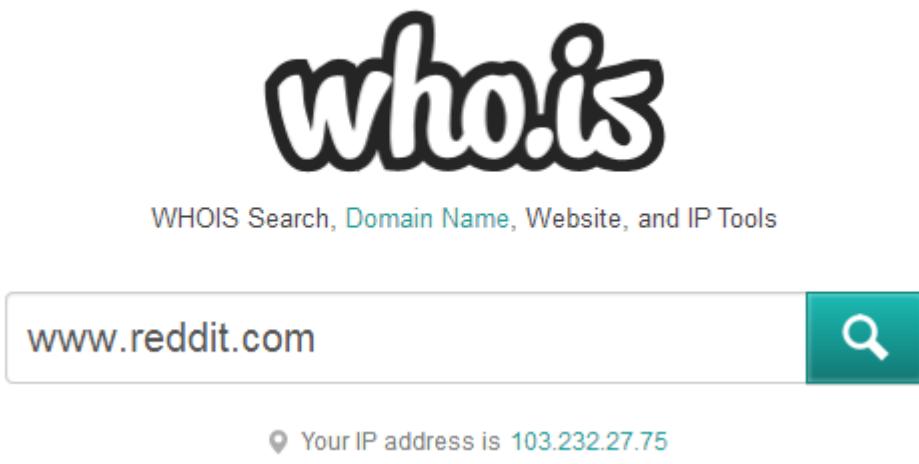


Practical 3:

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

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

Alexa Trend/Rank One Month: 50 (▼ 0)

Alexa Trend/Rank Three Month: 50 (▲ 6)

Page Views Per Visit One Month: 10.6 (▼ 3.36%)

Page Views Per Visit Three Month: 10.9 (▲ 0%)

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@gandi.net
Registrar Abuse Contact Phone: +33.170377661
Reseller:
Domain Status: clientTransferProhibited
Domain Status:
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:
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 strictly forbidden.

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

Website Info for reddit.com

Contact Information

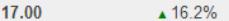
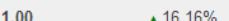
No contact info was available.

Content Data

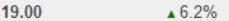
Title	Reddit
Description	User-generated news links. Votes promote stories to the front page.
Online Since	29-Apr-2005
Speed: Median Load Time	1307
Speed: Percentile	 62%
Adult Content	no
Language	en
Links In Count	469373

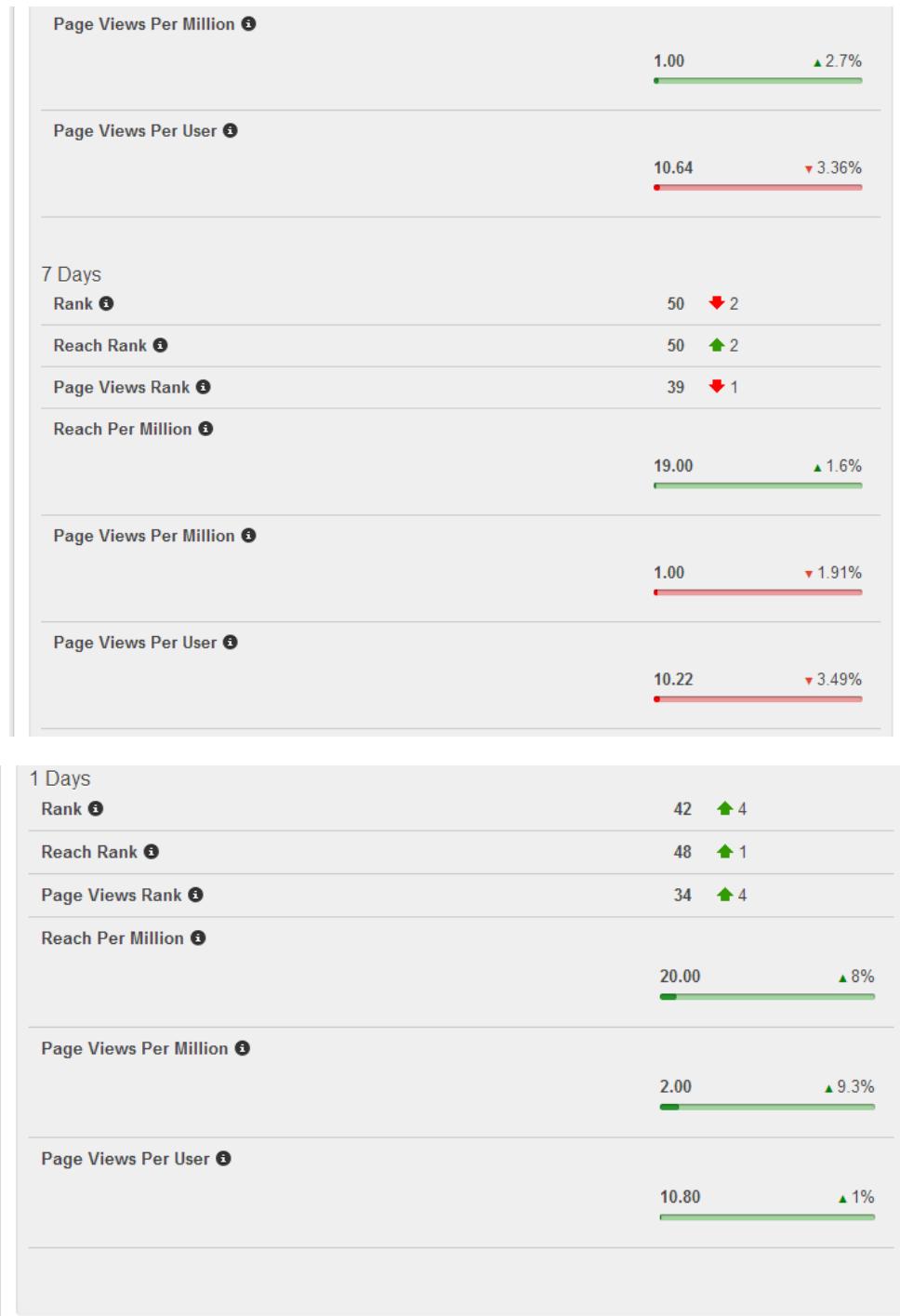
Traffic Data

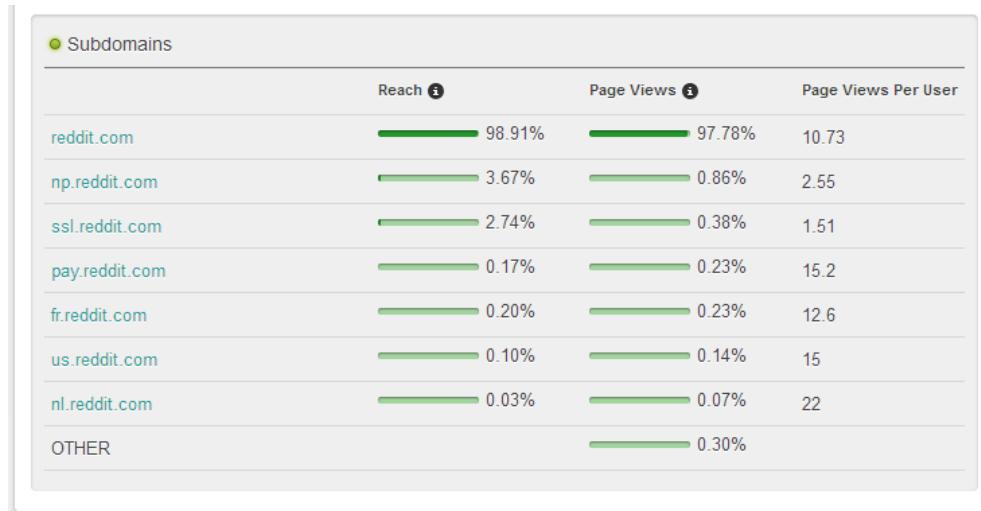
3 Months

Rank ⓘ	50  6
Reach Rank ⓘ	55  10
Page Views Rank ⓘ	40  2
Reach Per Million ⓘ	 17.00  16.2%
Page Views Per Million ⓘ	 1.00  16.16%
Page Views Per User ⓘ	

1 Months

Rank ⓘ	
Reach Rank ⓘ	
Page Views Rank ⓘ	37  1
Reach Per Million ⓘ	 19.00  6.2%





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

Want this archived information removed?

Old Registrar Info May 16, 2007		Registrar Info September 02, 2014	
Name	DSTR ACQUISITION PA I, LLC DBA DOMAINBANK.COM	Name	GANDI SAS
Whois Server	rs.domainbank.net	Whois Server	whois.gandi.net
Referral URL	http://www.domainbank.net	Referral URL	http://www.gandi.net
Status		Status	clientTransferProhibited
Important Dates		Important Dates	
Expires On	April 29, 2008	Expires On	April 29, 2017
Registered On	April 29, 2005	Registered On	April 29, 2005
Updated On	December 13, 2006	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 entities 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**

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 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:
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.

Whois Website Info History DNS Records Diagnostics

DNS for reddit.com

● Name Servers – reddit.com More Info

Name Server	IP	Location
cns1.reddit.com	173.245.58.24	
cns2.reddit.com	198.41.222.24	
cns3.reddit.com	198.41.223.24	

● SOA Record – reddit.com

Name Server	cns1.reddit.com
Email	dns@cloudflare.com
Serial Number	2016126715
Refresh	2 hours 46 minutes 40 seconds
Retry	40 minutes
Expiry	7 days
Minimum	1 hour

● 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.gmail.com

reddit.com	MX	5 minutes	10	aspmx3.gmail.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.gmail.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. 20161 26715 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 (0)
forum.reddit.com	A	5 minutes	198.41.209.143 (0)
forum.reddit.com	A	5 minutes	198.41.208.141 (0)
help.reddit.com	A	5 minutes	198.41.209.141 (0)
help.reddit.com	A	5 minutes	198.41.208.143 (0)
help.reddit.com	A	5 minutes	198.41.208.137 (0)
help.reddit.com	A	5 minutes	198.41.209.142 (0)
help.reddit.com	A	5 minutes	198.41.208.140 (0)
help.reddit.com	A	5 minutes	198.41.209.137 (0)
help.reddit.com	A	5 minutes	198.41.209.136 (0)
help.reddit.com	A	5 minutes	198.41.209.139 (0)
help.reddit.com	A	5 minutes	198.41.209.138 (0)
help.reddit.com	A	5 minutes	198.41.209.143 (0)
help.reddit.com	A	5 minutes	198.41.208.139 (0)
help.reddit.com	A	5 minutes	198.41.209.140 (0)
help.reddit.com	A	5 minutes	198.41.208.141 (0)
help.reddit.com	A	5 minutes	198.41.208.138 (0)
mail.reddit.com	A	5 minutes	174.129.203.189 (Seattle, WA, US)
test.reddit.com	A	5 minutes	198.41.209.140 (0)

test.reddit.com	A	5 minutes	198.41.209.140 (0)
test.reddit.com	A	5 minutes	198.41.208.139 (0)
test.reddit.com	A	5 minutes	198.41.209.141 (0)
test.reddit.com	A	5 minutes	198.41.209.136 (0)
test.reddit.com	A	5 minutes	198.41.208.141 (0)
test.reddit.com	A	5 minutes	198.41.208.140 (0)
test.reddit.com	A	5 minutes	198.41.209.137 (0)
test.reddit.com	A	5 minutes	198.41.209.143 (0)
test.reddit.com	A	5 minutes	198.41.208.143 (0)
test.reddit.com	A	5 minutes	198.41.209.139 (0)
test.reddit.com	A	5 minutes	198.41.209.142 (0)
test.reddit.com	A	5 minutes	198.41.209.138 (0)
test.reddit.com	A	5 minutes	198.41.208.138 (0)
test.reddit.com	A	5 minutes	198.41.208.137 (0)
www.reddit.com	A	5 minutes	198.41.208.137 (0)
www.reddit.com	A	5 minutes	198.41.209.138 (0)
www.reddit.com	A	5 minutes	198.41.208.139 (0)
www.reddit.com	A	5 minutes	198.41.209.140 (0)
www.reddit.com	A	5 minutes	198.41.209.136 (0)

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.

Whois Website Info History DNS Records **Diagnostics**

Diagnostic Tools for reddit.com

Updated: 3 hours ago

Ping

reddit.com Count: 10 Interval: 0.5s Start Ping

Ping is a computer network tool used to test whether a particular host is reachable or as a speed test. It works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. Ping estimates the round-trip time, generally in milliseconds, records any packet loss, and prints a statistical summary when finished.

Traceroute

reddit.com Probes: 3 Max Hops: 20 Traceroute

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network.

USING TRACE ROUTE

Step 1: Open cmd prompt.



A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window shows the Microsoft Windows [Version 6.1.7601] copyright notice and the command prompt line "C:\Users\Sonal\>". The window has a standard blue title bar and a black background.

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



A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window shows the Microsoft Windows [Version 6.1.7601] copyright notice and the command prompt line "C:\Users\Sonal\>cd\>". The window has a standard blue title bar and a black background.

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

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:>cd\

C:>tracert www.reddit.com

Tracing route to www.reddit.com [198.41.209.141]
over a maximum of 30 hops:
  1       1 ms      <1 ms      1 ms  192.168.0.1
  2       1 ms      1 ms      1 ms  212-1-226-103.intechonline.net [103.226.1.212]
  3       2 ms      4 ms      2 ms  249-0-226-103.intechonline.net [103.226.0.249]
  4      70 ms     69 ms     68 ms  61.8.56.0
  5      67 ms     66 ms     67 ms  be2.wr2.sin0.asianetcom.net [61.14.157.185]
  6      65 ms     65 ms     65 ms  gi0-0-0.gw2.sin3.asianetcom.net [61.14.157.170]
  7      65 ms     65 ms     65 ms  te0-0-0-4.gw3.sin3.asianetcom.net [202.147.32.10]
  8      61 ms     61 ms     61 ms  CDF-0014.asianetcom.net [203.192.169.226]
  9      63 ms     65 ms     68 ms  198.41.209.141

Trace complete.

C:>
```

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

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:>cd\

C:>tracert 198.41.209.142

Tracing route to 198.41.209.142 over a maximum of 30 hops
  1       1 ms      1 ms      <1 ms  192.168.0.1
  2       1 ms      1 ms      1 ms  212-1-226-103.intechonline.net [103.226.1.212]
  3       2 ms      4 ms      22 ms  249-0-226-103.intechonline.net [103.226.0.249]
  4      65 ms     67 ms     69 ms  61.8.56.0
  5      65 ms     68 ms     68 ms  be2.wr2.sin0.asianetcom.net [61.14.157.185]
  6      67 ms     66 ms     67 ms  te0-0-4-0.wr1.sin0.asianetcom.net [61.14.157.37]
  7      66 ms     65 ms     66 ms  te0-0-0-0.gw3.sin3.asianetcom.net [61.14.157.130]
  8     173 ms    311 ms    429 ms  CDF-0014.asianetcom.net [203.192.169.226]
  9      64 ms     63 ms     73 ms  198.41.209.142

Trace complete.

C:>
```

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

```
D:\>ping 192.168.2.1 -l 1500 -n 1

Pinging 192.168.2.1 with 1500 bytes of data:
Reply from 192.168.2.1: bytes=1500 time<1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\>ping 192.168.2.1 -l 1500 -n 1 -f

Pinging 192.168.2.1 with 1500 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.2.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

- 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

```
D:\>ping 192.168.2.1 -l 1478 -f

Pinging 192.168.2.1 with 1478 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

D:\>ping 192.168.2.1 -l 1474 -f

Pinging 192.168.2.1 with 1474 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- 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  
  
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 -l switches.
- -n means number of replies to show and -l means obtain reply from the machine in the next hop
- Open command prompt □
- Ping certifiedhacker.com -n 1 -l 1

```
D:\>ping certifiedhacker.com -n 1 -l 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 l value until the certifiedhacker.com site directly replies to the ping.
- At each l value, the device in the route will reply back

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

```
D:\>nslookup  
Default Server: UnKnown  
Address: 192.168.0.1
```

- 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

```
> set type=mx  
> certifiedhacker.com  
Server: UnKnown  
Address: 192.168.0.1  
  
Non-authoritative answer:  
certifiedhacker.com      MX preference = 10, mail exchanger = mail.certifiedhacker.com
```

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

```
> set type=a  
> certifiedhacker.com  
Server: UnKnown  
Address: 192.168.0.1  
  
Non-authoritative answer:  
Name: certifiedhacker.com  
Address: 202.75.54.101
```

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

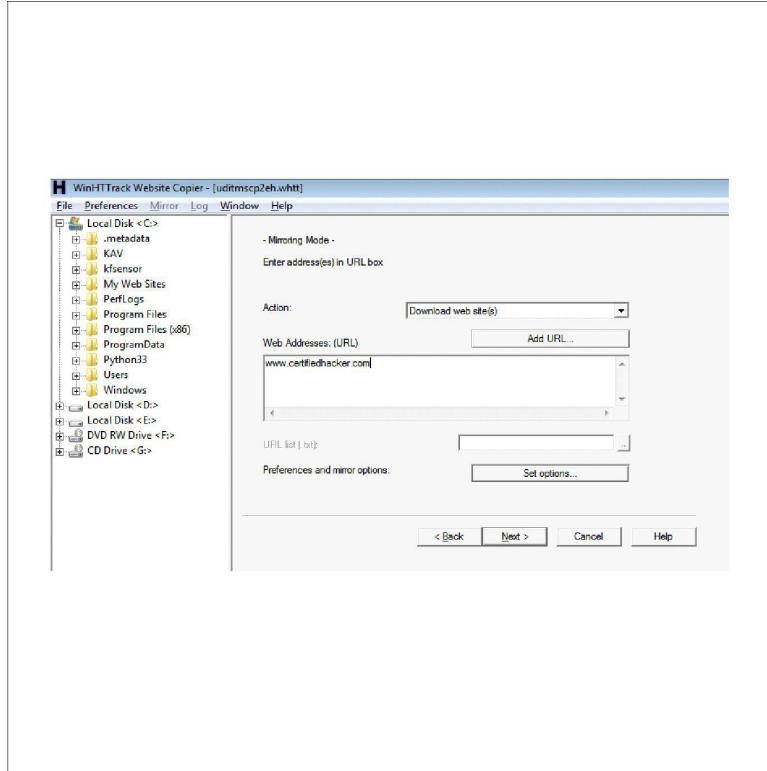
```
> set type=ns
> certifiedhacker.com
Server: UnKnown
Address: 192.168.0.1

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

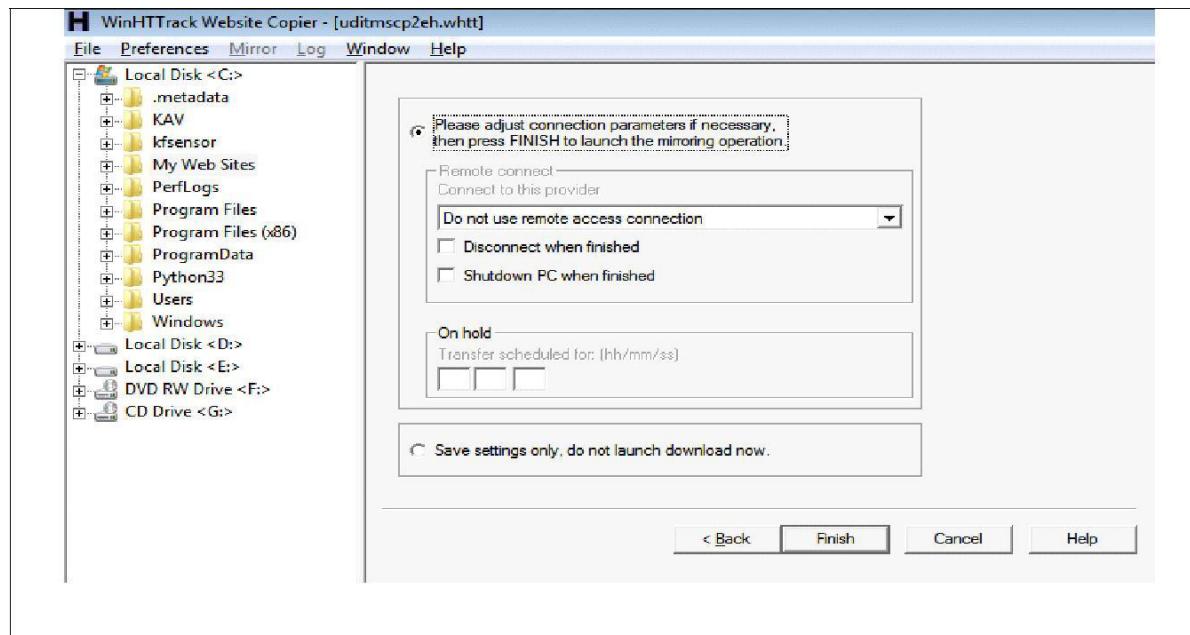
Aim: HTTrack Website Copier

Start > Programs >

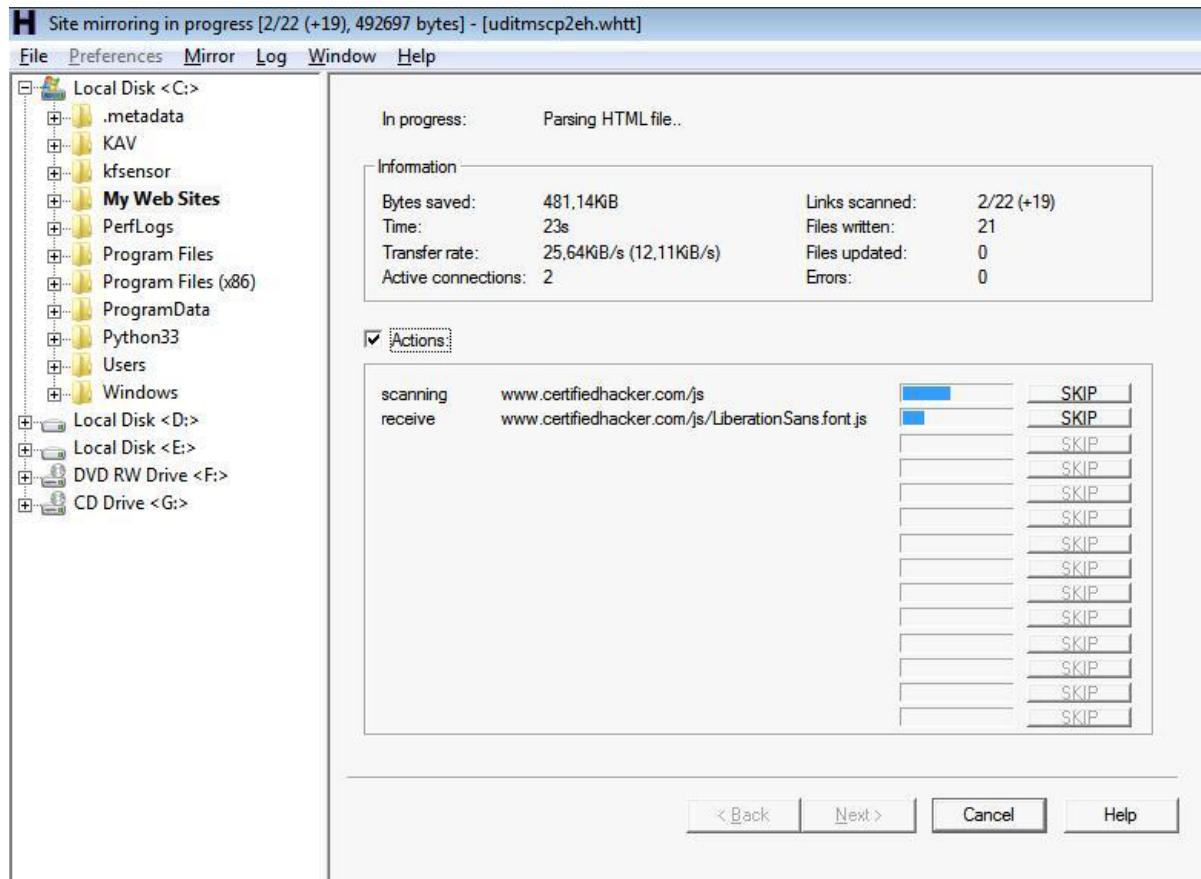
- HTTrack Website Copier
- Click on 'Next' to create Project
- Give a name to project Click on 'Next'



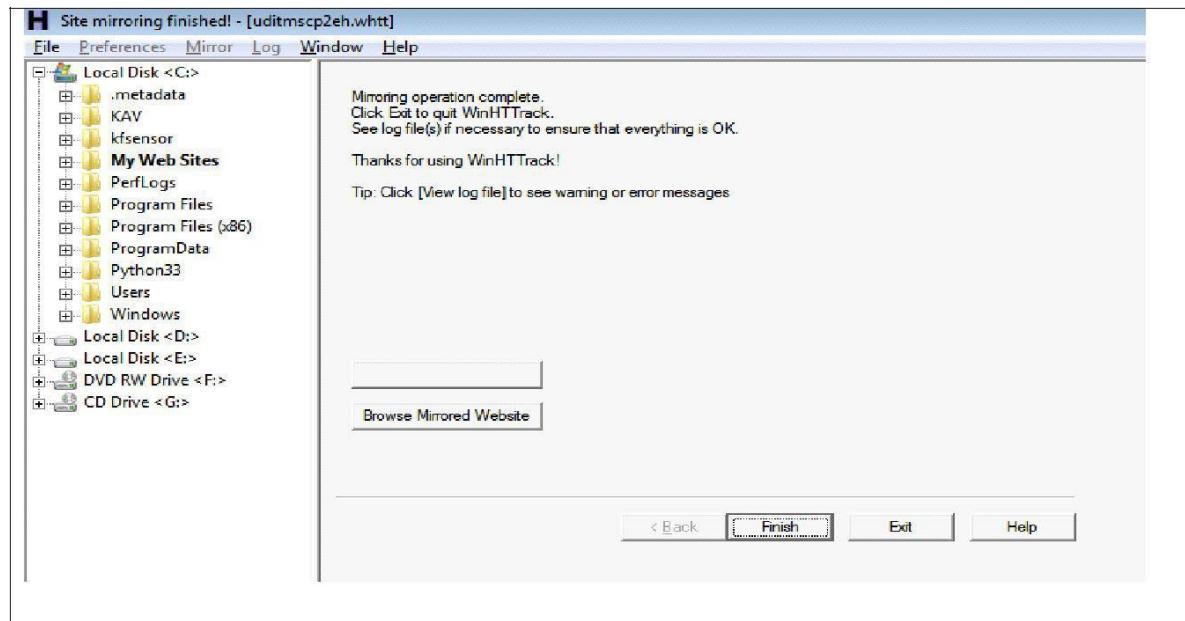
- Click on 'Add URL' and give the URL
 - Any additional options that need to be set
 - Then click 'Next'
-
- By default, the radio button will be selected for Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.



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



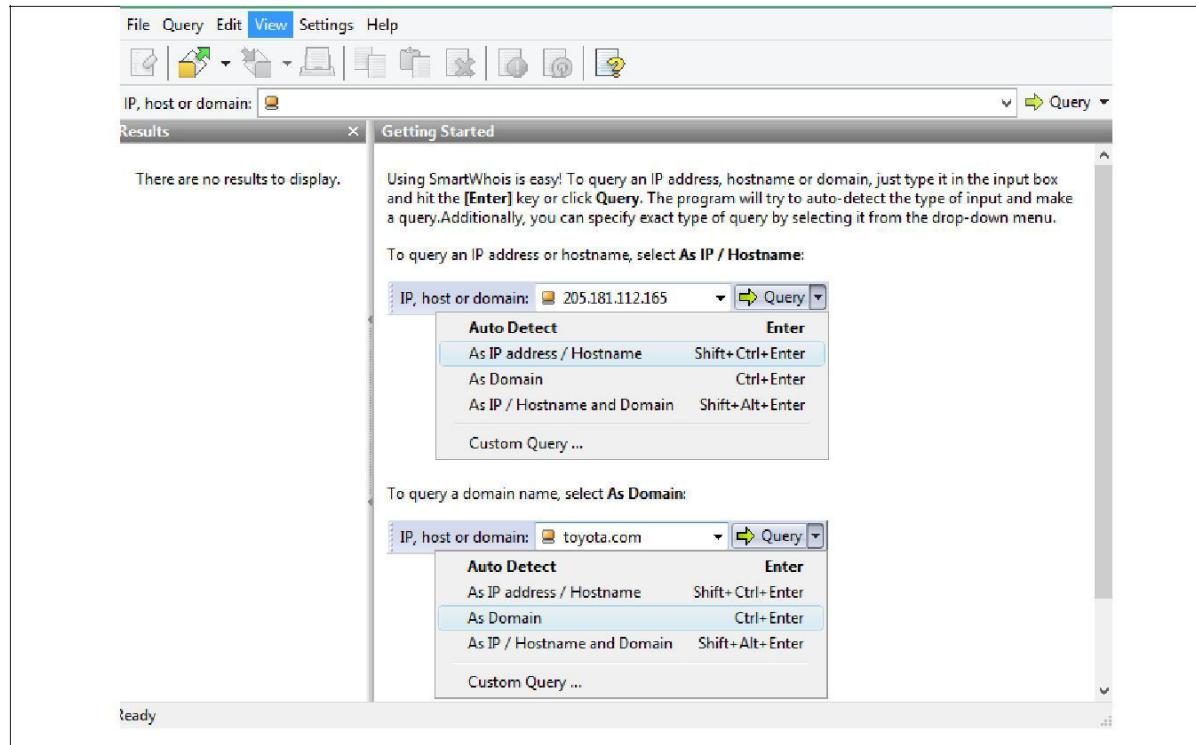
□ Process of mirroring the website.



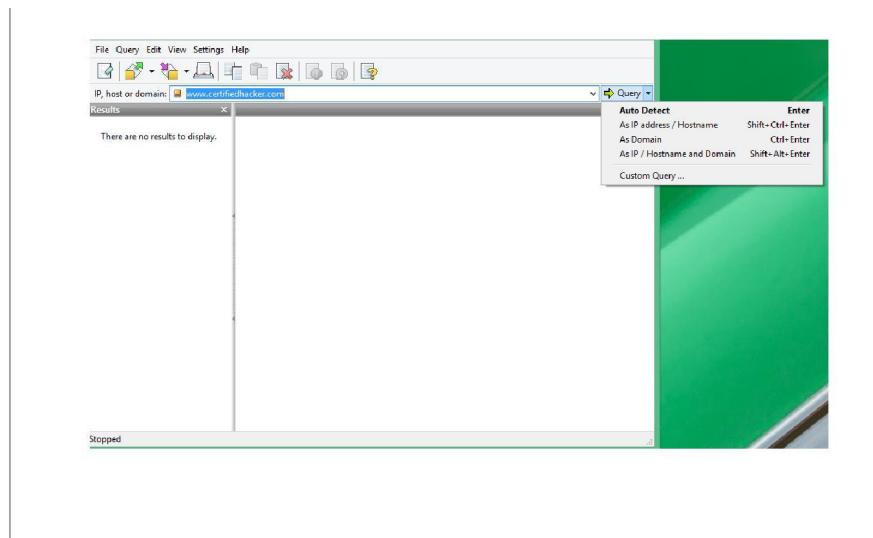
Once the Website Mirroring has been completed, you can click on the Browse Mirrored Website button and then browse the offline copy of the website. ☐



- SmartWHOis 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

IP, host or domain: www.certifiedhacker.com

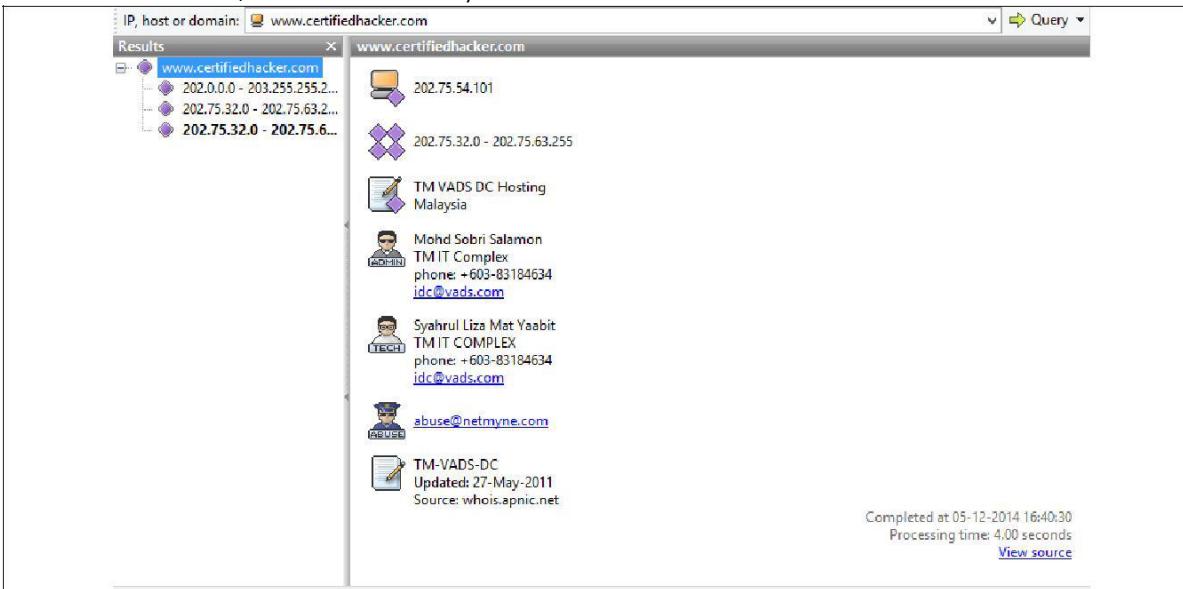
Results

- www.certifiedhacker.com
 - 202.0.0.0 - 203.255.255.255
 - 202.75.32.0 - 202.75.63.255
 - 202.75.32.0 - 202.75.6.255

www.certifiedhacker.com

- 202.75.54.101
- 202.75.32.0 - 202.75.63.255
- TM VADS DC Hosting Malaysia
 - Mohd Sobri Salamon
TM IT Complex
phone: +603-83184634
idc@vads.com
 - Syahrul Liza Mat Yaabit
TM IT COMPLEX
phone: +603-83184634
idc@vads.com
 - abuse@netmyne.com
- TM-VADS-DC
 - Updated: 27-May-2011
 - Source: whois.apnic.net

Completed at 05-12-2014 16:40:30
Processing time: 4.00 seconds
[View source](#)



IP, host or domain: www.certifiedhacker.com

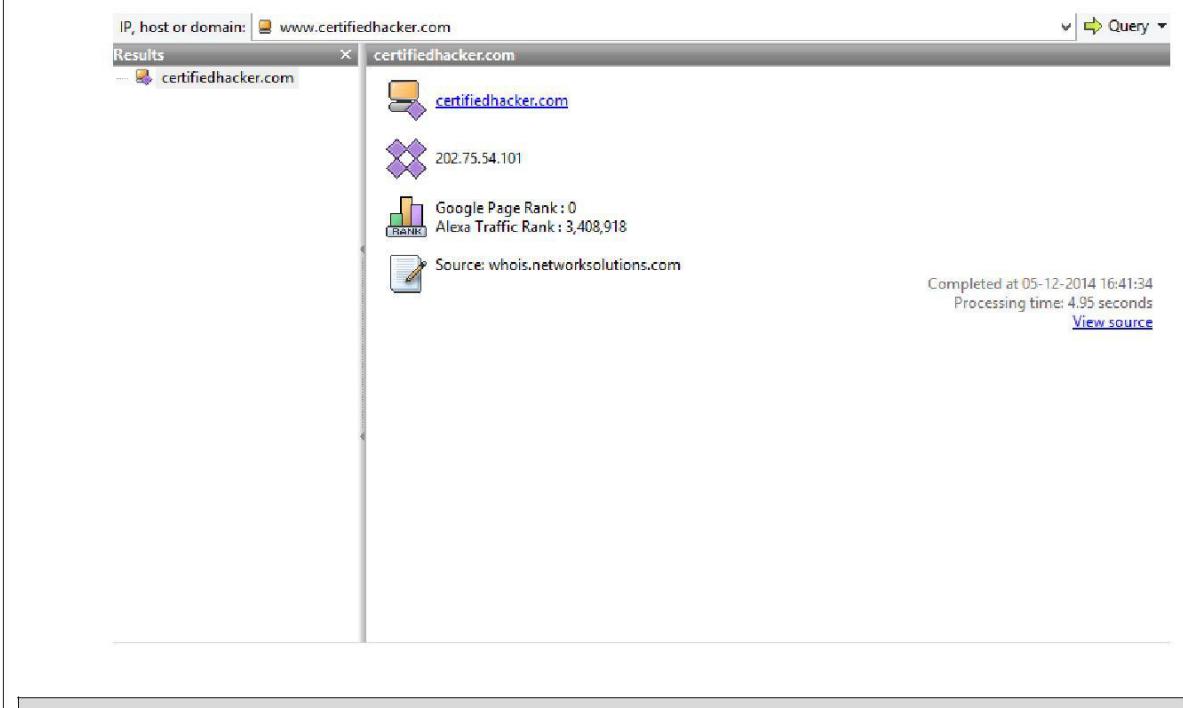
Results

- certifiedhacker.com

certifiedhacker.com

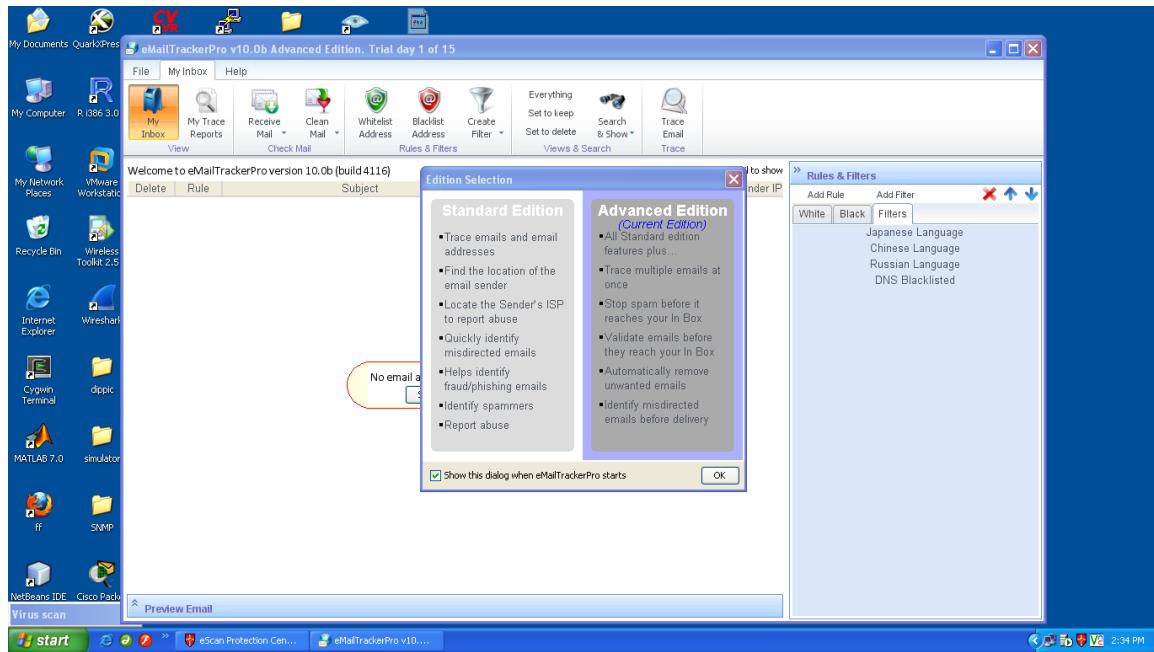
- certifiedhacker.com
- 202.75.54.101
- Google Page Rank : 0
Alexa Traffic Rank : 3,408,918
- Source: whois.networksolutions.com

Completed at 05-12-2014 16:41:34
Processing time: 4.95 seconds
[View source](#)

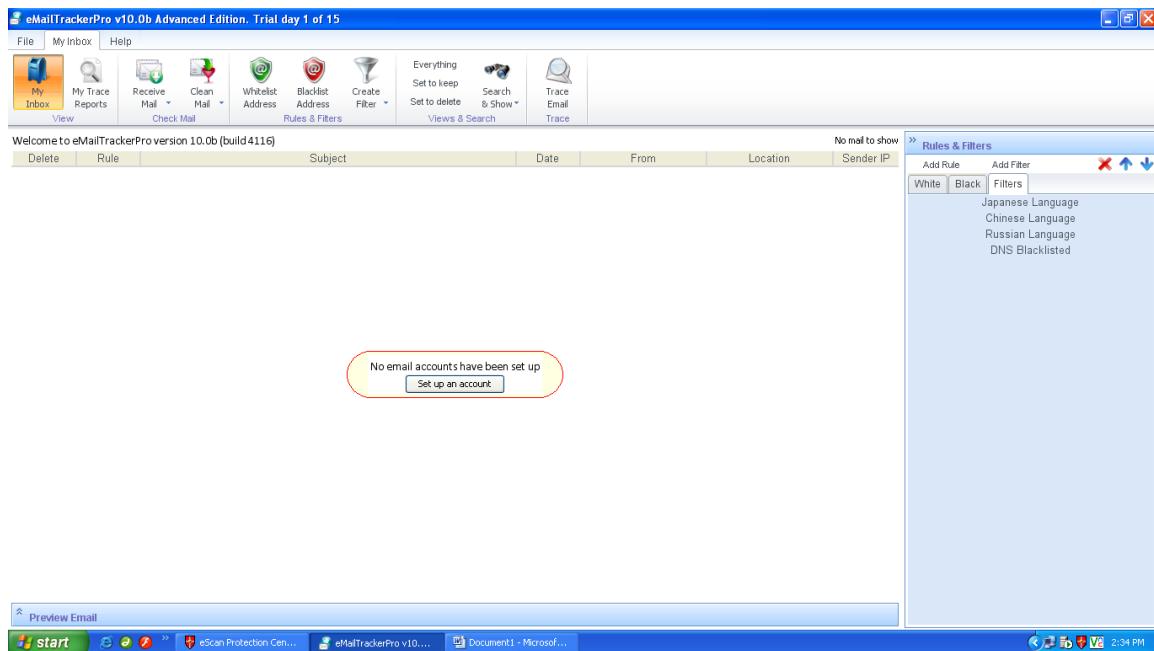


USING EMAIL TRACKER

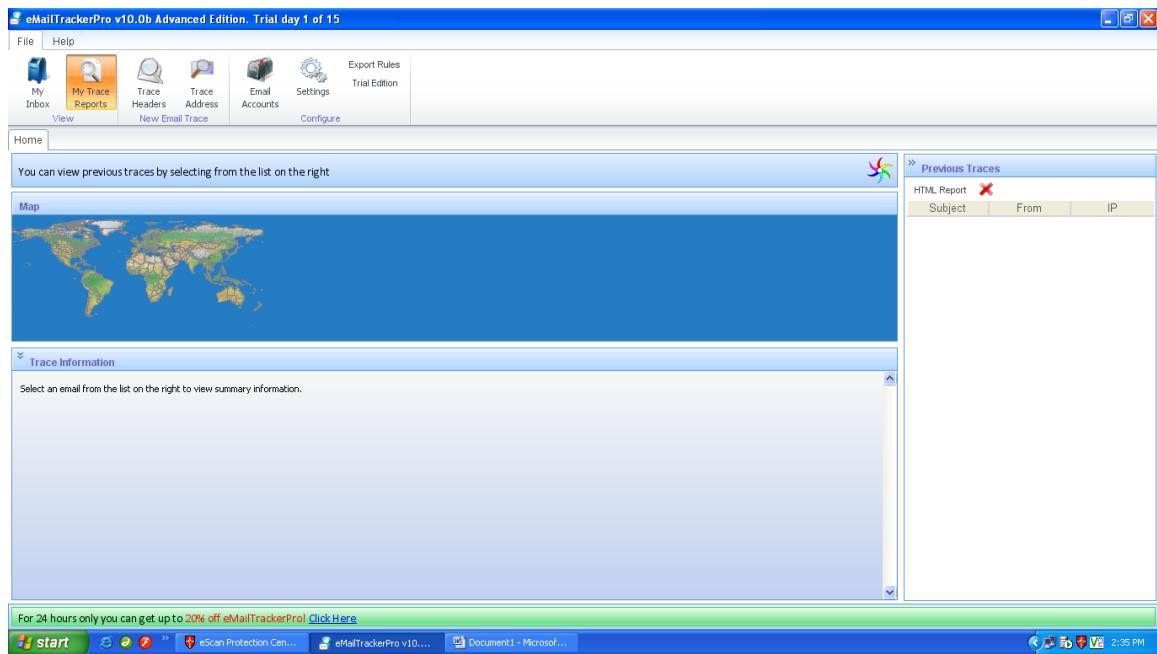
Step 1: Open emailTracker.



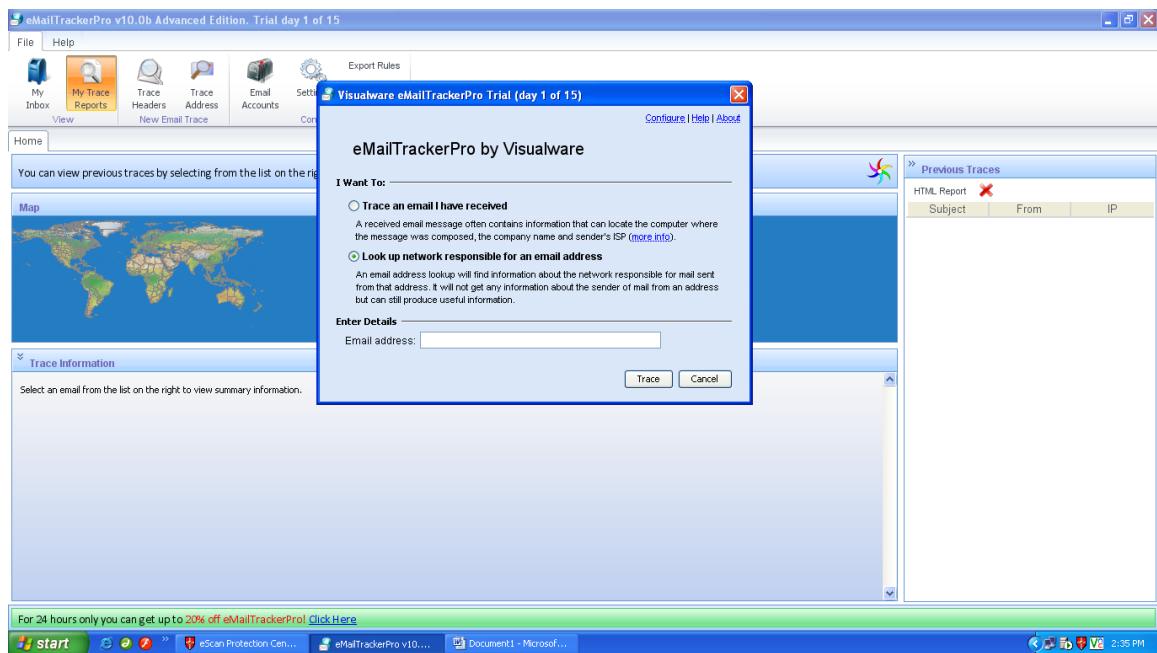
Step 2: Check if there are any reports generated previously.



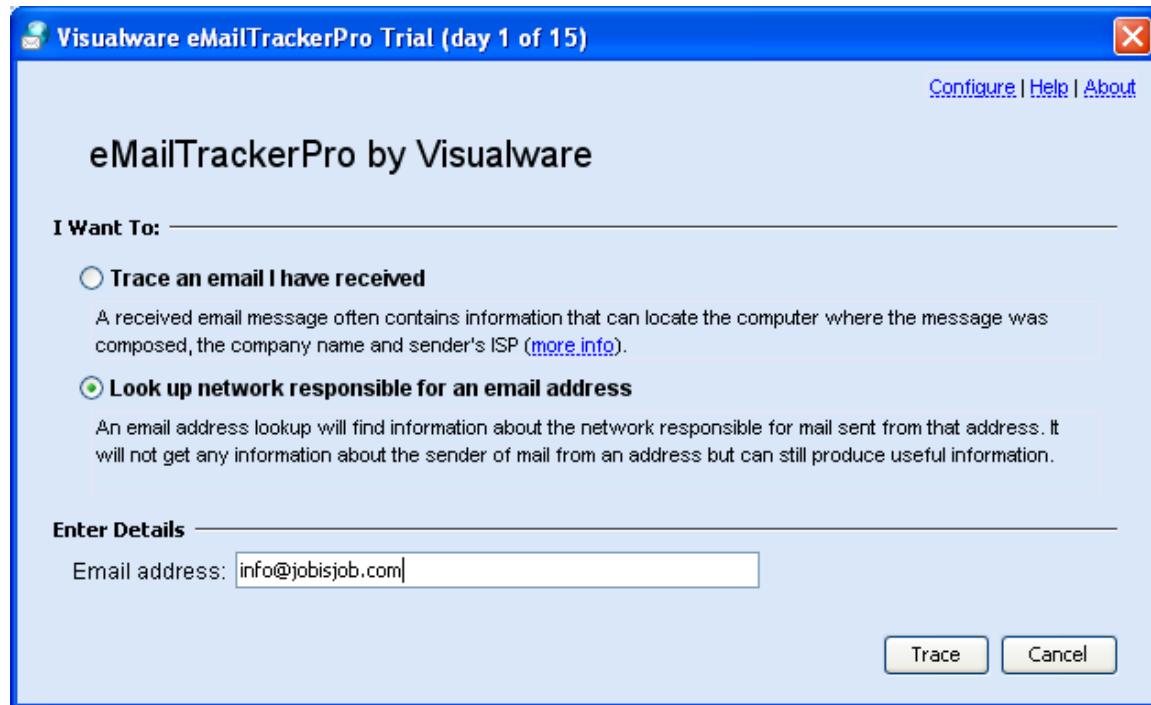
Step 3: Check for My trace Reports.



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.

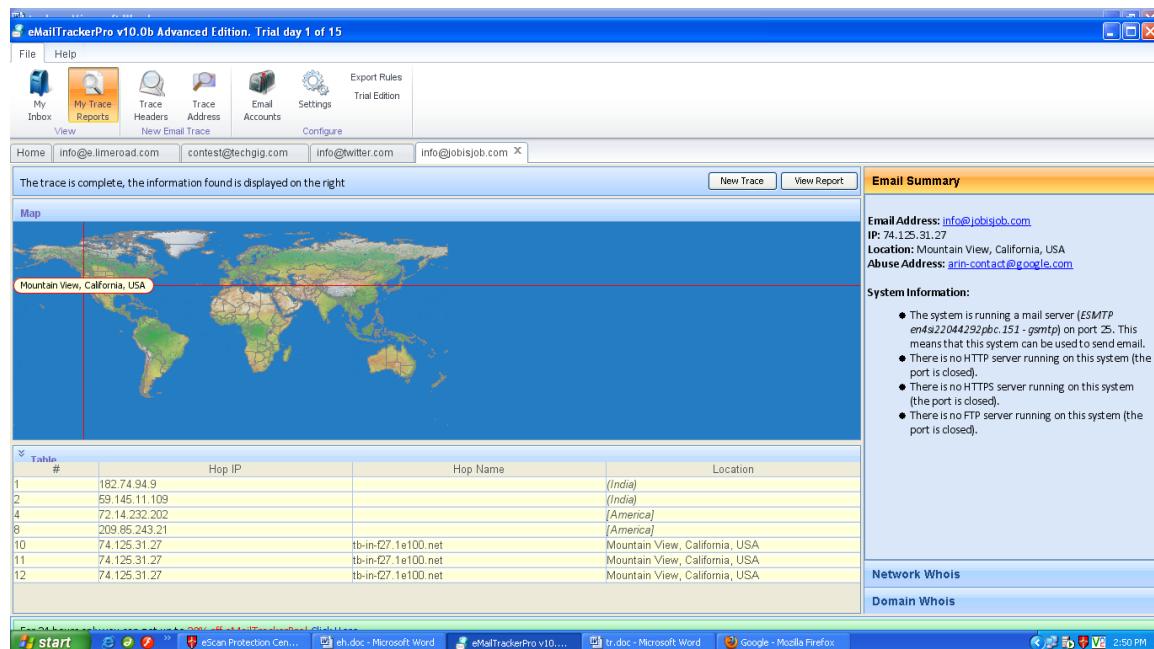


Figure: Location details and email summary.

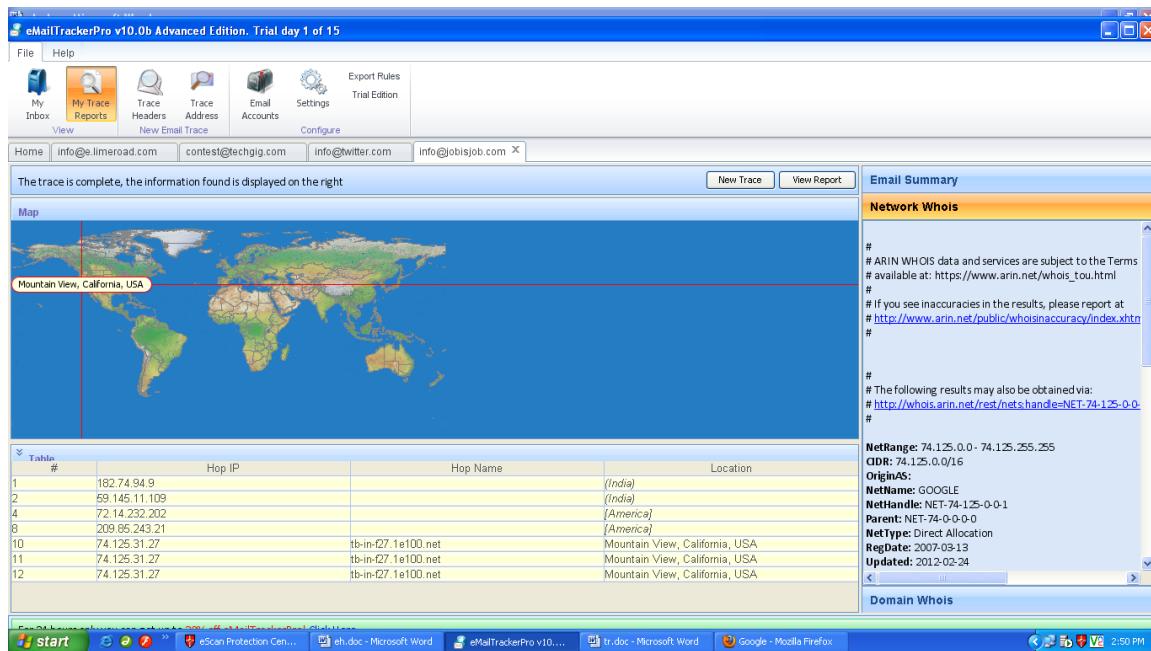


Figure: Location details and network summary.

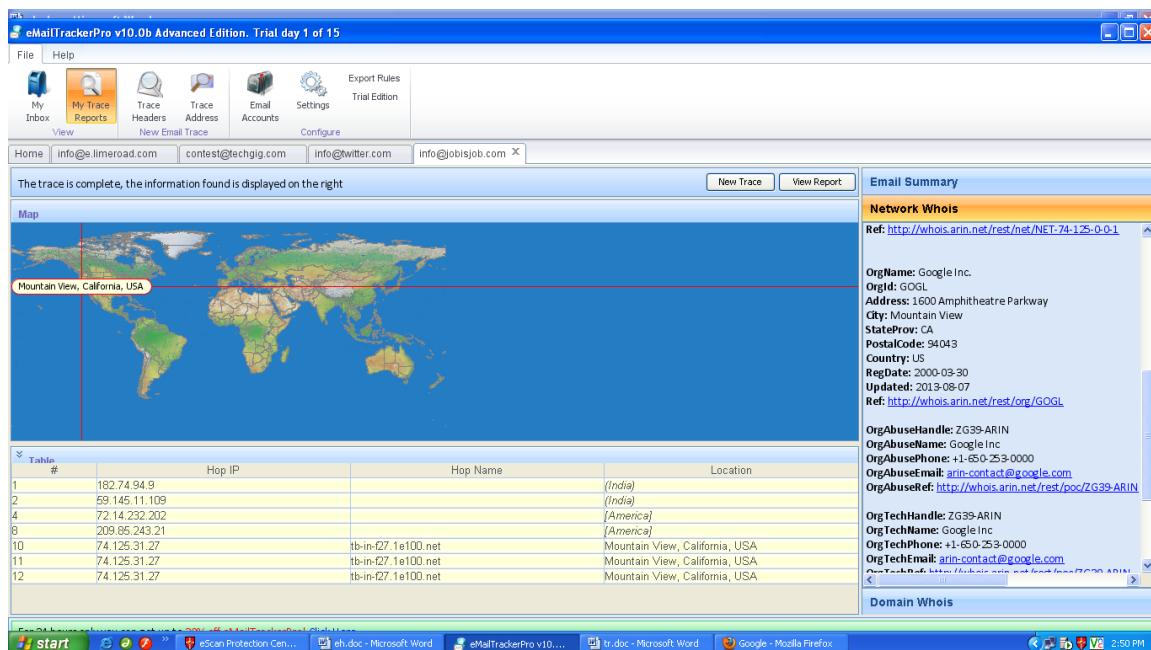


Figure: Location details and network summary.

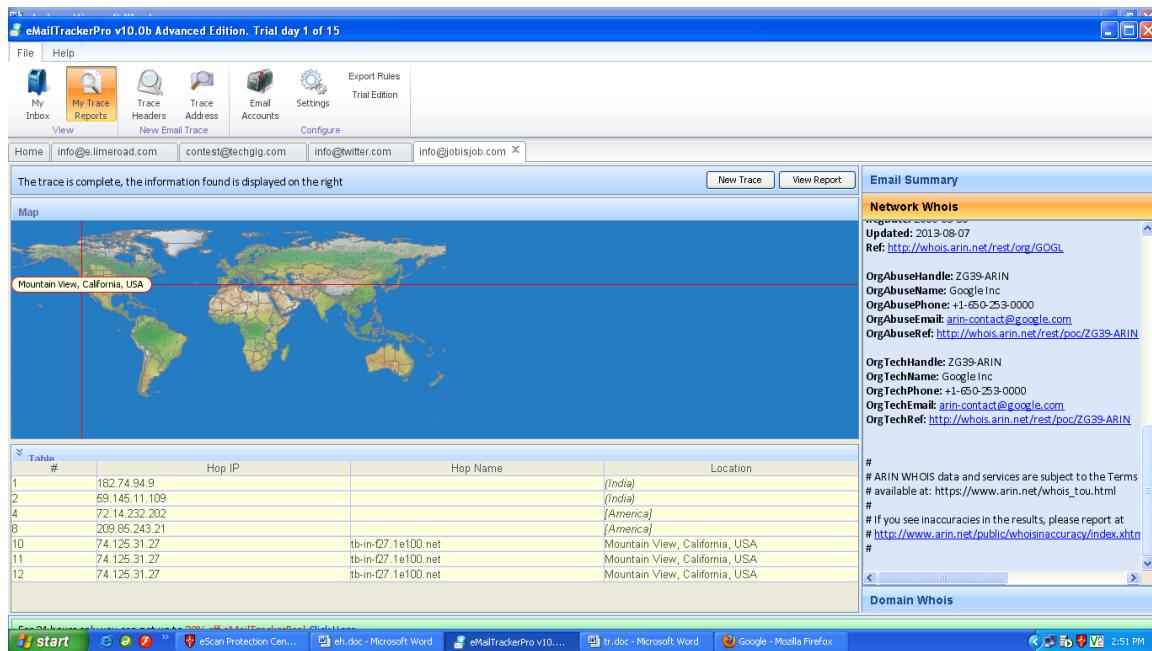


Figure: Location details and network summary.

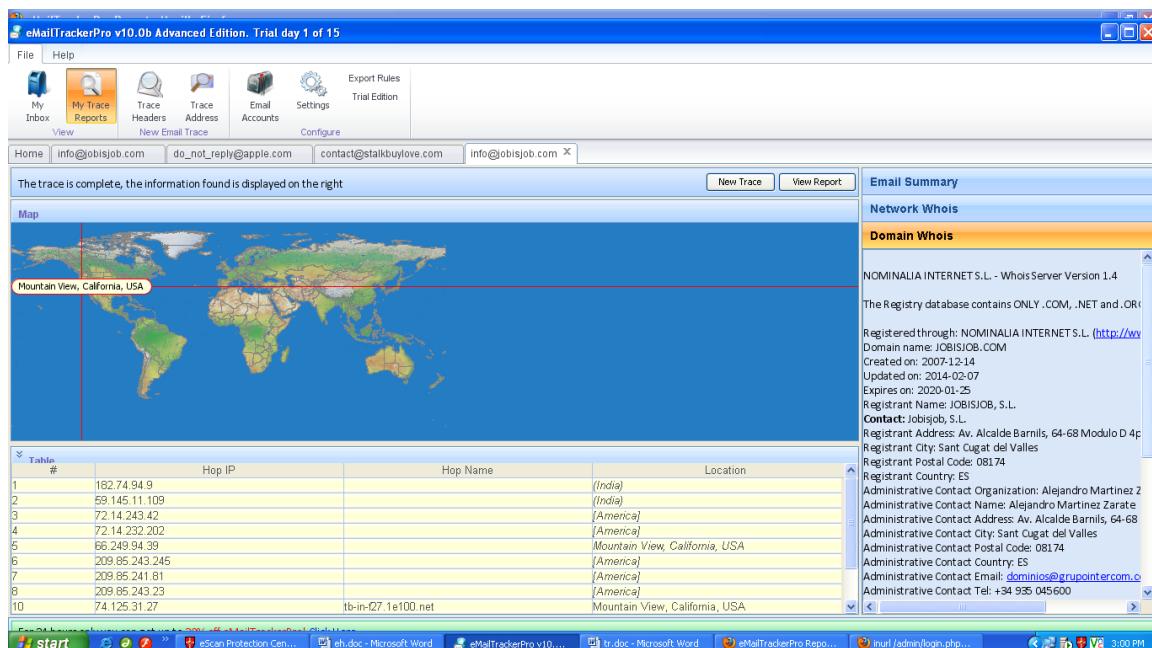


Figure: Location details and domain summary.

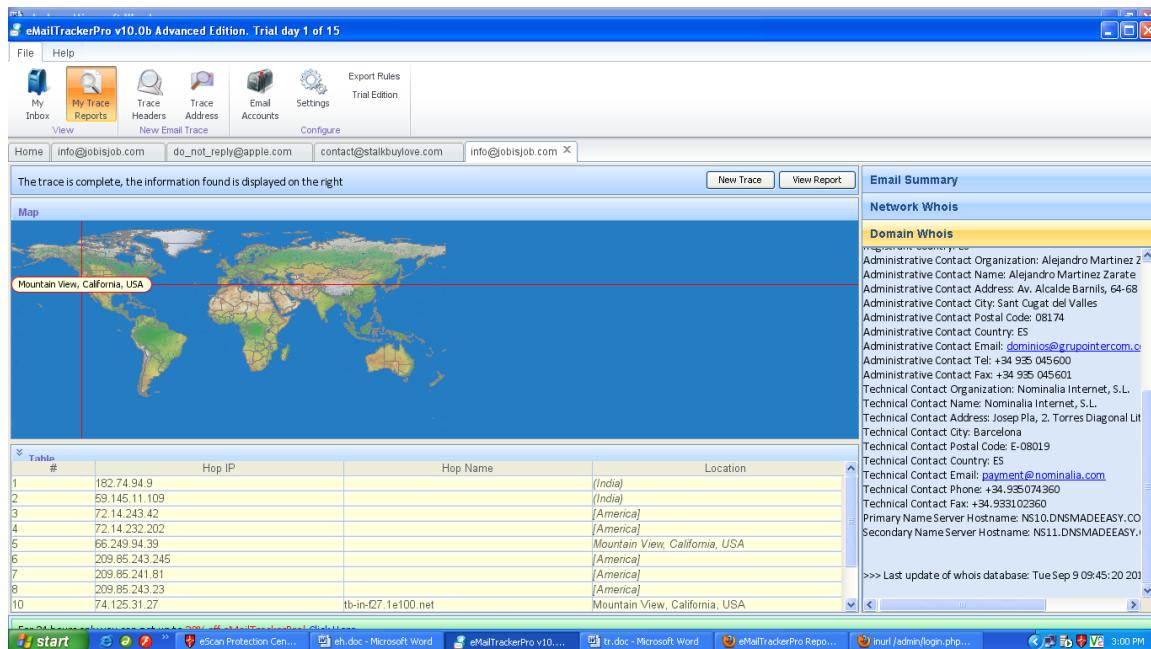


Figure: Location details and domain summary.

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

The screenshot shows a Mozilla Firefox browser window displaying the eMailTrackerPro Report. The title bar reads 'eMailTrackerPro Report - Mozilla Firefox'. The main content area is titled 'eMailTrackerPro® Report' and includes a 'How to Report Email Abuse' link. Below this is a 'Identification Report for 74.125.31.27' section. It contains a note about the trial period and a warning about email spoofing. It then provides network and domain contact information for the IP address 74.125.31.27, which is identified as being located in Mountain View, California, USA. The network contact information lists Google Inc. as the owner, with an email address and phone number. The domain contact information lists administrative contact details for a company in Spain.

eMailTrackerPro Report - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Google eMailTrackerPro Report

File:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html

94043 US

City: San Jose, California, USA 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: 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

start eScan Protection Cen... eh.doc - Microsoft Word eMailTrackerPro v10... tr.doc - Microsoft Word eMailTrackerPro Repo... inurl /admin/login.php... 3:00 PM

eMailTrackerPro Report - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Google eMailTrackerPro Report

File:///C:/Documents and Settings/Administrator/eMailTrackerPro/V8/reports/report-20140909-1459-6.html

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 domain registration details, which is often the head office location of the Internet Service Provider (ISP). The ISP location often differs from the location of the connection point, 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		<i>India</i>
59.145.11.109		<i>India</i>
72.14.243.42		<i>America</i>
72.14.232.202		<i>America</i>
66.249.94.39		<i>Mountain View, California, USA</i>
209.85.243.245		<i>America</i>
209.85.241.81		<i>America</i>
209.85.243.23		<i>America</i>
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	Domain Owner Information
<i>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)</i>	<i>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.</i>
# # ARIN WHOIS data and services are subject to the	NOMINALIA INTERNET S.L. - Whois Server Version 1.4

start eScan Protection Cen... eh.doc - Microsoft Word eMailTrackerPro v10... tr.doc - Microsoft Word eMailTrackerPro Repo... inurl /admin/login.php... 3:01 PM

eMailTrackerPro Report - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Google 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
OrgAbuseName: Google Inc.

Registered through: NOMINALIA INTERNET S.L.
(http://www.nominalia.com)
Domain name: JOBISJOB.COM
Created on: 2007-12-01
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 Zárate
Administrative Contact Name: Alejandro Martinez Zárate
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: dominicos@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: NC10.DCNMADREACIY.COM
```

start eScan Protection Cen... eh.doc - Microsoft Word eMailTrackerPro v10... tr.doc - Microsoft Word eMailTrackerPro Repo... inurl /admin/login.php... 3:01 PM

eMailTrackerPro Report - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Google 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	>>> 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 a15si22239089pd).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 eScan Protection Cen... eh.doc - Microsoft Word eMailTrackerPro v10... tr.doc - Microsoft Word eMailTrackerPro Repo... inurl /admin/login.php... 3:01 PM

Scan the network using the following tools:

i. Hping2 / Hping3

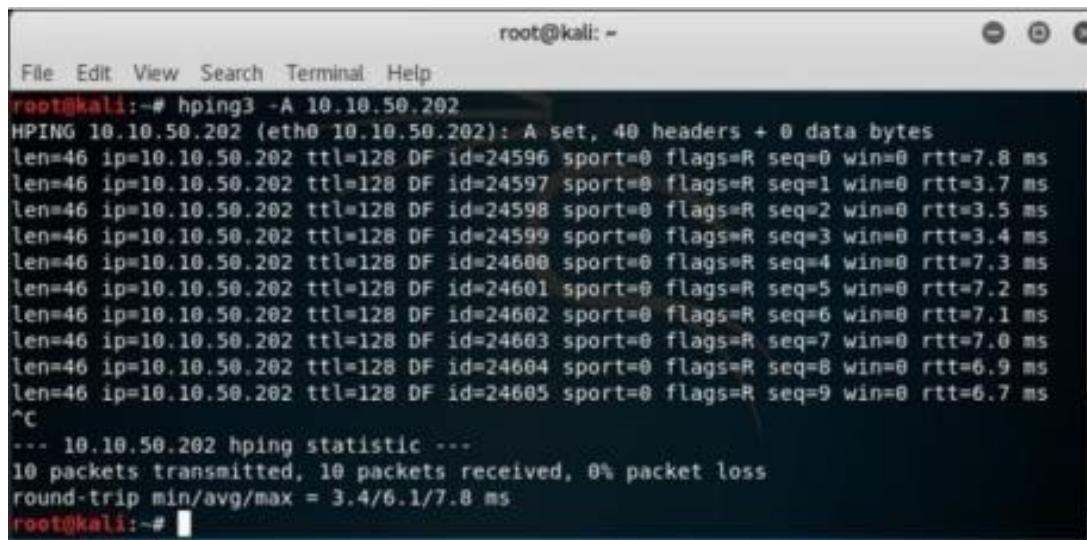
Hping is a command-line TCP/IP packet assembler and analyzer tool that is used to send customized TCP/IP packets and display the target reply as ping command display the ICMP Echo Reply packet from targeted host. Hping can also handle fragmentation, arbitrary packets body, and size and file transfer.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



The screenshot shows a terminal window with the following content:

```
root@kali:~# hping3 -A 192.168.0.1
HPING 192.168.0.1 (eth0 192.168.0.1): A set, 40 headers + 0 data bytes
len=40 ip=192.168.0.1 ttl=128 DF id=24596 sport=0 flags=R seq=0 win=0 rtt=7.8 ms
len=40 ip=192.168.0.1 ttl=128 DF id=24597 sport=0 flags=R seq=1 win=0 rtt=3.7 ms
len=40 ip=192.168.0.1 ttl=128 DF id=24598 sport=0 flags=R seq=2 win=0 rtt=3.5 ms
len=40 ip=192.168.0.1 ttl=128 DF id=24599 sport=0 flags=R seq=3 win=0 rtt=3.4 ms
len=40 ip=192.168.0.1 ttl=128 DF id=24600 sport=0 flags=R seq=4 win=0 rtt=7.3 ms
len=40 ip=192.168.0.1 ttl=128 DF id=24601 sport=0 flags=R seq=5 win=0 rtt=7.2 ms
len=40 ip=192.168.0.1 ttl=128 DF id=24602 sport=0 flags=R seq=6 win=0 rtt=7.1 ms
len=40 ip=192.168.0.1 ttl=128 DF id=24603 sport=0 flags=R seq=7 win=0 rtt=7.0 ms
len=40 ip=192.168.0.1 ttl=128 DF id=24604 sport=0 flags=R seq=8 win=0 rtt=6.9 ms
len=40 ip=192.168.0.1 ttl=128 DF id=24605 sport=0 flags=R seq=9 win=0 rtt=6.7 ms
^C
--- 192.168.0.1 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 3.4/6.1/7.8 ms
root@kali:~#
```

- To create SYN scan against different ports:

```
root@kali:~# hping3 -S 1-600 -S 192.168.0.1
```

```
root@kali:~# hping3 -B 1-600 -S 10.10.50.202
Scanning 10.10.50.202 (10.10.50.202), port 1-600
600 ports to scan, use -V to see all the replies
+-----+
|port| serv name | flags | ttl| id | win | len |
+-----+
 135 loc-srv : .S..A... 128 30572 8192   46
 139 netbios-ssn: .S..A... 128 31596 8192   46
 445 microsoft-d: .S..A... 128 35180 8192   46
 554 rtsp    : .S..A... 128 44652 8192   46
All replies received. Done.
Not responding ports:
root@kali:~#
```

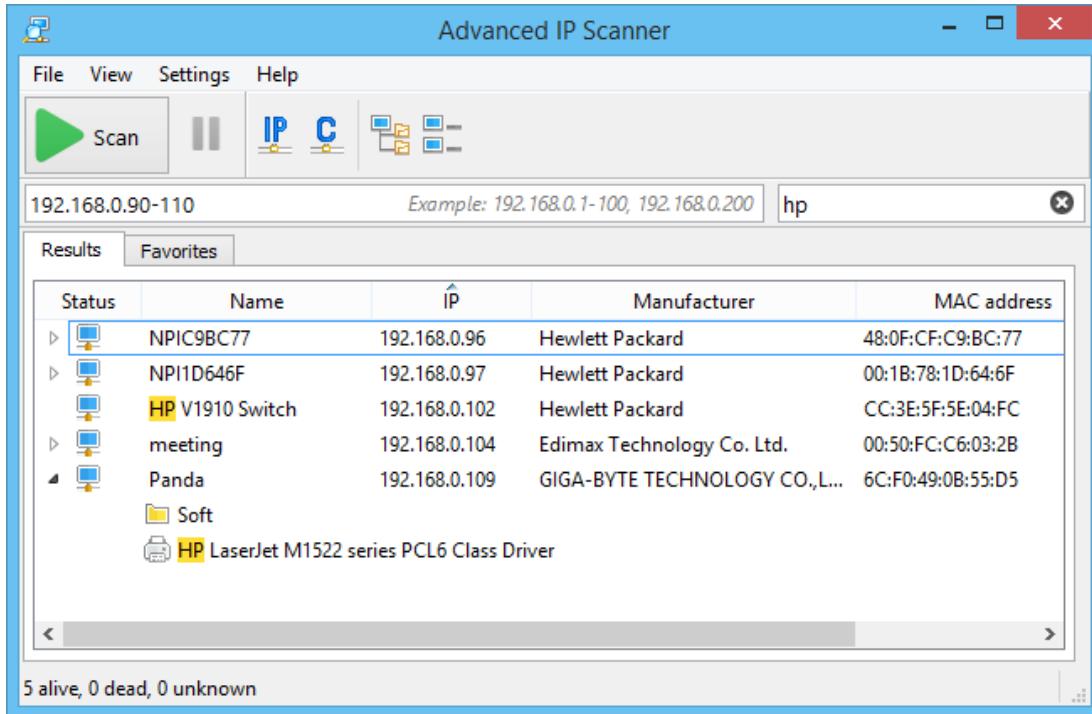
- To create a packet with FIN, URG, and PSH flags sets

```
root@kali:~# hping3 -F -P -U 10.10.50.202
```

```
root@kali:~# hping3 -F -P -U 10.10.50.202
HPING 10.10.50.202 (eth0 10.10.50.202): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.50.202 ttl=128 DF id=28237 sport=0 flags=RA seq=0 win=0 rtt=3.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28238 sport=0 flags=RA seq=1 win=0 rtt=3.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28239 sport=0 flags=RA seq=2 win=0 rtt=3.5 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28240 sport=0 flags=RA seq=3 win=0 rtt=3.4 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28241 sport=0 flags=RA seq=4 win=0 rtt=3.3 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28242 sport=0 flags=RA seq=5 win=0 rtt=3.2 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28243 sport=0 flags=RA seq=6 win=0 rtt=7.1 ms
^C
--- 10.10.50.202 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 3.2/4.0/7.1 ms
root@kali:~#
```

ii. Advanced IP Scanner

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



iii. Angry IP Scanner

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many other features.

It is widely used by network administrators and just curious users around the world, including large and small enterprises, banks, and government agencies.

It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well.

IP Range - Angry IP Scanner				
Scan Go to Commands Favorites Tools Help				
IP Range:		195.80.116.0	to	195.80.116.255
Hostname:		e-estonia.com	IP↑	/24
				Start
IP	Ping	Hostname	Ports [3+]	Web detect
195.80.116.226	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.227	9 ms	[n/a]	80,443	Resin/4.0.37
195.80.116.228	10 ms	[n/a]	80,443	[n/a]
195.80.116.229	9 ms	[n/a]	80,443	Apache
195.80.116.230	13 ms	mx3.rmk.ee	[n/a]	[n/a]
195.80.116.231	10 ms	mx4.rmk.ee	[n/a]	[n/a]
195.80.116.232	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.233	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.234	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.235	9 ms	[n/a]	80,443	[n/a]
195.80.116.236	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.237	[n/a]	[n/s]	[n/s]	[n/s]

iv. Masscan

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

Scan for a selection of ports (-p22,80,445) across a given subnet (192.168.1.0/24):

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

```
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 coordinates the use of numerous other open-source network tools, with the aim of gathering as much network information as possible in clear, easy-to-use formats. The core scanning engine finds and identifies network services, the modules test or enumerate those services, and the Neet Shell provides an integrated environment for processing the results and exploiting known vulnerabilities.

As such, it sits somewhere between manually running your own port scans and subsequent tests, and running a fully automated vulnerability assessment (VA) tool. It has many options which allow the user to tune the test parameters for network scanning in the most efficient and practical way.

```
r00t@r00t-Q470C-500P4C: ~/KaliPloit/neet 148x51
User Manuals
NEET(1)                               NEET(1)

NAME
    NEET - Network Enumeration and Exploitation Tool

SYNOPSIS
    neet [OPTIONS] <TARGETS> [<TARGET_RANGE>, <TARGET_RANGE> ...]

DESCRIPTION
    neet is a flexible, multi-threaded network penetration test tool which sits somewhere between manually running your own port scans and subsequent tests, and running a fully automated VA tool. It allows the user to fine-tune the test parameters, and is extensible by means of test modules and plugins. A shell ( neetsh(1) ) is included to help make sense of the results more quickly, and is also used to control the built-in exploitation framework and other aspects of the test.

ADDRESS and PORT SPECIFICATION
    IP addresses can be specified in a couple of ways - range notation (192.168.1.1-254) or CIDR notation (192.168.1.0/24). CIDR notation will automatically exclude the network and broadcast addresses. Nested ranges are also accepted - 192.168.1.10-1.20 for example.

    Port ranges can be included and excluded, and specified in comma and hyphen-separated form. For example, 1,2,3,4-20,50-60,61-70 is acceptable (though inefficient), and will be internally mapped by neet to 1-20,50-70. The default ranges are 1-65535 for TCP scans, and 1-10000 for UDP. Specification of an initial inclusive range on the command line will override these defaults; -t 1-5000 will change the TCP scan range from 1-65535 to 1-5000 for example. Further specifications will then add to this range; -t 6000-8000,10000-11000 will make the total TCP scan range equal to 1-5000,6000-8000,10000-11000.

OPTIONS
    The options and target hosts can specified in any order. The only rules are that parameters must immediately follow those options which require them, and that targets can be specified by IP address only - no hostnames will be accepted.

    -h, --help
        Displays usage information.

    Target HOST Specification

    -X, --exclude-host <IP_Range>
        Exclude this IP address range (may be specified more than once).

    -f, --include-hosts <File>
        Specify file containing a list of target IP addresses (may be specified more than once).

    -F, --exclude-hosts <File>
        Specify file containing a list of target IP addresses to be excluded (may be specified more than once).

    -L, --list-targets
        Print the list of targets to STDOUT, then exit.

    -O, --exclude-os
        Exclude hosts detected as running the specified operating system (may be specified more than once).

    Target and Service DISCOVERY

Manual page neet(1) line 1/200 23% (press h for help or q to quit)
```

vi. CurrPorts

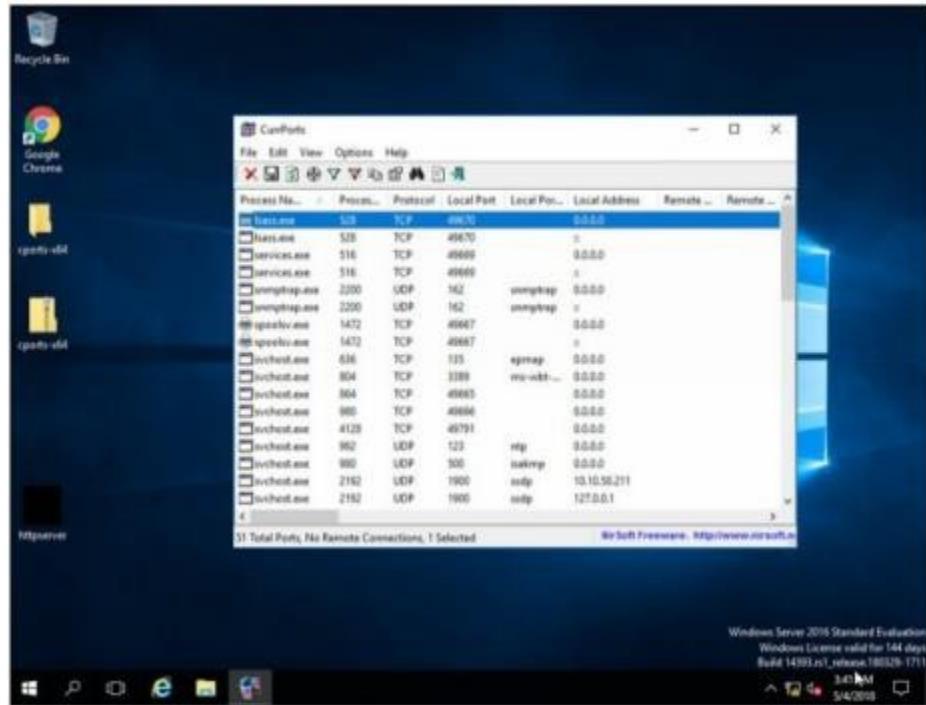
Case Study: Using the Previous lab, we are going to re-execute HTTP Remote Access Trojan (RAT) on Windows 12 machine (10.10.50.211) and observed the TCP/IP connections to detect and kill the connection.

Topology:

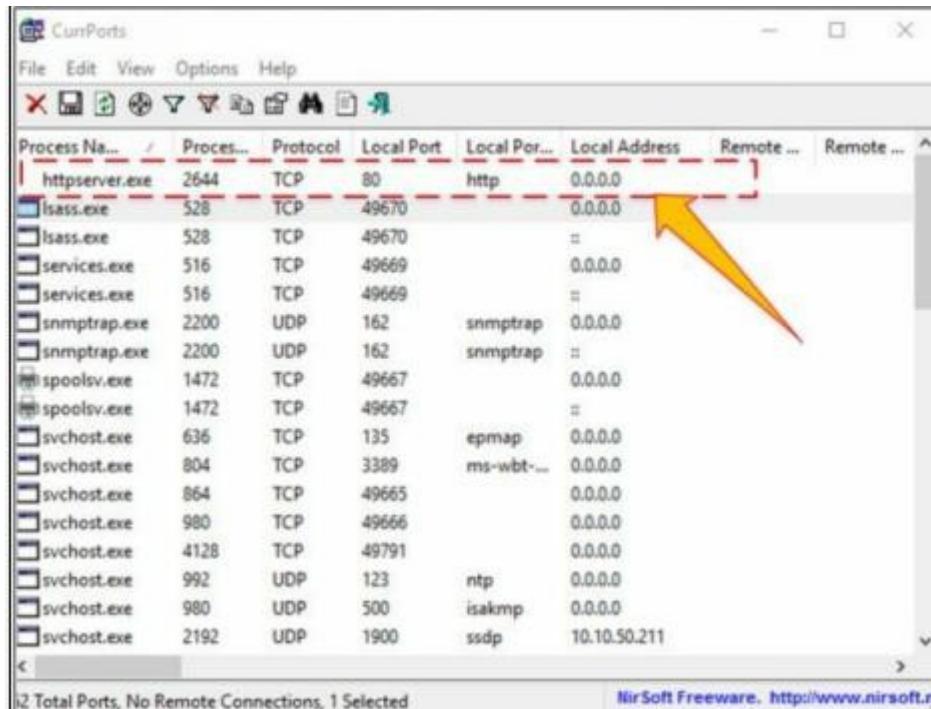


Configuration:

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



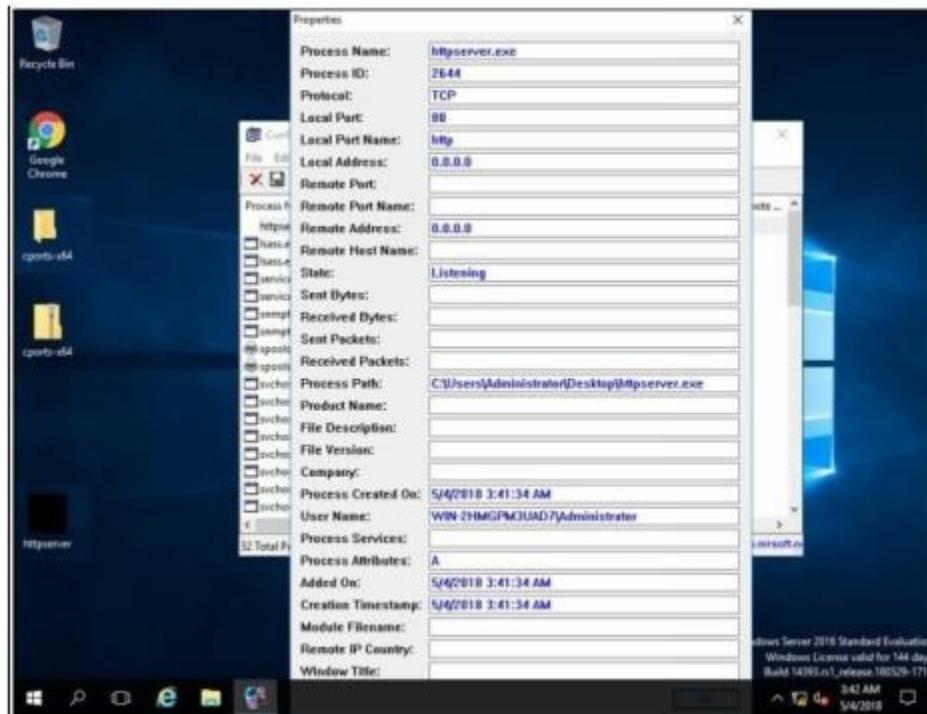
2.Run the HTTP Trojan created in the previous lab



The new process is added to the list.

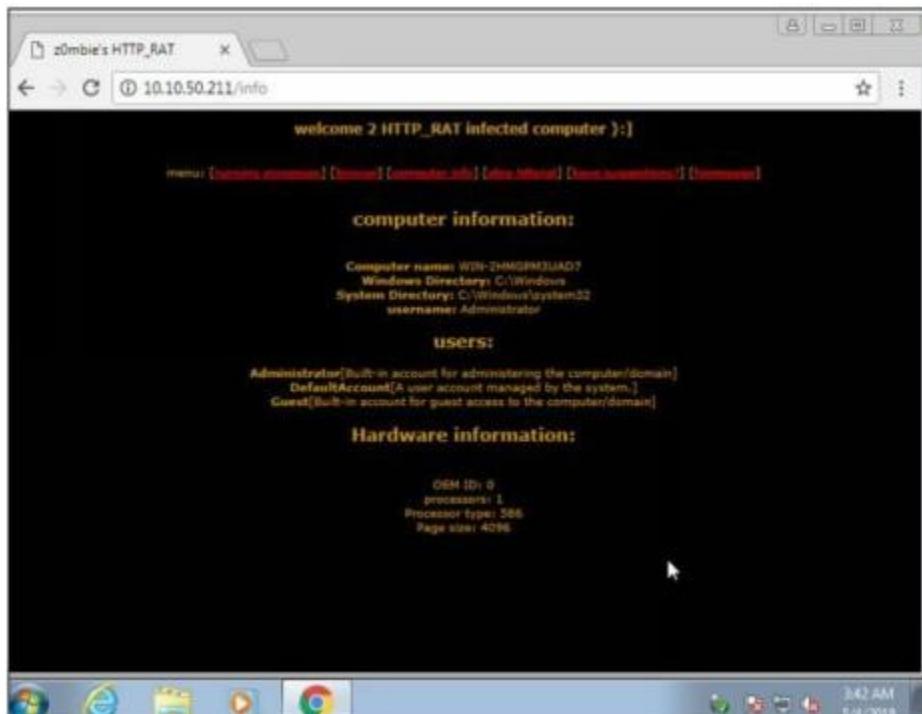
You can observe the process name, Protocol, Local and remote port and IP address information.

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



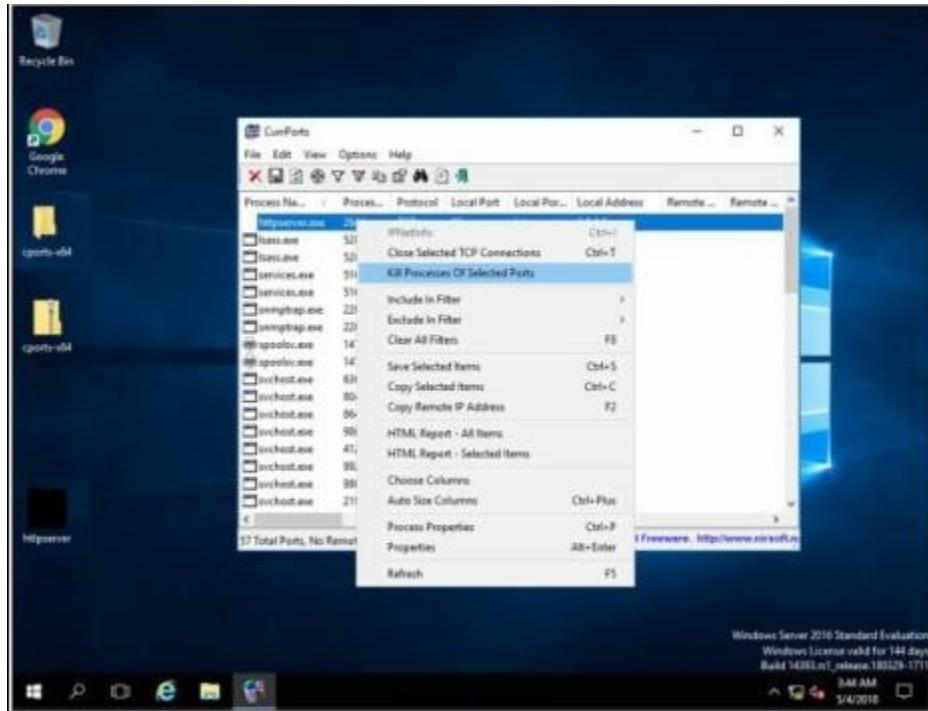
Properties are showing more details about tcp connection.

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

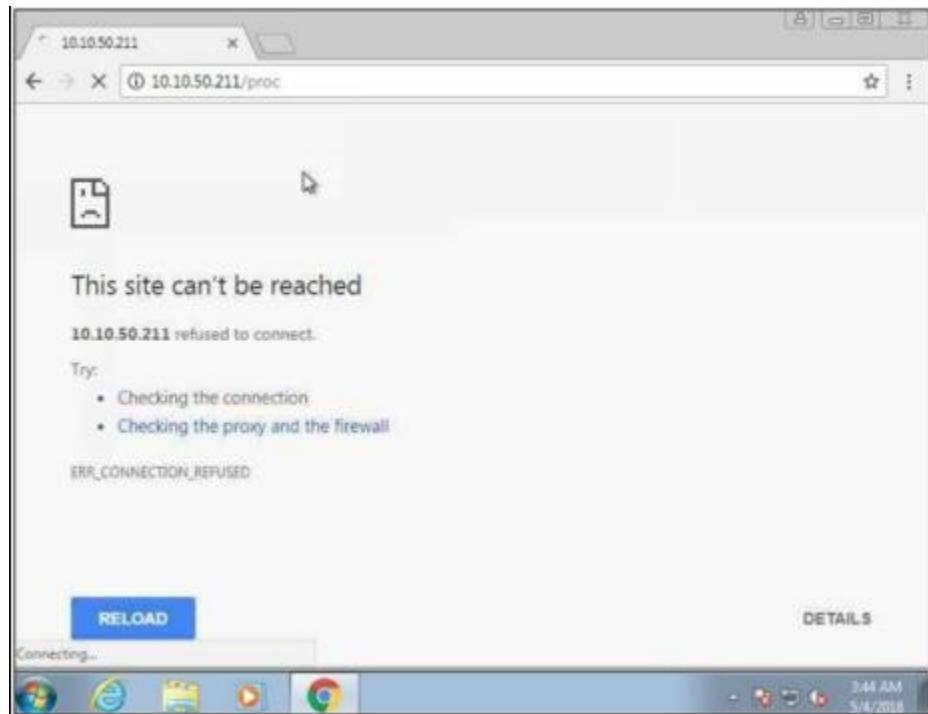


Connection successfully established.

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



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



vii. Colasoft Packet Builder

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

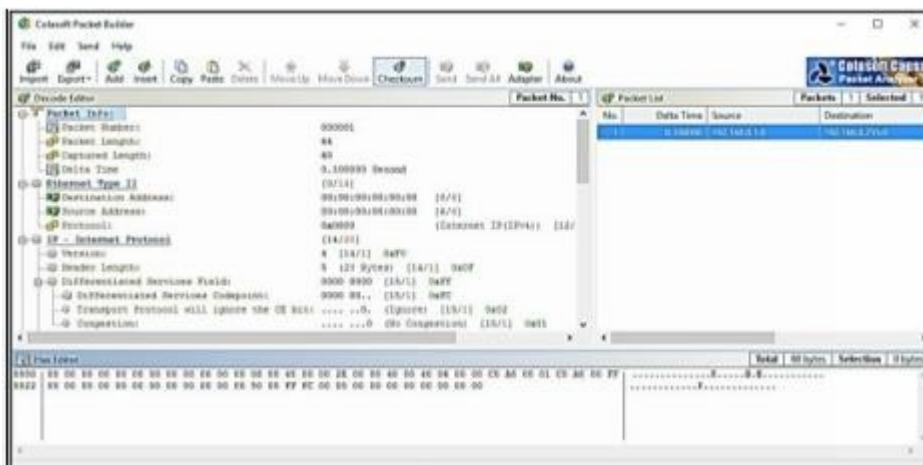
Customized Network packets can penetrate the network for attacks. Customization can also be used to create fragmented packets. You can download the software from www.colasoft.com.



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

Available options are:-

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



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

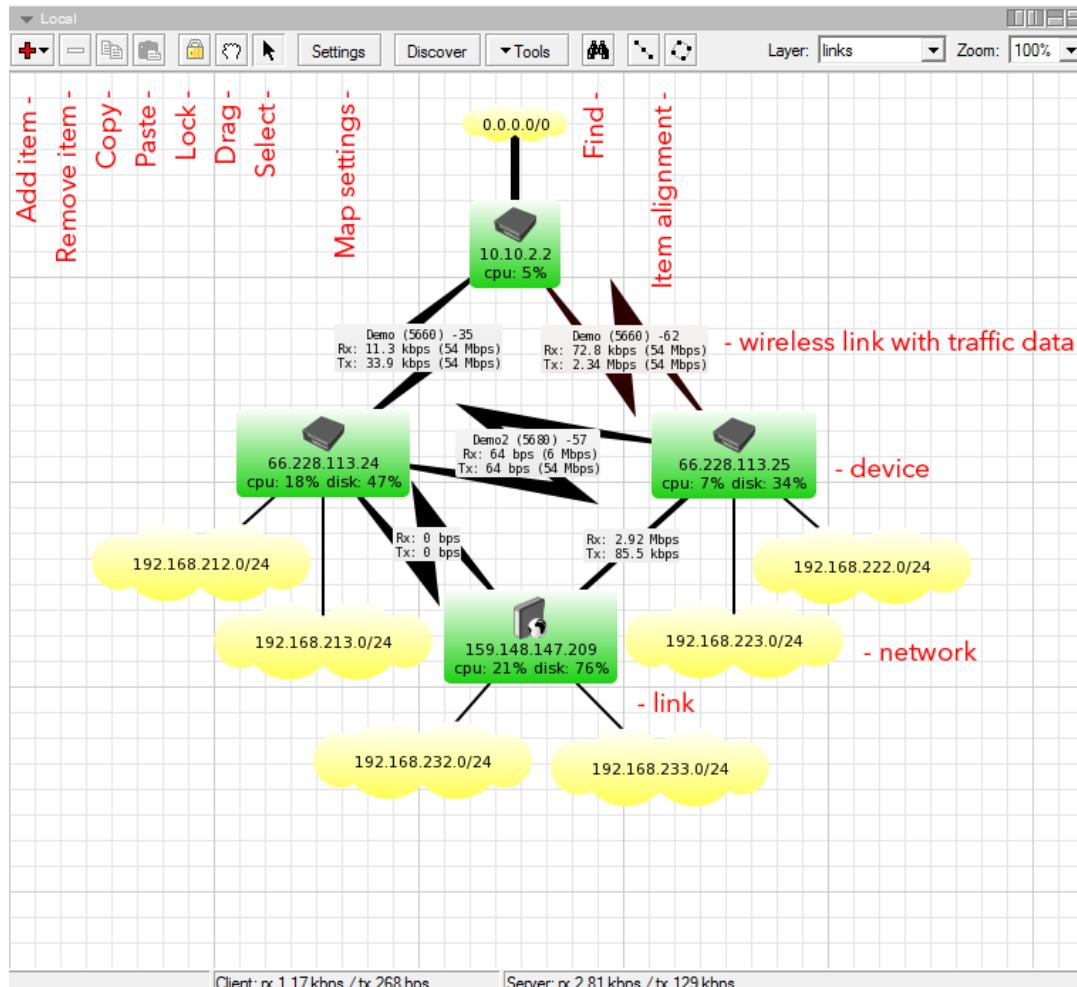
viii. The Dude

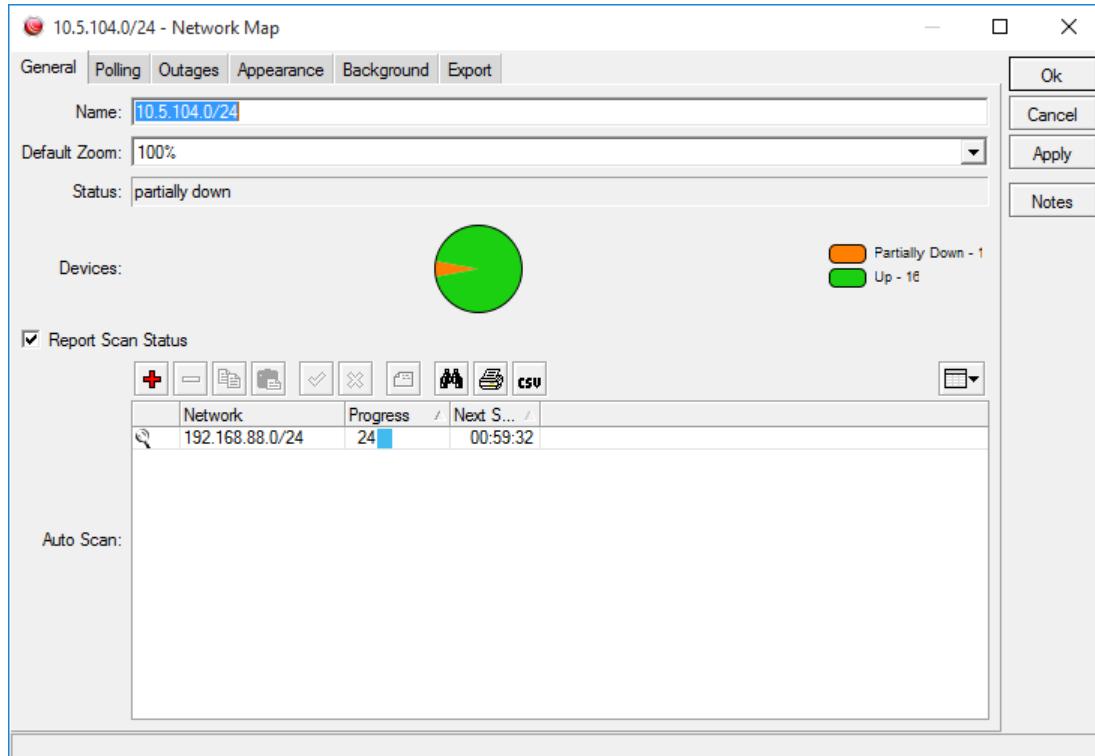
The Dude network monitor is a new application by MikroTik which can dramatically improve the way you manage your network environment. It will automatically scan all devices within

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:

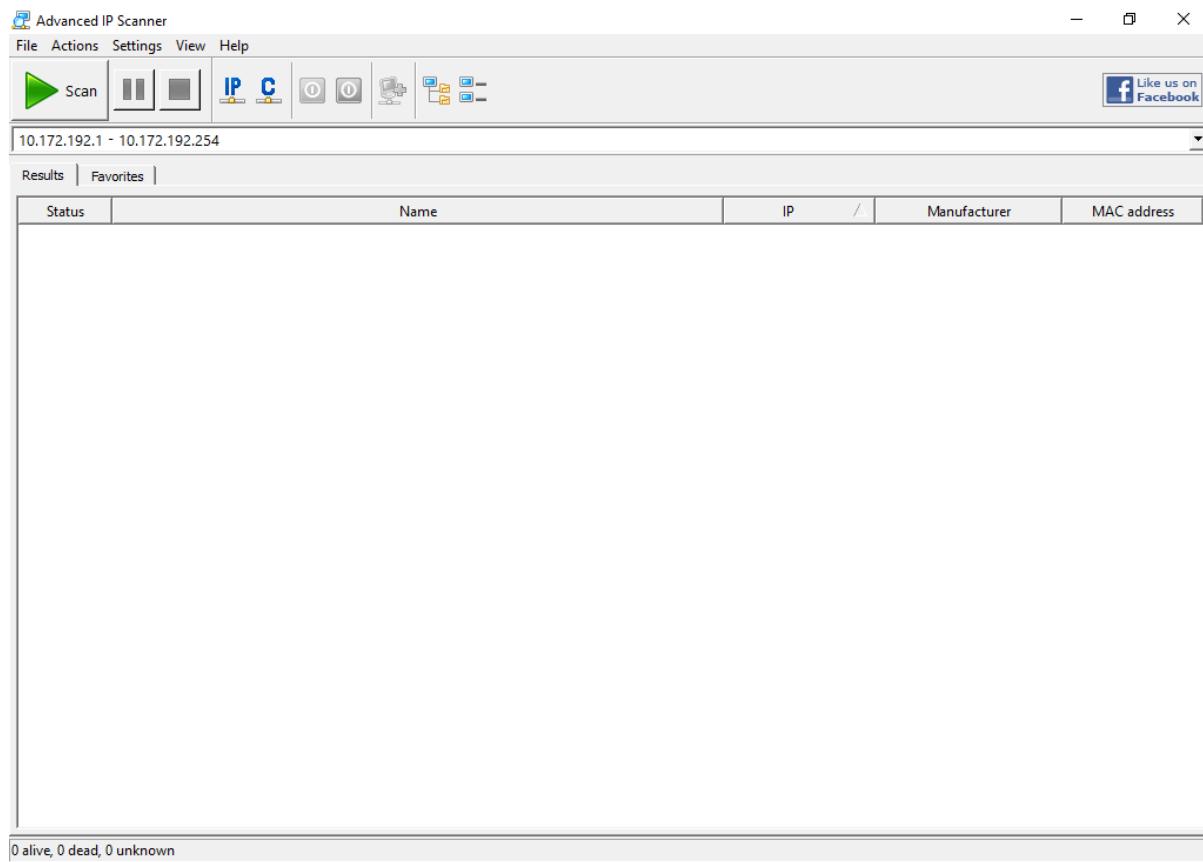
- Auto network discovery and layout
- Discovers any type or brand of device
- Device, Link monitoring, and notifications
- Includes SVG icons for devices, and supports custom icons and backgrounds
- Easy installation and usage
- Allows you to draw your own maps and add custom devices
- Supports SNMP, 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



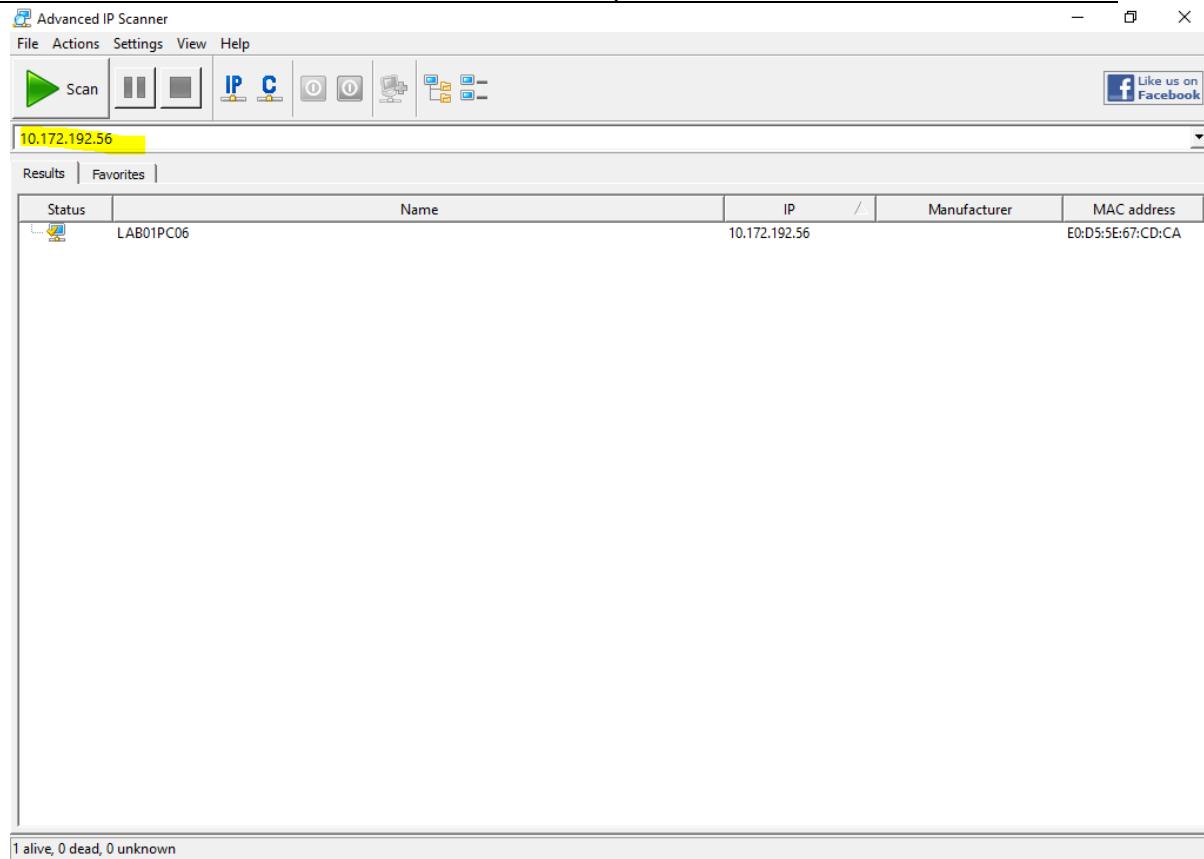


10.5.104.0/24 - Network Map						
General Polling Outages Appearance Background Export						
<input type="button" value="Remove Resolved"/> <input type="button" value="New"/> Status: <select>all</select> Device: <select>all</select> Service: <select>all</select> <input type="button" value="Print"/>						
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		
resolved	Dec/02 11:22:34	00:03:27	nine.lan	ftp		

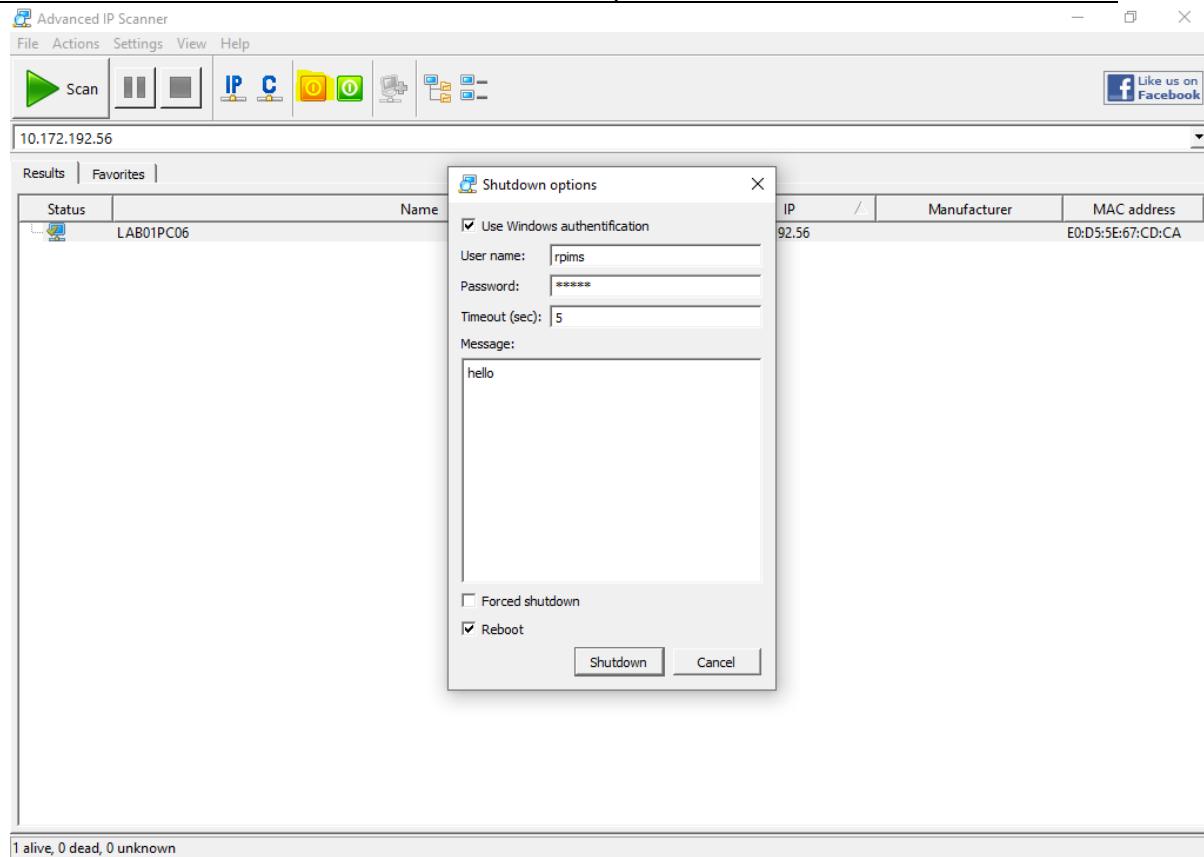
Advance ip scanner:



Insert ihte desired ip to be scan:



The click o the turnoff icon to shutdown the system:



CurrPorts:

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote ...	Remote ...	Remote Address	Remote Host Name	S ^
System	4	TCP	445	microsoft-ds	10.172.192.51	52996		10.172.192.69	DESKTOP-AGOAK7D	E
System	4	TCP	445	microsoft-ds	10.172.192.51	53310		10.172.192.56	LAB01PC06	E
System	4	TCP	445	microsoft-ds	10.172.192.51	53334		10.172.192.56	LAB01PC06	E
System	4	TCP	445	microsoft-ds	10.172.192.51	53335		10.172.192.56	LAB01PC06	E
System	4	TCP	445	microsoft-ds	10.172.192.51	53336		10.172.192.56	LAB01PC06	E
System	4	TCP	445	microsoft-ds	10.172.192.51	55949		10.172.192.71	LAB01COMP21	E
System	4	TCP	445	microsoft-ds	10.172.192.51	56610		10.172.192.71	LAB01COMP21	E
System	4	TCP	445	microsoft-ds	10.172.192.51	56611		10.172.192.71	LAB01COMP21	E
System	4	TCP	445	microsoft-ds	10.172.192.51	59265		10.172.192.55	LAB01PC05	E
System	4	TCP	445	microsoft-ds	10.172.192.51	59266		10.172.192.55	LAB01PC05	E
System	4	TCP	445	microsoft-ds	10.172.192.51	64301		10.172.192.55	LAB01PC05	E
System	4	TCP	445	microsoft-ds	10.172.192.51	64303		10.172.192.55	LAB01PC05	E
System	4	TCP	445	microsoft-ds	10.172.192.51	56609		10.172.192.71	LAB01COMP21	E
System	4	TCP	445	microsoft-ds	10.172.192.51	51018		10.172.192.58	DESKTOP-KCSVTMK	E
System	3188	TCP	808		0.0.0.0			0.0.0.0	L	
System	4	TCP	2323		127.0.0.1			0.0.0.0	L	
System	3428	TCP	3790		0.0.0.0			0.0.0.0	L	
System	4776	TCP	5040		0.0.0.0			0.0.0.0	L	
System	8204	TCP	7337		127.0.0.1			0.0.0.0	L	
System	3944	TCP	7680	ms-do	10.172.192.51	51096		10.172.192.58	DESKTOP-KCSVTMK	E
System	3944	TCP	7680	ms-do	10.172.192.51	51587		10.172.192.63	DESKTOP-POR9JUC	E
System	3944	TCP	7680	ms-do	10.172.192.51	55402		10.172.192.89	DESKTOP-PUQE6RH	E
System	3944	TCP	7680	ms-do	10.172.192.51	63119		10.172.192.70	DESKTOP-NENDCPU	E
System	3944	TCP	7680	ms-do	10.172.192.51	50154		10.172.192.86	DESKTOP-E8JBHKN	E
System	3264	TCP	27017		127.0.0.1			0.0.0.0	L	
System	848	TCP	49664		0.0.0.0			0.0.0.0	L	
System	760	TCP	49665		0.0.0.0			0.0.0.0	L	
System	1424	TCP	49666		0.0.0.0			0.0.0.0	L	
System	1132	TCP	49667		0.0.0.0			0.0.0.0	L	
System	2928	TCP	49668		0.0.0.0			0.0.0.0	L	
System	2316	TCP	49669		0.0.0.0			0.0.0.0	L	

163 Total Ports, 51 Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

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

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>

The screenshot shows the Zenmap interface with the target set to 192.168.0.109. The 'Services' tab is selected, displaying the following Nmap output:

```
nmap -O -v 192.168.0.109
Nmap scan report for 192.168.0.109
Host is up (0.0028s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
MAC Address: [REDACTED] (Device type: general purpose)
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::= cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Uptime guess: 50.139 days (since Tue Dec 05 20:51:59 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
```

ii. NetBIOS Enumeration Tool

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

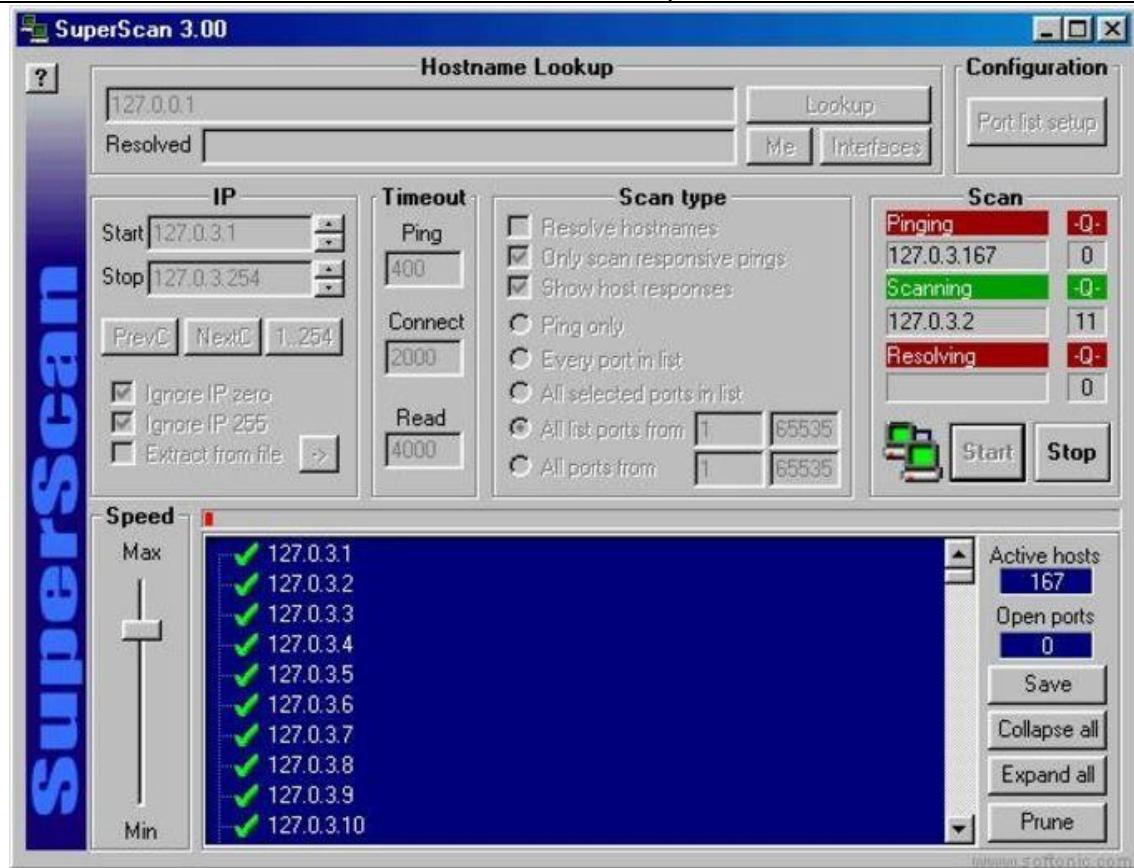
```

[~] (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

```

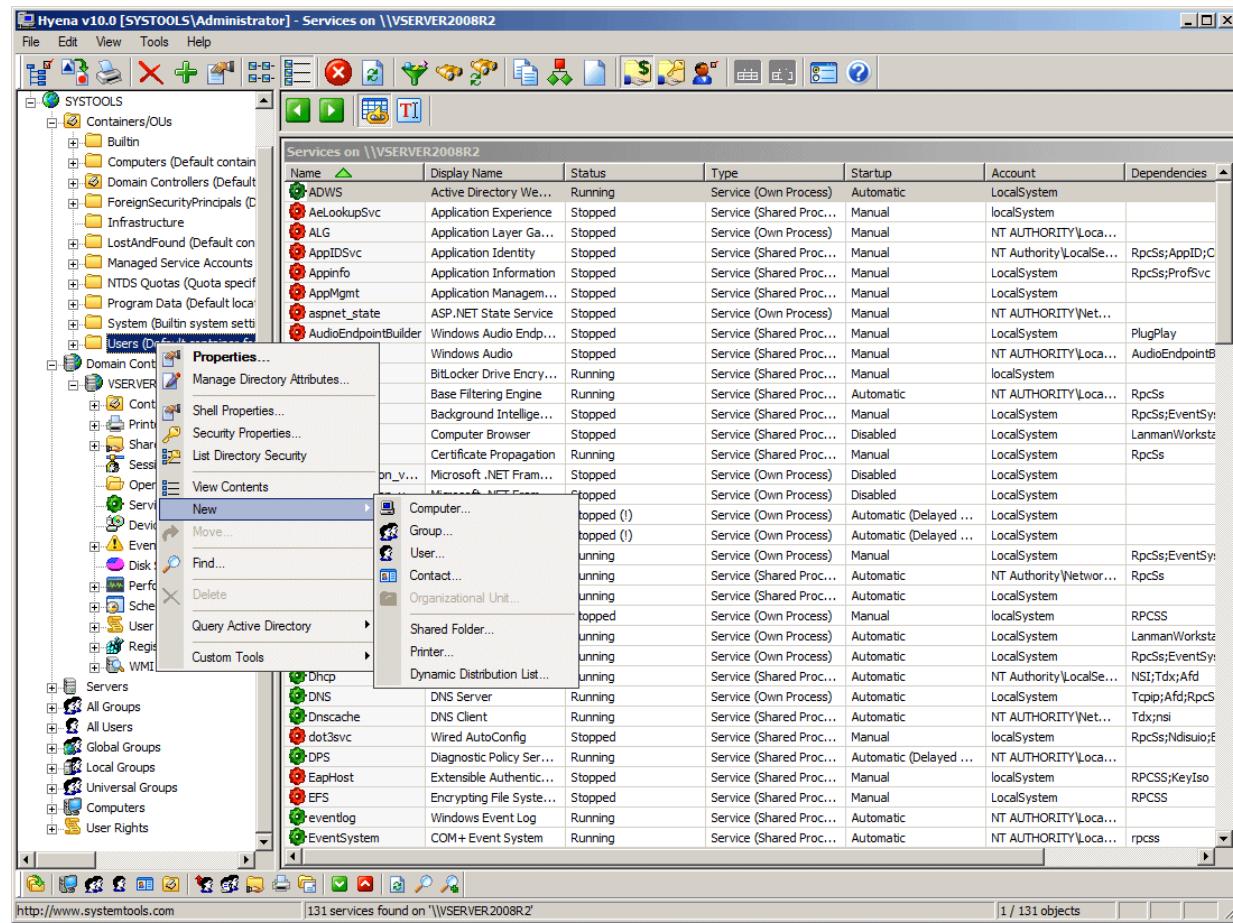
iii. SuperScan

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.



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.

SoftPerfect Network Scanner																																																																															
File View Actions Options Bookmarks Help																																																																															
IPv4 From 192 . 168 . 1 . 0 To 192 . 168 . 1 . 255		+ X ↻ ⚡ 📁 📂		Start Scanning																																																																											
<table><thead><tr><th>IP Address</th><th>MAC Address</th><th>Response Time</th><th>Host Name</th><th></th></tr></thead><tbody><tr><td>192.168.1.1</td><td>58-6D-8F-83-9E-EB</td><td>2 ms</td><td></td><td></td></tr><tr><td>192.168.1.116</td><td>6C-0B-84-67-FB-69</td><td>0 ms</td><td>P710</td><td></td></tr><tr><td>192.168.1.115</td><td>64-D8-14-61-E2-6E</td><td>1 ms</td><td></td><td></td></tr><tr><td>192.168.1.119</td><td>00-24-D7-A6-D3-90</td><td>5 ms</td><td>THINKPAD-W510</td><td></td></tr><tr><td>print\$</td><td></td><td></td><td></td><td></td></tr><tr><td>192.168.1.120</td><td>7C-5C-F8-F2-00-58</td><td>5 ms</td><td>P710</td><td></td></tr><tr><td>192.168.1.117</td><td>88-63-DF-8F-40-7D</td><td>84 ms</td><td>ANDREWS-IMAC</td><td></td></tr><tr><td>192.168.1.121</td><td>08-00-27-ED-4F-4C</td><td>0 ms</td><td>IK-PC</td><td></td></tr><tr><td>Media</td><td></td><td></td><td></td><td></td></tr><tr><td>Public</td><td></td><td></td><td></td><td></td></tr><tr><td>Download</td><td></td><td></td><td></td><td></td></tr><tr><td>Exchange</td><td></td><td></td><td></td><td></td></tr><tr><td>Users</td><td></td><td></td><td></td><td></td></tr><tr><td>192.168.1.114</td><td>C4-0B-CB-A5-A5-CD</td><td>273 ms</td><td></td><td></td></tr></tbody></table>					IP Address	MAC Address	Response Time	Host Name		192.168.1.1	58-6D-8F-83-9E-EB	2 ms			192.168.1.116	6C-0B-84-67-FB-69	0 ms	P710		192.168.1.115	64-D8-14-61-E2-6E	1 ms			192.168.1.119	00-24-D7-A6-D3-90	5 ms	THINKPAD-W510		print\$					192.168.1.120	7C-5C-F8-F2-00-58	5 ms	P710		192.168.1.117	88-63-DF-8F-40-7D	84 ms	ANDREWS-IMAC		192.168.1.121	08-00-27-ED-4F-4C	0 ms	IK-PC		Media					Public					Download					Exchange					Users					192.168.1.114	C4-0B-CB-A5-A5-CD	273 ms		
IP Address	MAC Address	Response Time	Host Name																																																																												
192.168.1.1	58-6D-8F-83-9E-EB	2 ms																																																																													
192.168.1.116	6C-0B-84-67-FB-69	0 ms	P710																																																																												
192.168.1.115	64-D8-14-61-E2-6E	1 ms																																																																													
192.168.1.119	00-24-D7-A6-D3-90	5 ms	THINKPAD-W510																																																																												
print\$																																																																															
192.168.1.120	7C-5C-F8-F2-00-58	5 ms	P710																																																																												
192.168.1.117	88-63-DF-8F-40-7D	84 ms	ANDREWS-IMAC																																																																												
192.168.1.121	08-00-27-ED-4F-4C	0 ms	IK-PC																																																																												
Media																																																																															
Public																																																																															
Download																																																																															
Exchange																																																																															
Users																																																																															
192.168.1.114	C4-0B-CB-A5-A5-CD	273 ms																																																																													

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. OpUtils complements existing management tools by providing trouble shooting and real-time monitoring capabilities.

The screenshot shows the OpUtils interface with the 'Switch Port Mapper' tab selected. On the left, a tree view displays network segments like 'Your Company', 'Default Group', 'ME', and 'Zoho' with specific switch ports listed. The main panel shows a table of switches with columns for Switch Name / IP, IP Address, DNS Name, Total, Used, Available, Transient, Usage, Status, Last Scan Time, and Sys Name. Each row contains a status bar with a progress bar and a green checkmark indicating it's scanned. A summary bar at the bottom indicates 'View 1 - 8 of 8'.

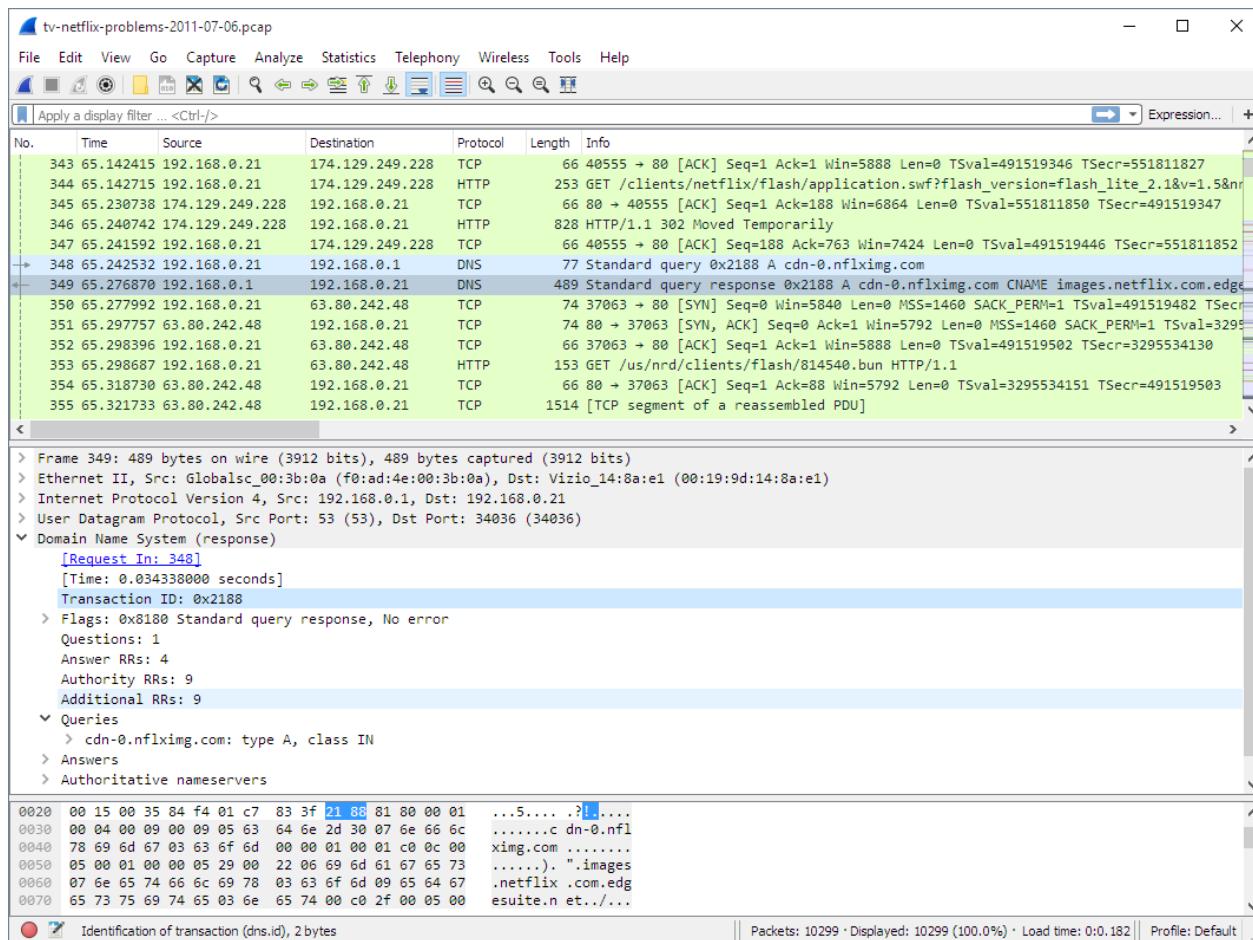
vii. SolarWinds Engineer's Toolset

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.

The screenshot shows the SolarWinds Toolset Launch Pad. The left sidebar lists categories like 'Quick Start', 'My recent tools', 'My favorites', 'All Tools', 'Network Discovery', 'Network Monitoring' (which is selected), 'Configuration Management...', 'IPAM/DNS/DHCP', 'Diagnostics', 'Log Management', 'General/Other', 'Security', and 'SNMP'. Below this is a 'Download new tools' button. The main area displays six tool cards: 'Advanced CPU Load', 'Bandwidth Gauges', 'CPU Gauges', 'Neighbor Map', 'Netflow Realtime', and 'Network Monitor'. Each card has a brief description and a 'Launch' button.

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.

Basic Network [Back to My Scans](#)

Configure Audit Trail Launch Export

Hosts 1 Vulnerabilities 66 Remediations 2 History 1

Filter Search Vulnerabilities 66 Vulnerabilities

Sev	Name	Family	Count	Actions
Critical	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1	○ /
Critical	MS17-010: Security Update f...	Windows	1	○ /
High	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1	○ /
High	Jenkins < 2.138.4 LTS / 2.150....	CGI abuses	1	○ /
High	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1	○ /
High	MS12-020: Vulnerabilities in ...	Windows	1	○ /
Medium	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1	○ /
Medium	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1	○ /
Medium	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1	○ /
Medium	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1	○ /
Medium	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1	○ /
Medium	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1	○ /
Medium	Microsoft Windows Remote ...	Windows	1	○ /

Scan Details

Name: Basic Network
 Status: Completed
 Policy: Basic Network Scan
 Scanner: Local Scanner
 Start: February 25 at 9:03 AM
 End: February 25 at 9:07 AM
 Elapsed: 4 minutes

Vulnerabilities

● Critical
 ● High
 ● Medium
 ● Low
 ● Info

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 and daily 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.

OpenVAS Vulnerability Report

Scan started: Wed Feb 13 04:26:48 2019 UTC
Scan ended: Wed Feb 13 04:31:16 2019 UTC

Summary

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.

High	Medium	Low	Log
3	4	0	0
3	4	0	0

Schedule a new OpenVAS Scan

TARGET ADDRESS
IP address(es) or Hostname(s)
Valid formats: 192.168.168.168 or hostname.com or multiple targets in list

ICD LABEL
Optional Label
Optional label for identifying scan (used in table and e-mail subject)

SCAN TYPE
Full Server Scan

RECURRANCE
Monthly on the 3rd

Hour on Day
08:00

time of day is based on UTC, current server time is 08:53

OpenVAS Vulnerability Report

Details: CVE-2018-1000197 Microsoft RDP Server Private Key Disclosure Vulnerability (ID: 11420) [2018-02-01]

Summary
This host is running Remote Desktop Protocol server and is prone to information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to gain sensitive information.
Impact Level: System/Application

Solutions
Solution type: Remap fix
No solution or patch yet made available for at least one year since disclosure of this vulnerability. A hotfix will be provided as possible. Generic solutions include: use to upgrade to a newer version, disable respective features, remove the product or replace the product by another one.

A Weakness can't be mapped only to terminal services or terminal notebooks.

Affected Software/OS
All Microsoft compatible RDP (3.0 or earlier) softwares.

Vulnerability Insight
The flaw is due to RDP Turner which stores an RSA private key used for signing a terminal servers public key in the message digest library, which allows remote attackers to calculate a valid signature and further performs a man-in-the-middle (MitM) attack to obtain sensitive information.

Vulnerability Detection Method
Details: Microsoft RDP Server Private Key Disclosure Vulnerability (ID: 11420) [2018-02-01]

Version used: Microsoft 1440.0

References
CVSS: CVSS:4.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
ID: 1000197
Other: Microsoft.com/technet/security/advisory/1000197

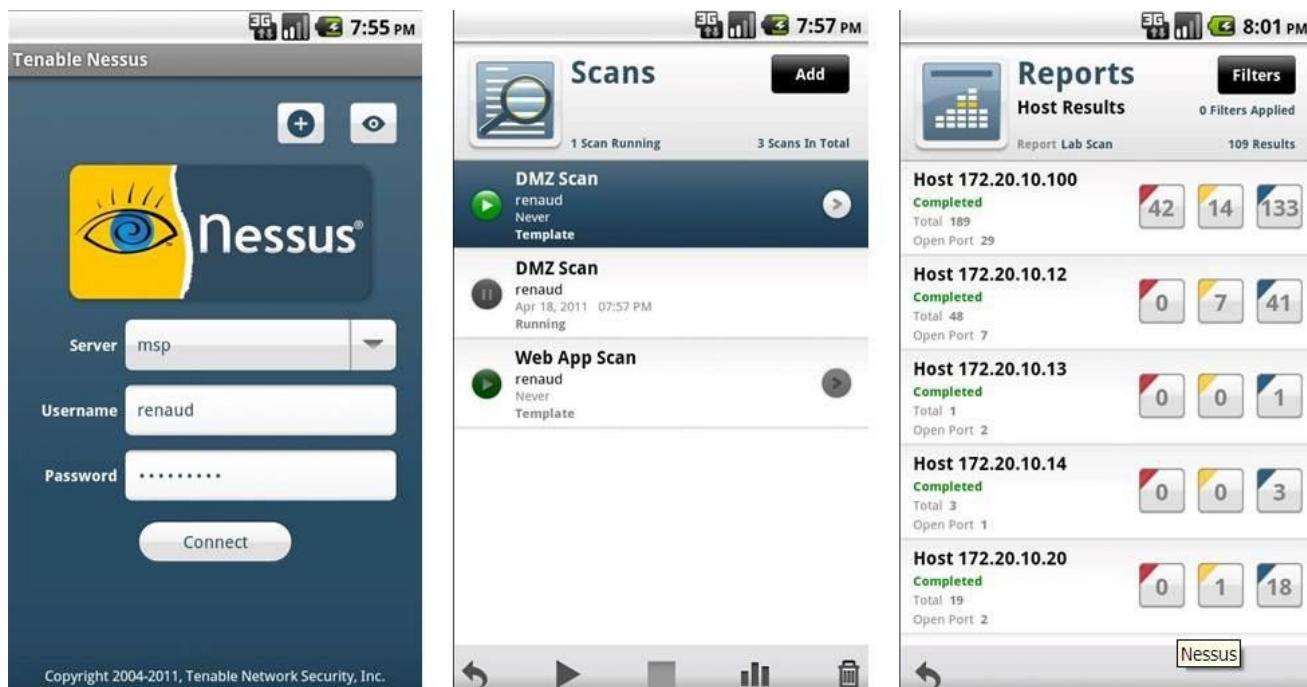
All discovered issues are given a severity rating and detailed for remediation / mitigation.

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.

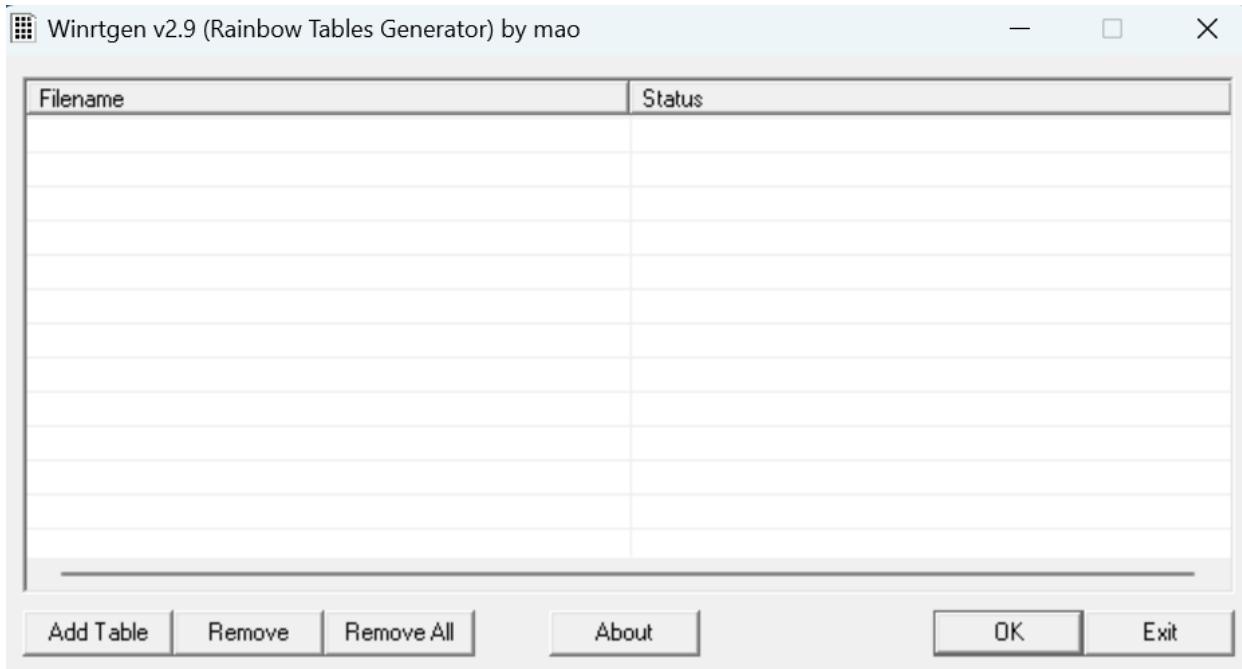
- To query for information, the Nessus scanner must be able to reach the Mobile DeviceManagement servers. Ensure no screening devices block traffic to these systems fromthe Nessus scanner. In addition, you must give Nessus administrative credentials (for example, domain administrator) to the Active Directory 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.



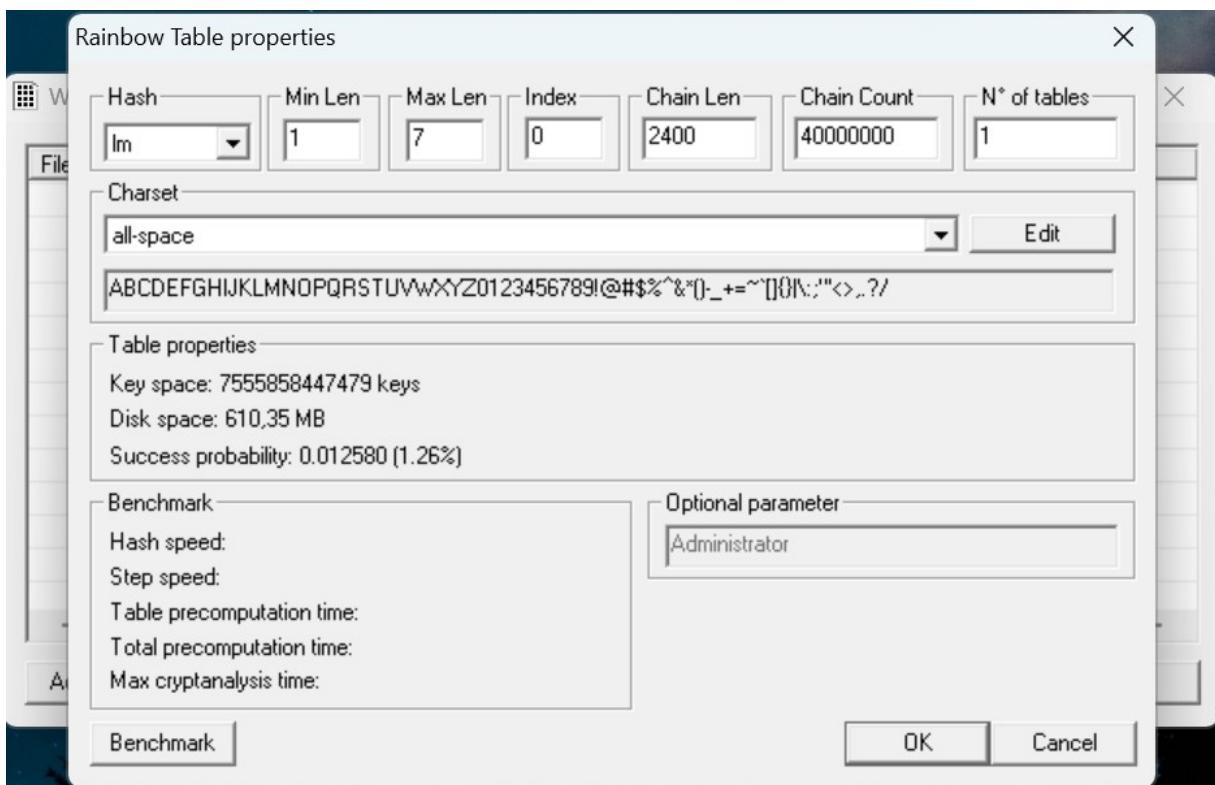
b. Perform the System Hacking using the following tools:

i. Winrtgen

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

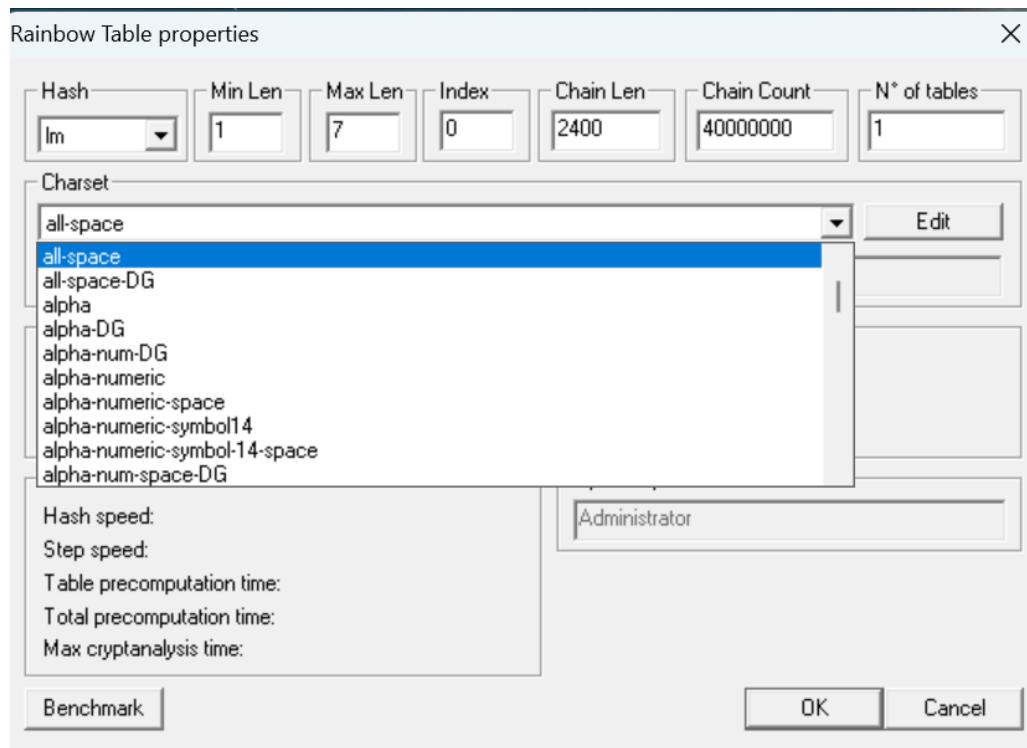
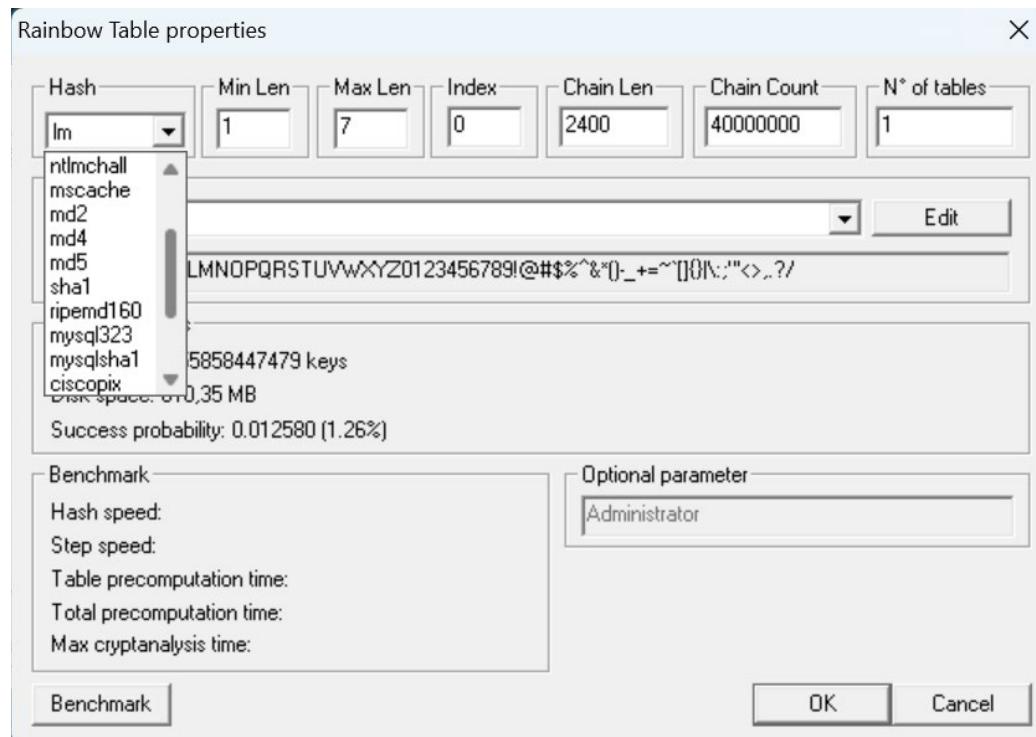


To generate rainbow tables first we will have to modify the properties of WinRTGen according to our need, and to do so Click on “Add Table”. After this, a new box will appear named “Rainbow Table Properties”

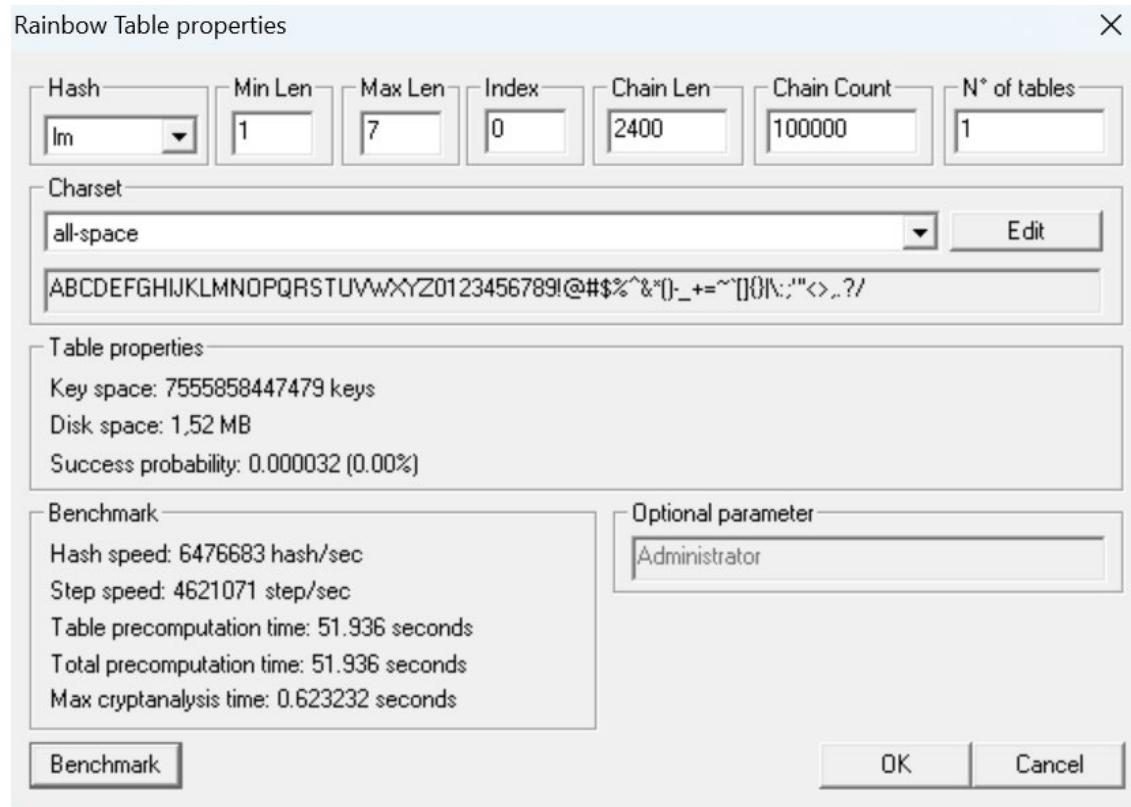


In the “Rainbow Table Properties” window we have the option to modify settings in order to generate rainbow tables according to our needs. The following properties can be modified:

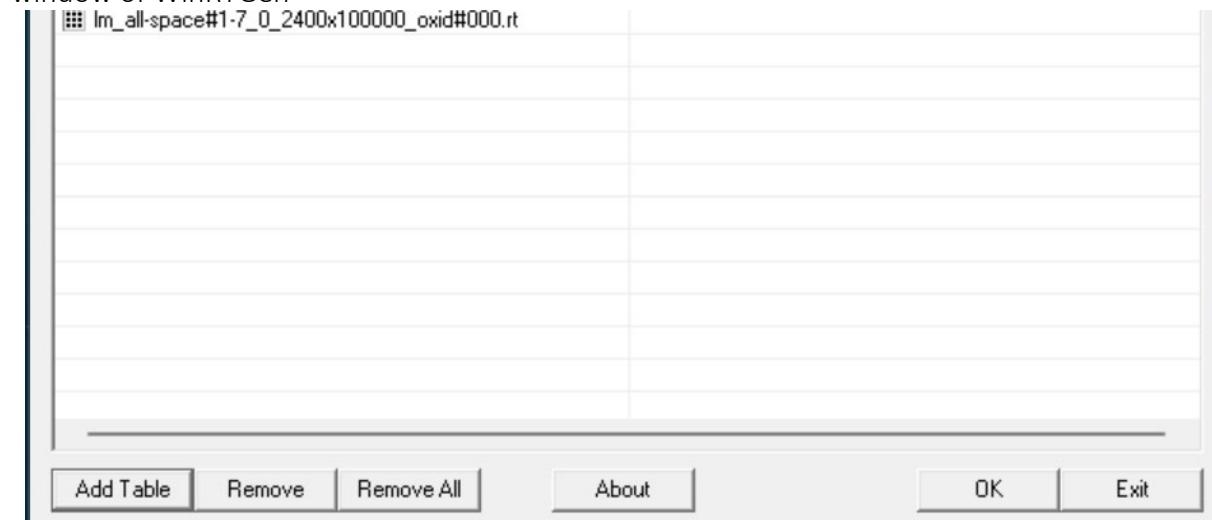
- Hash:** The type of encryption we want the rainbow table to be generated. For example MD5, MD4, SHA1, etc.



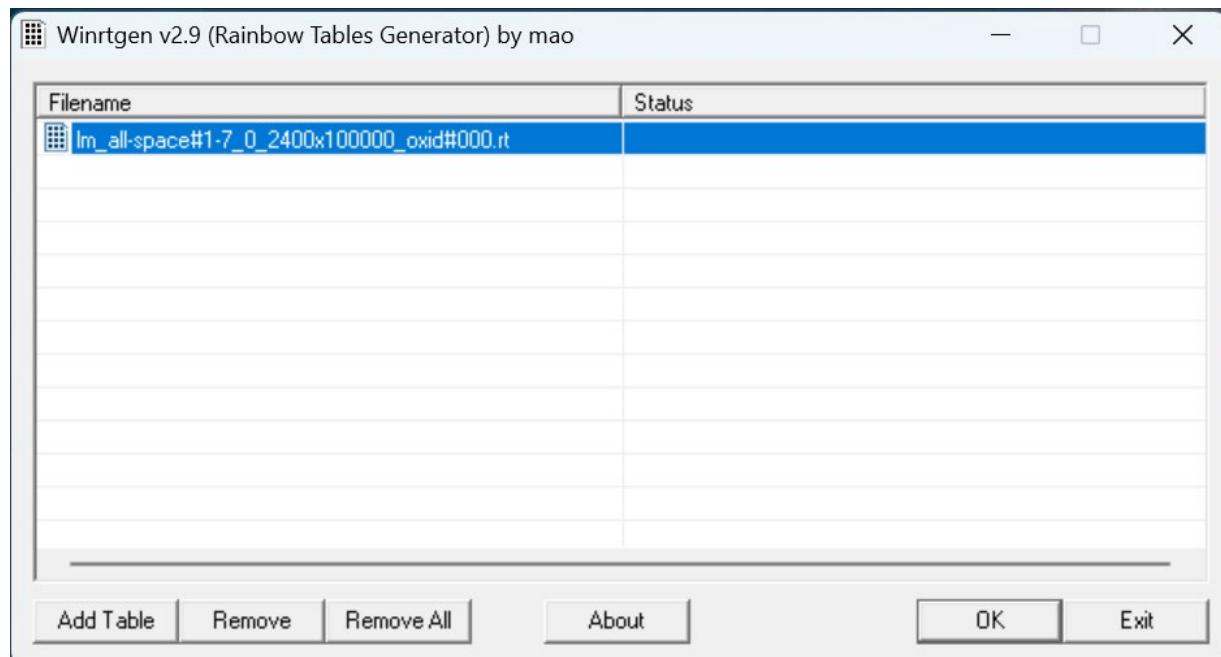
After assigning the values to the properties according to our needs click on “Benchmarks”. This will show the estimated time, Hash speed, Step speed, Table Pre-computing time, etc. that will be required to generate the Rainbow Table according to assigned properties.



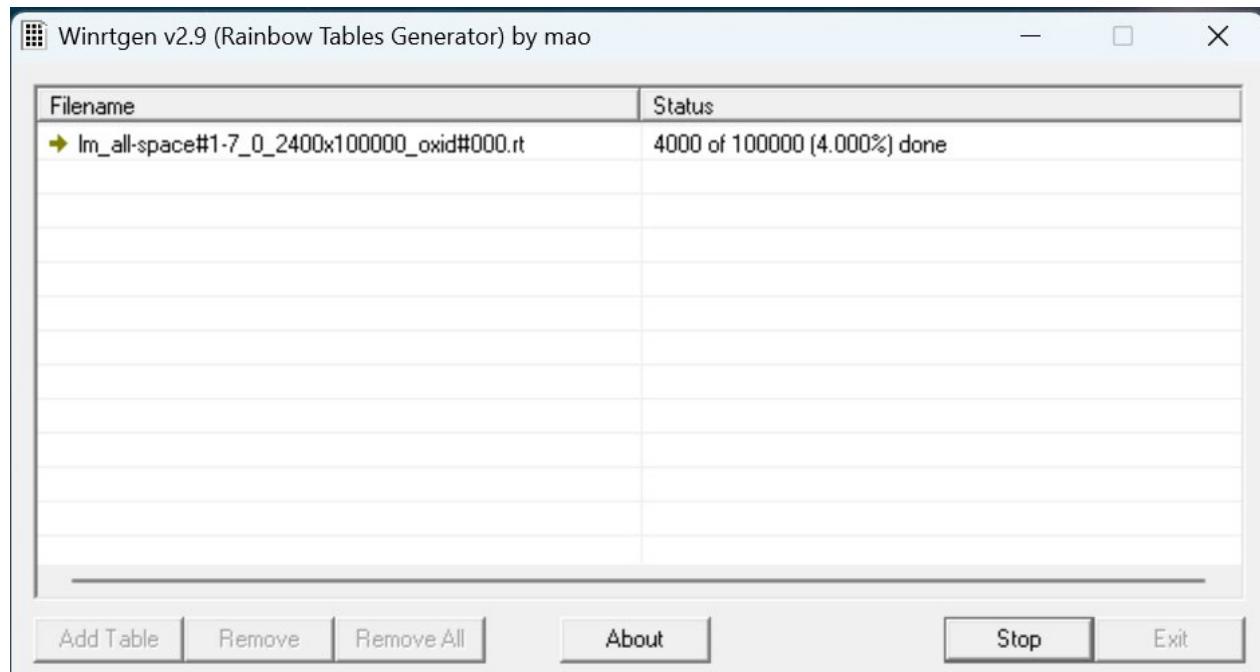
After “Benchmark” click on “Ok”. This will add the Rainbow Table to the queue in the main window of WinRTGen



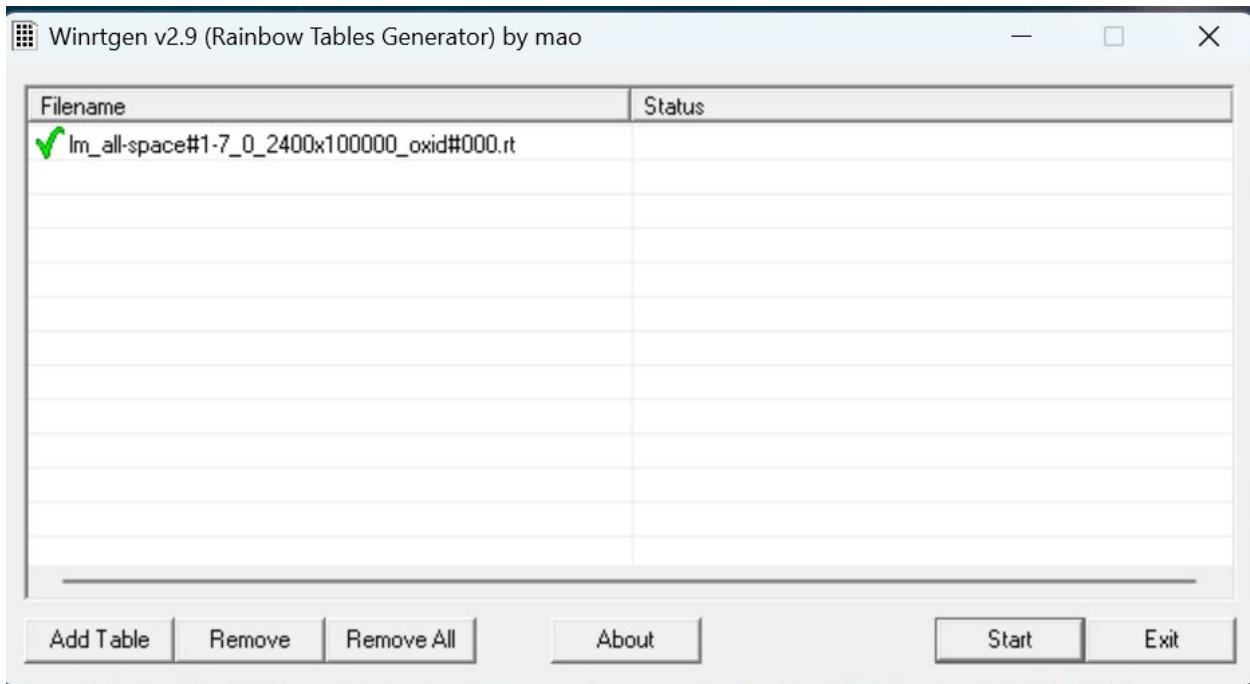
After this click on “Rainbow Table” You want to start processing and click “OK” .



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



After completion, the window will appear as follows.



This table will be saved to your WinRTGen Directory.

winrtgen		▼	C	Search winrtgen
Name		Date modified	Type	Size
charset		07-12-2008 23:34	Text Document	6 KB
info		04-11-2010 14:02	Text Document	1 KB
lm_all-space#1-7_0_2400x100000_oxid#000.rt		11-10-2022 21:03	RT File	1,563 KB
Tables.lst		11-10-2022 21:02	LST File	1 KB
Winrtgen		4:34	Application	259 KB
Winrtgen.exe.sig		20-02-2009 21:23	SIG File	1 KB

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:

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
```

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

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

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

C:\Users\Desktop\pwdump7
```

iii. Ophcrack

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

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

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

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

Step 4 : Remove the bootable media from the second PC and insert it into your locked Windows machine. Let the computer boot up from this media instead of the native Windows installation. This is made possible by the fact that Ophcrack itself contains a small

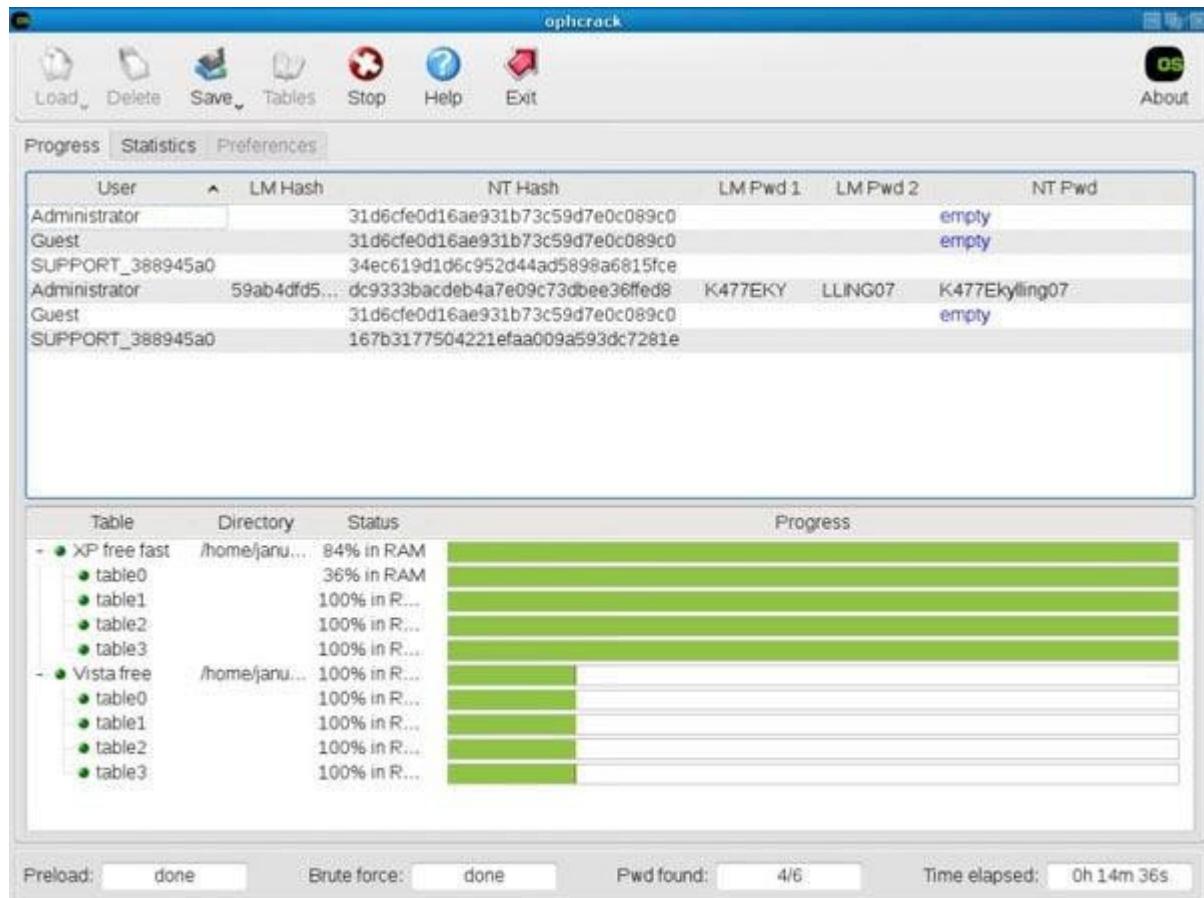
operatingsystem that can run independently of your Windows OS. In a few moments, you will see theOphcrack interface on your computer.

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.



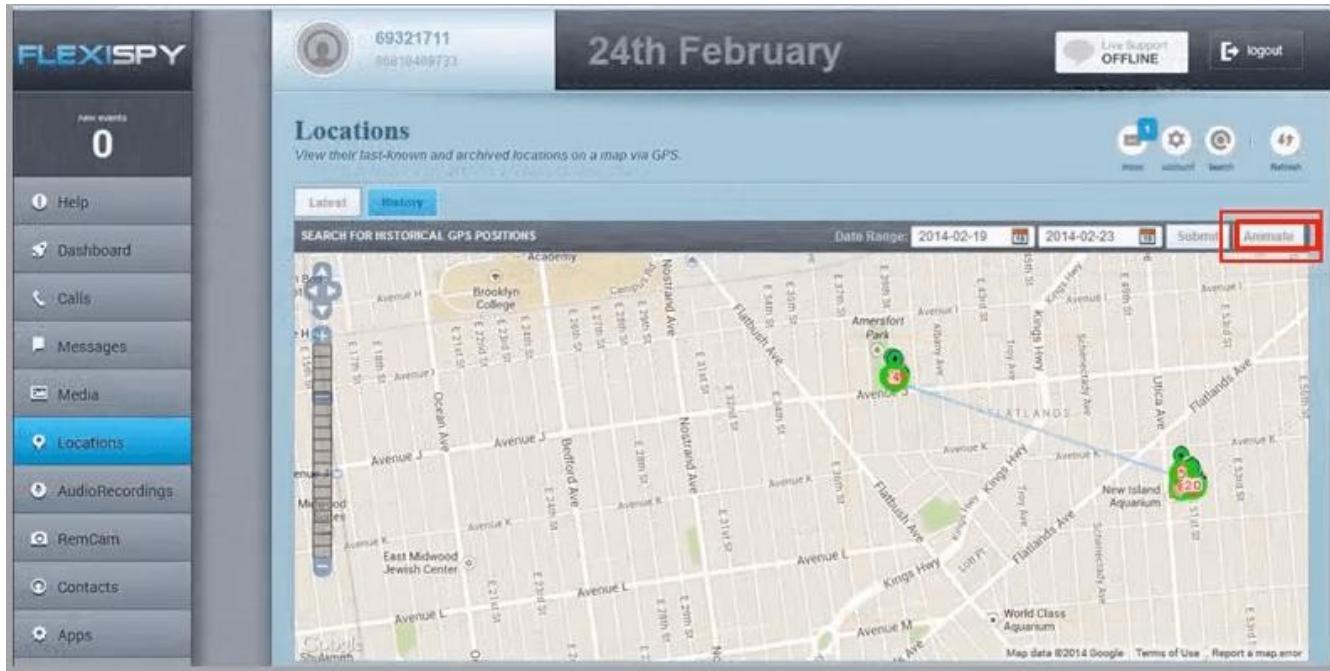
iv. Flexispy

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. Another form of the data stream that can be found within each file is an alternate data stream (ADS).

ADS is a file attribute available solely in NTFS, and it refers to any type of data associated with a file but not in the file itself on an NTFS system. NTFS ADS is a Windows hidden stream that stores file metadata such as properties, word count, access and author name, and modification timings.

ADSs can fork data into existing files without changing or altering their functionality, size, or display to file-browsing utilities. They enable an attacker to inject malicious code into files on a vulnerable system and execute them without the user knowing. Attackers use ADS to hide rootkits or hacker tools on a breached system and allow users to execute them while hiding from the system administrator.

Once the ADS is attached to a file, the size of the original file will not change. One can only identify the changes in files through modification of timestamps, which can be innocuous.

Creation of NTFS streams:

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

filename.extension:alternativeName

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

```
C:\Windows\System32\cmd.exe

C:\test>echo "this is file no 1" > file_1.txt
C:\test>echo "this is hidden file inside the file_1.txt" > file_1.txt:secret.txt
C:\test>dir
Volume in drive C has no label.
Volume Serial Number is 9445-3BC5

Directory of C:\test

27-05-2022  16:01    <DIR>   .
27-05-2022  16:15                22 file_1.txt
                           1 File(s)       22 bytes
                           1 Dir(s)  155,960,602,624 bytes free

C:\test>
```

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

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

The screenshot shows a Windows environment with a Command Prompt window and a Notepad window.

In the Command Prompt window (C:\Windows\System32\cmd.exe), the command entered is:

```
C:\test>notepad file_1.txt:secret.txt
```

The output shows the command was executed successfully:

```
C:\test>
```

In the Notepad window, the title bar is:

```
file_1.txt:secret - Notepad
```

The content of the Notepad window is:

```
"this is hidden file inside the file_1.txt"
```

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

Hiding Trojan.exe in note.txt file stream:

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

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

Here type command is used to hide trojan in the ADS inside an existing file.

After hiding trojan.exe behind note.txt, we need to create a link to launch the trojan.exe file from the stream. The following command is used to create a shortcut in the stream.

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

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

The screenshot shows two windows. The top window is a Command Prompt with administrator privileges, displaying the following commands and output:

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

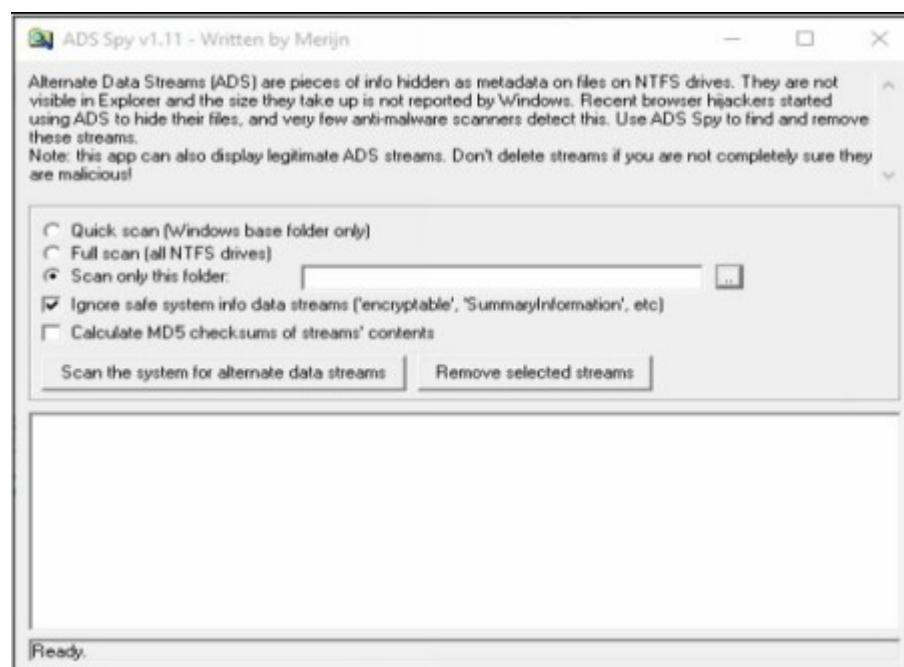
The bottom window is a File Explorer showing the contents of the 'test' folder on the Local Disk (C:). The folder contains three items: 'game', 'note', and 'Trojan'. The 'game' item is highlighted with a red box, and its details are shown in the status bar: Name: game, Date modified: 27-05-2022 04:14, Type: .symlink, Size: 0 KB. The 'note' and 'Trojan' files are also listed.

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

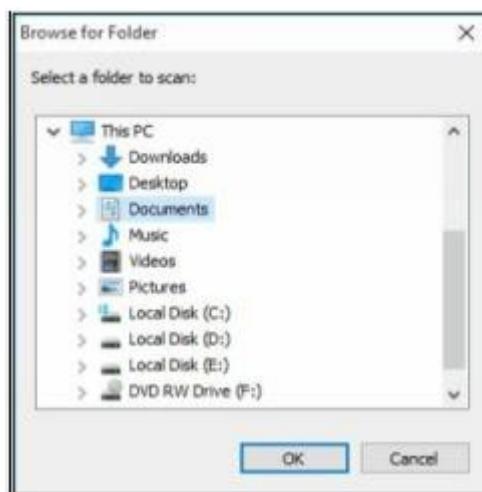
vi. ADS Spy

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

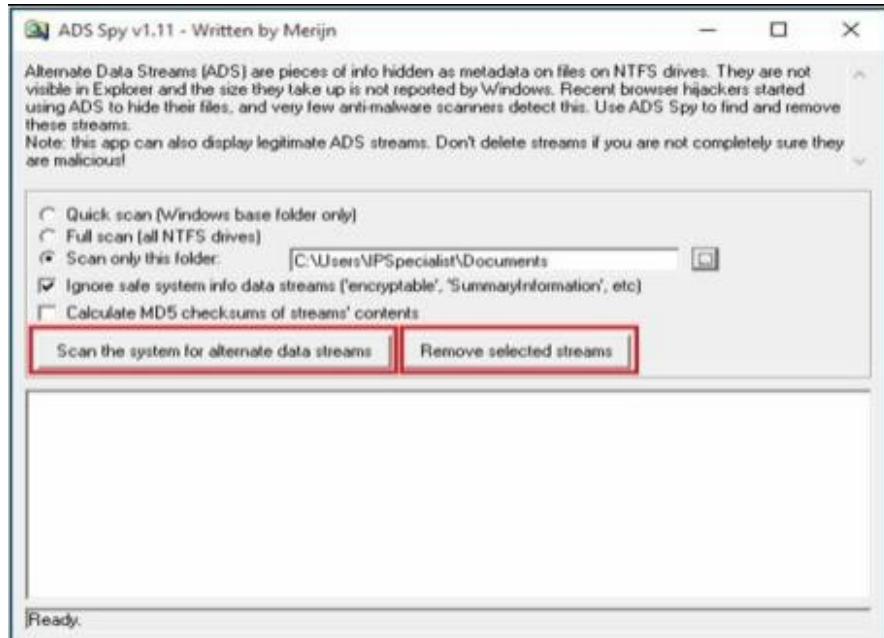


As we store the file in the Document folder, Selecting Document folder to scan particular folder only.



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.

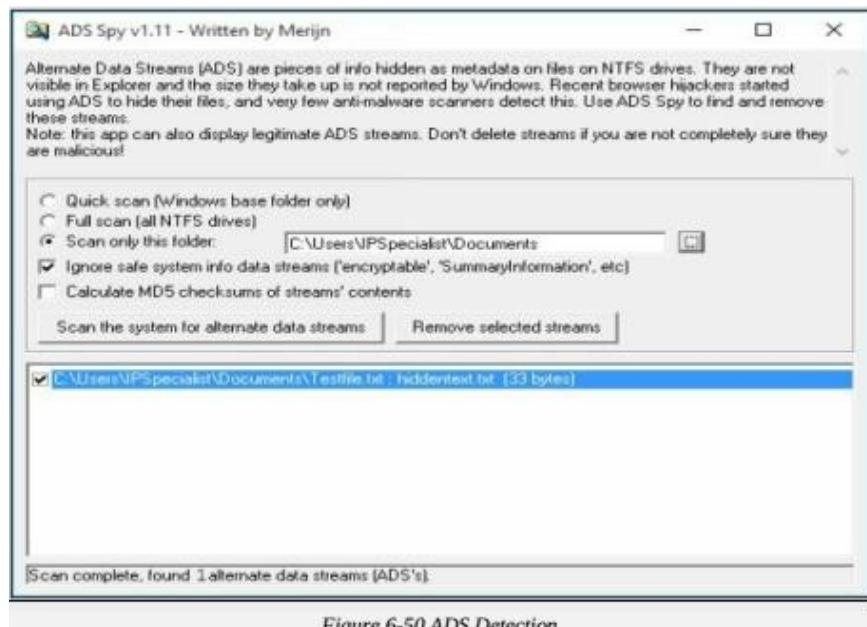
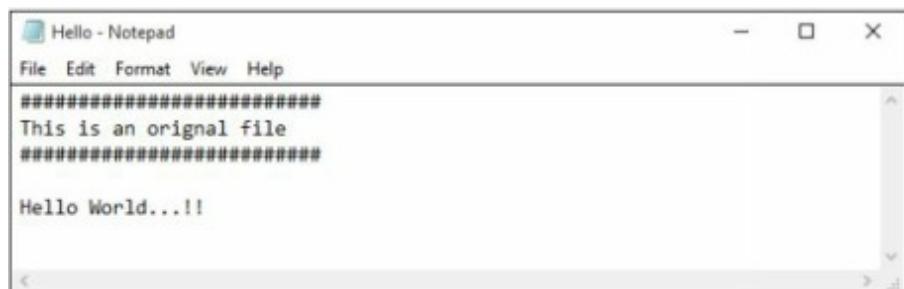


Figure 6-50 ADS Detection

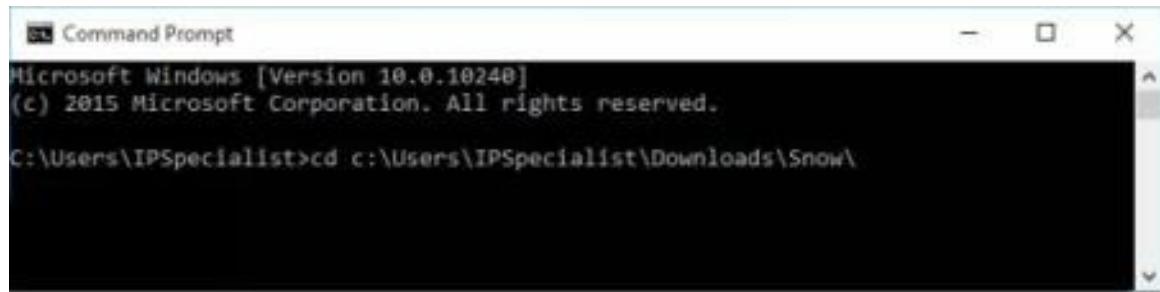
vii. Snow

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



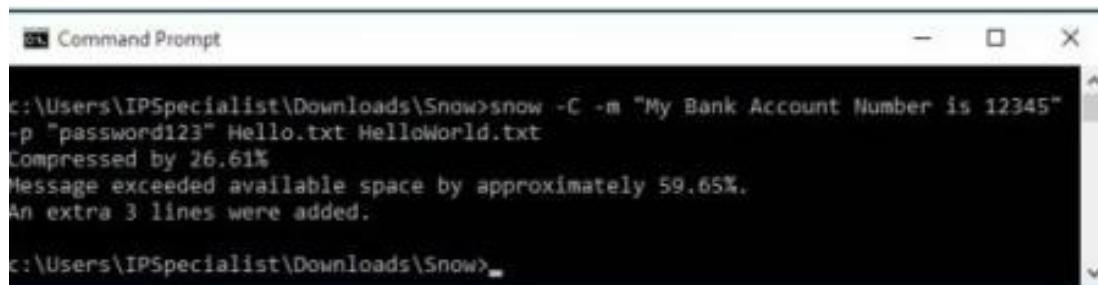
```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>cd c:\Users\IPSpecialist\Downloads\Snow\
```

Type the command

```
Snow -C -m "text to be hide" -p "password" <Sourcefile> <Destinationfile>
```

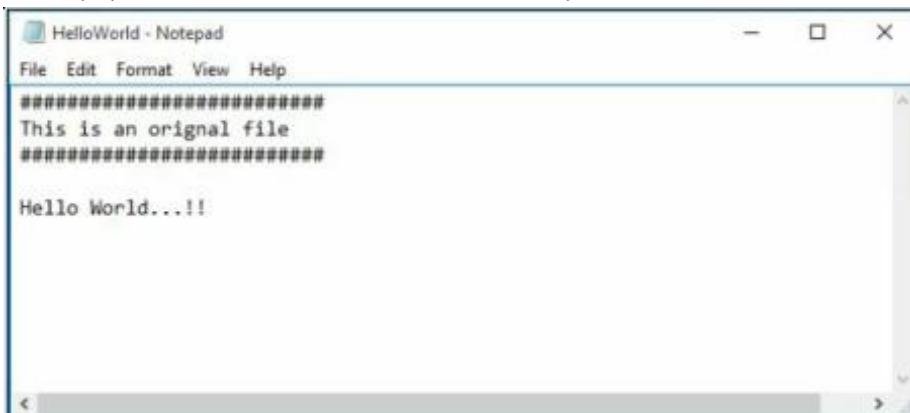
The source file is a Hello.txt file as shown above. Destination file will be the exact copy of source file containing hidden information.



```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -m "My Bank Account Number is 12345"
-p "password123" Hello.txt HelloWorld.txt
Compressed by 26.61%
Message exceeded available space by approximately 59.65%.
An extra 3 lines were added.

c:\Users\IPSpecialist\Downloads\Snow>
```

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

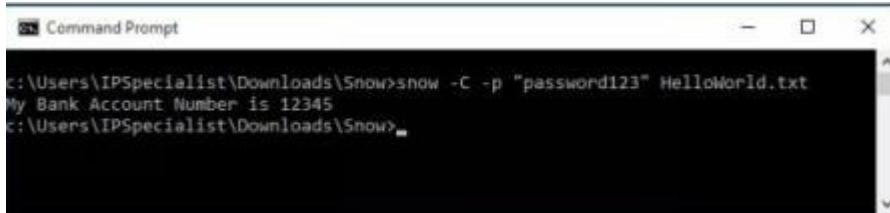


New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command

```
Snow -C -p "password123" HelloWorld.txt
```



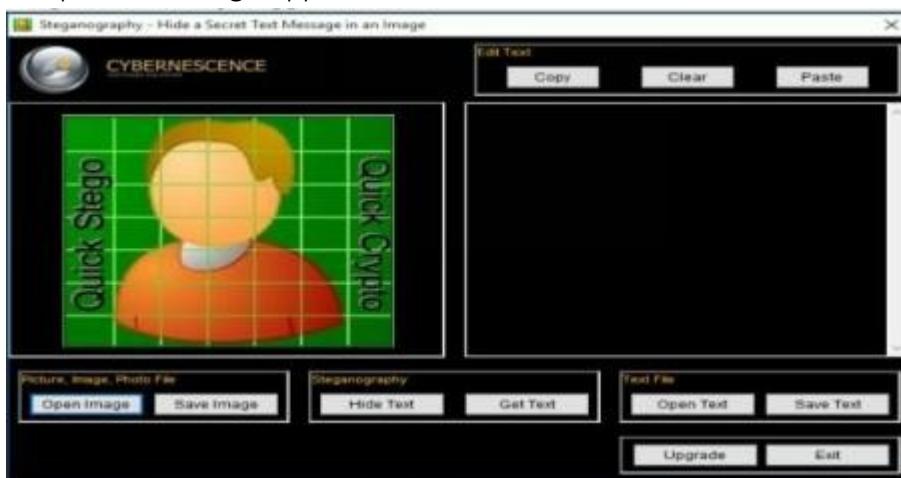
```
c:\Users\IPSpecialist\Downloads\Snow>show -C -p "password123" HelloWorld.txt
My Bank Account Number is 12345
c:\Users\IPSpecialist\Downloads\Snow>
```

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

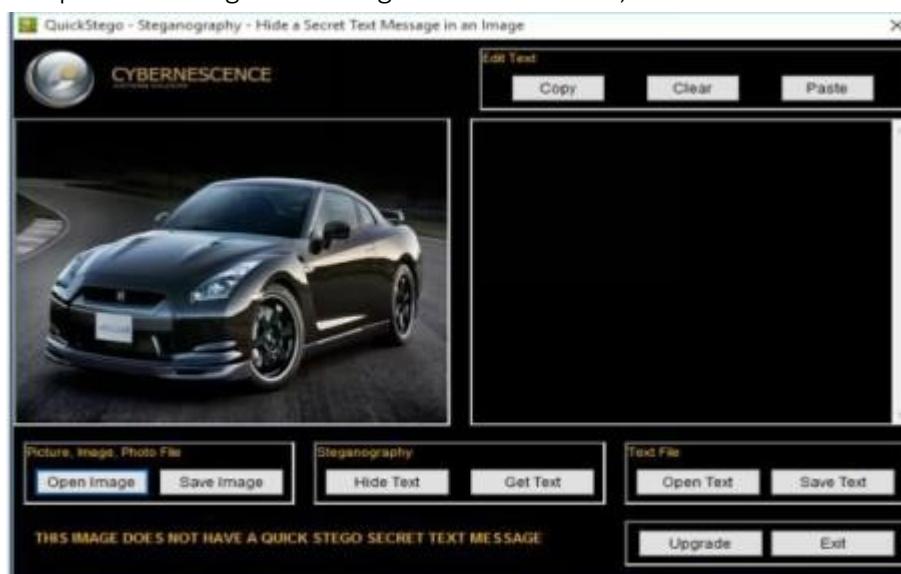
viii. Quickstego

Image Steganography using QuickStego

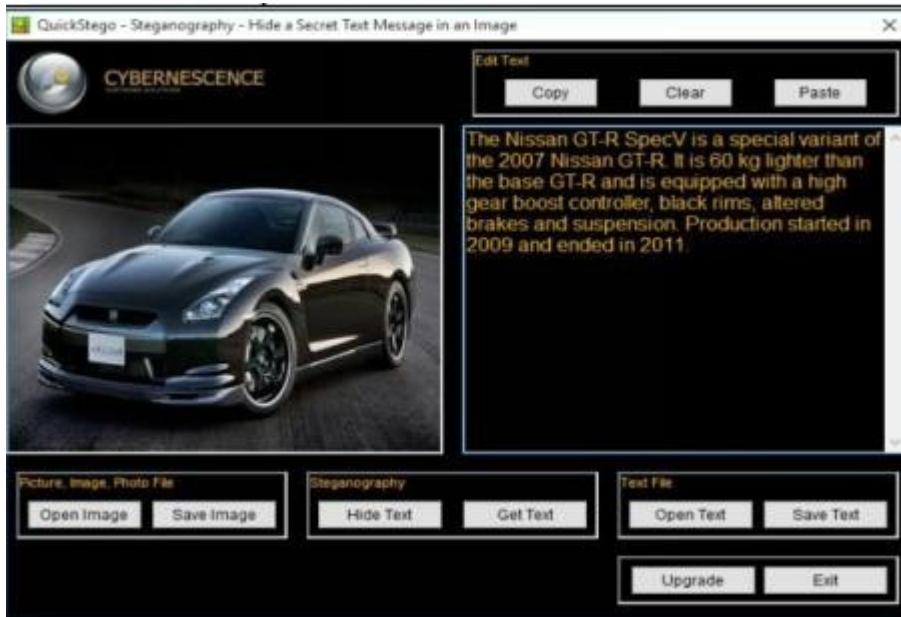
1. Open QuickStego Application



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

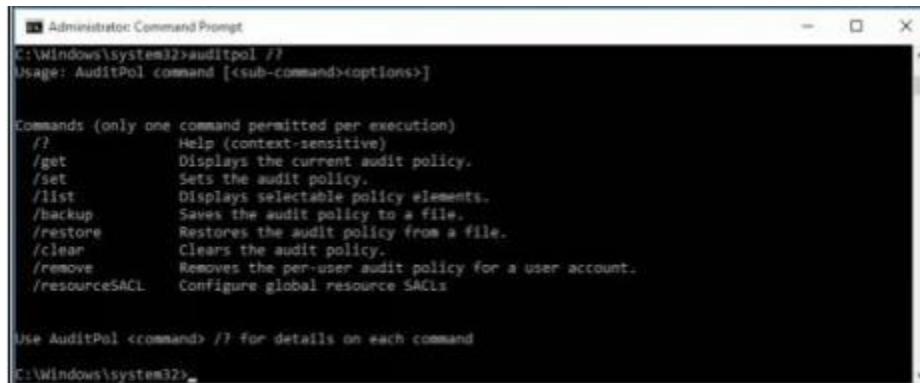


ix. Clearing Audit Policies

Enabling and Clearing Audit Policies

To check command's available option Enter

C:\Windows\system32> auditpol /?



The screenshot shows an Administrator Command Prompt window titled "Administrator: Command Prompt". The command entered is "auditpol /?". The output displays the usage information and a list of commands:

```
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
```



```
Administrator: Command Prompt

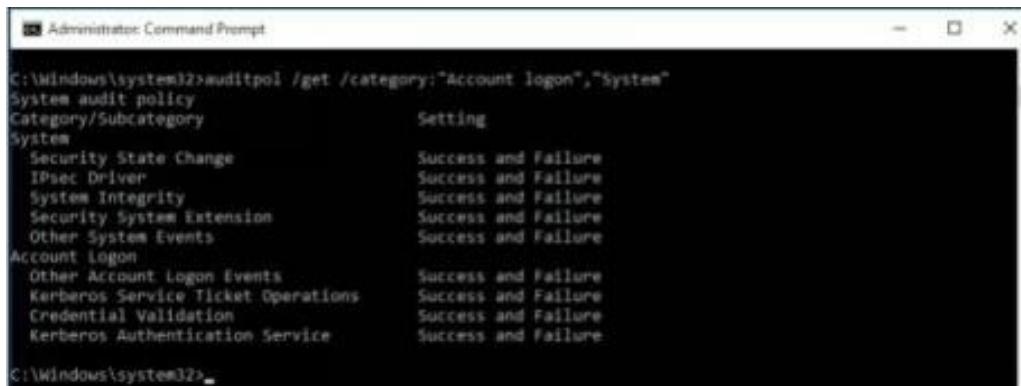
Commands (only one command permitted per execution)
/?           Help (context-sensitive)
/get          Displays the current audit policy.
/set          Sets the audit policy.
/list          Displays selectable policy elements.
/backup       Saves the audit policy to a file.
/restore      Restores the 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>auditpol /set /category:"System","Account logon" /success:enable /failure:enable
The command was successfully executed.

C:\Windows\system32>
```

To check Auditing is enabled, enter the command

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



```
Administrator: Command Prompt

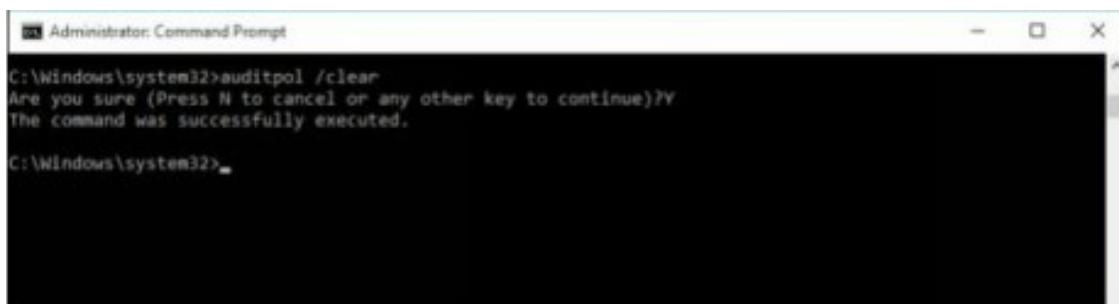
C:\Windows\system32>auditpol /get /category:"Account logon","System"
System audit policy
Category/Subcategory      Setting
System
  Security State Change    Success and Failure
  IPSet Driver             Success and Failure
  System Integrity          Success and Failure
  Security System Extension Success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

C:\Windows\system32>
```

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



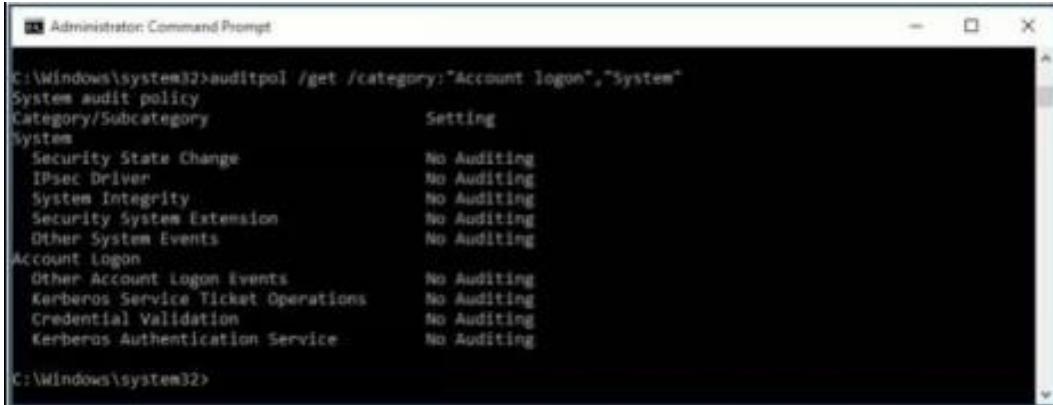
```
Administrator: Command Prompt

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

C:\Windows\system32>
```

To check Auditing, enter the command

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

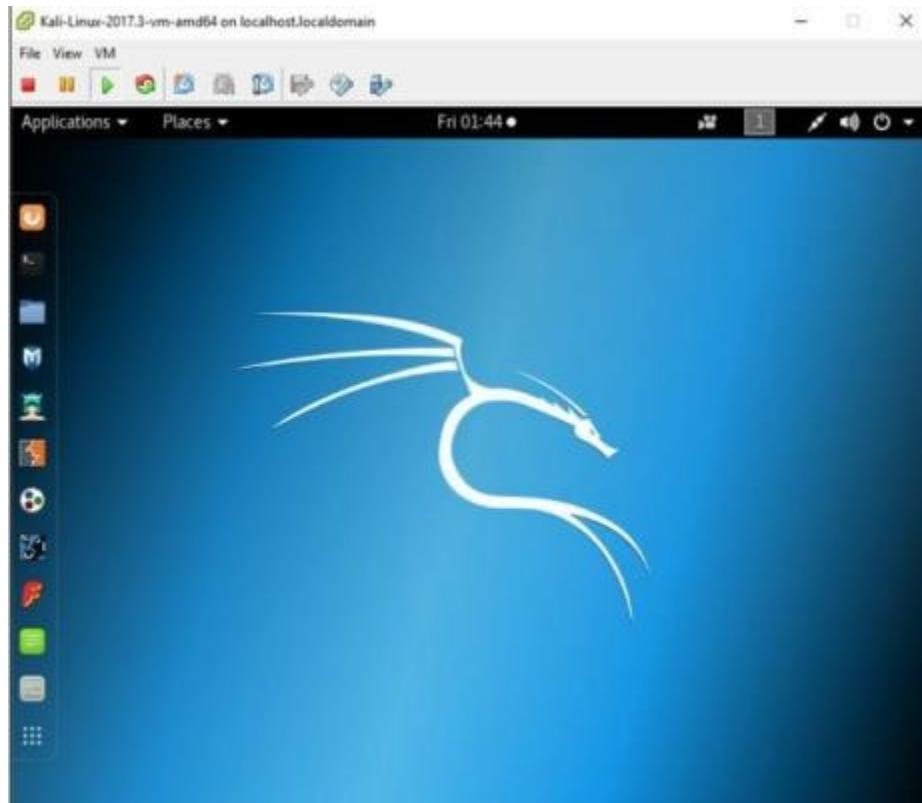


```
C:\Windows\system32>auditpol /get /category:"Account logon","System"
System audit policy
Category/Subcategory          Setting
System
    Security State Change      No Auditing
    IPsec Driver                No Auditing
    System Integrity             No Auditing
    Security System Extension   No Auditing
    Other System Events         No Auditing
Account Logon
    Other Account Logon Events  No Auditing
    Kerberos Service Ticket Operations  No Auditing
    Credential Validation       No Auditing
    Kerberos Authentication Service  No Auditing

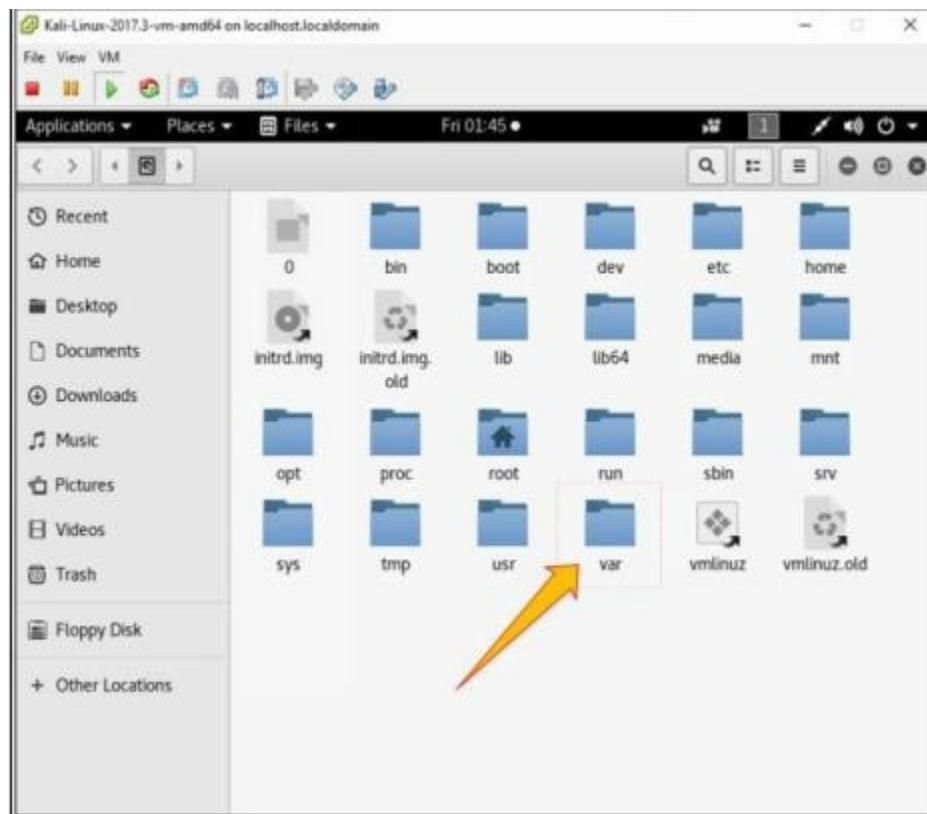
C:\Windows\system32>
```

X. Clearing Logs

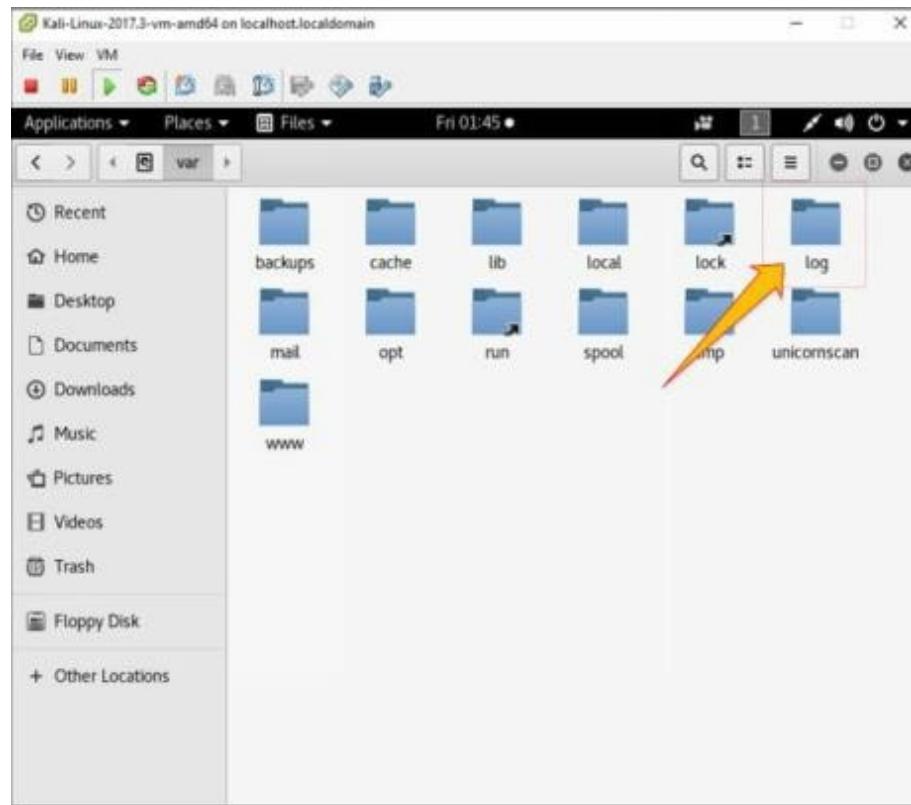
1. Go to Kali Linux Machine



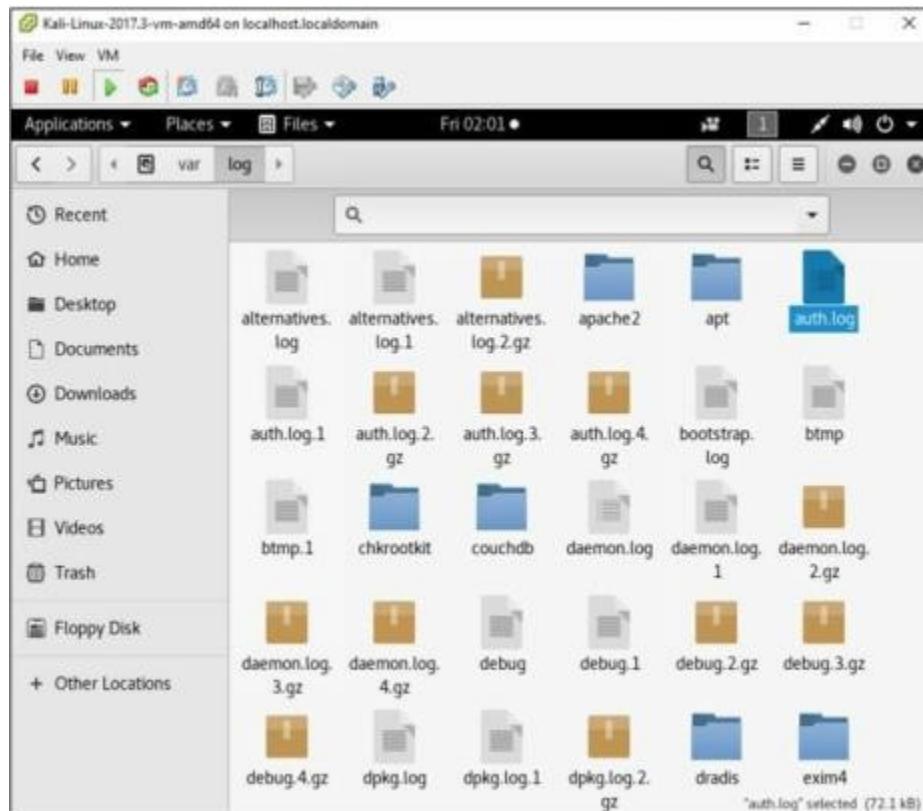
2. Open the **/var** directory:



3. Go to **Logs** folder:



4. Select any log file:



5. Open any log file; you can delete

```

May 2 07:25:08 kali CRON[32135]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:25:08 kali CRON[32135]: pam_unix(cron:session): session closed for user root
May 2 07:30:04 kali CRON[32149]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:30:04 kali CRON[32149]: pam_unix(cron:session): session closed for user root
May 2 07:31:42 kali gdm-password: gkr-pam: unlocked login keyring
May 2 07:34:10 kali sudo:      root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/mv /root/Desktop/Test.exe /var/www/html/share
May 2 07:34:10 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 2 07:34:10 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:34:23 kali sudo:      root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/mv /root/Desktop/Test.exe /var/www/html/share
May 2 07:34:23 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 2 07:34:23 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:34:45 kali sudo:      root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/mv /Desktop/Test.exe /var/www/html/share
May 2 07:34:45 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 2 07:34:45 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:35:09 kali CRON[32255]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:35:09 kali CRON[32255]: pam_unix(cron:session): session closed for user root
May 2 07:39:04 kali CRON[32396]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:39:04 kali CRON[32396]: pam_unix(cron:session): session closed for user root

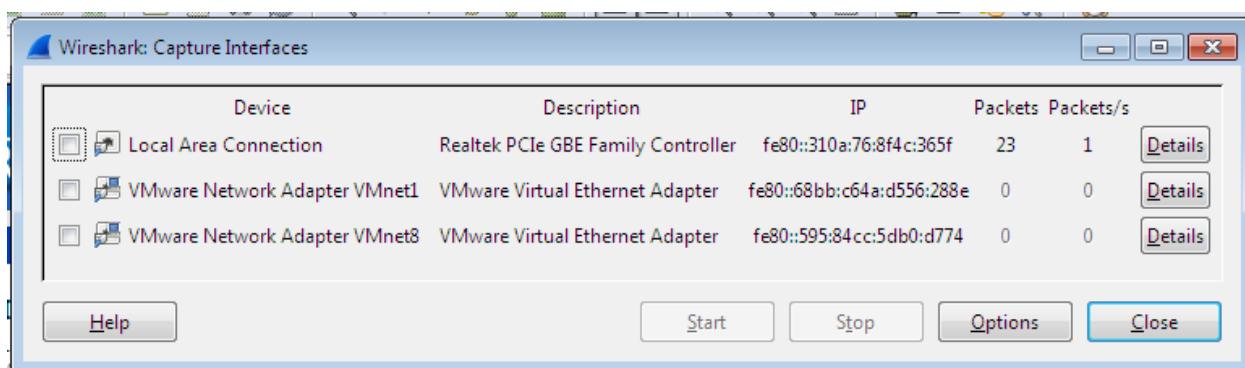
```

Practical No. 5**a. Use wireshark to sniff the network.**

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

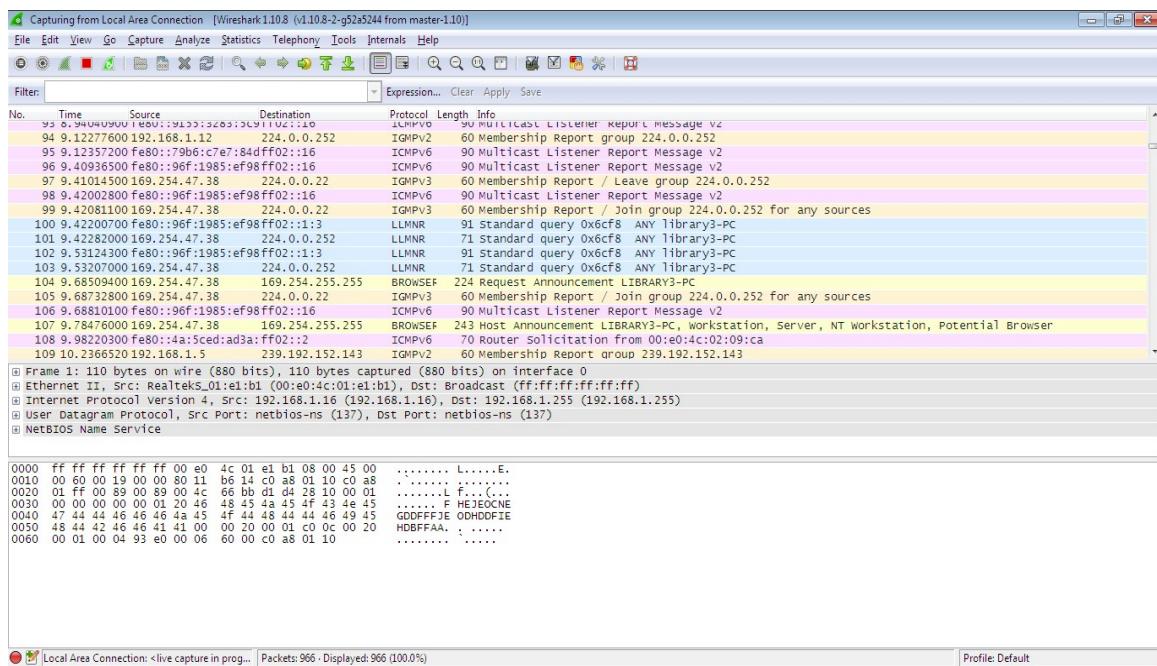
- Start Wireshark. Under the “Capture” header, select the “Interface List” option; or click on the “Interfaces” button on the toolbar:

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



List of available capture interfaces

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



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

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

Filtering the Packet List

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

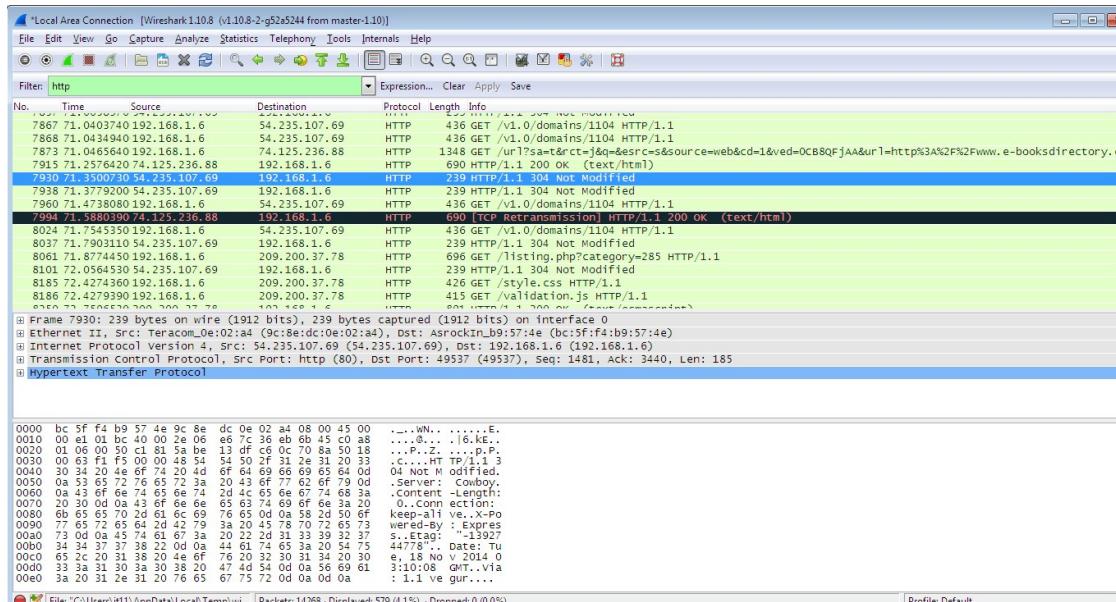
We may not be interested in all of these, depending on what we are trying to achieve. Fortunately, Wireshark allows us to filter the list based on different criteria using the “Filter” toolbar:



Filter toolbar

Let us take a look at the HTTP traffic that occurs when we browse the web.

In the filter toolbar, type “http” and then click on “Apply”. The window will now list only captured packets related to HTTP traffic:



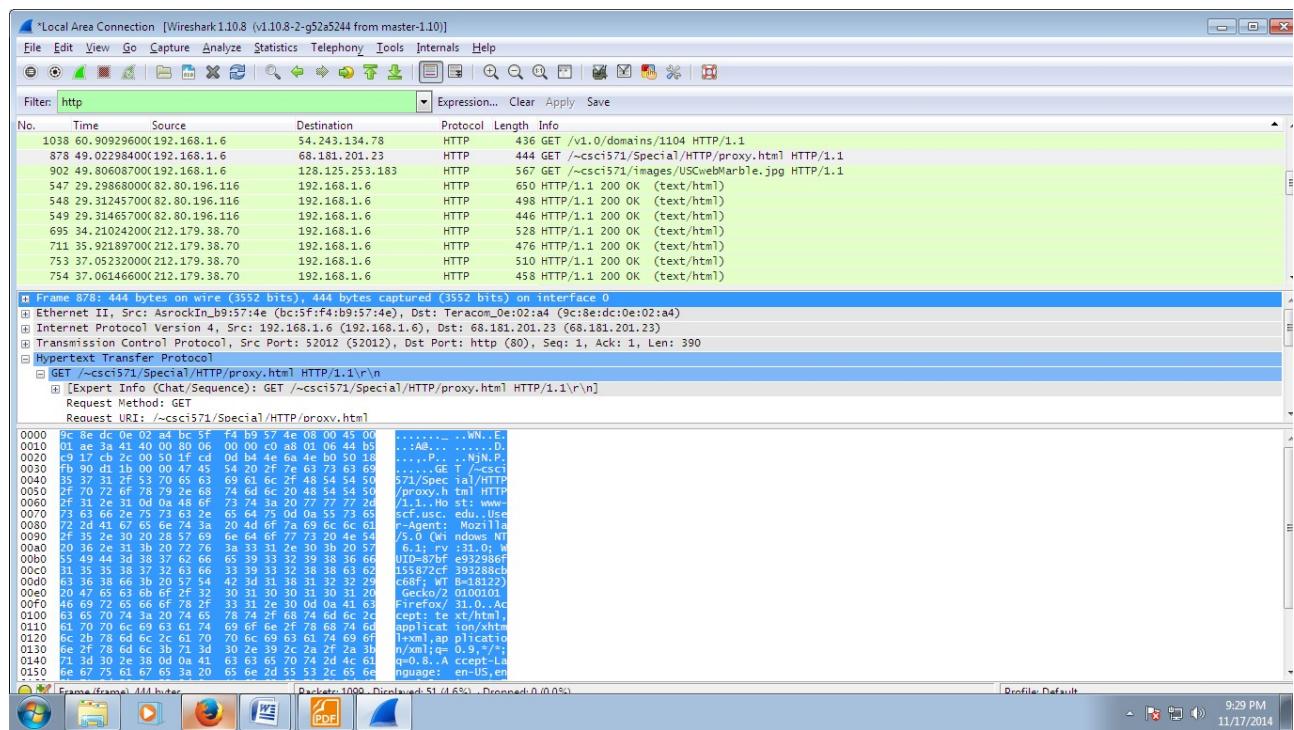
Examining HTTP Traffic

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. Select this packet.
- In the middle frame of the Wireshark window, expand the “Hypertext Transfer Protocol” section. Notice the details given for the:
 - GET request
 - Host
 - User-Agent
 - Accepts
 - cookie
 - etc

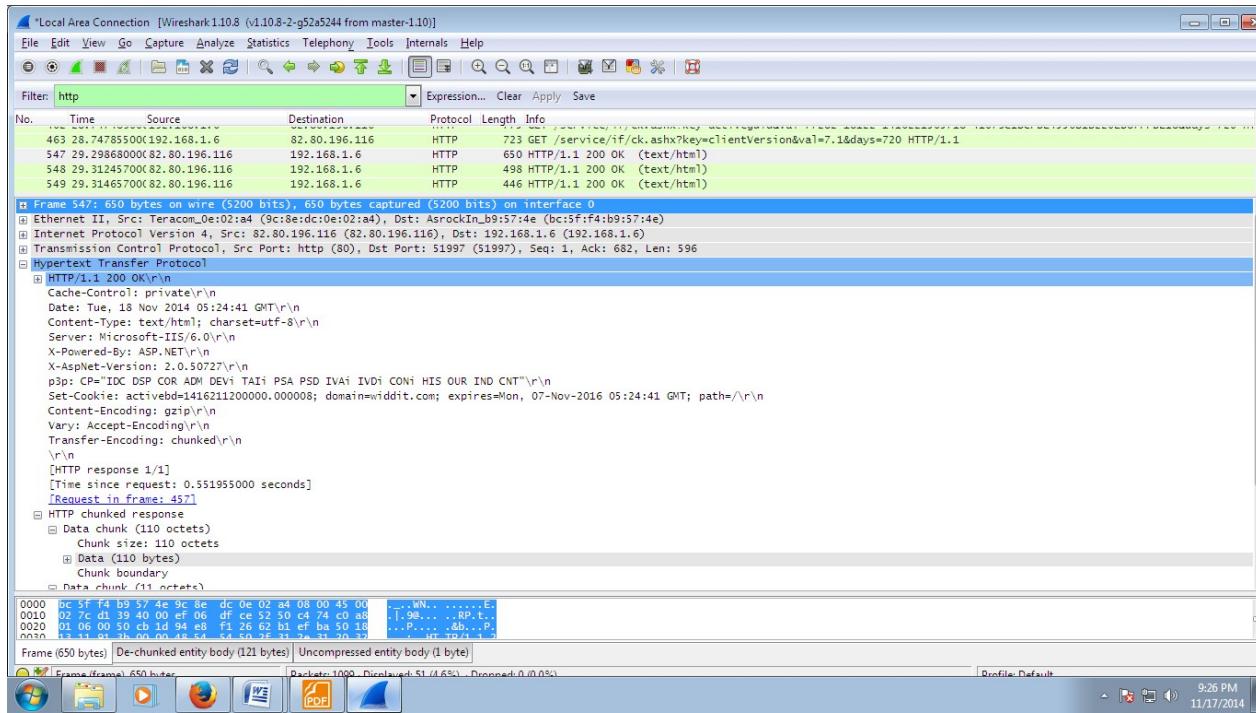


Take a look at the HTTP response to the above request.

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 the requested 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 appreciate the 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

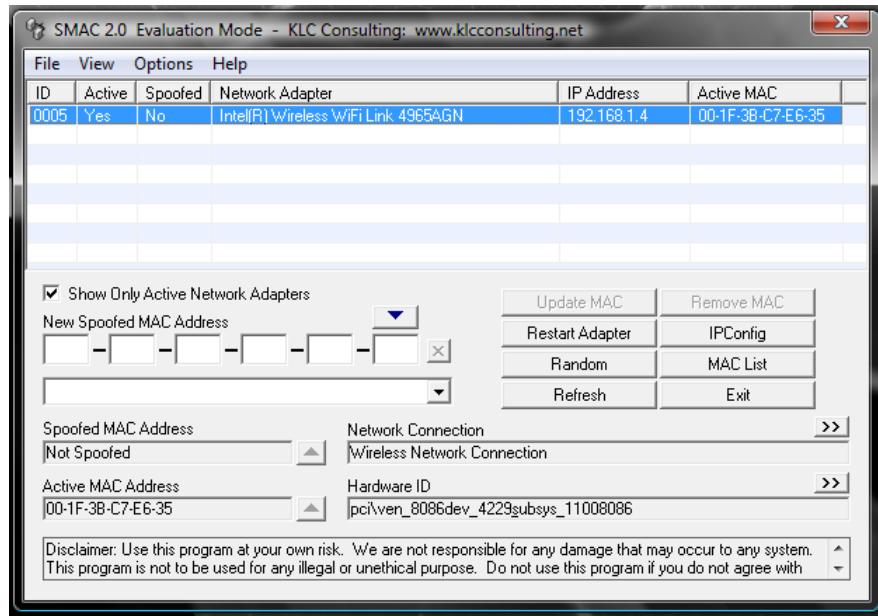
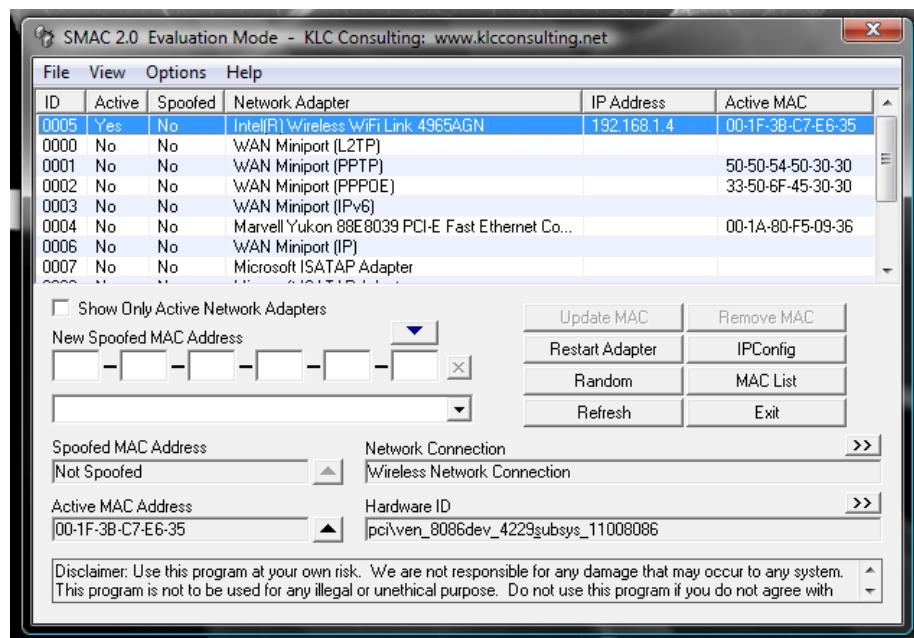


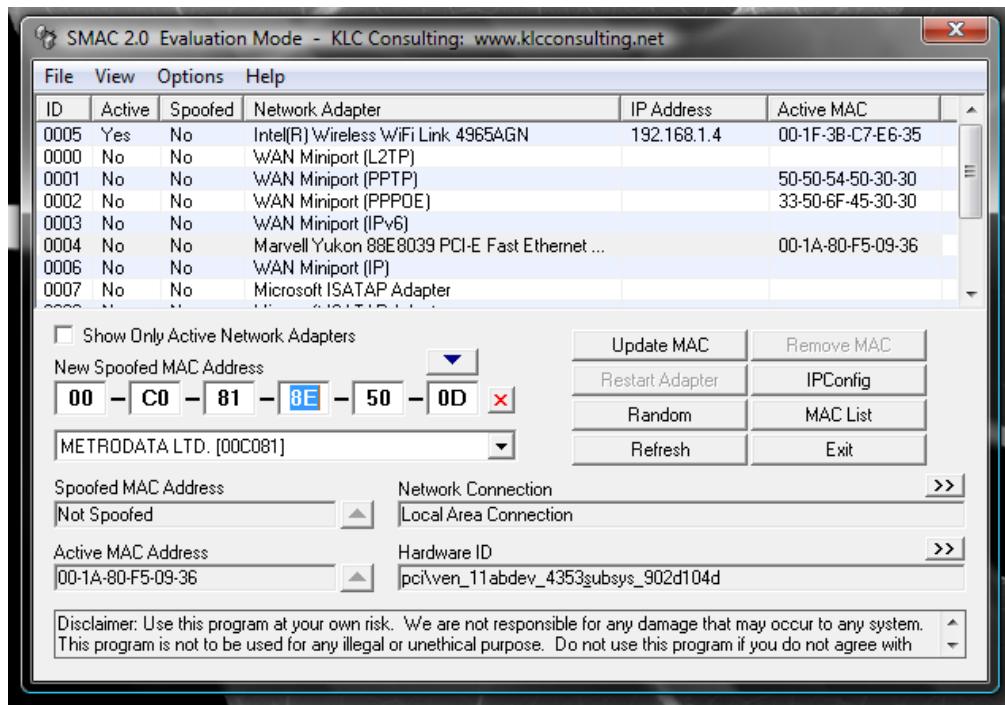
Figure B



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.

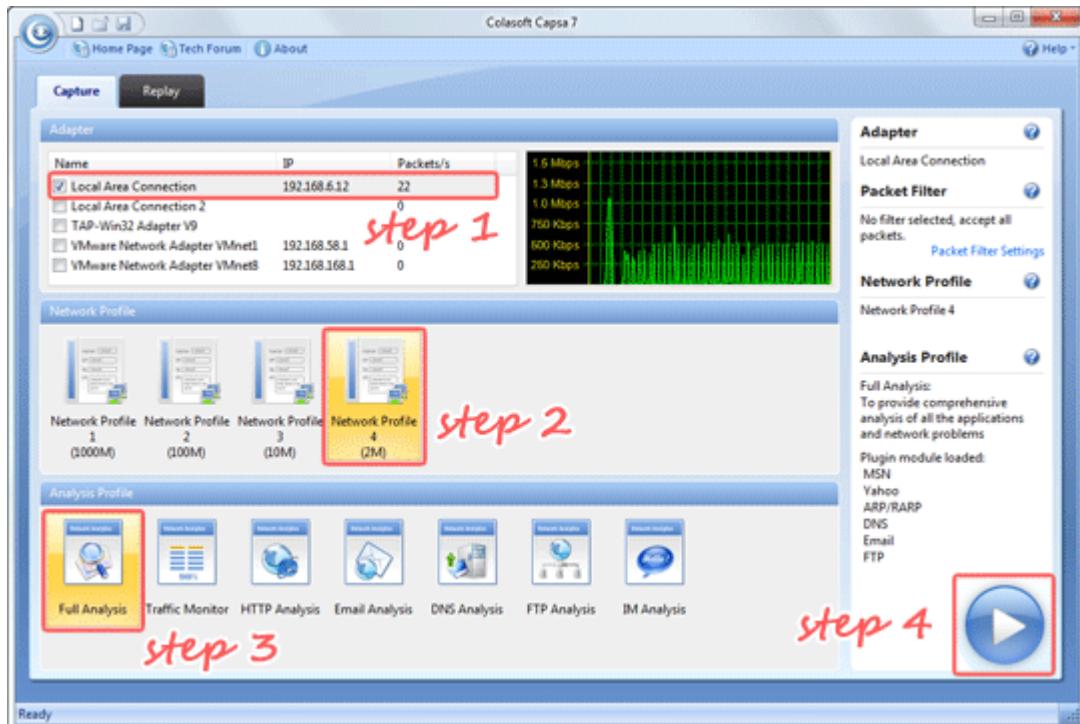
If you know you want to spoof your MAC address to that of a specific manufacturer you can select a different manufacturer from the drop-down list. When you make this selection, the address listed will change. You can keep hitting Random until you get an address you like (or you can just take the first 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.

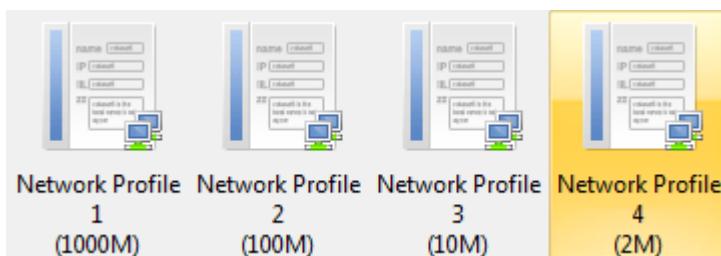
Capsa7's new Start Page guides us start an accurate capture mission step by step:



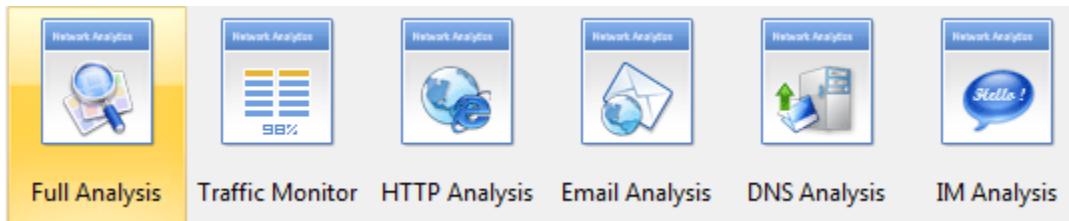
1. Double-click the eye icon on the desktop.
2. In the Start Page, select your NICs (multiple selections available) in the Capture panel first.

Name	IP	Packets/s
<input checked="" type="checkbox"/> Local Area Connection	192.168.6.12	22
<input type="checkbox"/> Local Area Connection 2		0
<input type="checkbox"/> TAP-Win32 Adapter V9		0
<input type="checkbox"/> VMware Network Adapter VMnet1	192.168.58.1	0
<input type="checkbox"/> VMware Network Adapter VMnet8	192.168.168.1	0

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.



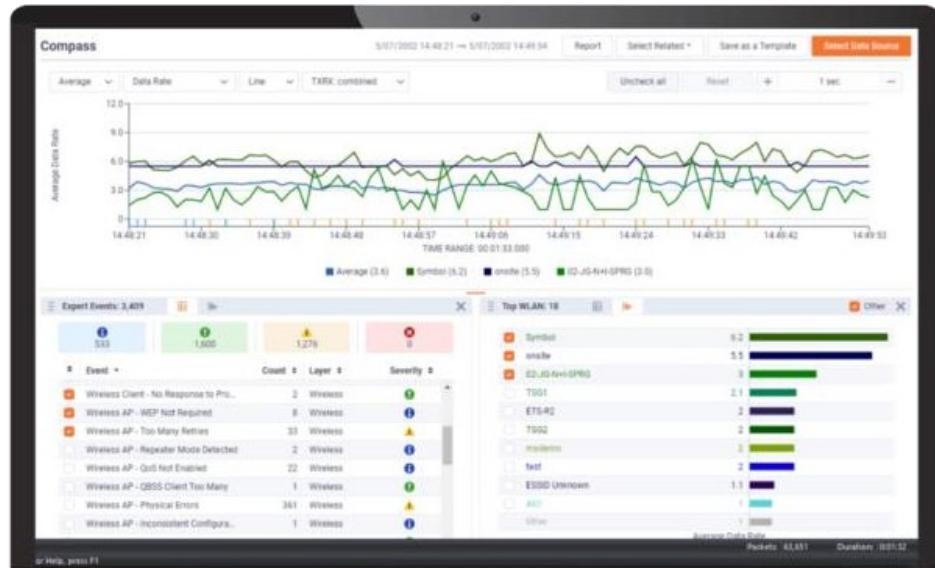
This is the common procedure to start a capture, which helps us get accurate and useful analysis data: Select NIC -> Select Network Profile -> Select Analysis Profile -> Run.

d. Use Omnipcap Network Analyzer.

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

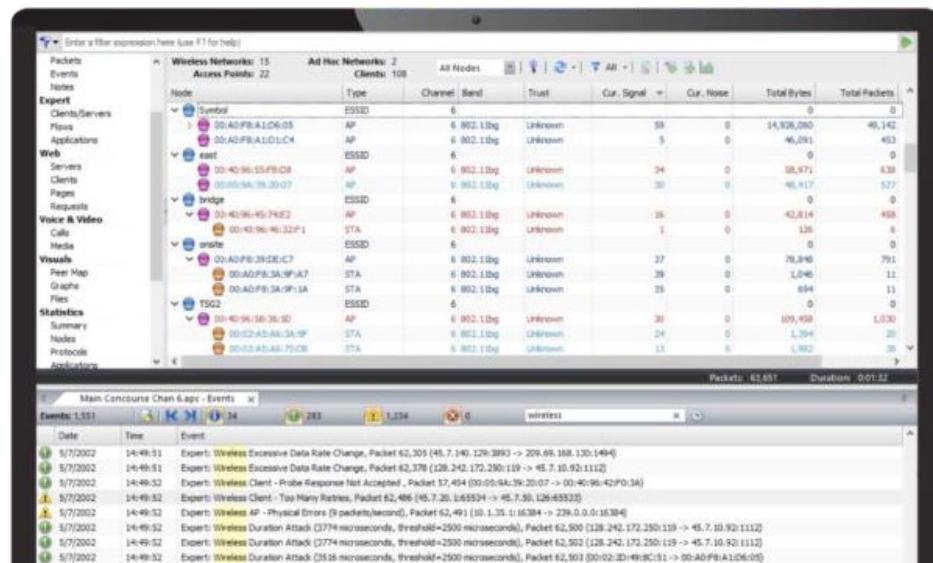
Real-Time Network Protocol Analyzer

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.



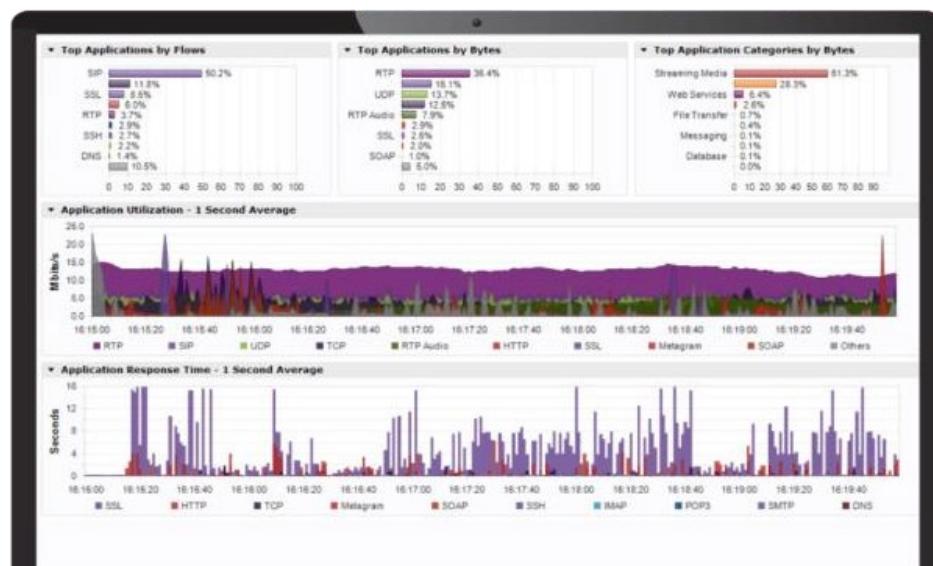
Intuitive Graphic Displays and Visualization

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



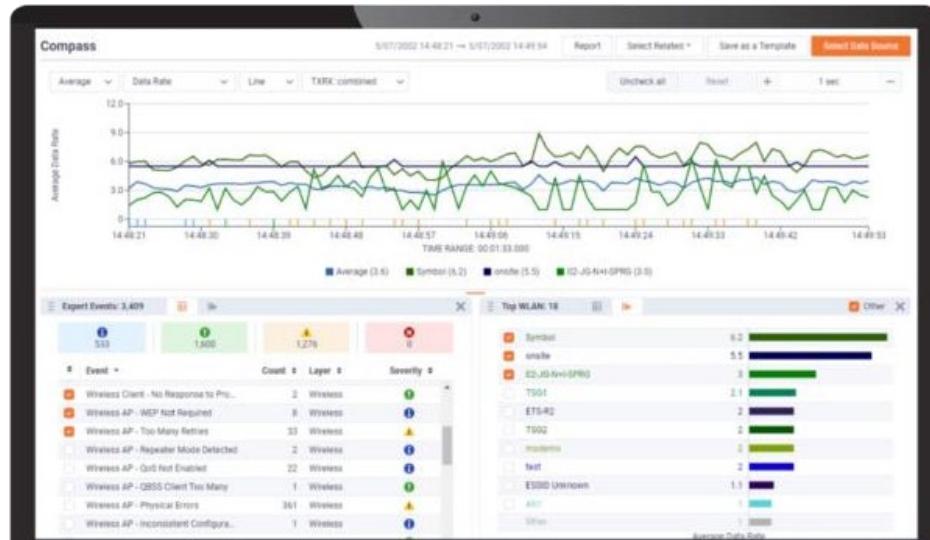
Best-In-Class Network Analysis Workflow

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



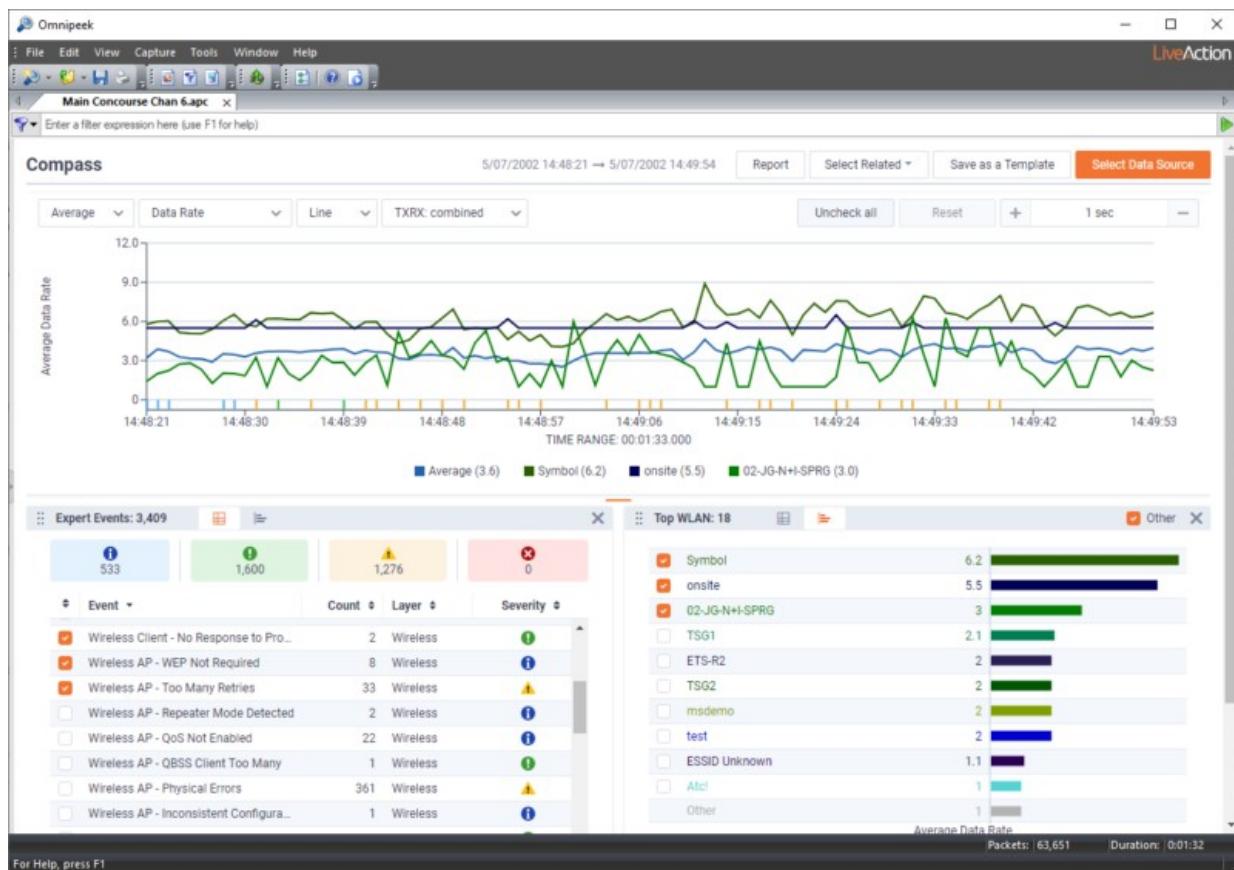
Voice and Video Monitoring and Troubleshooting

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.



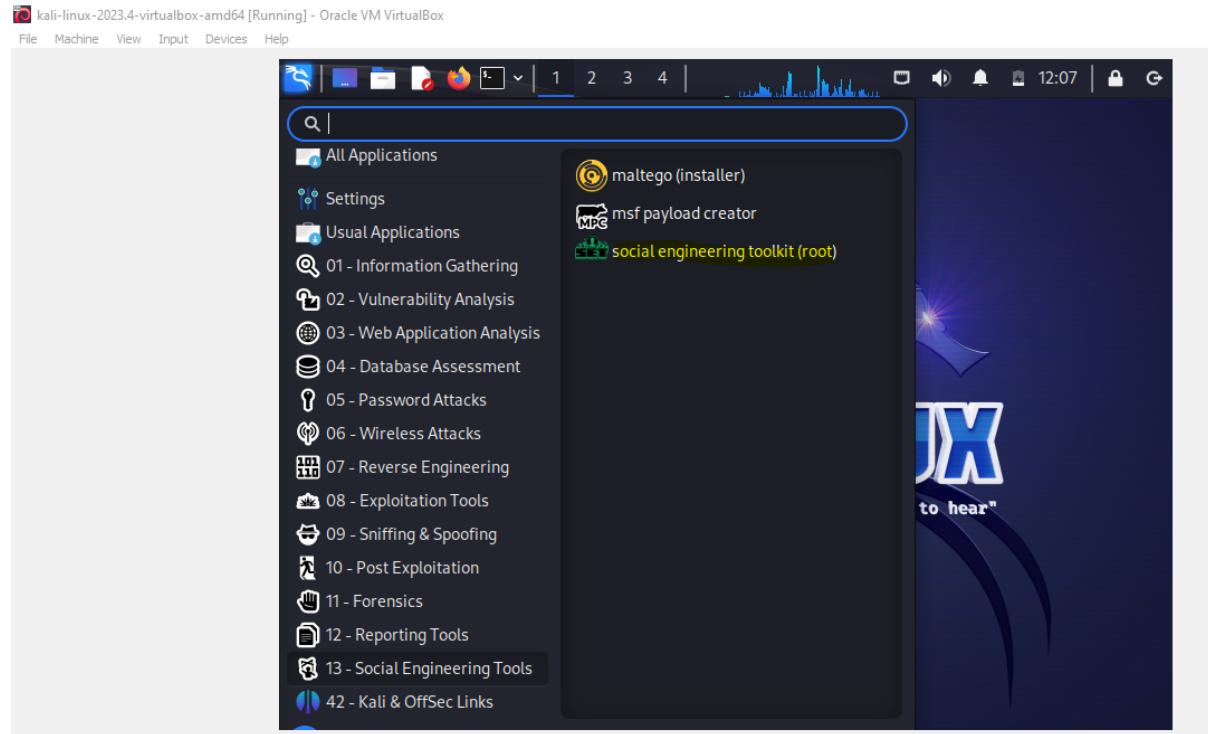
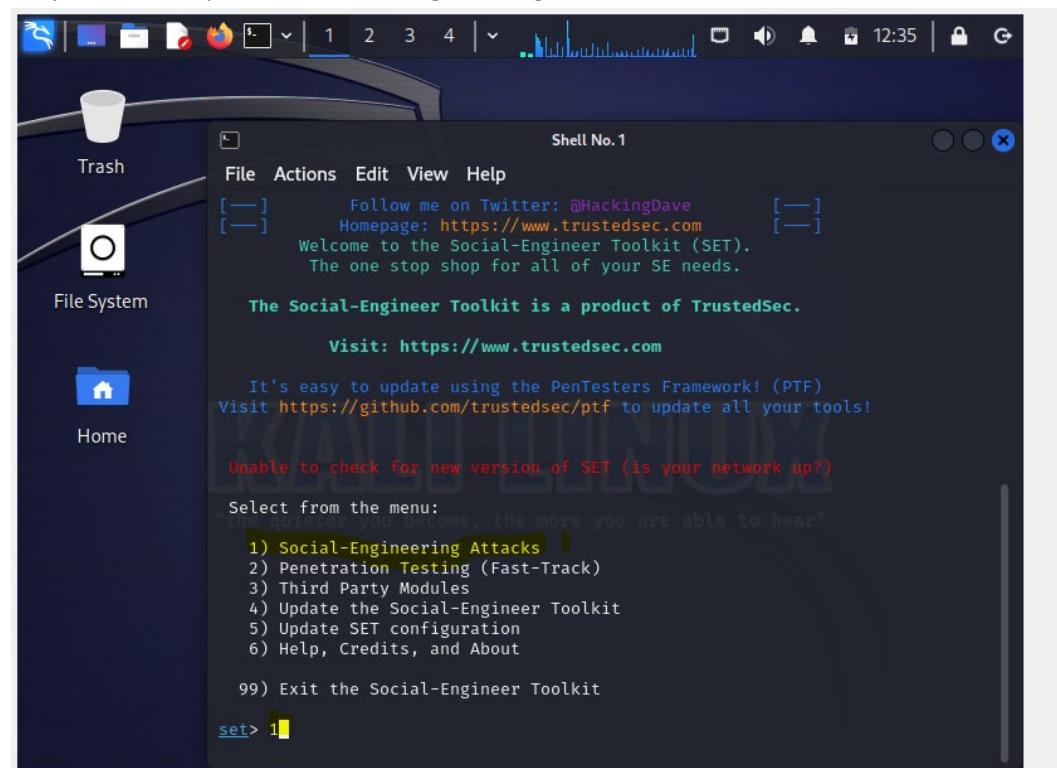
Simplify Troubleshooting Remote Devices

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

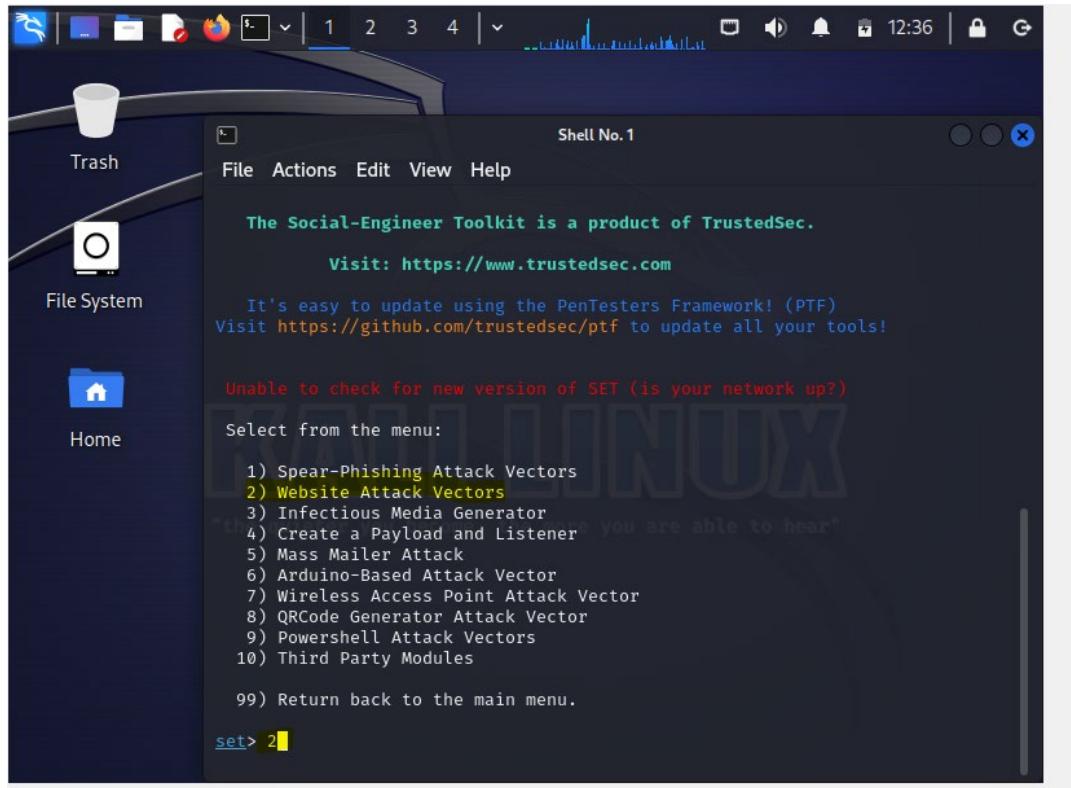


Section III A.

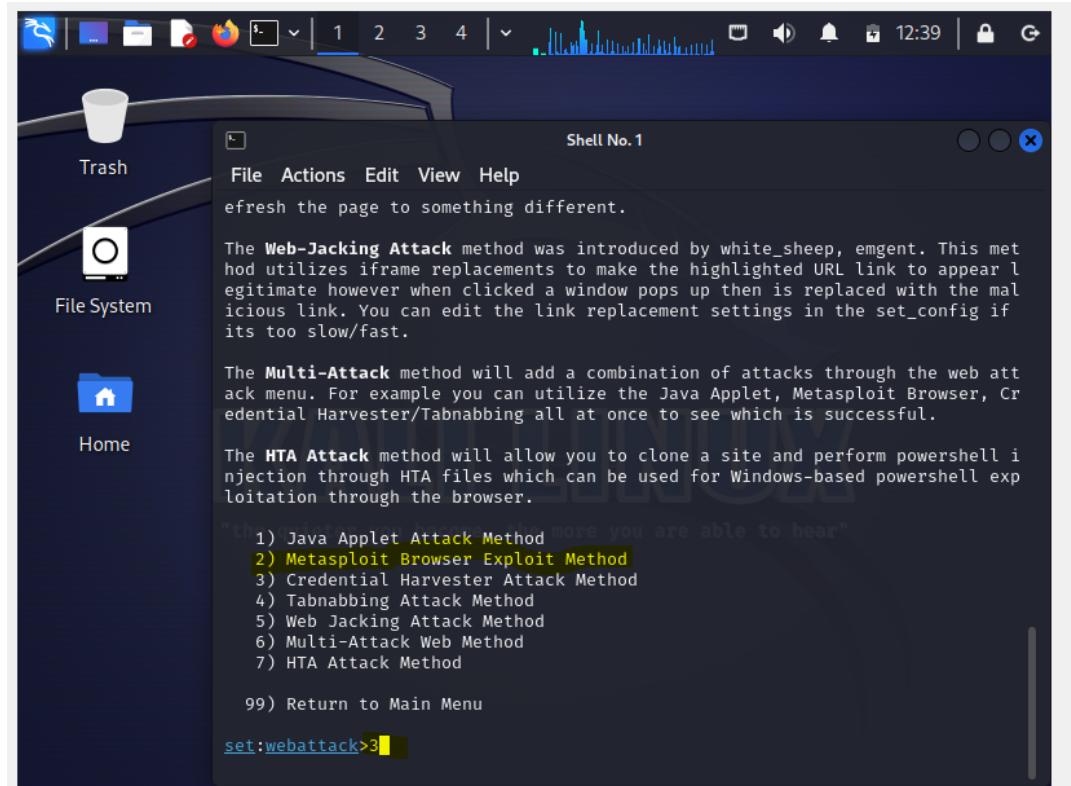
- a. Aim: Use Social Engineering Toolkit on Kali Linux.

Step 1: Select social engineering toolkit in the Kali Linux.**Step 2:** Select option 1. Social engineering attack

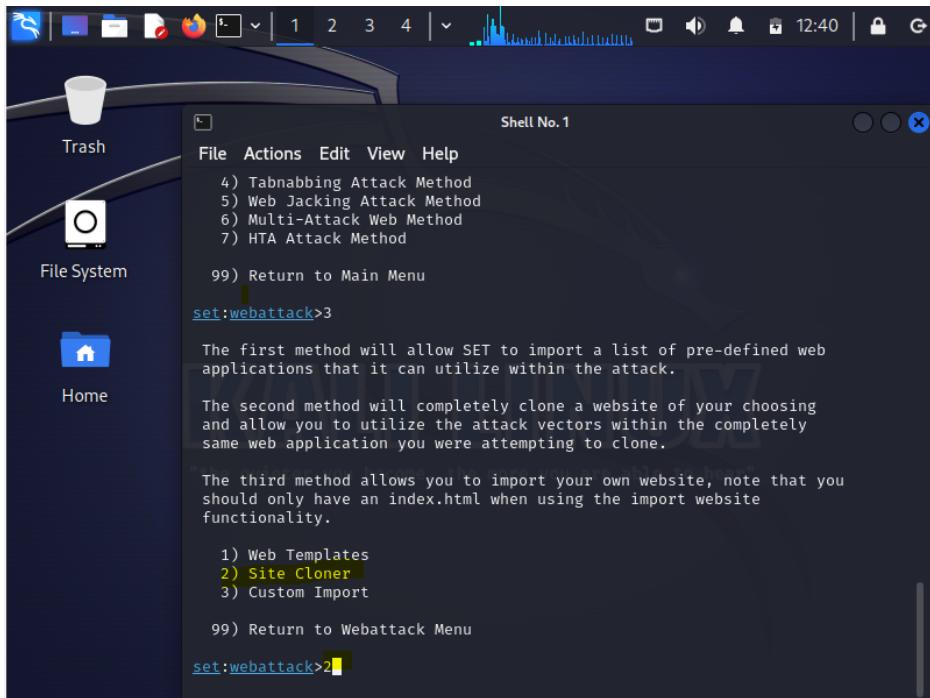
Step 3: Select option 3, website attack vectors



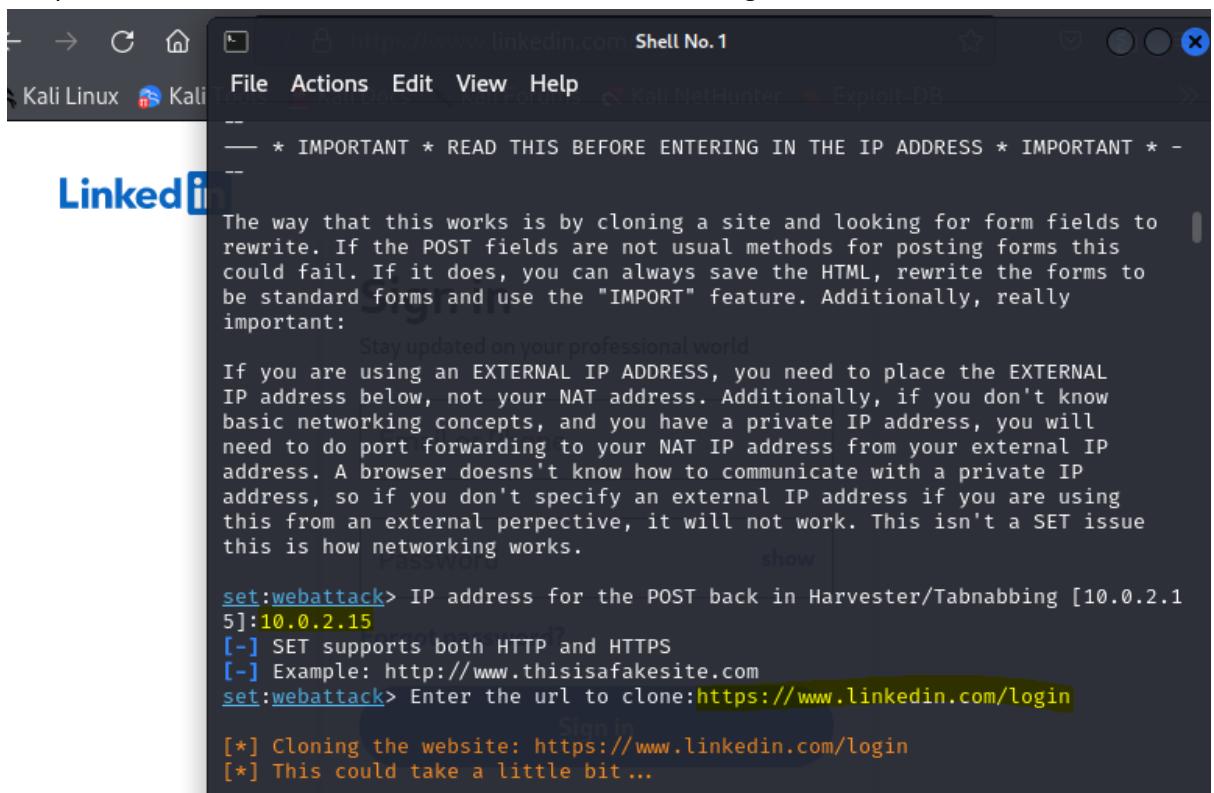
Step 4: Select Credential Harvester attack method



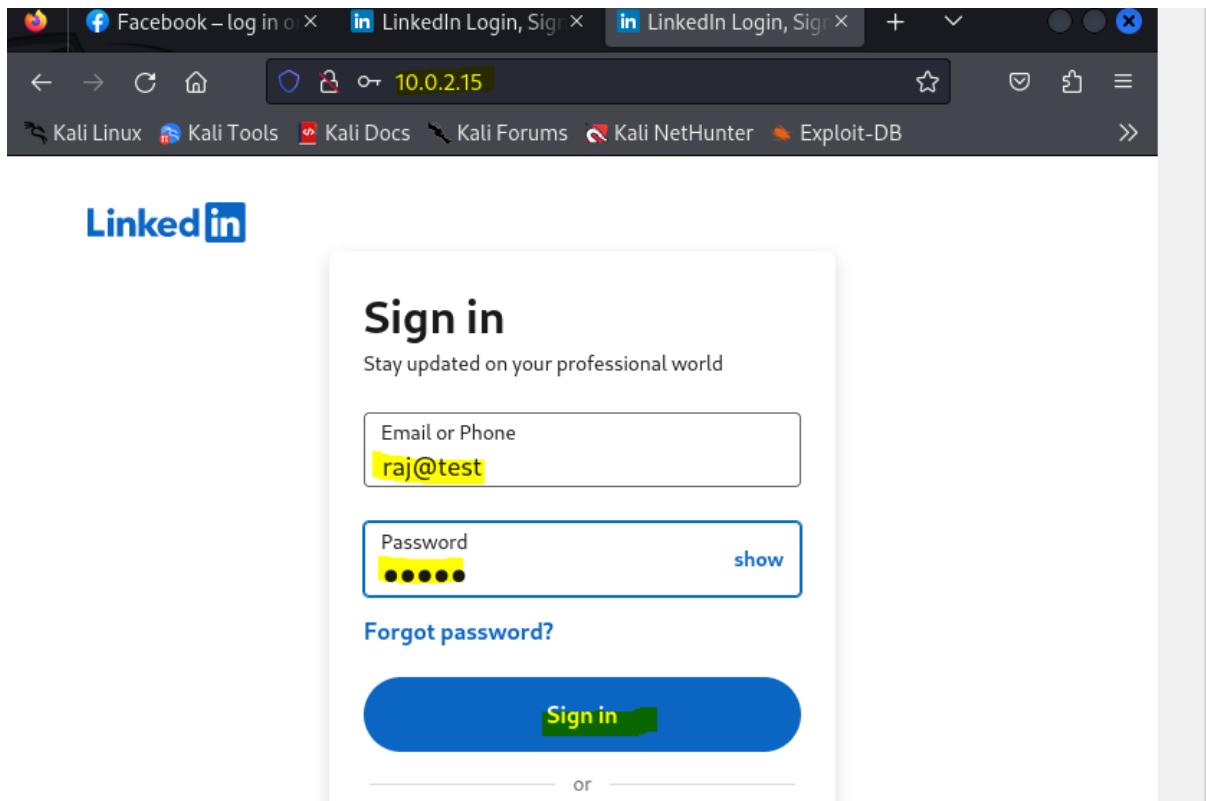
Step4: Select option 2 Site cloner.



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



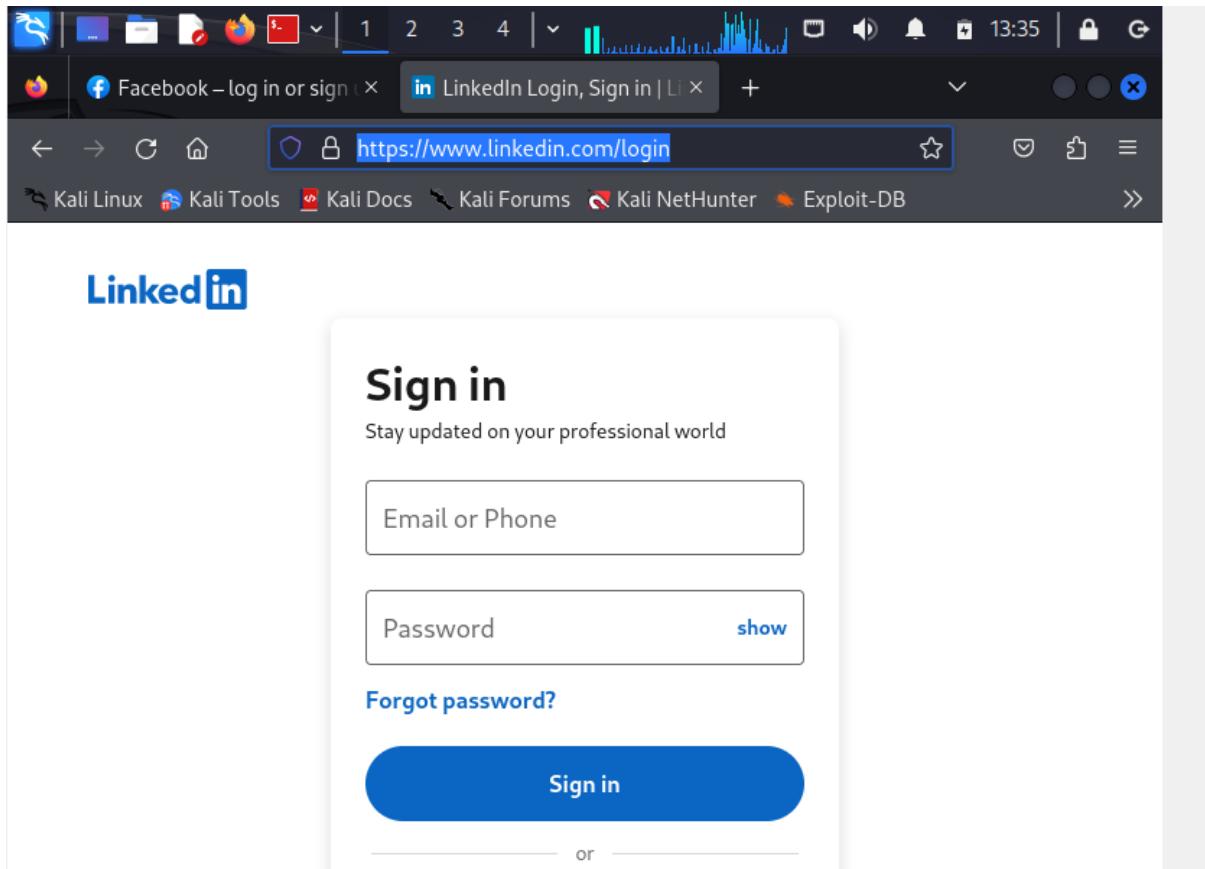
Step 6: now enter the ip in the browser, you will find clone website:



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

```
10.0.2.15 - - [24/Feb/2024 13:33:31] "POST /li/track HTTP/1.1" 302 -
[!] WE GOT A HIT! Printing the output:
PARAM: csrfToken=ajax:6296578694457994505
PARAM: session_key=raj@test
PARAM: ac=0
PARAM: pkSupported=false
PARAM: sIdString=bbb55fc8-fdc2-40ea-b700-88079ab70fe2
POSSIBLE_USERNAME_FIELD FOUND: parentPageKey=d_checkpoint_lg_consumerLogin
POSSIBLE_USERNAME_FIELD FOUND: pageInstance=urn:li:page:checkpoint_lg_login_d
efault;PCr1hOJ2QLSRtd+V1Nd26A==
PARAM: trk=
PARAM: authUUID=
PARAM: session_redirect=
POSSIBLE_USERNAME_FIELD FOUND: loginCsrfParam=733d3080-4d37-48ae-8dc6-a41581a
52935
PARAM: fp_data=default
PARAM: apfc={"df":{"a":"8Gb03Wm1VcPZt9aeKM9hw==","b":null,"c":null,"error":"
TypeError:+window.crypto[_0x561f( ... )]+is+undefined"}}
PARAM: _d=d
POSSIBLE_USERNAME_FIELD FOUND: showGoogleOneTapLogin=true
POSSIBLE_USERNAME_FIELD FOUND: controlId=d_checkpoint_lg_consumerLogin-login_
submit_button
POSSIBLE_PASSWORD_FIELD FOUND: session_password=R@123457
```

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

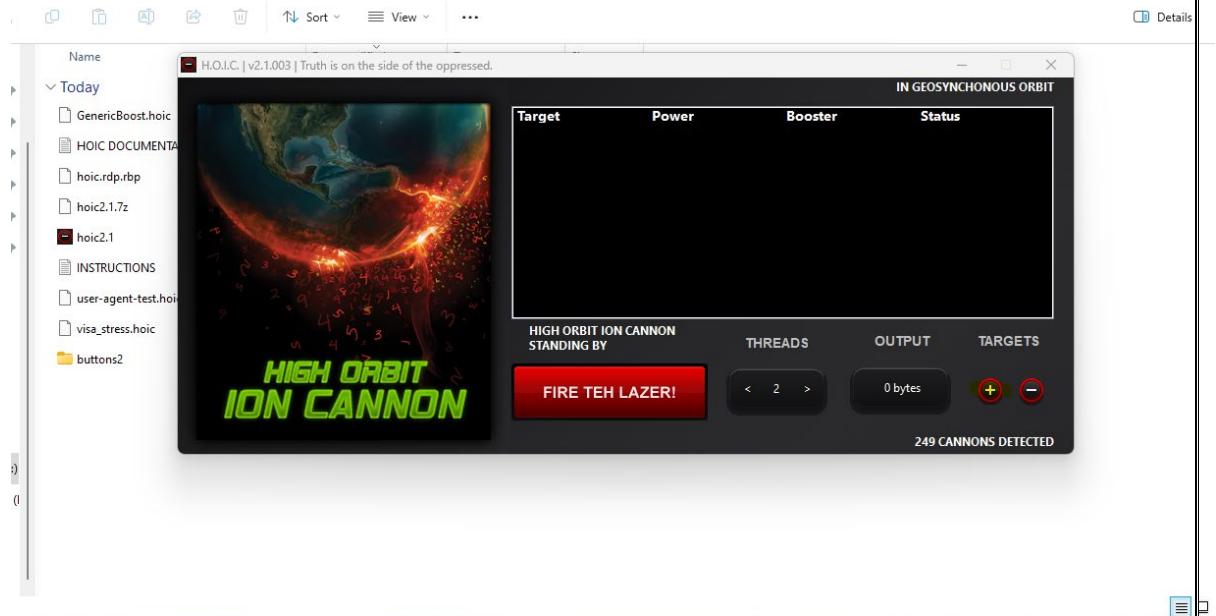


Section III A.

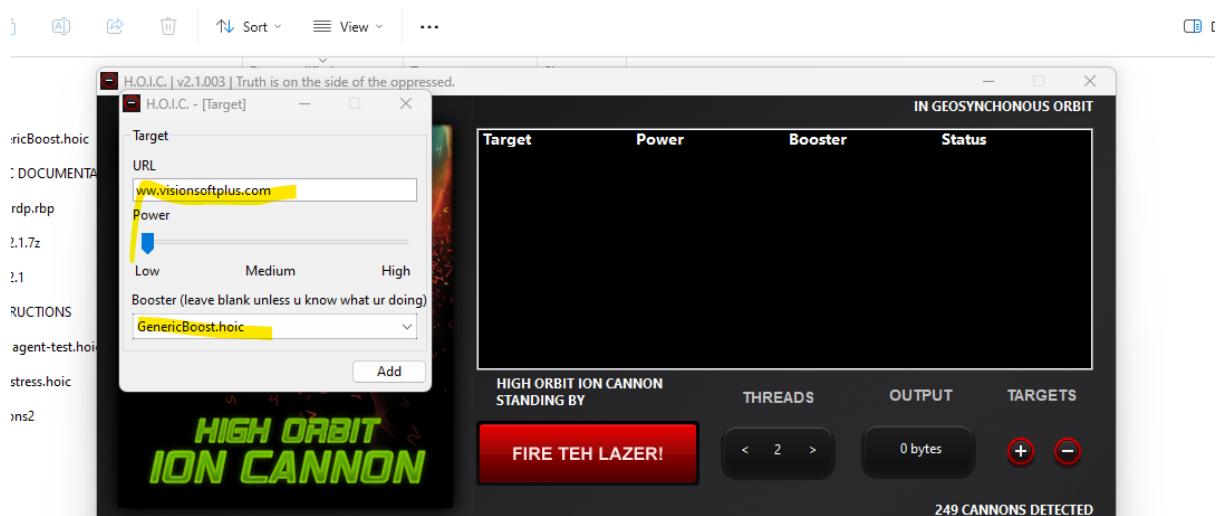
- b. Aim: Perform the DDOS attack using the following tools

I. HOIC

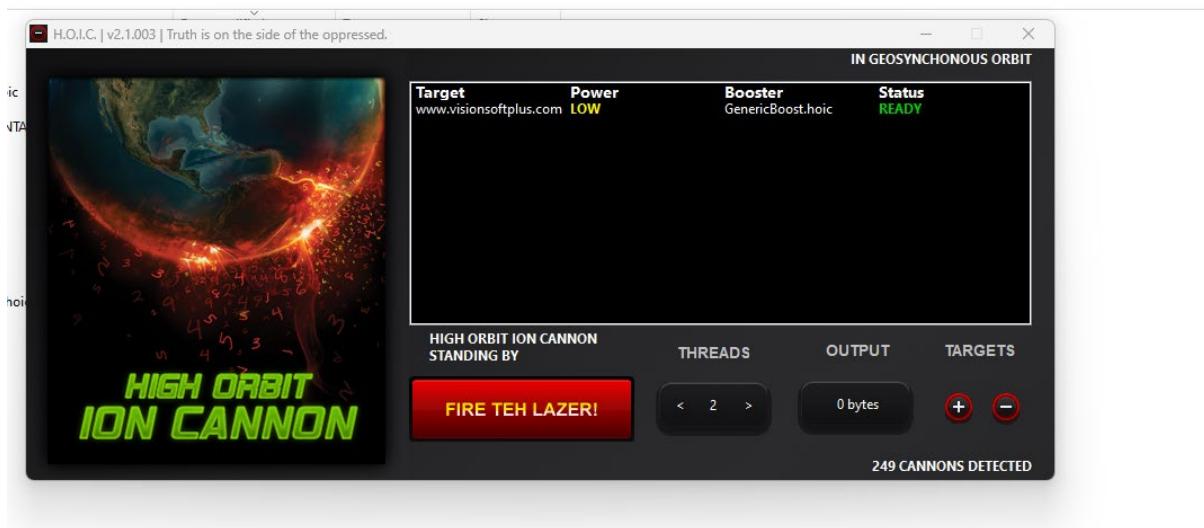
Step 1. Open hoic2.1.exe, once it open click on the “+” button



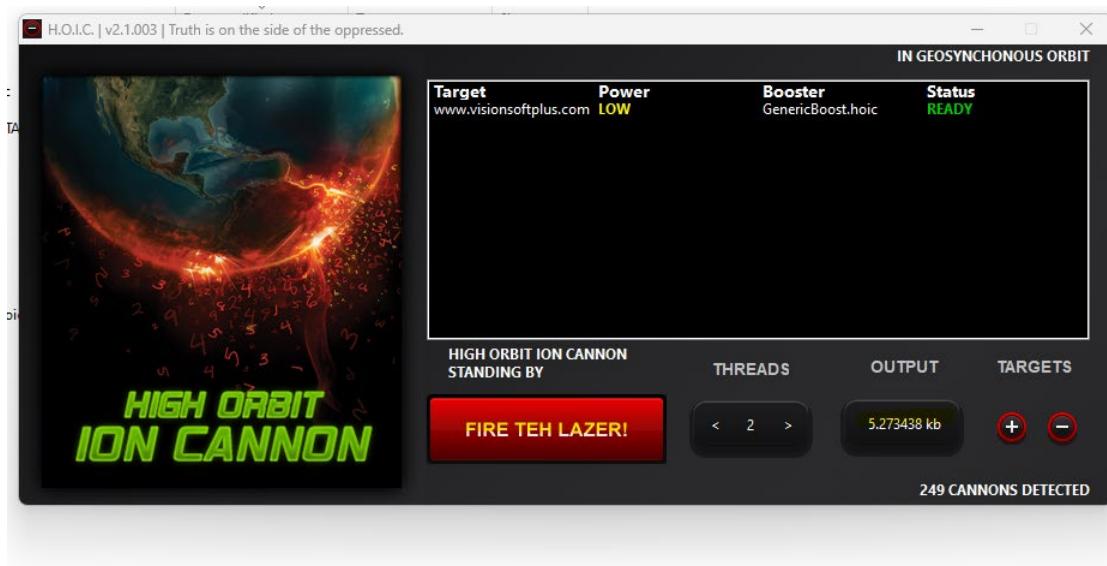
Step2: enter the url you want to attack, then click on add button.



Step 3: Click on fire button to attack



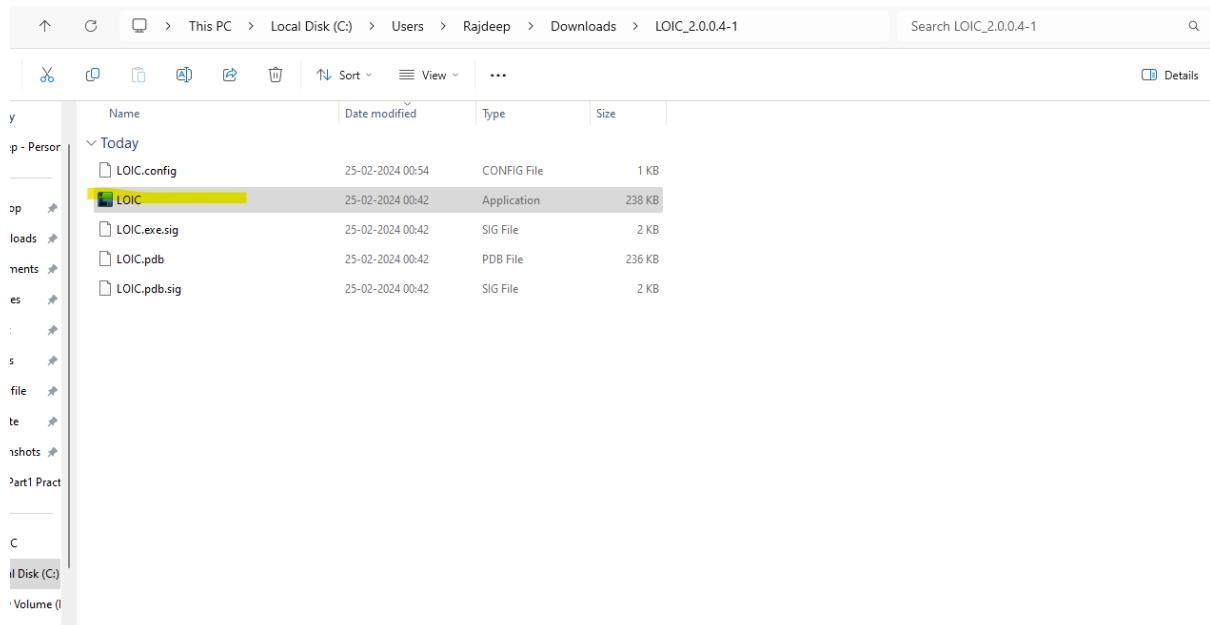
Step 4: you can see the attack is carried on and check the same on wire shark also



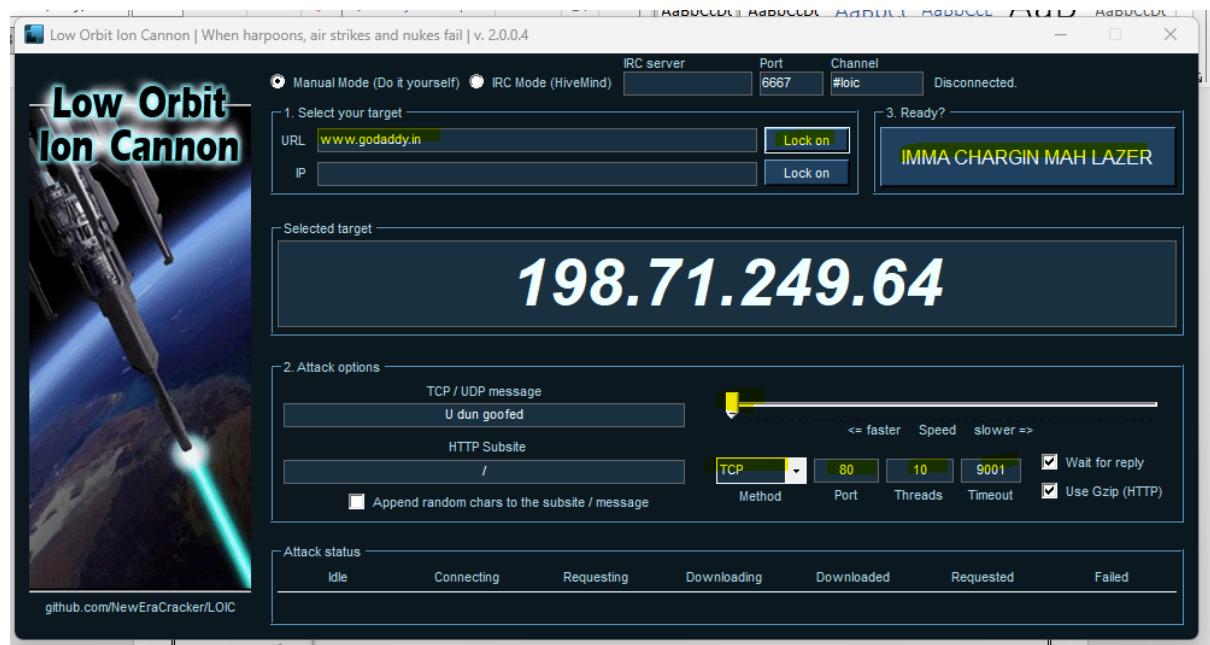
Step 5: To stop the attack again click on the Fire button.

II. LOIC

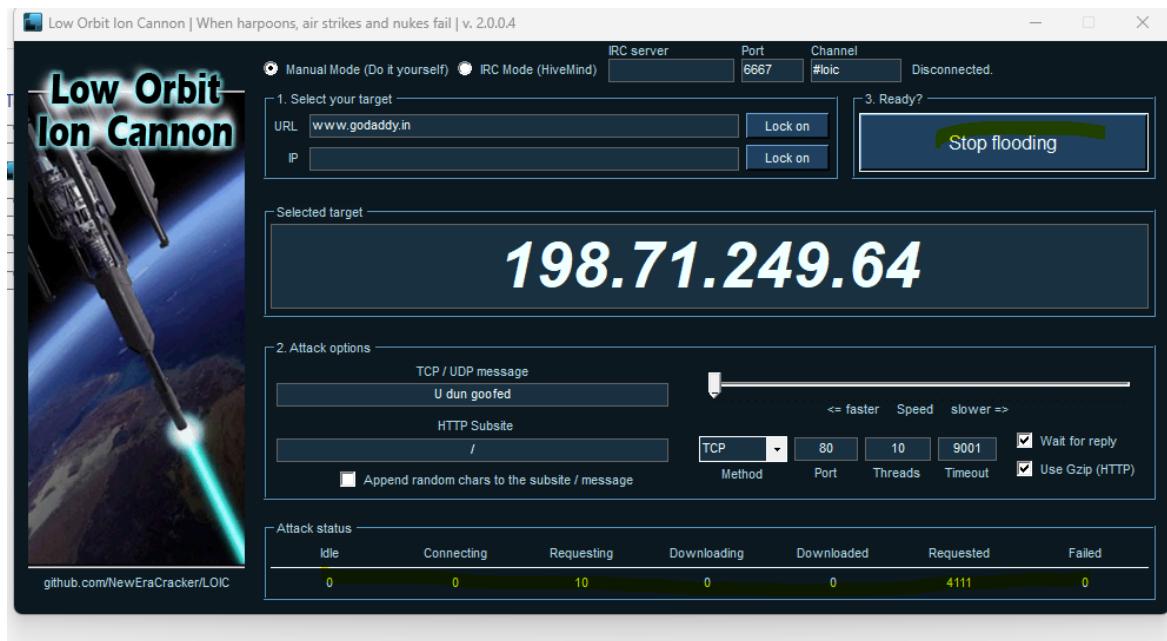
Step 1. Click on the loic.exe:



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.



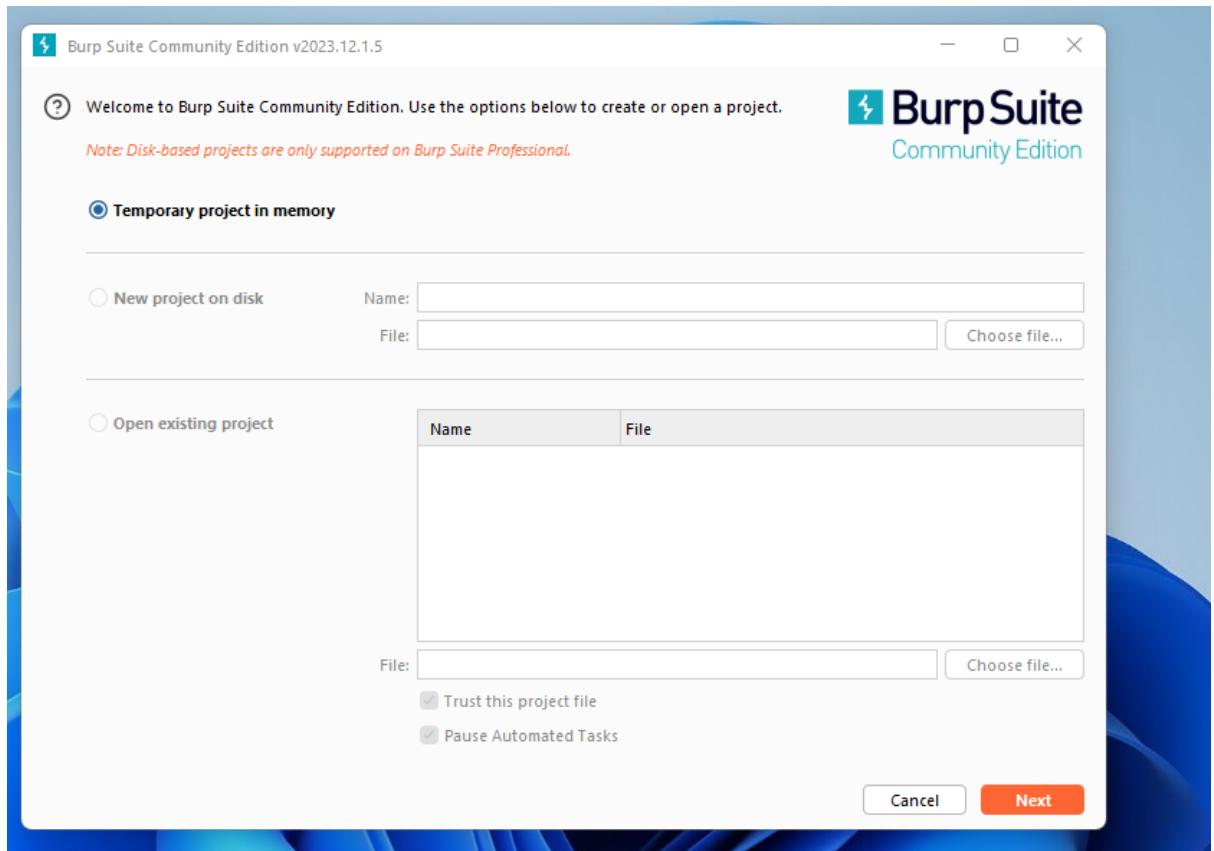
Step 3: You can see the number of requests getting hit. Click on Stop button to stop the DDOS attack.



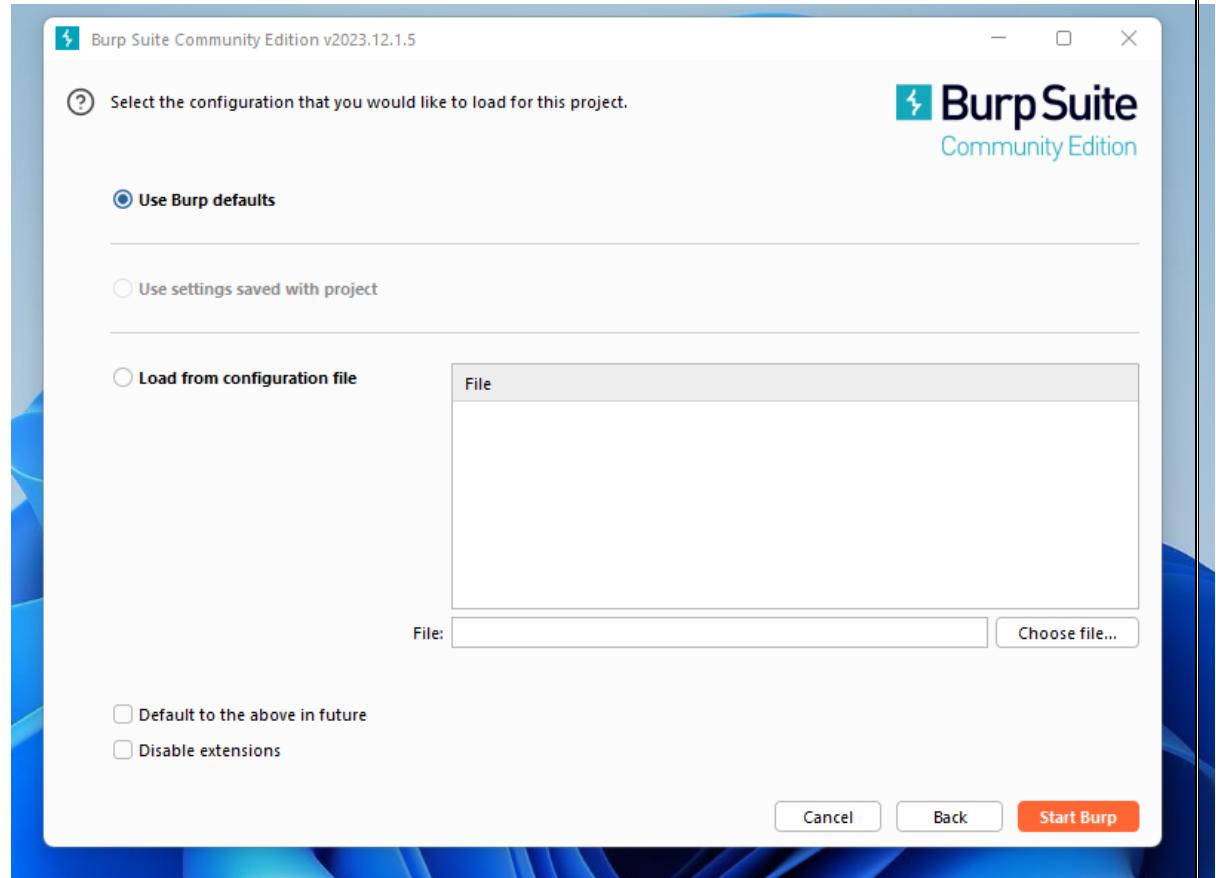
C. Aim: Using Burp Suite to inspect and modify traffic between the browser and target application

Application name : Burp tool

1. Open Burp Tool: Click on next



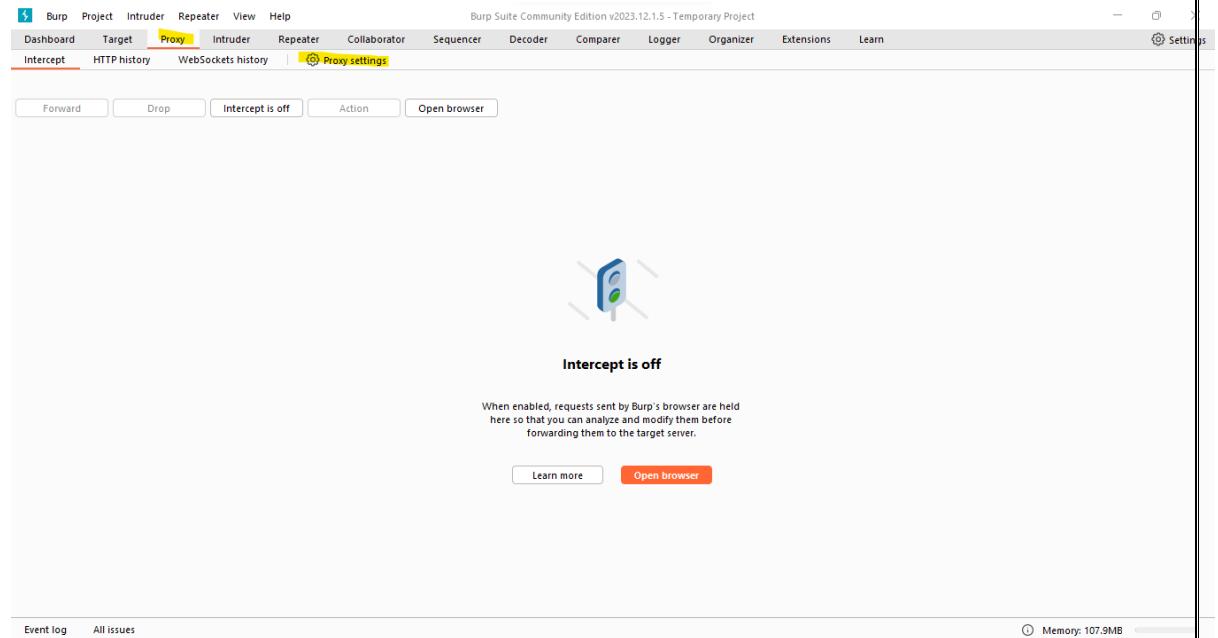
2. Click on start Burp



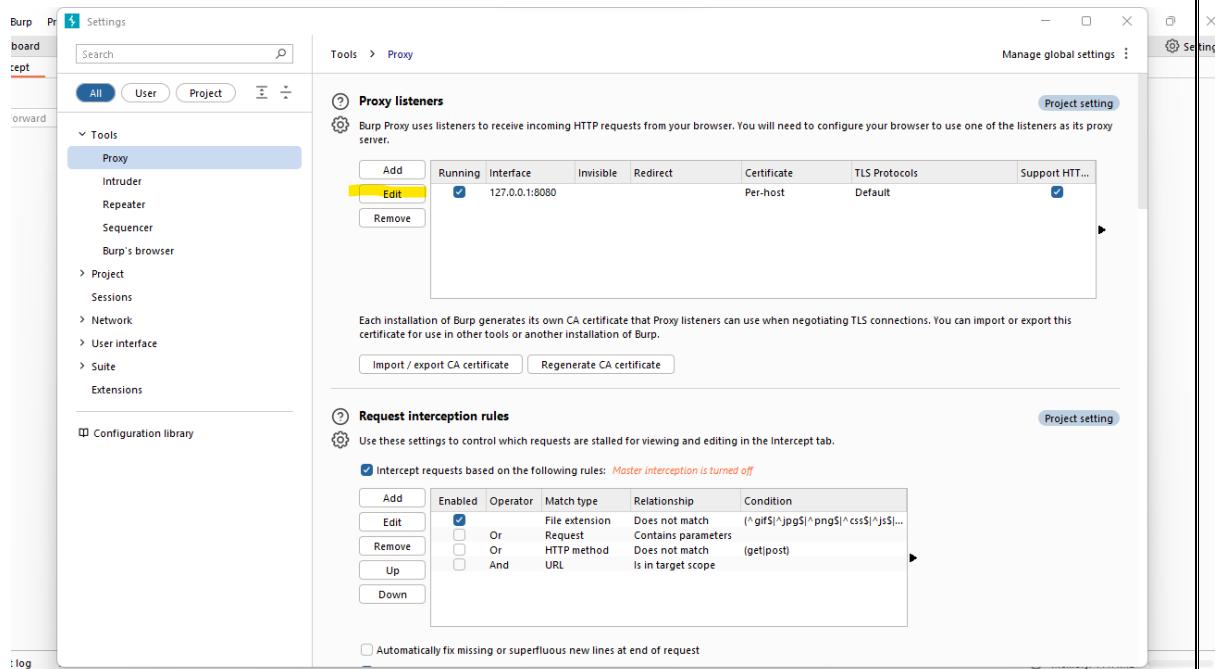
3. Select Proxy in the tab:

A screenshot of the Burp Suite interface. The top navigation bar includes "Burp", "Project", "Intruder", "Repeater", "View", "Help", and "Proxy" (which is highlighted in yellow). Below the tabs, there are buttons for "Forward", "Drop", "Intercept is off" (which is currently active), "Action", and "Open browser". In the center, there is a blue shield icon with a green checkmark and the text "Intercept is off". Below this, a small explanatory text reads: "When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server." At the bottom, there are "Learn more" and "Open browser" buttons. The footer includes "Event log" and "All issues" buttons, and a status bar showing "Memory: 104.6MB".

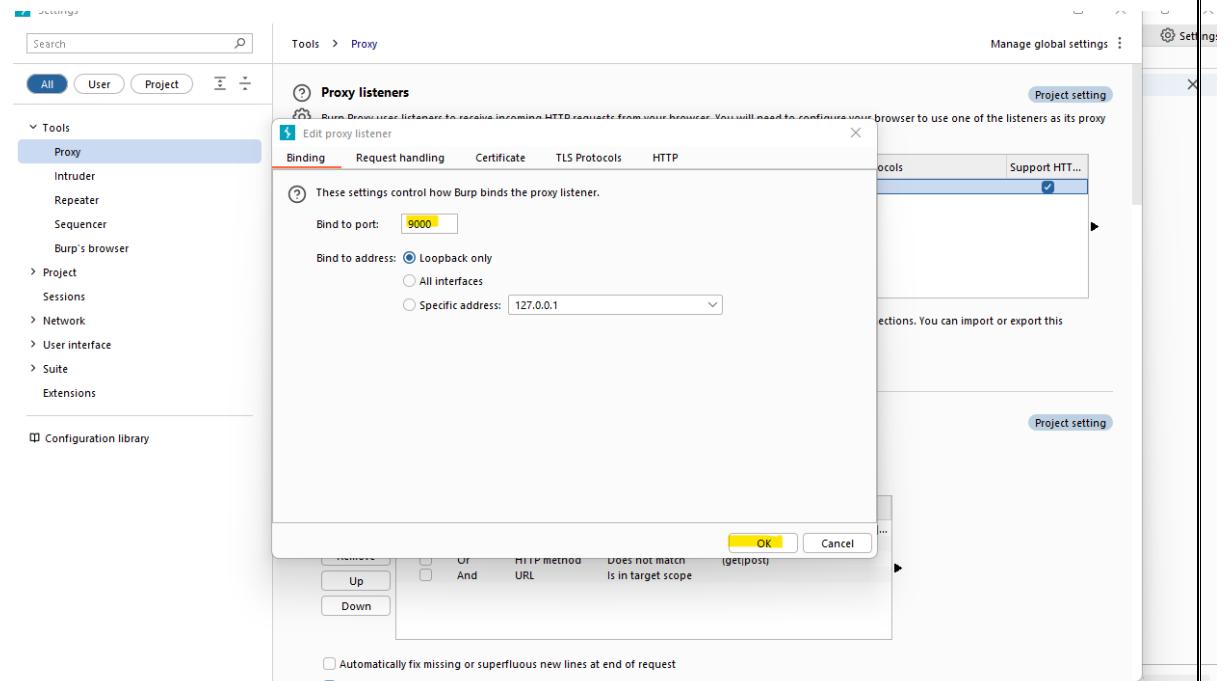
4. Go to proxy setting:



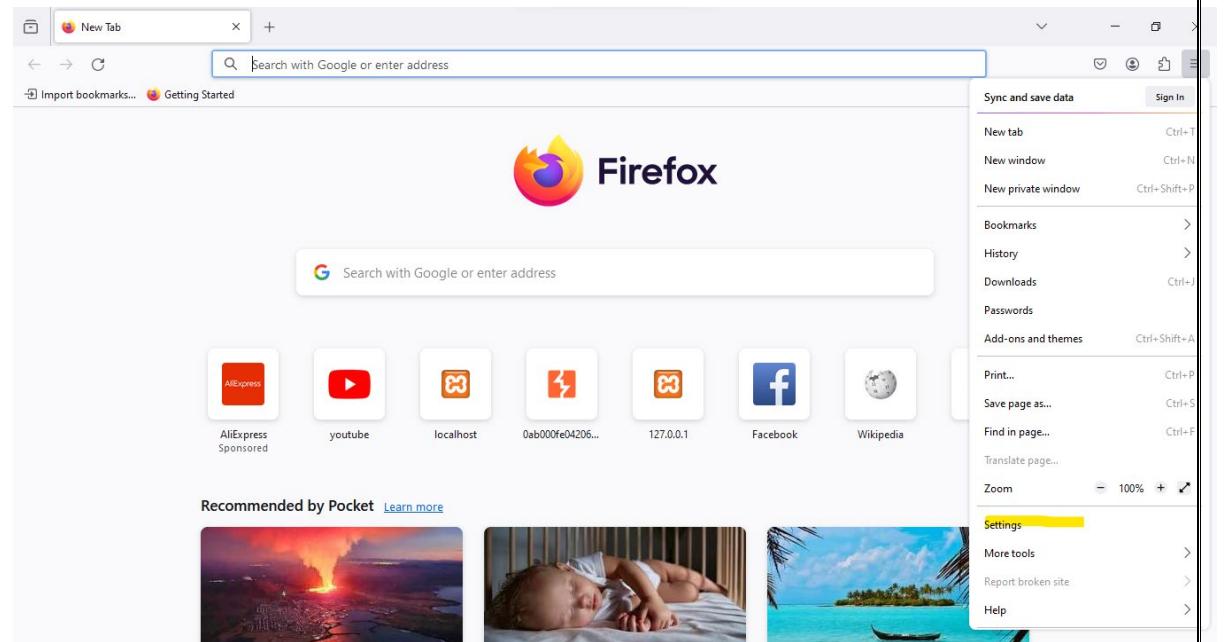
5. Click on Edit:



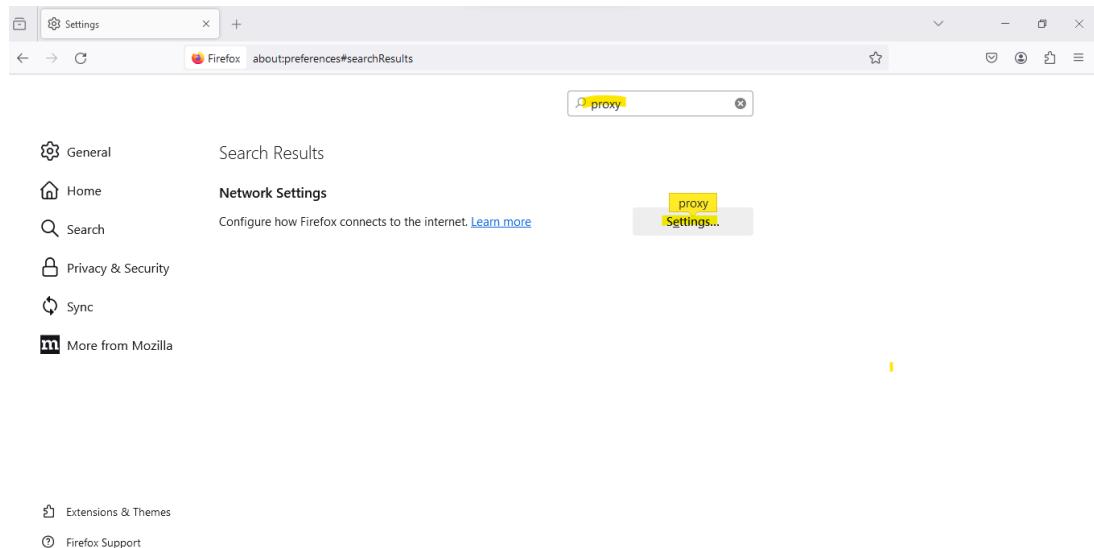
6. Change the port number in our case its change from 8080 to 9000. And then click on OK.



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

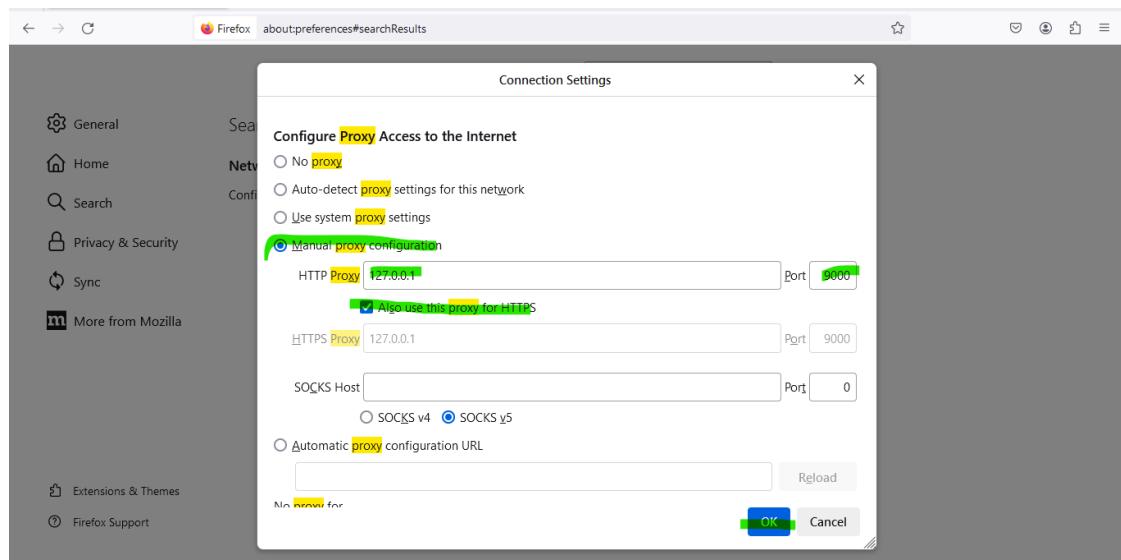


10. Search for proxy in the search bar and then click on setting:

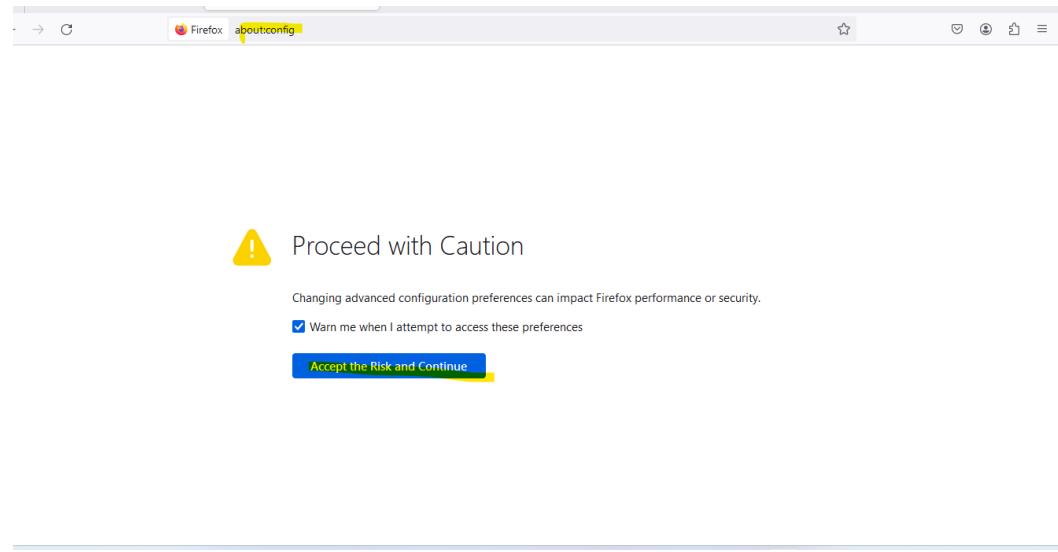


11. Now do the following steps:

- select manual
- Enter ip as 127.0.0.1 and port as 9000.
- select option also use this proxy for HTTPS
- 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:

A screenshot of the Firefox 'Advanced Preferences' window. The search bar at the top contains 'network.proxy'. The table below lists various proxy-related preferences. The 'network.proxy.allow_hijacking_localhost' entry has its value 'true' highlighted with a yellow box, indicating it needs to be changed to 'true'. Other entries include 'network.proxy.backup.ssl' set to '127.0.0.1', 'network.proxy.backup.ssl_port' set to '8080', and 'network.proxy.http' set to '127.0.0.1'. Each row has edit and delete icons on the right.

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

Welcome back!

Learn to secure the web one step at a time, with our practical, interactive learning materials. Covering the latest research, and completely free.

New topic: Web LLM attacks

Learn how to perform attacks using Large Language Models (LLMs). We'll show you how to construct attacks that take advantage of an LLM's access to data, APIs, and user information that you would not be able to access directly.

[Learn more →](#)

Your learning progress

Ready to keep learning? Pick up where you left off, or start a new path ...

[VIEW ALL PATHS](#)

15. scroll down click on all path button:

All learning paths

Learning Path	Level	Progress	Action Buttons
Server-side vulnerabilities	APPRENTICE	3 of 51	View progress → RESUME →
SQL injection	PRACTITIONER	0 of 51	View path → GET STARTED →
API testing	PRACTITIONER	0 of 29	View path → GET STARTED →

16. click on access Lab:

APPRENTICE
Server-side vulnerabilities 3 of 51

Lab: File path traversal, simple case

APPRENTICE LAB Not solved

This lab contains a path traversal vulnerability in the display of product images. To solve the lab, retrieve the contents of the `/etc/passwd` file.

ACCESS THE LAB

Solution BACK SKIP THIS LAB →

Up next: What is access control?

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.

Burp Suite Community Edition v2023.12.1.5 - Te...

Dashboard Target Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history Proxy settings

Request to http://0ac600b0039964a880b3c678008500eb.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is ... Action Open brow... Add notes

Pretty Raw Hex

```

1 GET / HTTP/1.1
2 Host: 0ac600b0039964a880b3c678008500eb.web-security-academy.net
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Te: trailers
13 Connection: close
14
15

```

Inspector Request attributes 2 Request query parameters 0 Request body parameters 0 Request cookies 0 Request headers 12

Request attributes Request query parameters Request body parameters Request cookies Request headers

Event log All issues Memory: 111.4MB

The proxy server is refusing connections

An error occurred during a connection to 0ac600b0039964a880b3c678008500eb.web-security-academy.net.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

18. To load the field click on forward button.

Note you will have to click multiple time to load the entire page.

The screenshot shows a web browser window with a URL like <https://0ac600b0039964a880b3c678008500eb.web-security-.star>. The page content includes a header 'WE LIKE TO SHOP' with a hanger icon, and a grid of four items: 'Poo Head - It's not just an insult anymore.', 'The Lazy Dog', 'BBQ Suitcase', and 'Vintage Neck Defender'. Below each item is a 'View details' button. The Burp Suite proxy window is open, showing the intercepted request for the 'Poo Head' item. The 'Proxy' tab is active, and the 'Intercept' button is highlighted in green.

19. click on the first grid view details button:

The screenshot shows a web browser window with a URL like <https://0ac600b0039964a880b3c678008500eb.web-security-.star>. The page content includes a grid of four items: 'Poo Head - It's not just an insult anymore.', 'The Lazy Dog', 'BBQ Suitcase', and 'Vintage Neck Defender'. The first item, 'Poo Head', has its 'View details' button highlighted with a yellow box. The Burp Suite proxy window is overlaid, showing the intercepted request for the 'Poo Head' item. The 'Inspector' tab is active, displaying various request parameters and headers.

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

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request is being edited in the 'Raw' tab with the following content:

```

1 GET /product?productId=1 HTTP/1.1
2 Host: 0ac600b0039964a880b3c678008500eb.web-security-academy.net:443
3 Cookie: session=RtXcmigJpSoJofLKAhhuvrPJAJ6WteGxj
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ac600b0039964a880b3c678008500eb.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16

```

The response pane displays four product cards:

- Poo Head - It's not just an insult anymore.
- The Lazy Dog
- BBQ Suitcase
- Pest Control Umbrella

The 'Pest Control Umbrella' card is highlighted with a yellow arrow pointing to it.

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

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. The 'Inspector' panel shows the 'productId' parameter with a value of '3'. The 'Apply changes' button is highlighted in orange.

The request body now contains:

```

1 GET /product?productId=3 HTTP/1.1
2 Host: 0ac600b0039964a880b3c678008500eb.web-security-academy.net:443
3 Cookie: session=RtXcmigJpSoJofLKAhhuvrPJAJ6WteGxj
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ac600b0039964a880b3c678008500eb.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16

```

The response pane displays the same four product cards as before, but the 'Pest Control Umbrella' card is no longer highlighted.

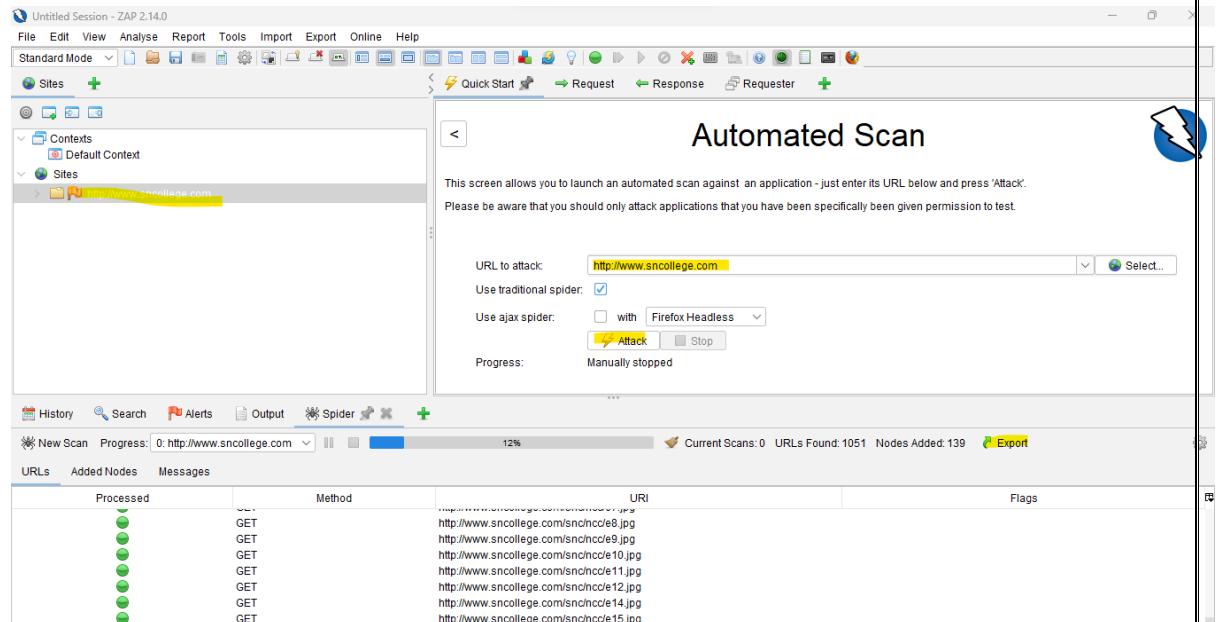
4. Then click on forward you will observe, page for item 3 will open instead of 1.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A browser window displays a lab titled 'File path traversal, simple case' from 'Web Security Academy'. The page content includes a product listing for 'BBQ Suitcase' with a star rating of 4.5 and a price of \$71.72, accompanied by an image of skewered food on a grill. The Burp Suite toolbar at the bottom shows 'Intercept is on'.

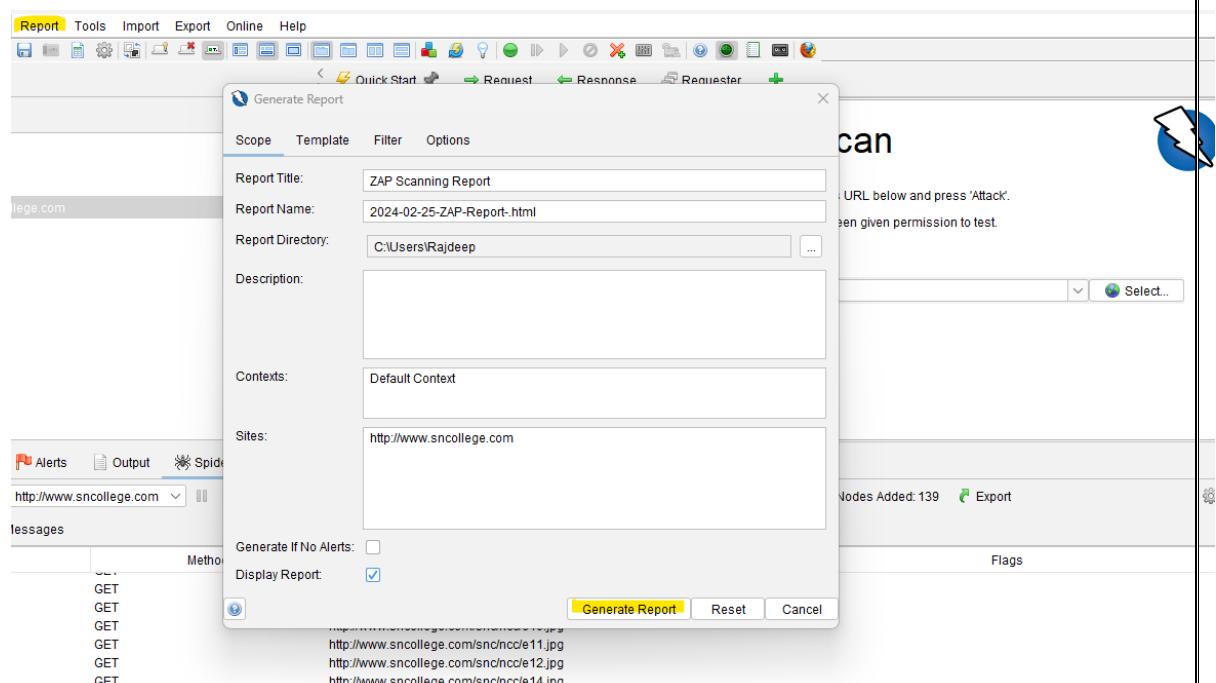
Section 3 B.

- 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:

ZAP Scanning Report
Generated with [ZAP](#) on Sun 25 Feb 2024, at 05:40:09
ZAP Version: 2.14.0

Contents

- [About this report](#)
- [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(1\)](#)
 - [Risk=Medium, Confidence=Low \(1\)](#)
 - [Risk=Low, Confidence=Medium \(2\)](#)
 - [Risk=Informational, Confidence=Medium \(2\)](#)
- [Appendix](#)
 - [Alert types](#)

About this report

[Report parameters](#)

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

[**Content Security Policy \(CSP\) Header Not Set \(1\)**](#)

► GET <http://www.sncollege.com>

Risk=Medium, Confidence=Medium (1)

[http://www.sncollege.com \(1\)](http://www.sncollege.com)

[**Missing Anti-clickjacking Header \(1\)**](#)

► GET <http://www.sncollege.com>

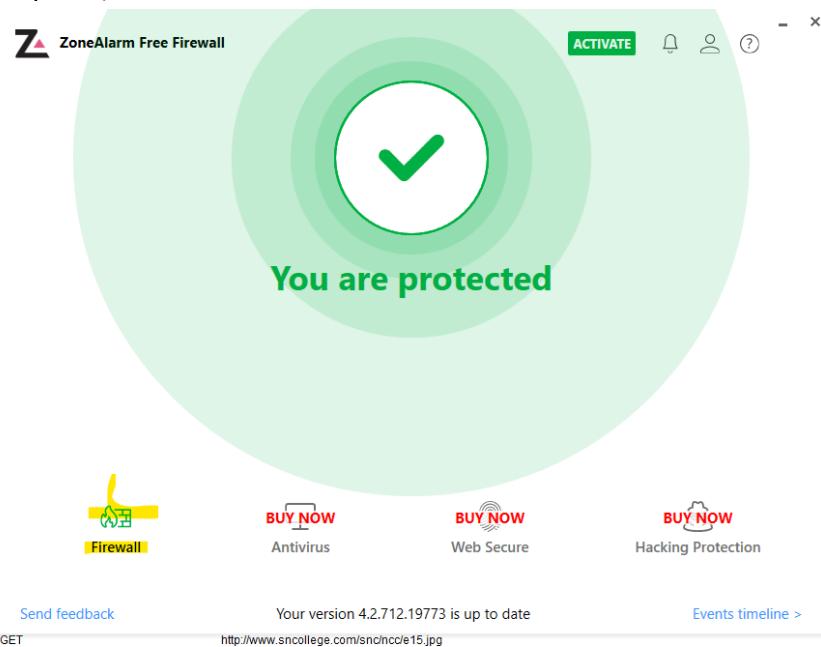
Risk=Medium, Confidence=Low (1)

...

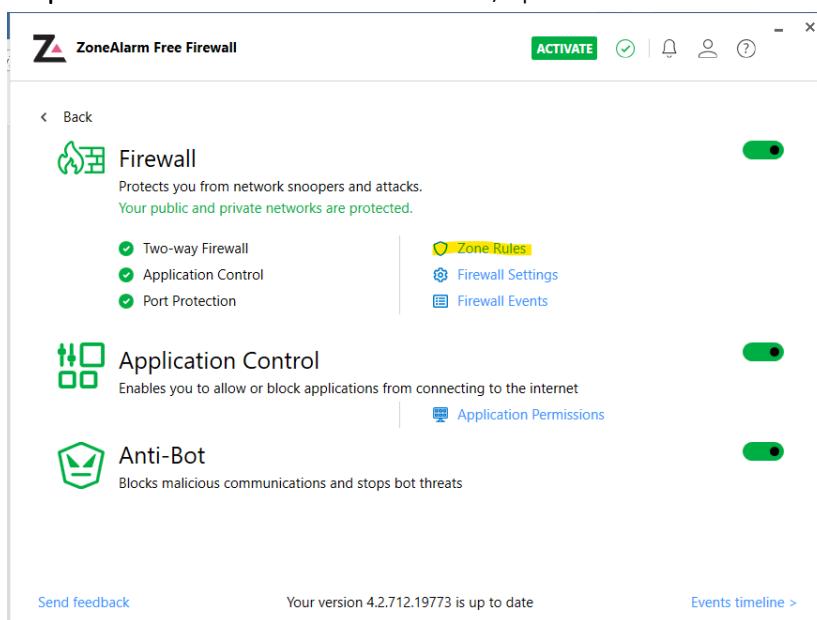
C: Demonstrate the use of the following firewalls

- 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:



The screenshot shows the ZoneAlarm Free Firewall interface. At the top, there's a navigation bar with the ZoneAlarm logo, the text "ZoneAlarm Free Firewall", and buttons for "ACTIVATE", a checkmark icon, a bell icon, a user icon, and a help icon. Below the navigation is a "Manage Zone Rules" section with a table:

NAME	IP ADDRESS/SITE	ENTRY TYPE	ZONE	EDIT	DELETE
Ethernet (Network)	192.168.29.0/255.255.255.0	Network	Public		

Below the table, a modal window titled "Add Zone Rule" is displayed. It contains fields for "Entry Type" (set to "Subnet"), "Zone" (set to "Public"), "IP Address" (empty), "Subnet Mask" (set to "255.255.255.0"), and "Description" (set to "New Zone Rule"). There are "ADD" and "Cancel" buttons at the bottom of the modal.

This screenshot shows the same ZoneAlarm interface after adding a new rule. The "Manage Zone Rules" table now includes a new row:

NAME	IP ADDRESS/SITE	ENTRY TYPE	ZONE	EDIT	DELETE
Ethernet (Network)	192.168.29.0/255.255.255.0	Network	Public		
New Zone Rule	192.168.2.120	IP Address	Trusted		

At the bottom of the interface, there are "Send feedback", "Your version 4.2.712.19773 is up to date", and "Events timeline >" links.

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

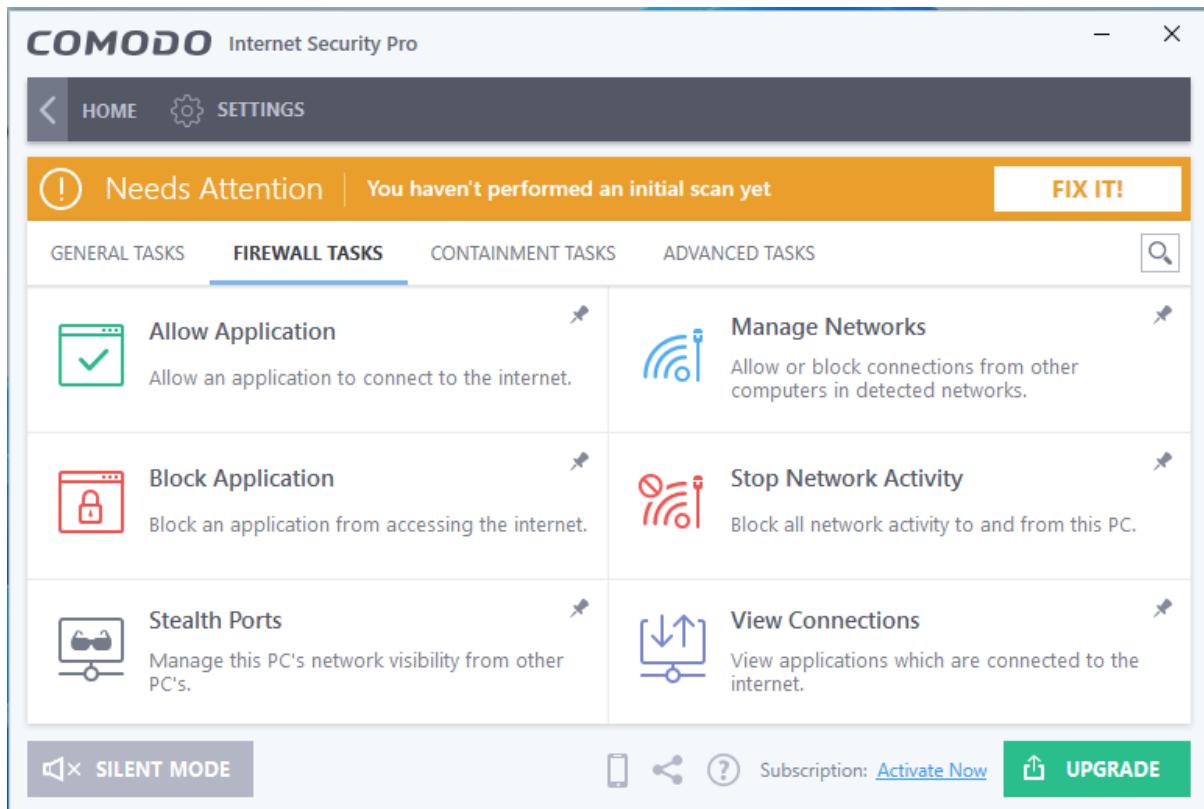
Public
 Your Public Zone security is **High**. Lets you connect to a network, but prevents anyone on the network from connecting with you. Recommended.

Trusted
 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 >](#)

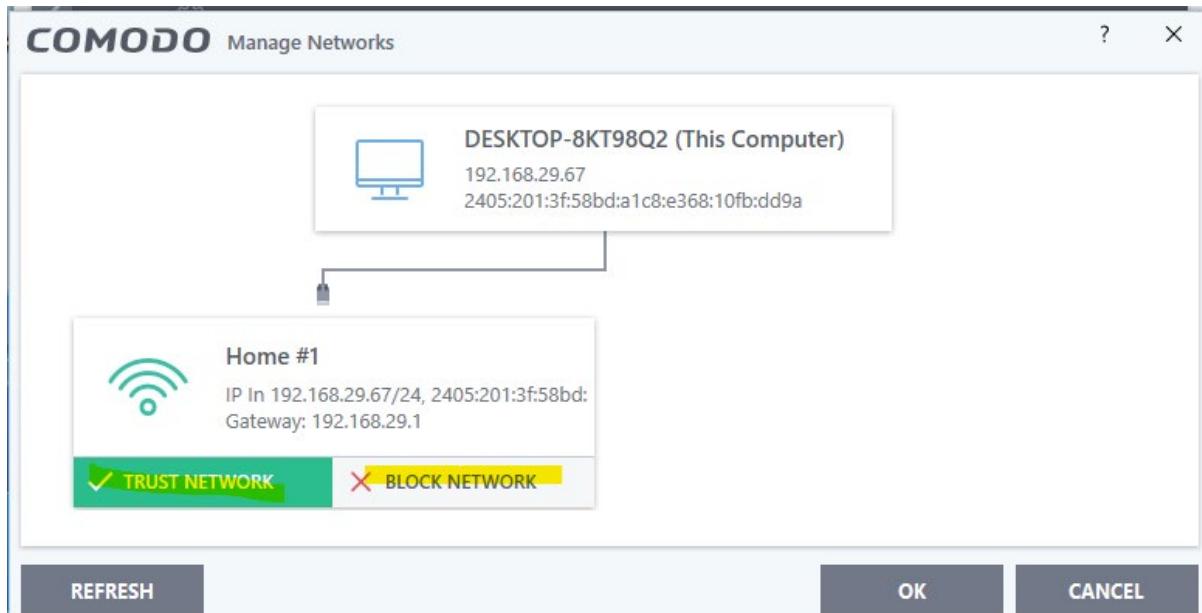
II Comodo Firewall:

Step 1: Open comodo-> go to firewall.

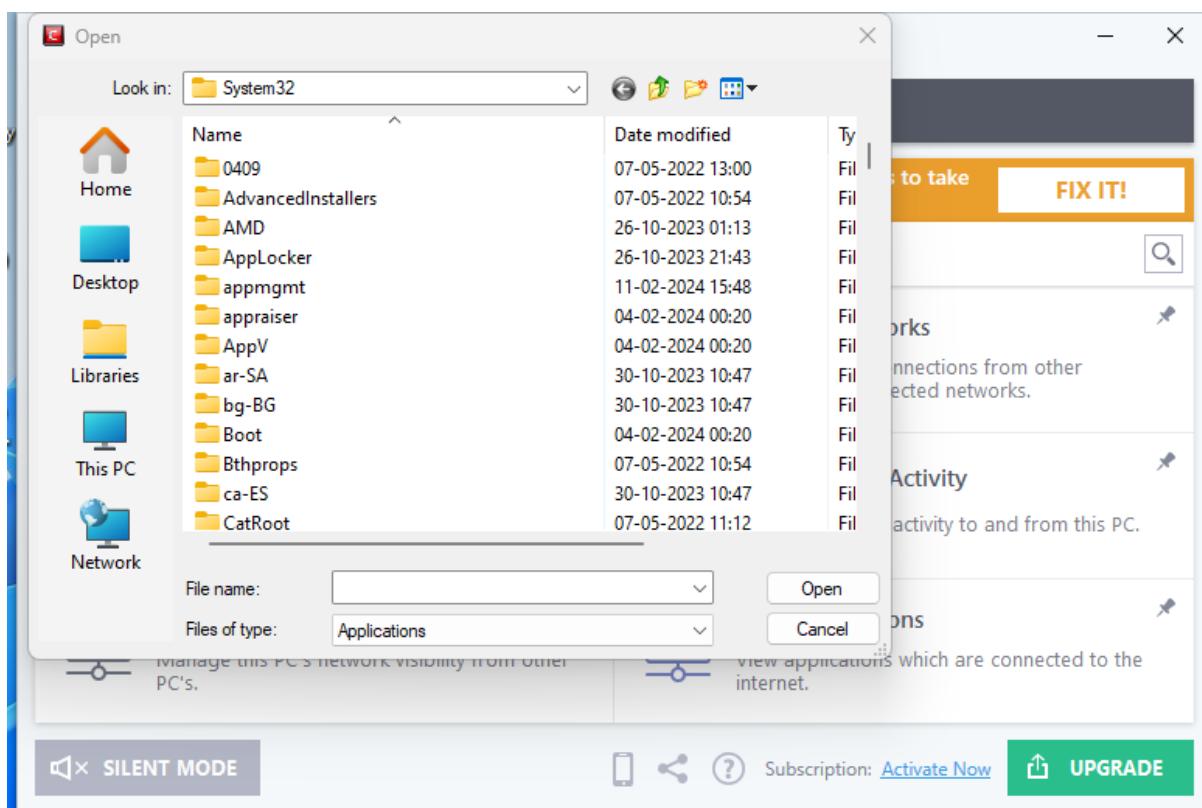


Step 2 : You can select and perform different Network activity like

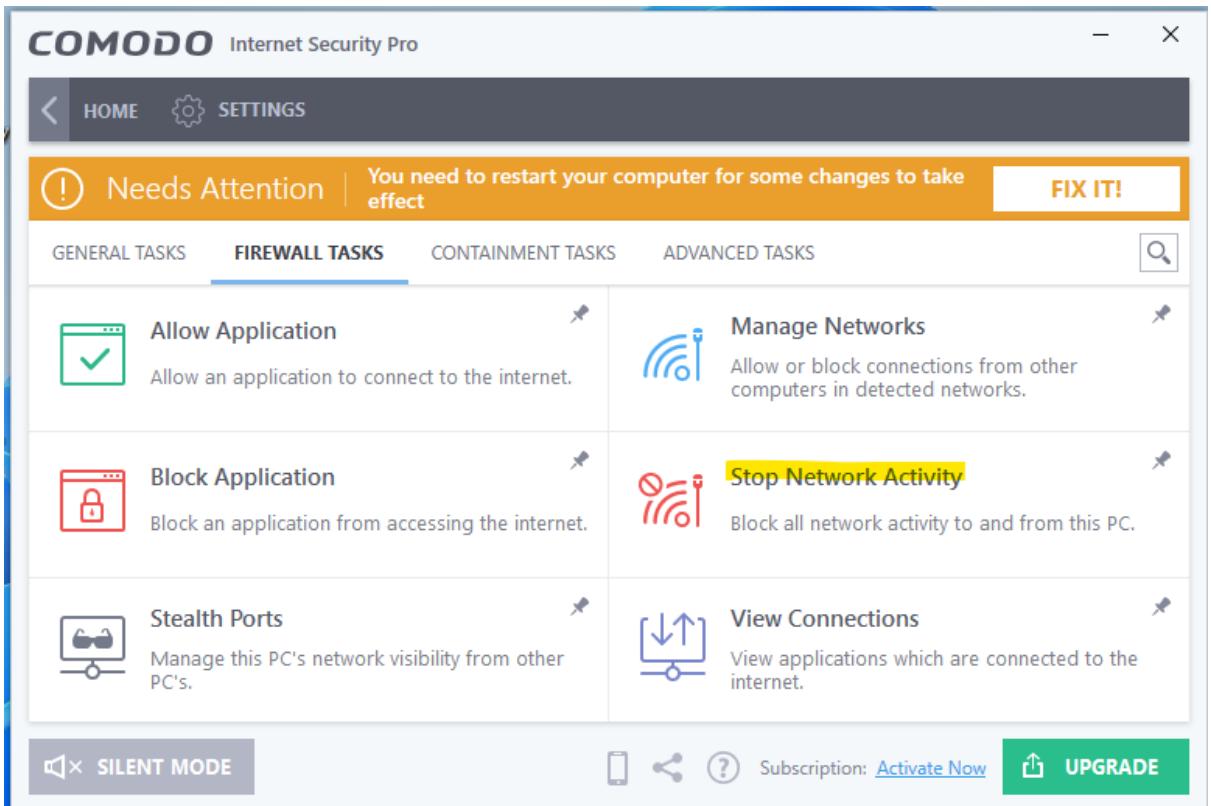
- a. Manage network: Like trust or block any network:



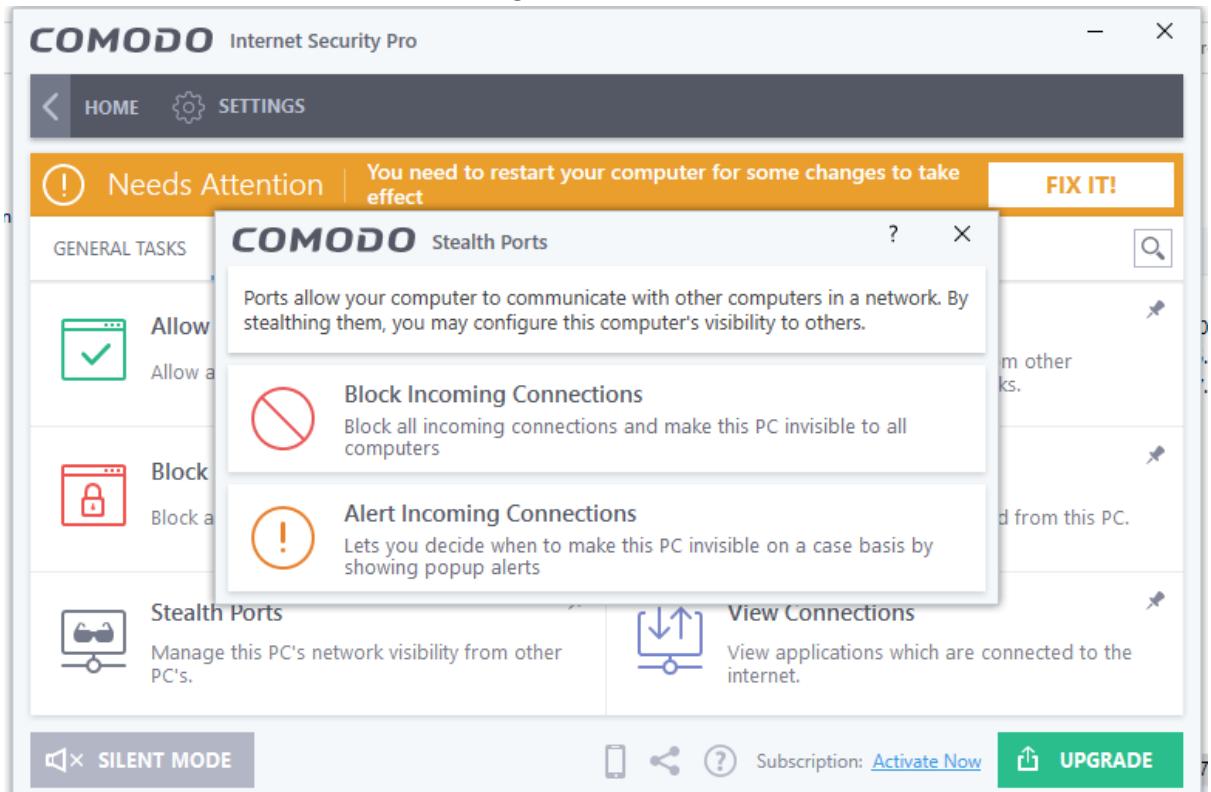
B. allow or block any application by selecting application path:



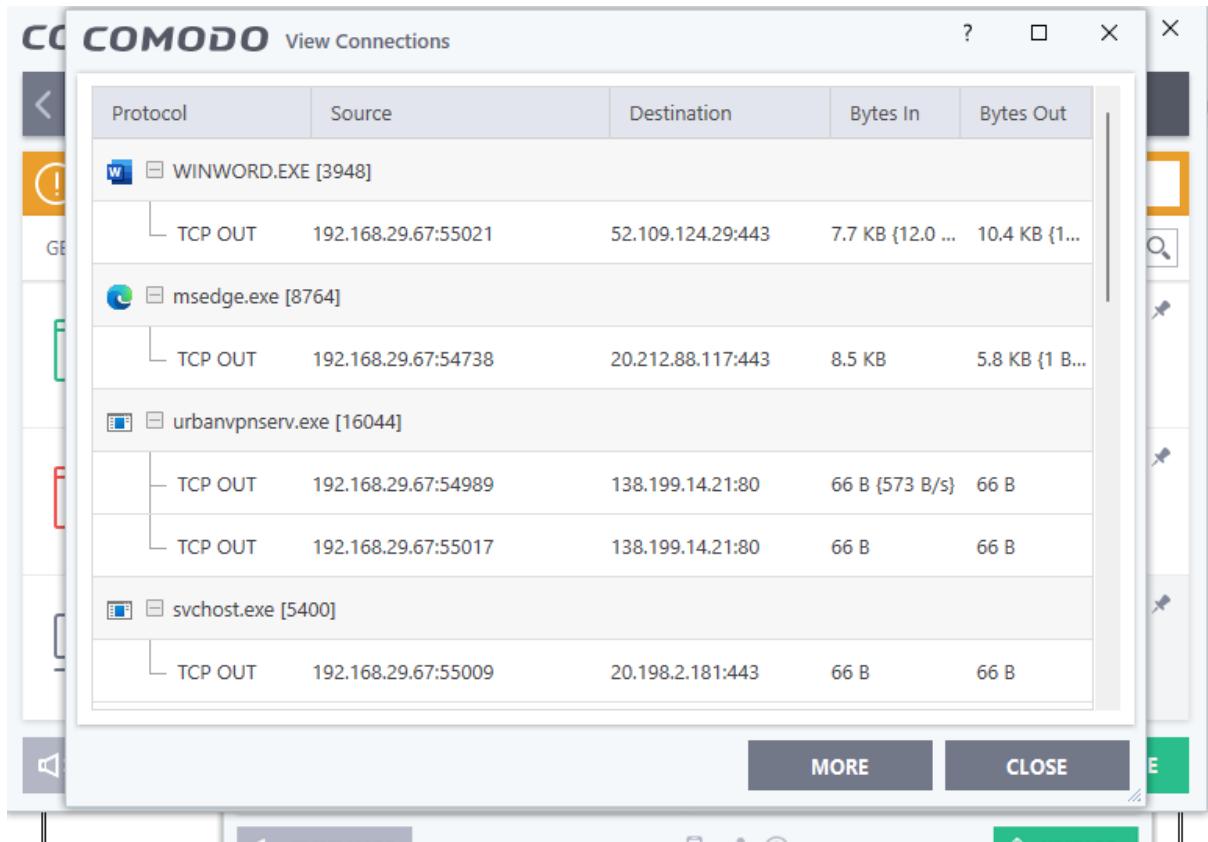
c. Allow or block network traffic in our machine:



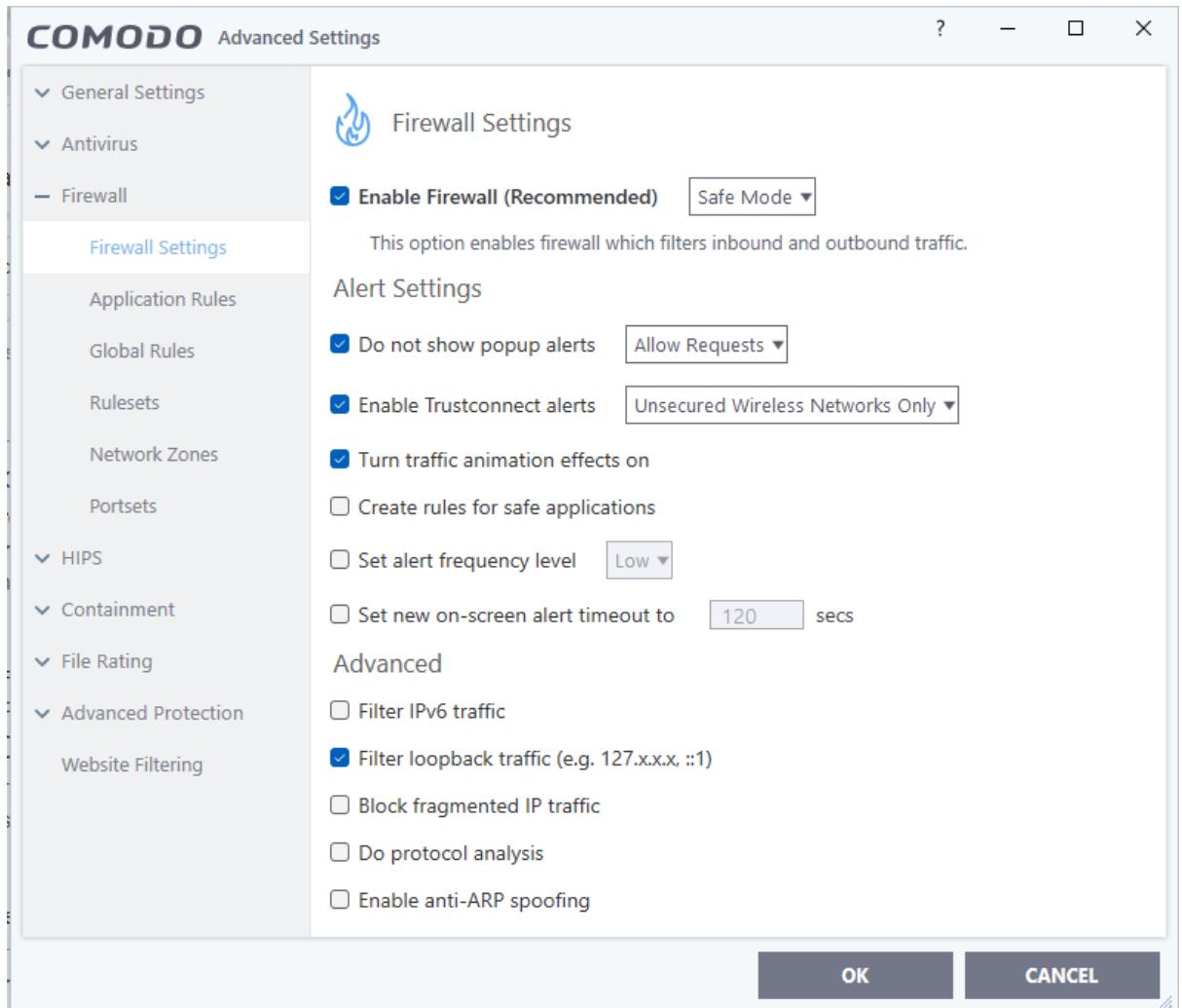
- d. Stealth mode: allow or block on incoming network:



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



Step 3: Go to firewall setting:



COMODO Advanced Settings

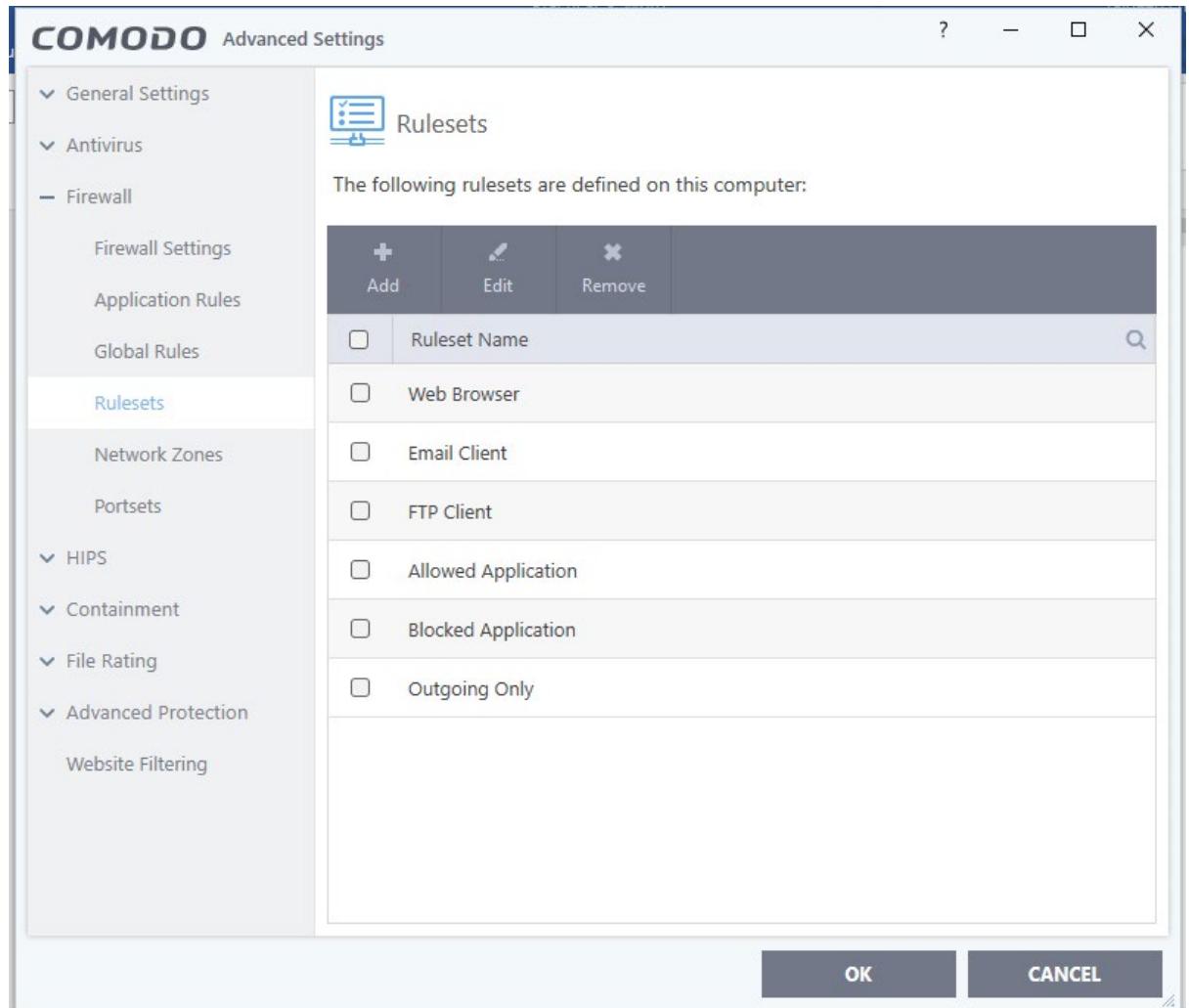
Application Rules

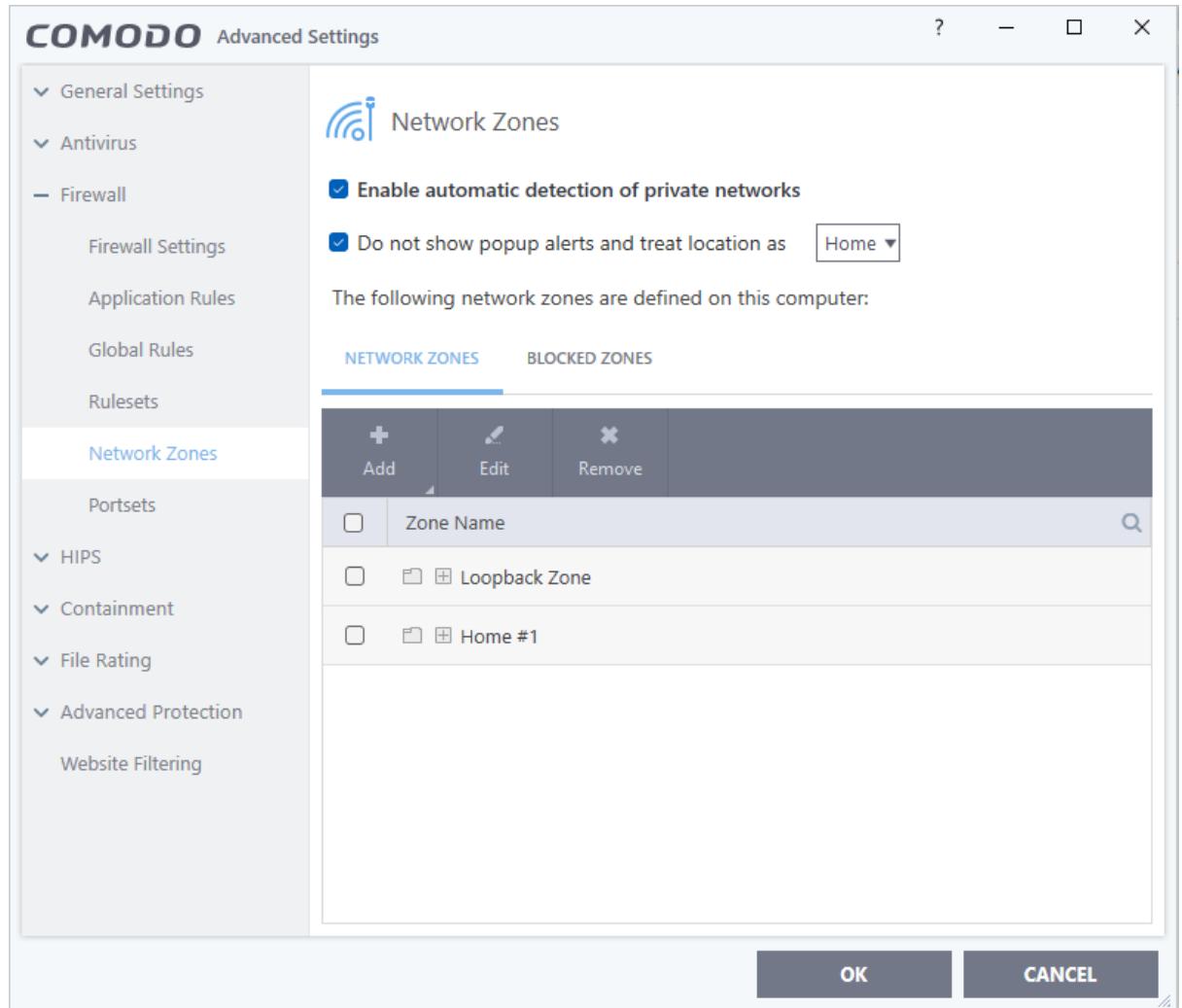
The following firewall application rules are active on this computer.

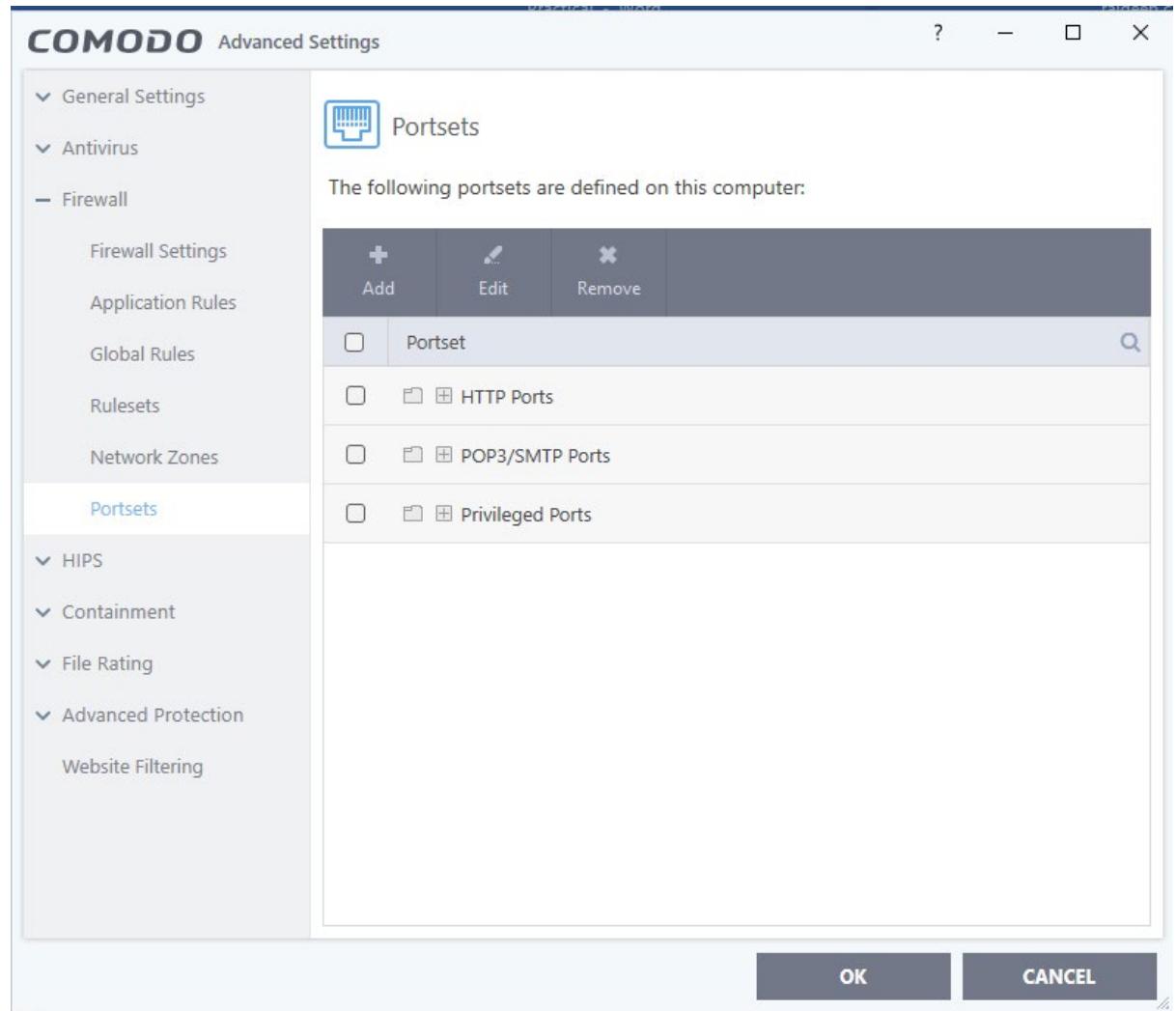
	Add	Edit	Remove	Move Up	Move Down	Purge
<input type="checkbox"/>	Application	<input type="text"/>	Treat as	<input type="button" value=""/>		
<input type="checkbox"/>	<input type="checkbox"/> System		Custom			
<input type="checkbox"/>	<input checked="" type="checkbox"/> Allow System To Send Requests If The Targe...					
<input type="checkbox"/>	<input checked="" type="checkbox"/> Allow System To Receive Requests If The Se...					
<input type="checkbox"/>	<input type="checkbox"/> COMODO Internet Security		Outgoing Only			
<input type="checkbox"/>	<input type="checkbox"/> Windows Updater Applications		Custom			
<input type="checkbox"/>	<input type="checkbox"/> Windows System Applications		Custom			
<input type="checkbox"/>	<input type="checkbox"/> Metro Apps		Outgoing Only			

OK CANCEL

Detailed description: This screenshot shows the 'Application Rules' section of the COMODO Advanced Settings. On the left is a navigation tree with 'Firewall Settings' selected under 'Firewall'. The main pane displays a table of rules. There are two main entries under 'System': one for 'Allow System To Send Requests If The Target...' (checked) and one for 'Allow System To Receive Requests If The Se...' (checked). Other entries include 'COMODO Internet Security' (Outgoing Only), 'Windows Updater Applications' (Custom), 'Windows System Applications' (Custom), and 'Metro Apps' (Outgoing Only). Buttons for 'OK' and 'CANCEL' are at the bottom right.

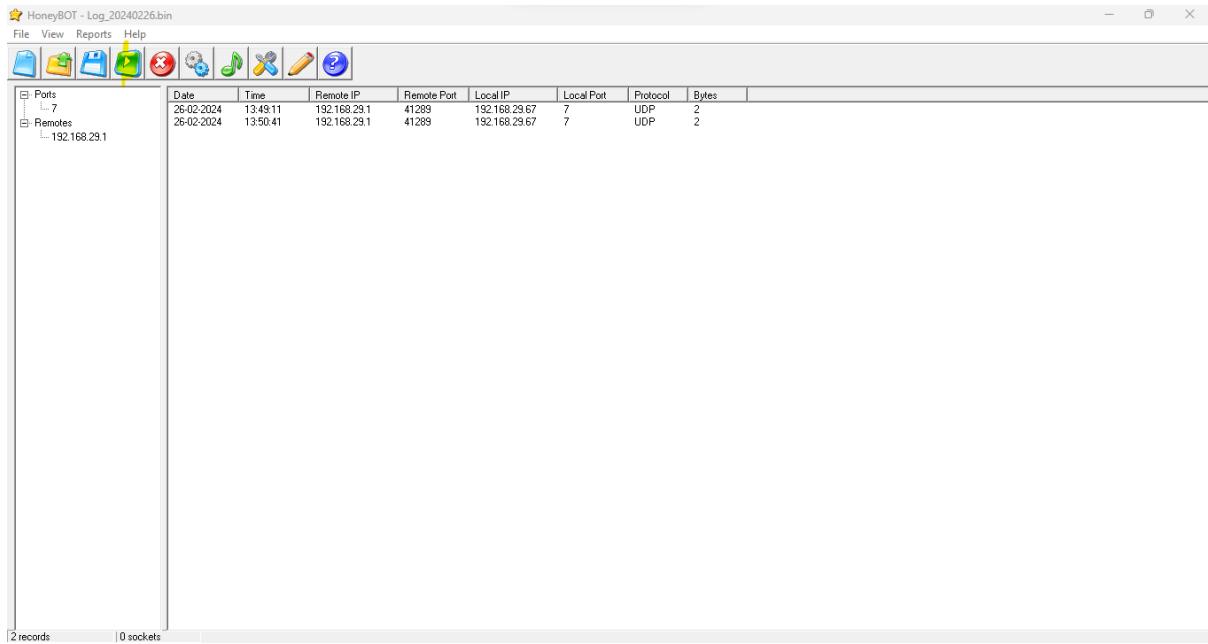






d. Aim: Use HoneyBOT to capture malicious network traffic.

1. Open HoneyBot click on start icon.

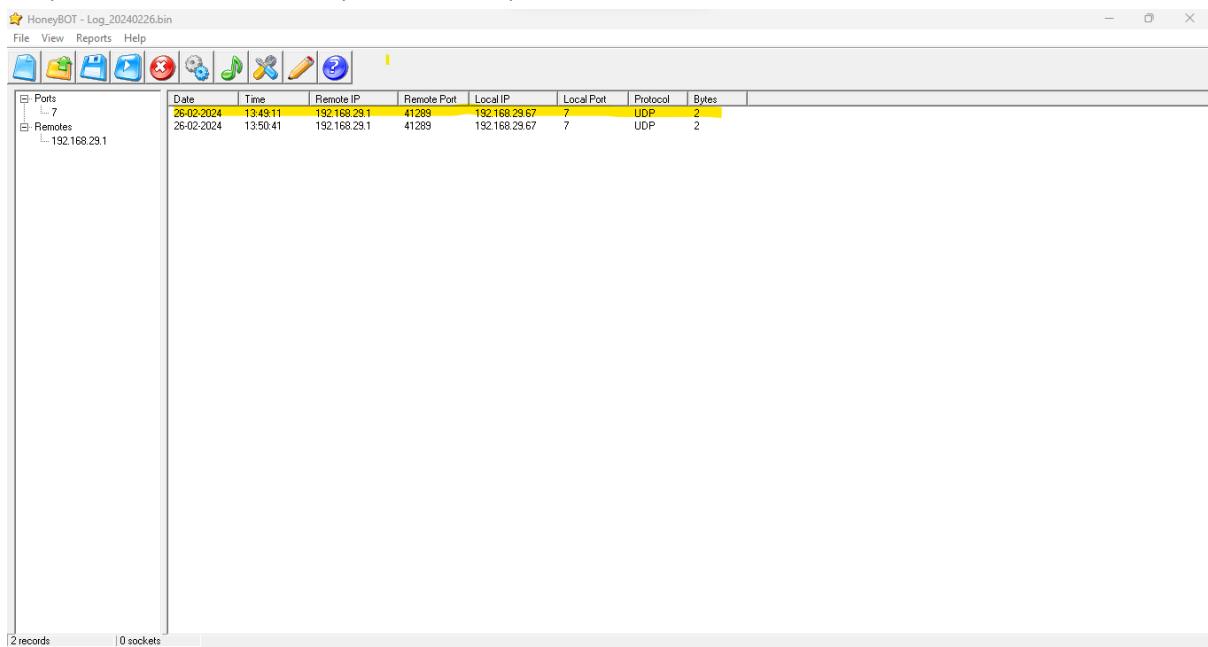


The screenshot shows the HoneyBOT application window. The menu bar includes File, View, Reports, and Help. The toolbar contains icons for file operations, ports, remotes, and analysis. On the left, a tree view shows 'Ports' (7 entries) and 'Remotes' (1 entry: 192.168.29.1). The main area displays a table of captured traffic logs:

Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
26-02-2024	13:49:11	192.168.29.1	41289	192.168.29.67	7	UDP	2
26-02-2024	13:50:41	192.168.29.1	41289	192.168.29.67	7	UDP	2

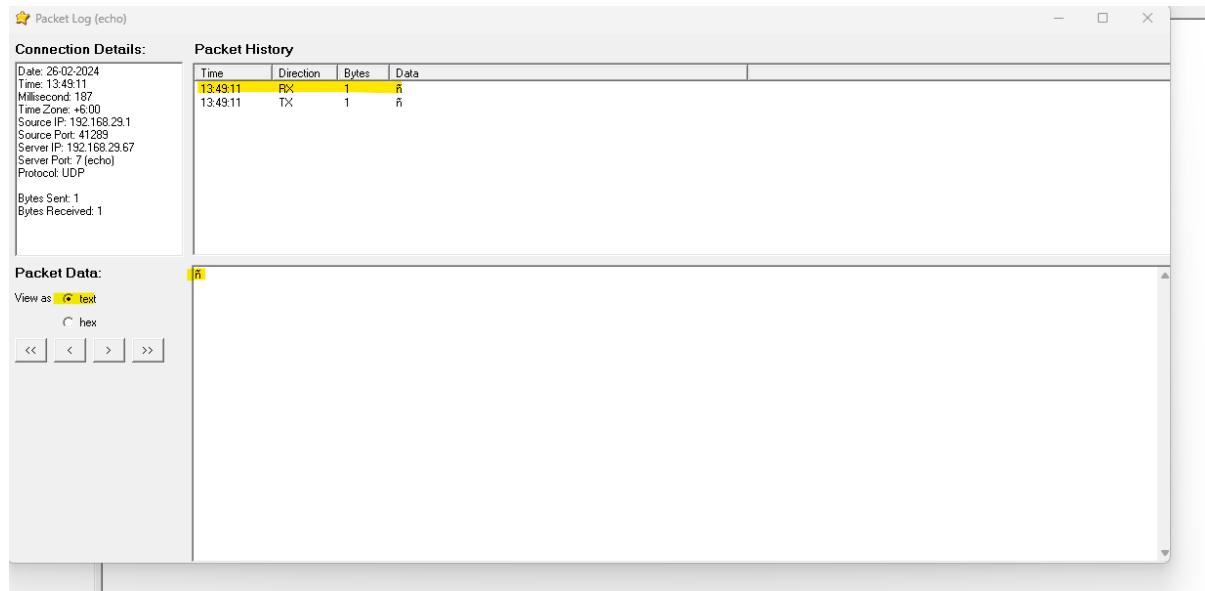
At the bottom, status bars show '2 records' and '0 sockets'.

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



The screenshot shows the HoneyBOT application window with the same interface as the previous step. A specific row in the log table is highlighted with yellow background and black text, indicating it has been selected. The selected row corresponds to the first entry in the log table.

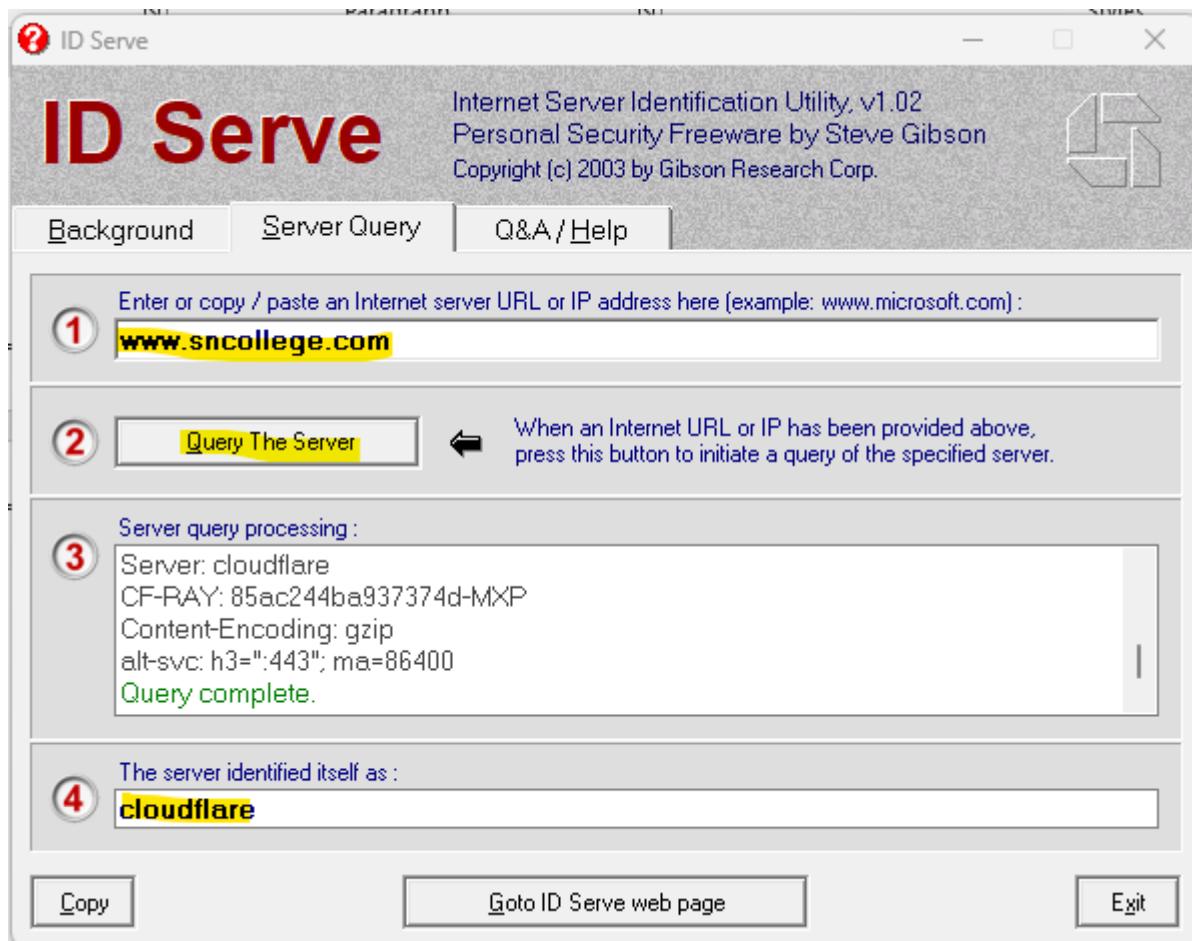
Step 3: Select any of the packet , then select from the option of text or hex format to see the output.



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

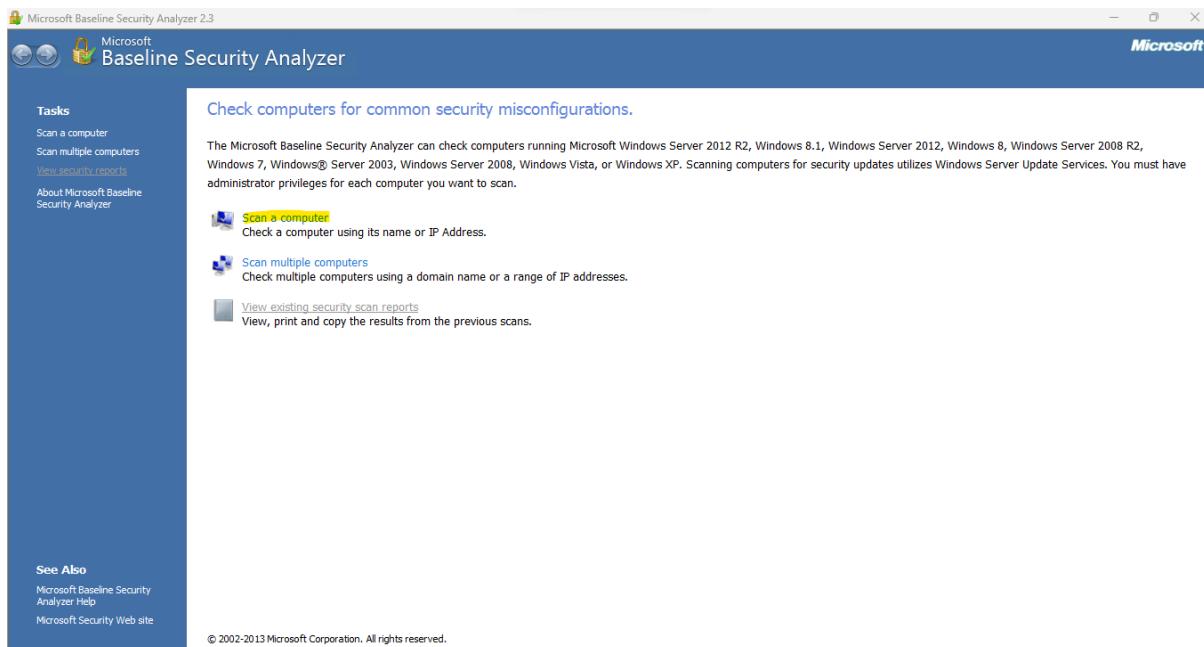
1. ID Server

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

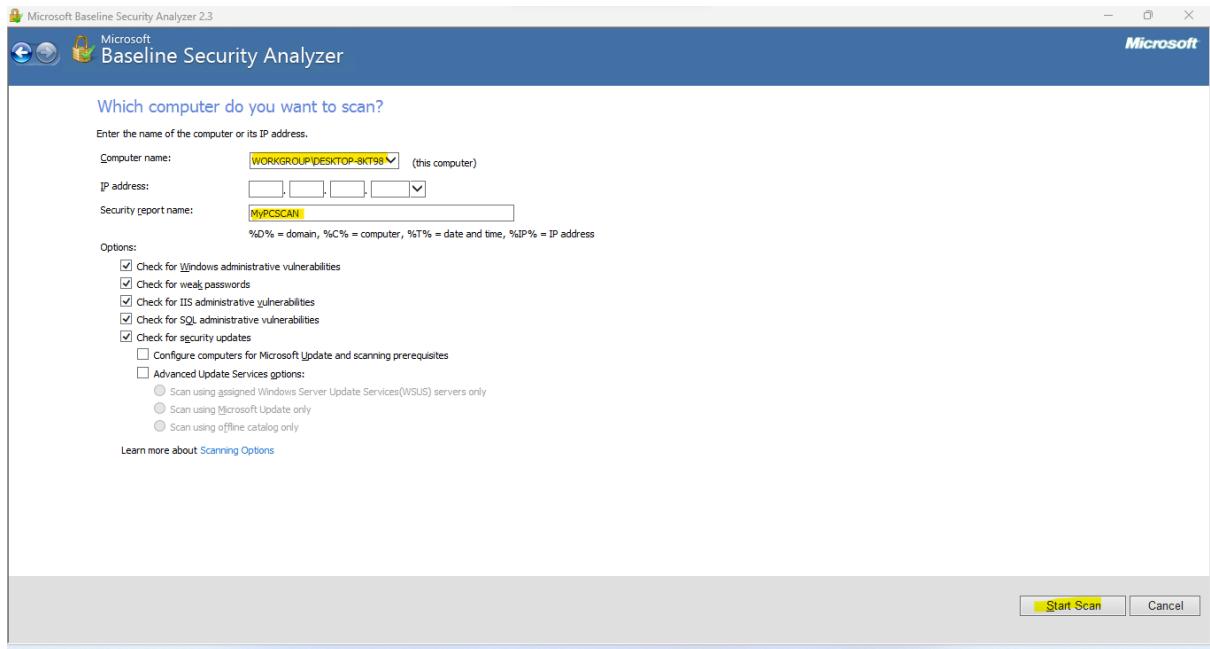


ii. Aim: Microsoft Baseline Security Analyzer

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:

Report Details for WORKGROUP - DESKTOP-8KT98Q2 (2024-02-25 02:31:17)

Security assessment:
Incomplete Scan (Could not complete one or more requested checks.)

Computer name:	WORKGROUP\DESKTOP-8KT98Q2
IP address:	192.168.29.67
Security report name:	MyPCSCAN
Scan date:	25-02-2024 02:31
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	Security updates scan not performed

Sort Order: [Score \(worst first\)](#)

Security Update Scan Results

Score	Issue	Result
!	Security Updates	Cannot load security CAB file. How to correct this

Windows Scan Results

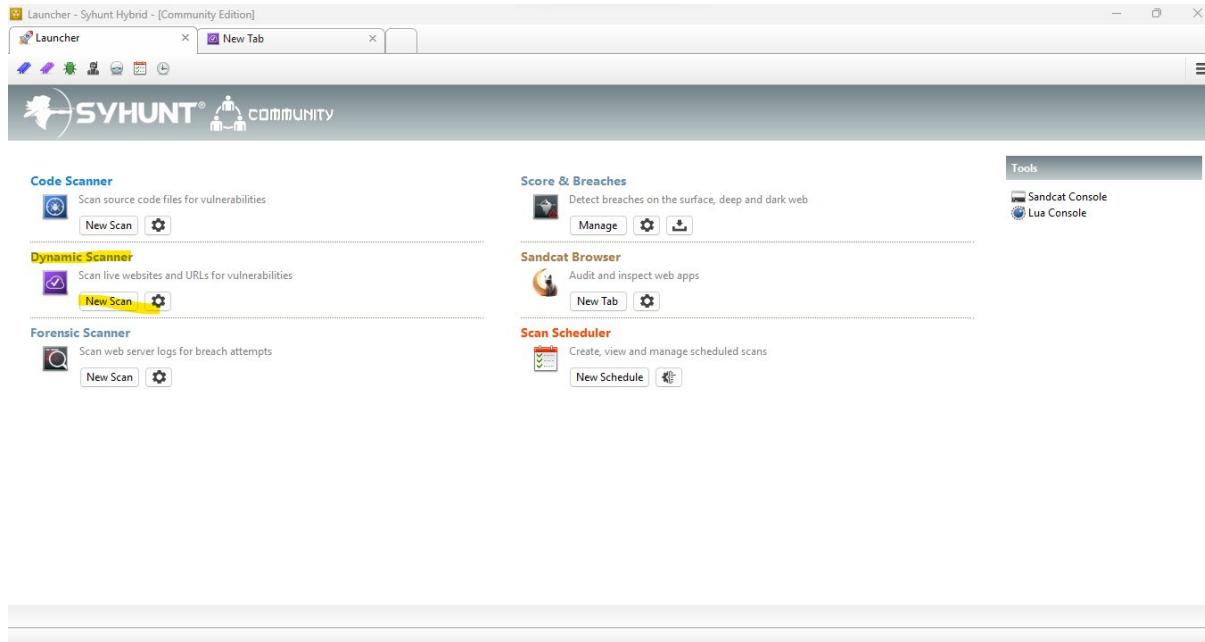
Administrative Vulnerabilities

Score	Issue	Result
!	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
!	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this

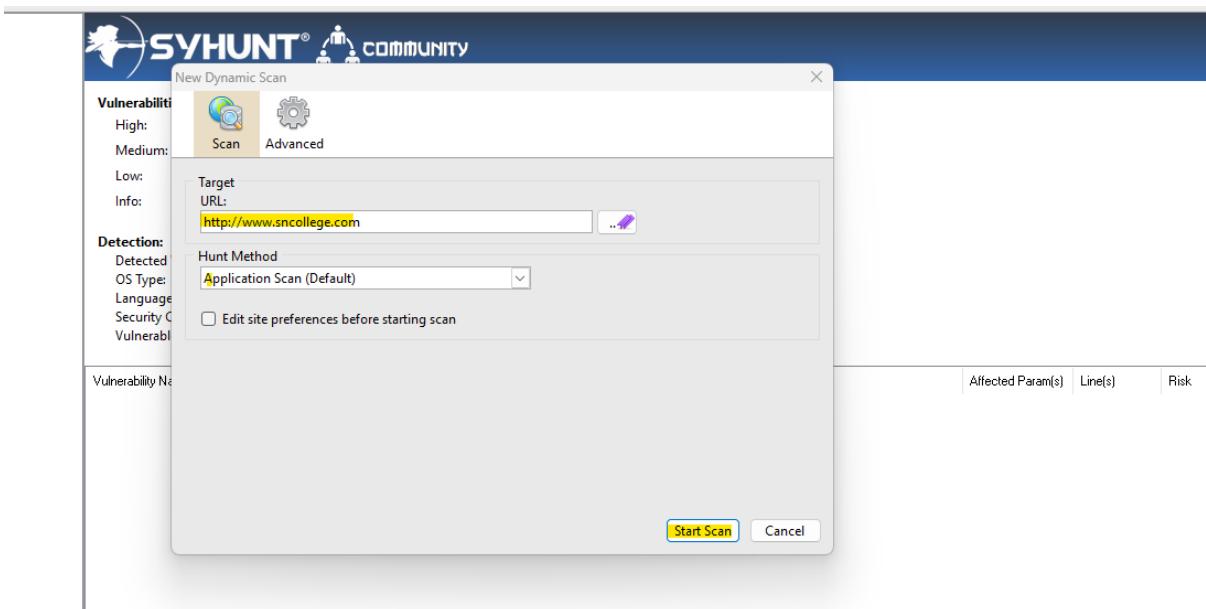
[Print this report](#) [Copy to clipboard](#) [Previous security report](#) [Next security report](#) [OK](#)

III. Syhunt Hybri

Step 1: Open Syhunt hunt Application -> 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:

Vulnerability Name	Location (Double-click for details)	Affected Param(s)	Line(s)	Risk
INFO Content Security Policy (CSP) ...	http://www.sncollege.com/			info
LOW Missing Cache-Control Header	http://www.sncollege.com/			low
LOW Missing Content Sniffing XSS ...	http://www.sncollege.com/			low
LOW Missing Clickjacking Protectio...	http://www.sncollege.com/			low
INFO Content Security Policy (CSP) ...	http://www.sncollege.com/			info
LOW Missing Cache-Control Header	http://www.sncollege.com/			low
LOW Missing Content Sniffing XSS ...	http://www.sncollege.com/			low
LOW Missing Clickjacking Protectio...	http://www.sncollege.com/			low

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

Vulnerabilities:

High:	0
Medium:	0
Low:	3
Info:	1

Detection:

Detected Web Technologies:	2
OS type:	Undetermined
Languages:	JS/HTML
Security Checks:	0
Vulnerable URLs:	1

Spidering

Duration:	1min7sec
Reached Depth:	2
URLs (Key):	175
URLs detected:	8311
URLs dismissed:	878
URLs using POST:	0
URLs using Form Auth:	0
URLs using HTTP Auth:	0
URLs using JS:	0
URLs (Logout):	0
URLs ignored:	0
Entry Points:	0
Emails:	0

Vulnerability Name **Location (Double-click for details)** **Affected Param(s)** **Line(s)** **Risk**

[Info] Content Security Policy (CSP) ...	http://www.sncollege.com/			info
[Low] Missing Cache-Control Header	http://www.sncollege.com/			low
[Low] Missing Content Sniffing XSS ...	http://www.sncollege.com/			low
[Low] Missing Clickjacking Protec...	http://www.sncollege.com/			low
[Info] Content Security Policy (CSP) ...	http://www.sncollege.com/			info
[Low] Missing Cache-Control Header	http://www.sncollege.com/			low
[Low] Missing Content Sniffing XSS ...	http://www.sncollege.com/			low
[Low] Missing Clickjacking Protec...	http://www.sncollege.com/			low

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

General

Report Details for: 17088453307492
Report Title: Syhunt Scan Report

Template
Choose a report template:
 Standard
 Comparison
 Compliance (Web App)
 Compliance (Mobile App)
 Complete

Notes:

Footer:

Choose a vulnerability sorting method:
 CVSS3
 CVSS2
 Four Step (High, Medium, Low, Info)

The following items will be included:

- Organization Logo
- User Notes
- Session Details
- Charts
- Dynamic Content
- Comparison Info
- Compliance Info
- Compliance (CWE/SANS Top 25 2011 Most Dangerous Software Errors)
- Compliance (CWE/SANS Top 25 2019 Most Dangerous Software Errors)
- Compliance (CWE/SANS Top 25 2020 Most Dangerous Software Errors)
- Compliance (CWE/SANS Top 25 2021 Most Dangerous Software Errors)

Open report after generation

Section 3 B

a. Tyrant SQL

Tyrant SQL is a Havij based cross-platform. It's Sqlmap's gui version.

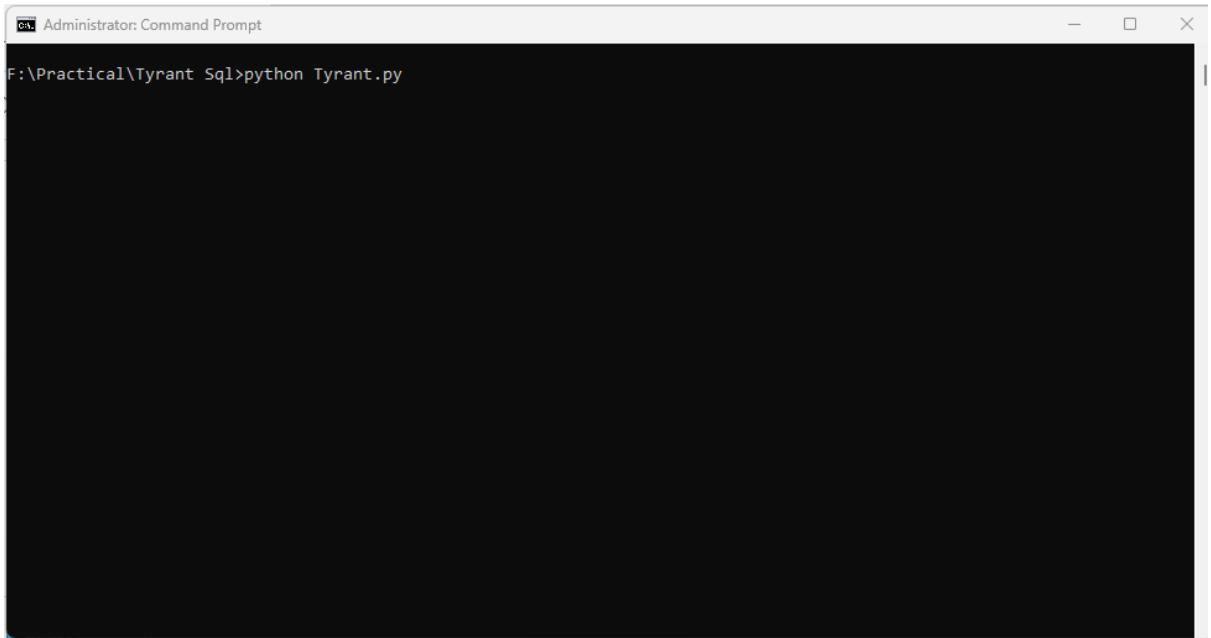
Follow the below process to run the Tyrant SQL :

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>

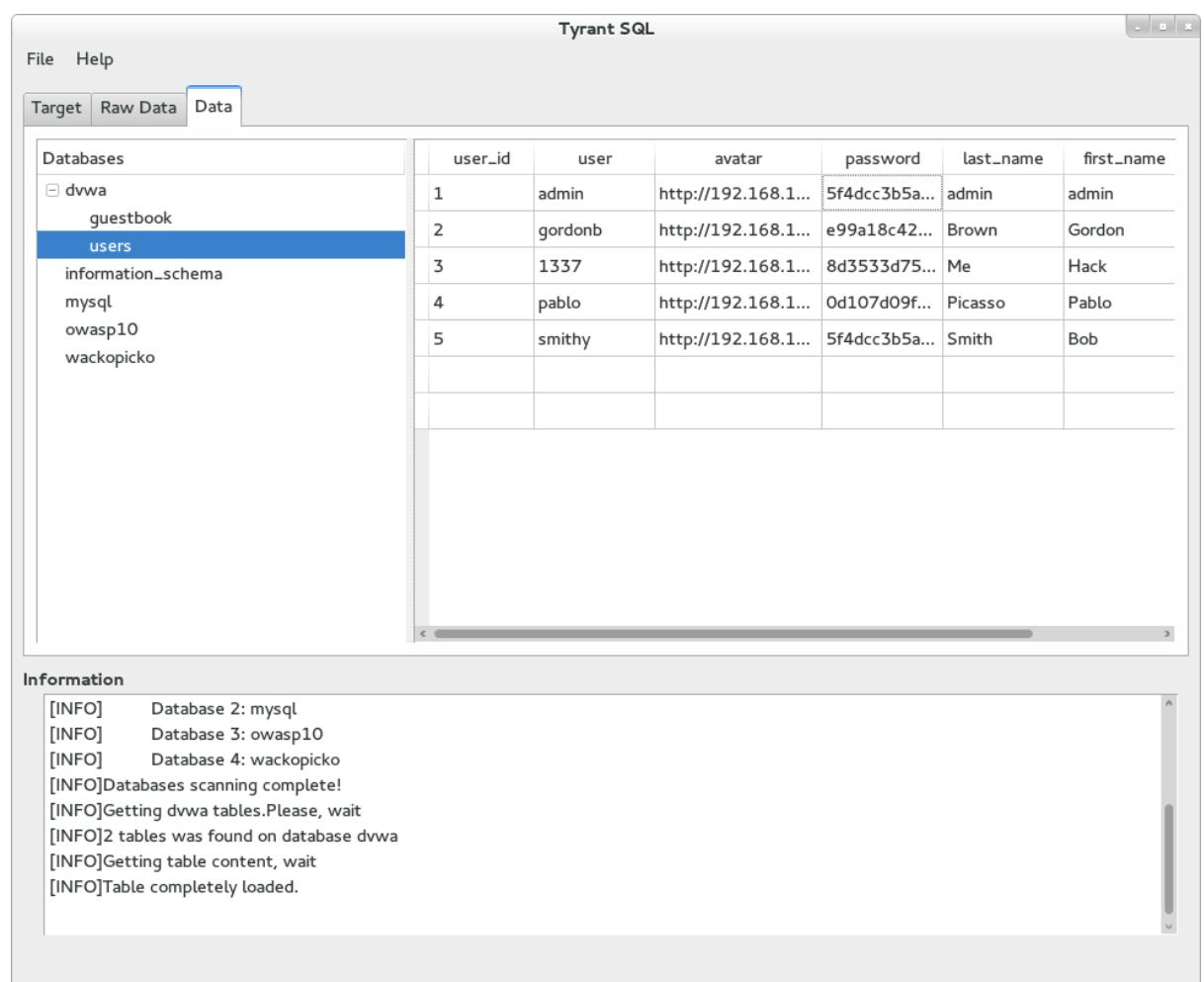
Step 2: Run the file from command prompt



Administrator: Command Prompt
F:\Practical\Tyrant_SQL>python Tyrant.py

Step 3: Use the vulnerable URL in target :

Example: <http://redtiger.labs.overthewire.org/level1.php?cat=1>



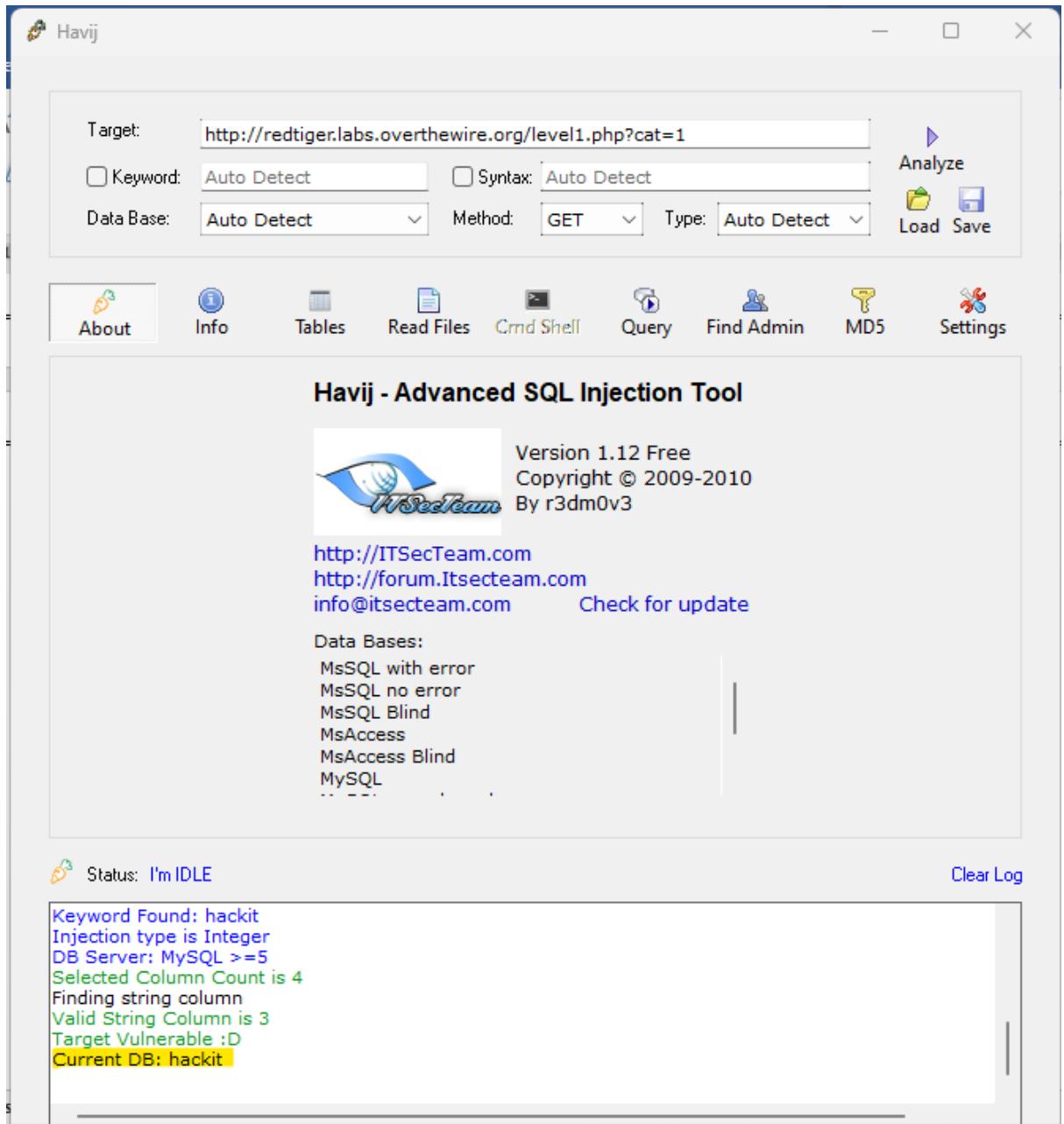
The screenshot shows the Tyrant SQL application interface. The top menu bar includes File, Help, Target, Raw Data, and Data. The Data tab is selected. On the left, a tree view of databases shows 'dvwa' expanded, with 'guestbook' and 'users' selected. Other databases listed are 'information_schema', 'mysql', 'owasp10', and 'wackopicko'. The main pane displays a table with the following data:

user_id	user	avatar	password	last_name	first_name
1	admin	http://192.168.1...	5f4dcc3b5a...	admin	admin
2	gordonb	http://192.168.1...	e99a18c42...	Brown	Gordon
3	1337	http://192.168.1...	8d3533d75...	Me	Hack
4	pablo	http://192.168.1...	0d107d09f...	Picasso	Pablo
5	smithy	http://192.168.1...	5f4dcc3b5a...	Smith	Bob

At the bottom, the Information panel shows log output:

```
[INFO] Database 2: mysql
[INFO] Database 3: owasp10
[INFO] Database 4: wackopicko
[INFO]Databases scanning complete!
[INFO]Getting dvwa tables.Please, wait
[INFO]2 tables was found on database dvwa
[INFO]Getting table content, wait
[INFO]Table completely loaded.
```

- 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>



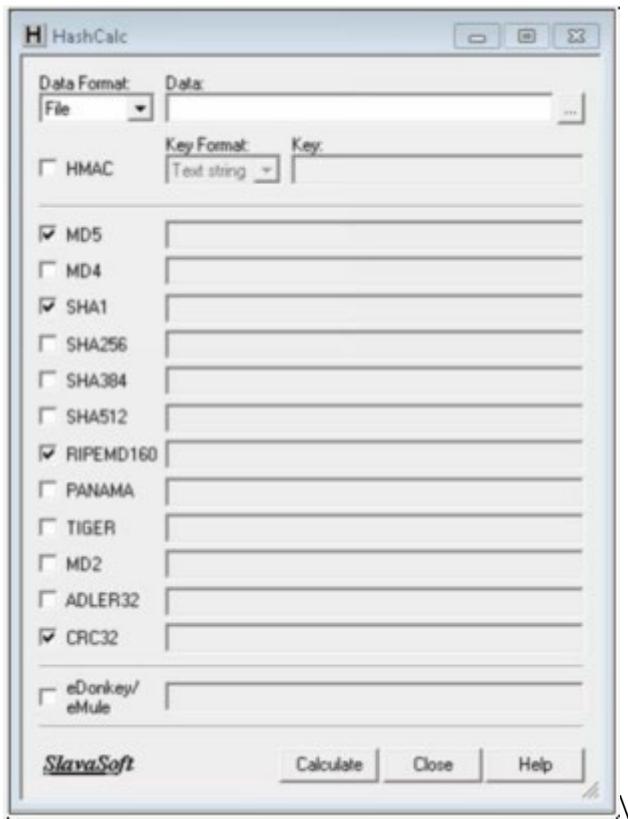
c. BBQSQL

Aim: Use the following tools for cryptography.

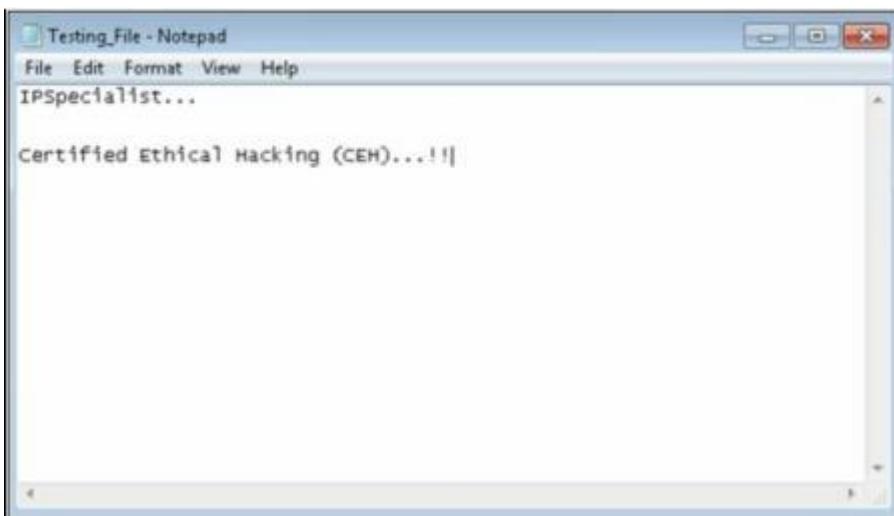
i. HashCalc

Calculating MD5 value using HashCalc

1. Open HashCalc tool



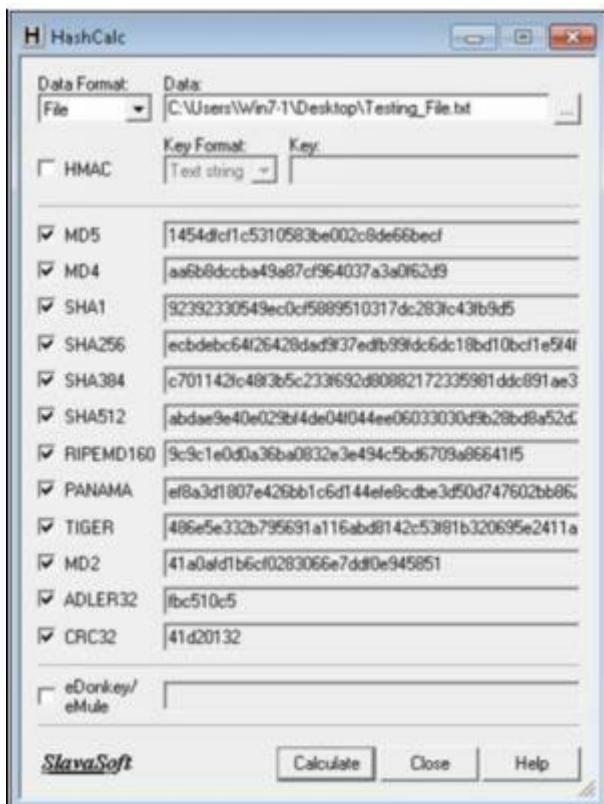
2. Create a new file with some content in it as shown below.



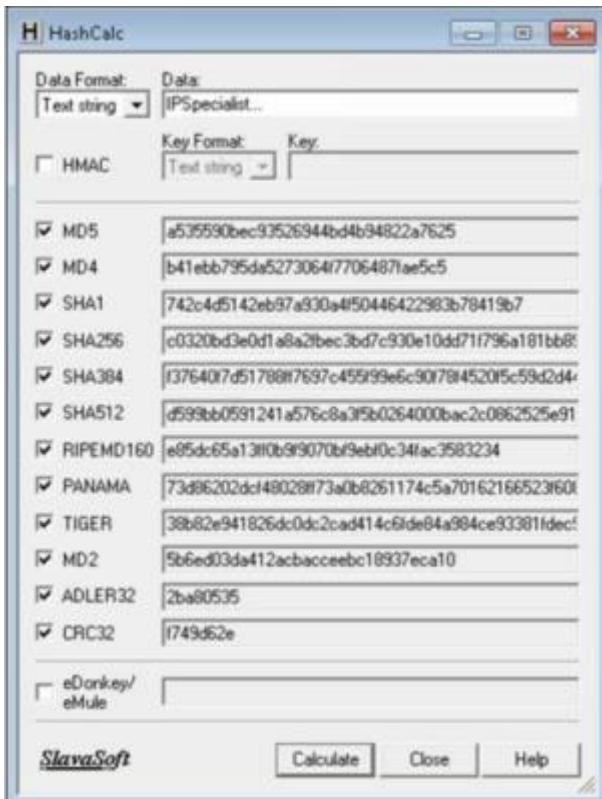
3. Select Data Format as "File" and upload your file



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”

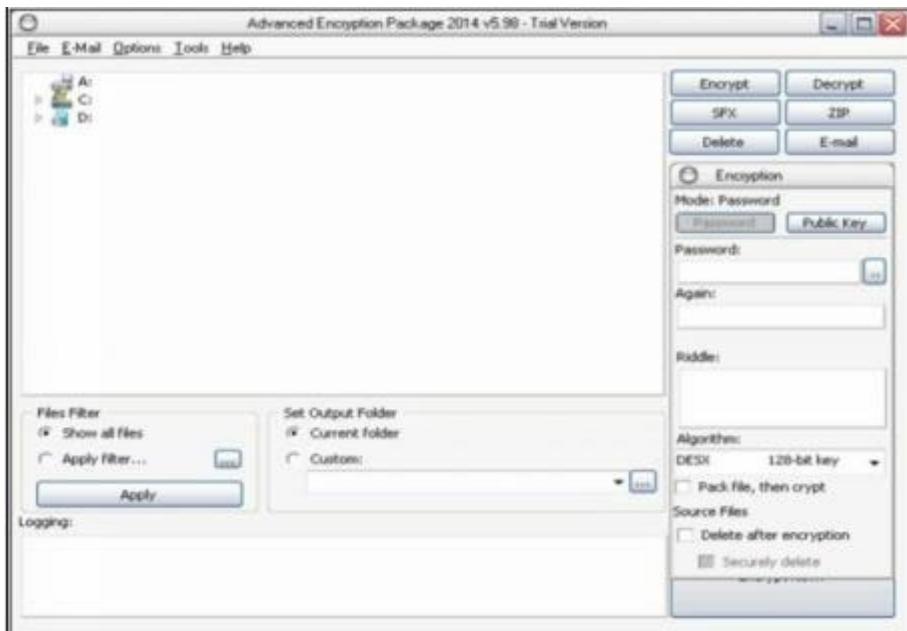
- Now, let's see how MD5 value is changed from minor change.



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

ii. Advanced Encryption Package

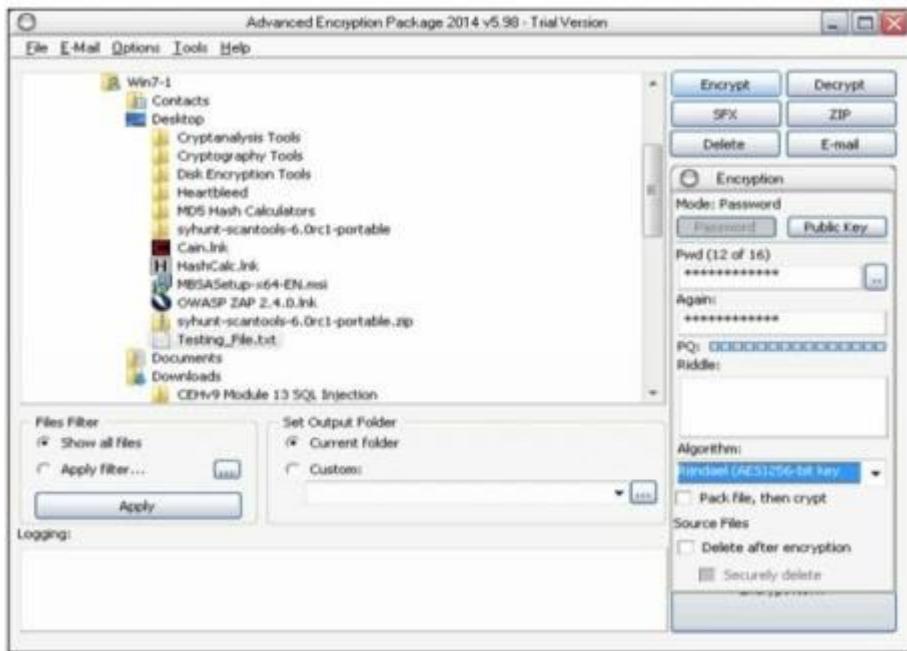
- Download and Install Advance Encryption Package Latest Version. In this Lab, we are using Advanced Encryption Package 2014 and 2017 to ensure compatibilities on Windows 7 and Windows 10.



2. Select the File you want to Encrypt.

3. Set password

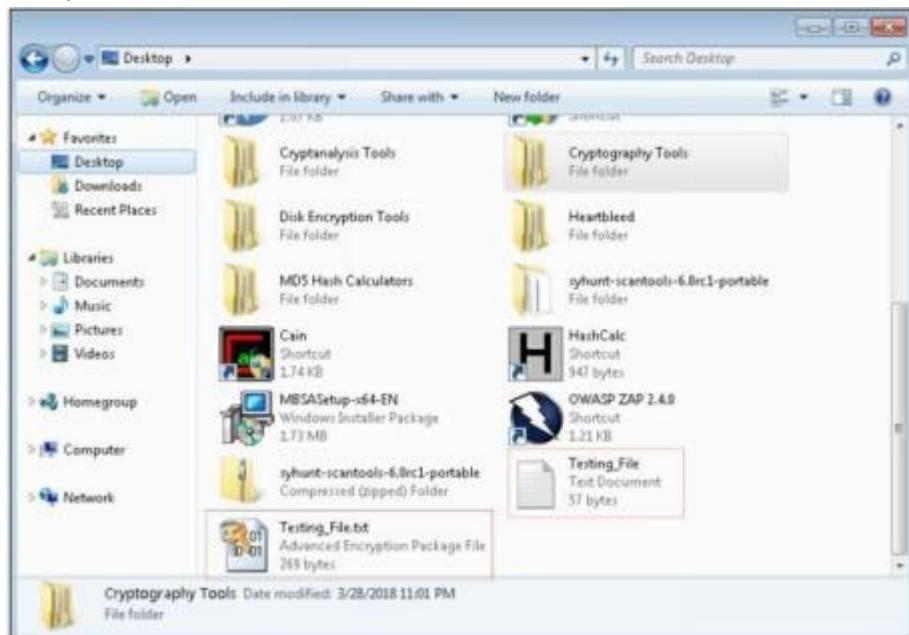
4. Select Algorithm



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

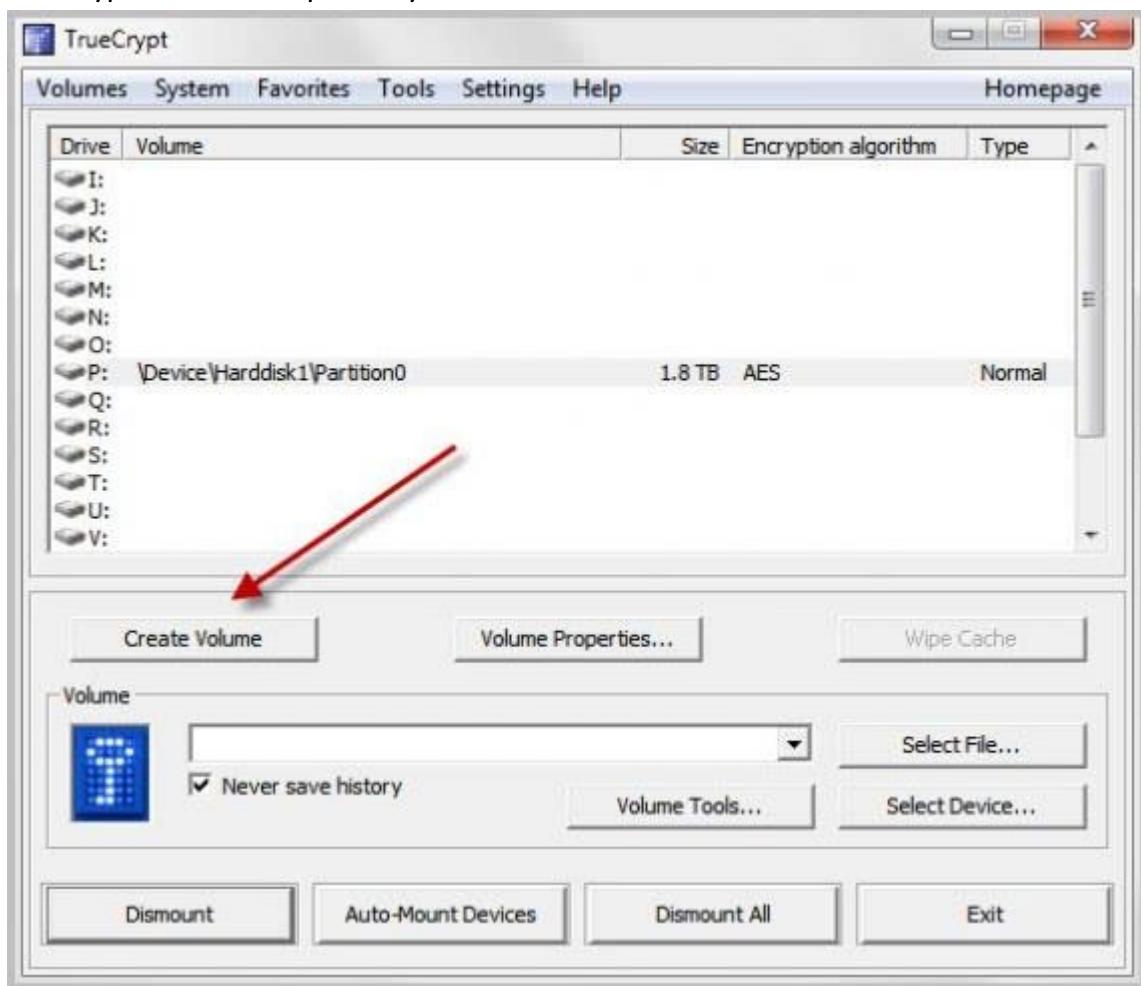


9. File Successfully decrypted.



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.

