Practical Journal

SECURITY BREACHES AND COUNTERMEASURES

A Practical Report

Submitted in partial fulfilment of the

Requirements for the award of the Degree of

MASTER OF SCIENCE (INFORMATION TECHNOLOGY)

Part I – SEM I

Submitted by

BHAVIK MISTRY

Department of Information Technology

Shri Vile Parle Kelavani Mandal's

USHA PRAVIN GANDHI COLLEGE OF ARTS, SCIENCE AND COMMERCE

NAAC Reaccredited 'A+' Grade

(Affiliated to University of Mumbai)

MUMBAI, 400056

MAHARASHTRA

2023-24

Practical Journal

SECURITY BREACHES AND COUNTERMEASURES

A Practical Report

Submitted in partial fulfilment of the

Requirements for the award of the Degree of

MASTER OF SCIENCE (INFORMATION TECHNOLOGY)

Part I – SEM I

Submitted by

BHAVIK MISTRY –

Department of Information Technology

Shri Vile Parle Kelavani Mandal's

USHA PRAVIN GANDHI COLLEGE OF ARTS, SCIENCE AND COMMERCE

NAAC Reaccredited 'A+' Grade

(Affiliated to University of Mumbai)

MUMBAI, 400056

MAHARASHTRA

2023-24

INDEX

	1)	Netbios enumeration tool		
	2)	Superscan software		
	3)	Wireshark		
	4)	SoftPerfect Network Scanner		
	5)	Nmap		
	6)	Hyena		
	B.	**Perform system hacking using the following tools**		
	1)	ADS Spy		
	2)	QuickStego		
	3)	Rainbow Crack		
	4)	Crackstation / MD5 Hash Generator		
	5)	Ophcrack		
	C.	**Perform network sniffing using the following tools**		
	1)	Cain and Abel		
	2)	Caspa Network Analyser		
	3)	Omnipeek Network Analyser		
	4)	Sniff-o-matic		
	5)	Wireshark		
	6)	SMAC for MAC Spoofing		
3.	**A.**	**Perform web app scanning using the following tool**		
	1)	OWASP ZAP		
	B.	**Use the following tools to perform attacks on the web servers**		
	1)	ID Serve		
	2)	Httprecon		
	C.	**Use the following tools for cryptography**		

	1)	Advance Encryption Package		
	2)	CrypTool		
	3)	Hash Calc		
	D.	**Study of Trojans**		
	1)	Prorat		
	2)	Theef		

Practical1

1) WhoIS and Who.is

A WHOIS lookup is a query or search to retrieve information about a domain name or IP address on the internet. The term "WHOIS" stands for "Who Is," and it's a protocol used to look up domain registration and ownership information.

Step1: - Search on google “Whois.com”

Step2: - Enter any domain name or IP address

cricbuzz.com Updated 3 days ago

Domain Information

Domain:	cricbuzz.com
Registrar:	eNom, LLC
Registered On:	2004-04-16
Expires On:	2024-04-16
Updated On:	2019-02-28
Status:	clientTransferProhibited
Name Servers:	ns1.softlayer.com ns2.softlayer.com

Registrant Contact

Name:	Whois Agent (997947323)
Organization:	Whois Privacy Protection Service, Inc.
Street:	PO Box 639 C/O cricbuzz.com
City:	Kirkland
State:	WA
Postal Code:	98083
Country:	US
Phone:	+1.4252740657
Fax:	+1.4259744730
Email:	fjjqnygqr@whoisprivacyprotect.com

Technical Contact

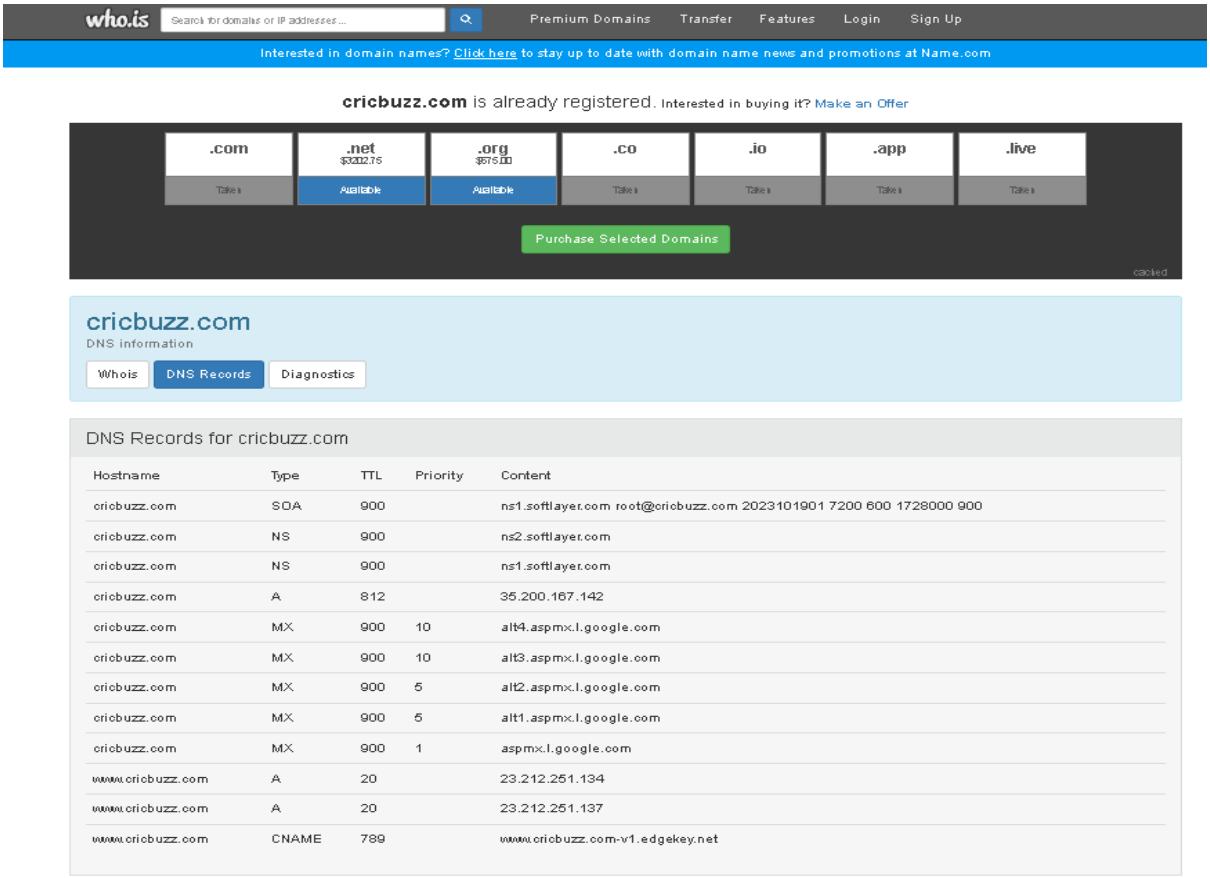
Name:	Whois Agent
Organization:	Whois Privacy Protection Service, Inc.
Street:	PO Box 639 C/O cricbuzz.com
City:	Kirkland
State:	WA
Postal Code:	98083
Country:	US
Phone:	+1.4252740657
Fax:	+1.4259744730
Email:	fjjqnygqr@whoisprivacyprotect.com

Raw Whois Data

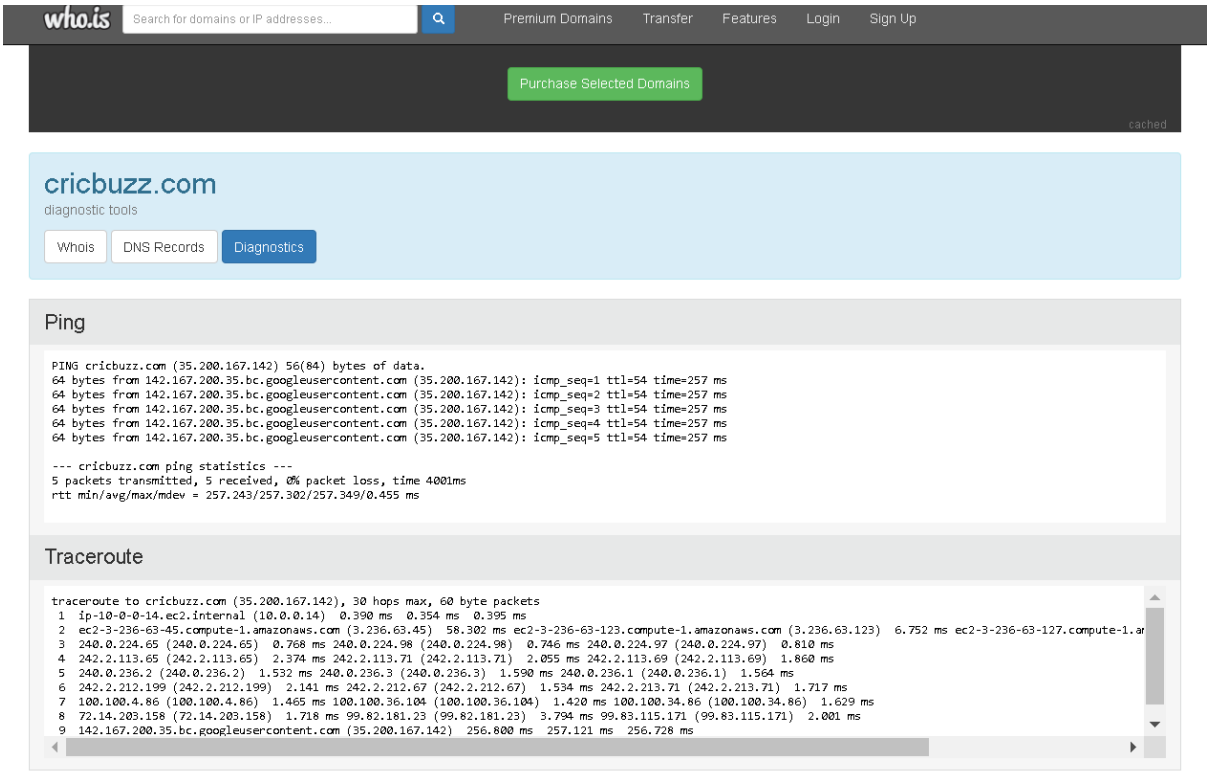
```
Domain Name: cricbuzz.com
Registry Domain ID: 117323961_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOMDOMAINS.COM
Updated Date: 2019-02-28T14:07:24.00Z
Creation Date: 2004-04-16T04:27:32.00Z
Registrar Registration Expiration Date: 2024-04-16T08:27:00.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registrant Name: Whois Agent (997947323)
Registrant Organization: Whois Privacy Protection Service, Inc.
Registrant Street: PO Box 639
Registrant Street: C/O cricbuzz.com
Registrant City: Kirkland
Registrant State/Province: WA
Registrant Postal Code: 98083
Registrant Country: US
Registrant Phone: +1.4252740657
Registrant Phone Ext:
Registrant Fax: +1.4259744730
Registrant Email: fjjqnygqr@whoisprivacyprotect.com
Admin Name: Whois Agent
Admin Organization: Whois Privacy Protection Service, Inc.
Admin Street: PO Box 639
Admin Street: C/O cricbuzz.com
Admin City: Kirkland
Admin State/Province: WA
Admin Postal Code: 98083
Admin Country: US
Admin Phone: +1.4252740657
Admin Phone Ext:
Admin Fax: +1.4259744730
Admin Email: fjjqnygqr@whoisprivacyprotect.com
Tech Name: Whois Agent
Tech Organization: Whois Privacy Protection Service, Inc.
Tech Street: PO Box 639
Tech Street: C/O cricbuzz.com
Tech City: Kirkland
Tech State/Province: WA
Tech Postal Code: 98083
Tech Country: US
Tech Phone: +1.4252740657
Tech Phone Ext:
Tech Fax: +1.4259744730
Tech Email: fjjqnygqr@whoisprivacyprotect.com
Name Server: NS1.SOFTLAYER.COM
Name Server: NS2.SOFTLAYER.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: ABUSE@ENOM.COM
Registrar Abuse Contact Phone: +1.4259744689
URL of the ICANN WHOIS Data Problem Reporting System: HTTPS://ICANN.ORG/WICF
>>> Last update of WHOIS database: 2023-10-28T03:52:16.00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Step3: - search for who.is and give any domain you want to search for.

DNS Records

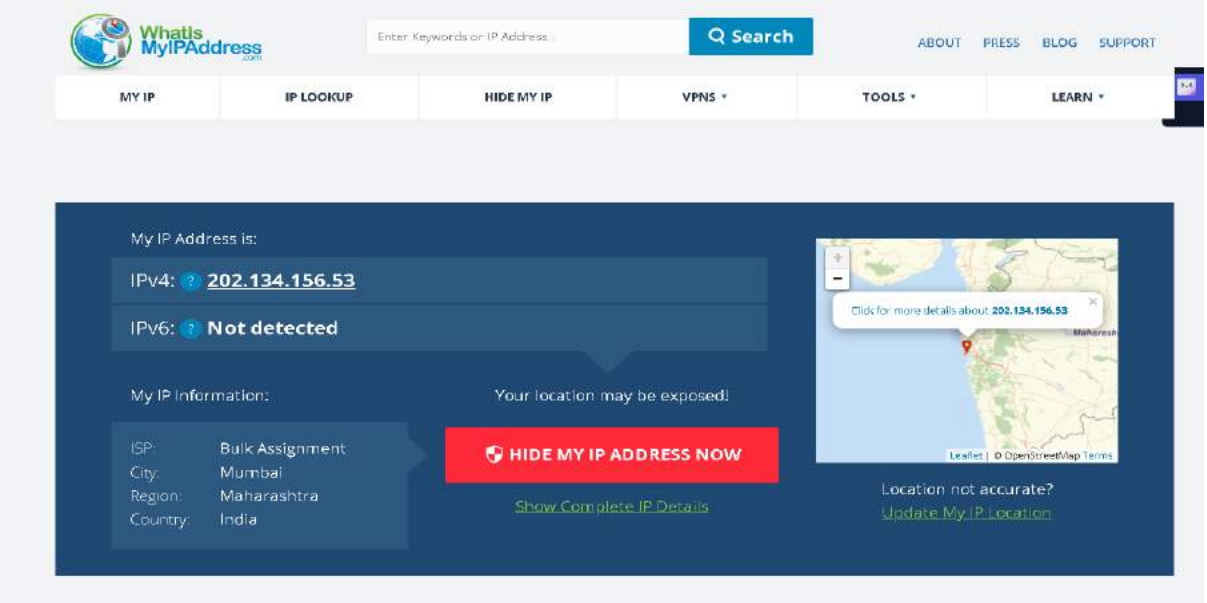


Diagnosis

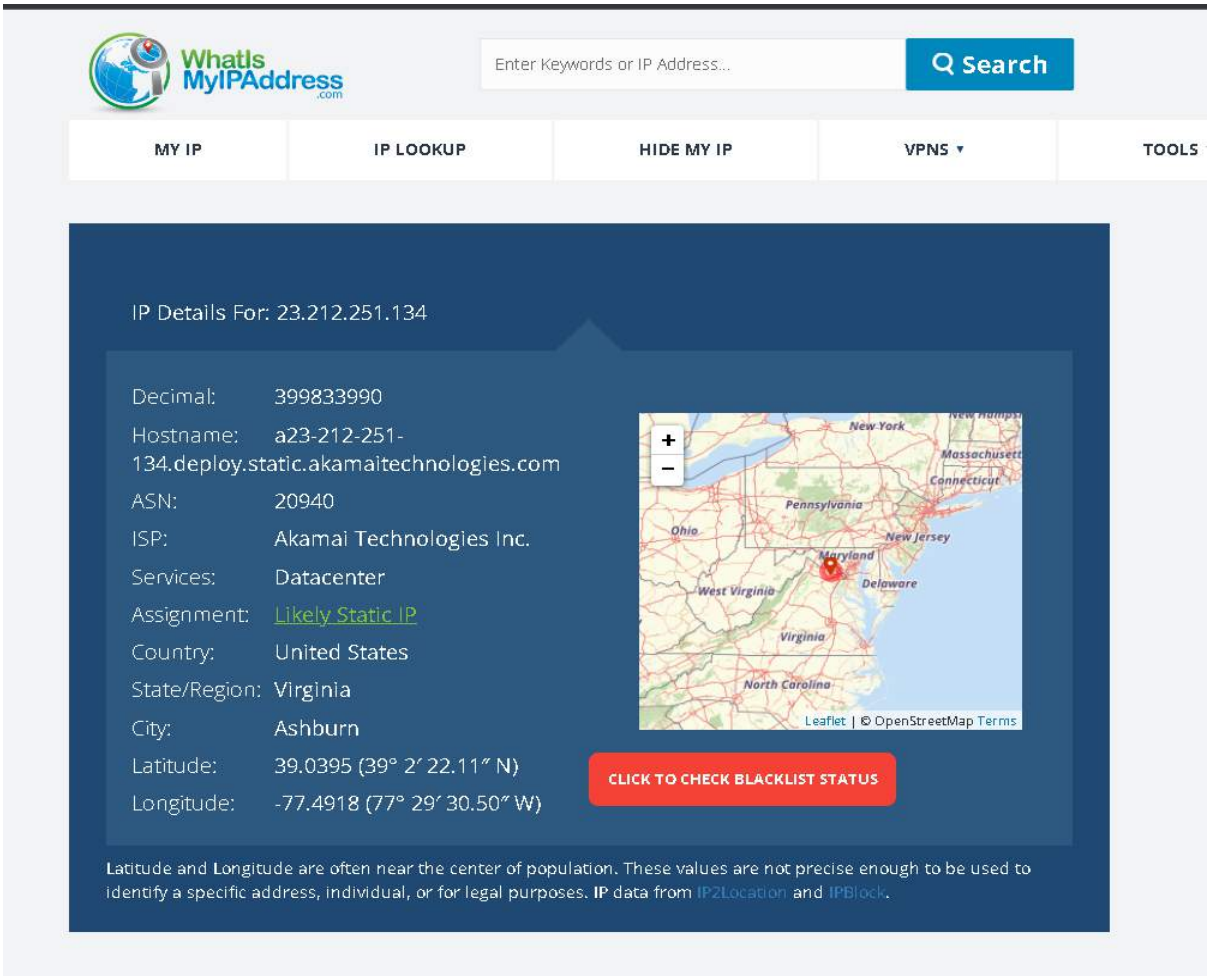


2) What is my IP Address

Step1: - Type https://whatismyipaddress.com/on browser and search. It will give information about your IP address

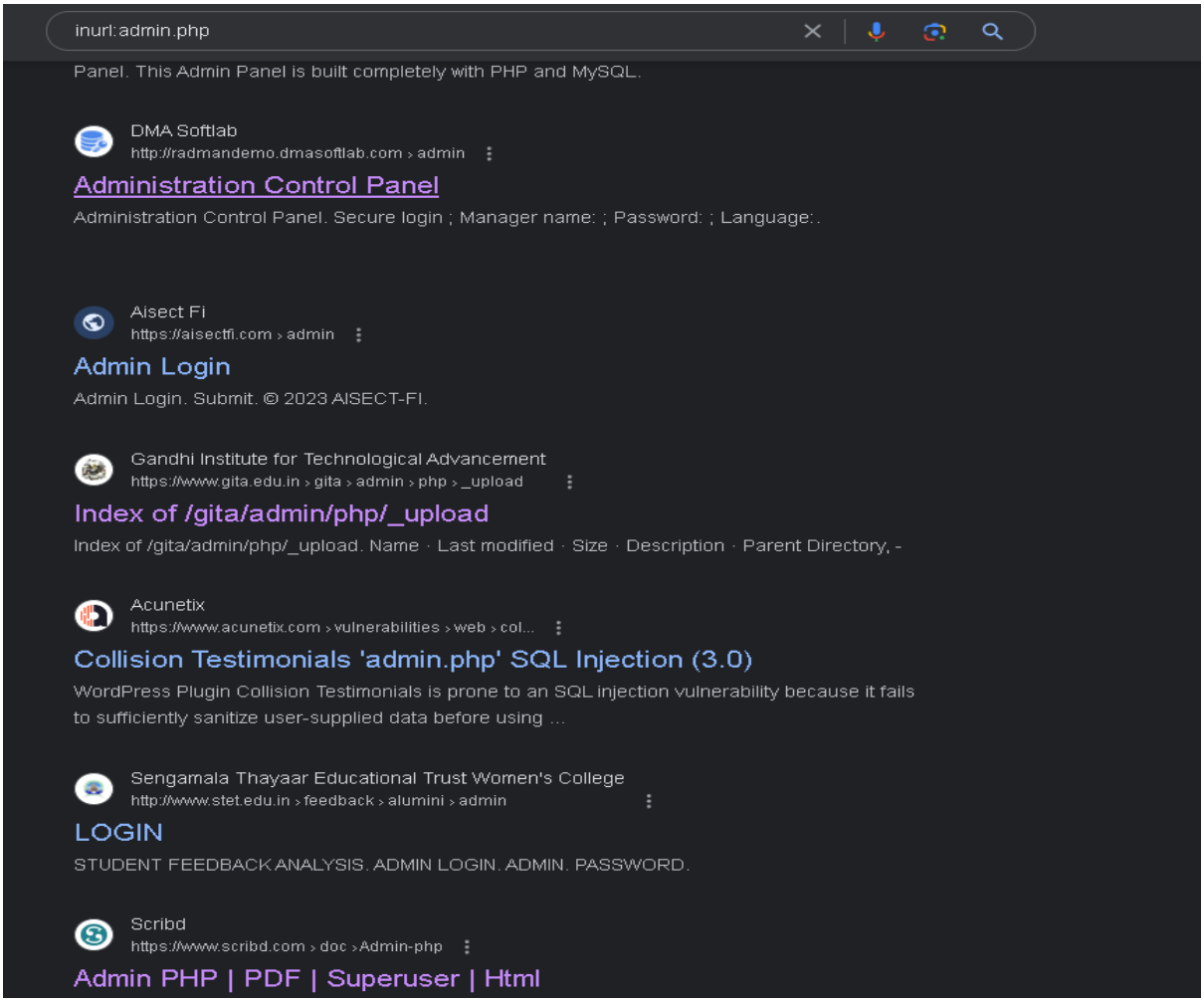


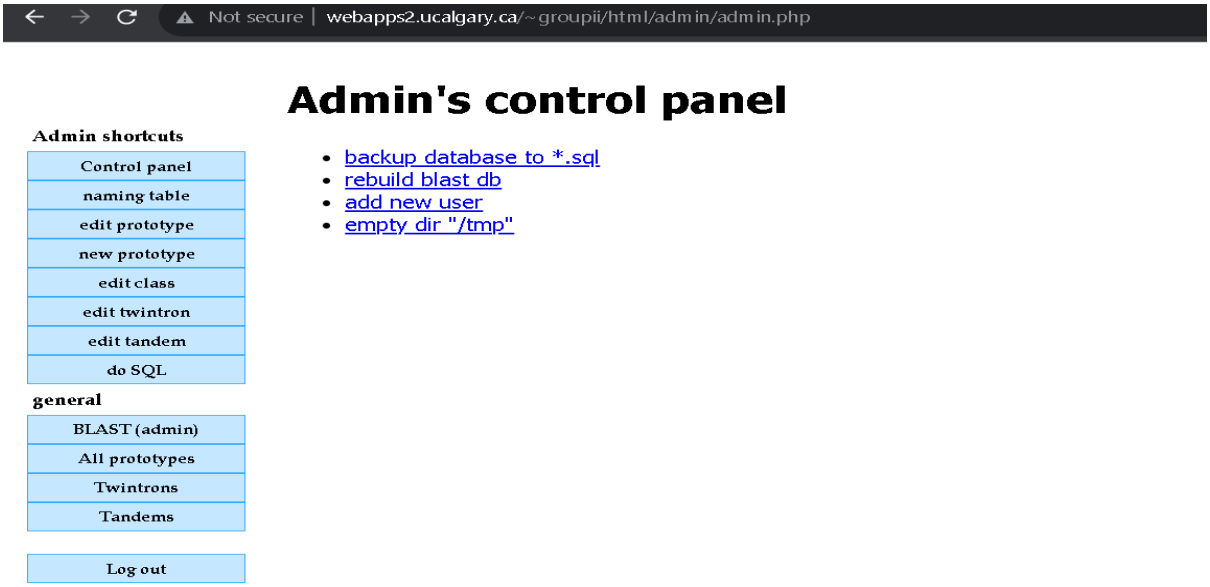
Step3: - enter the Ip address



3)inurl:admin.php

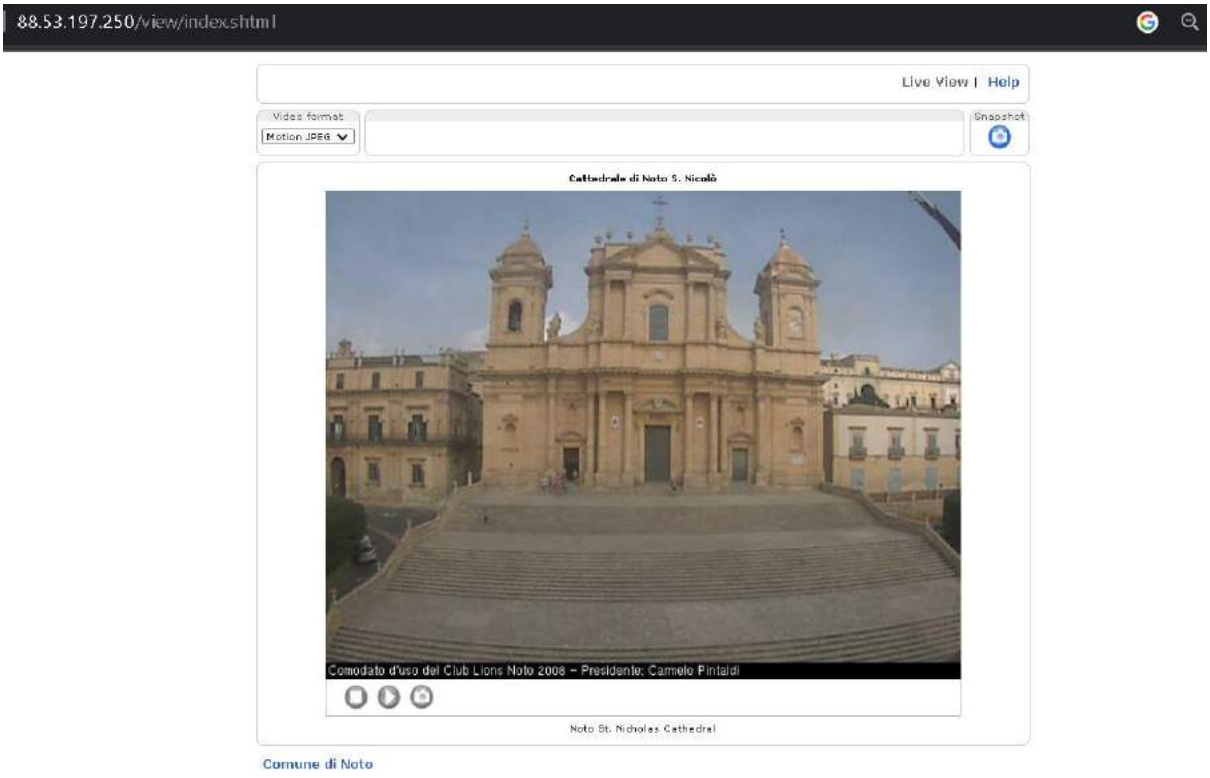
Step1:- enter the inurl:admin.php in the browser an search you'll get all the admin panels which are created using php.





4) inurl:index.shtml

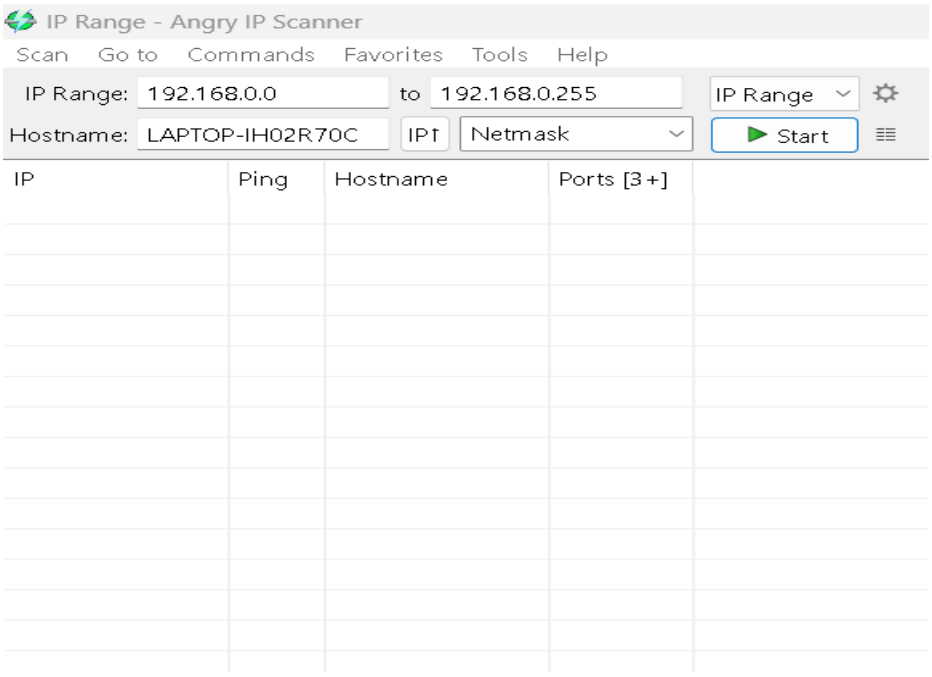
Setp1:- Enter inurl:index.shtml in the browser. It will show you the live view anywhere from the world.



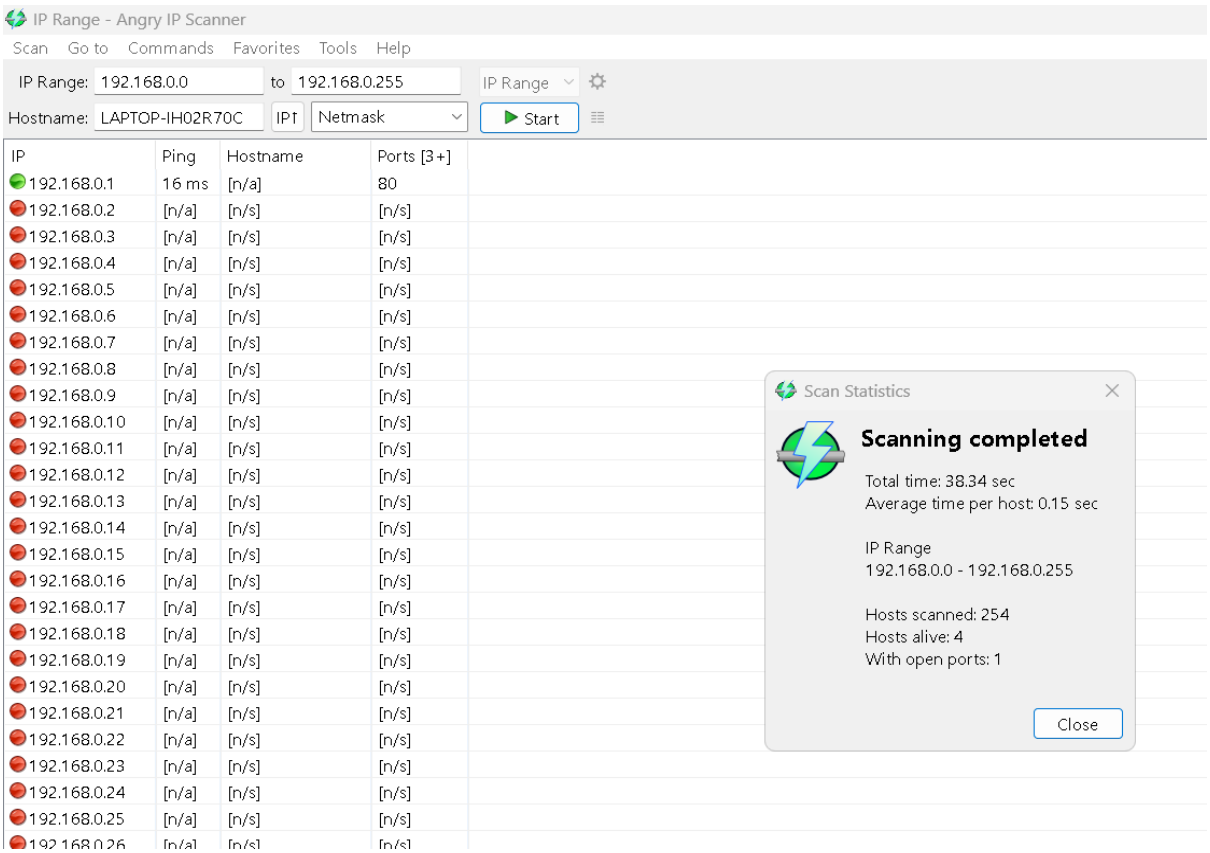
Practical2

1) Angry IP Scanner

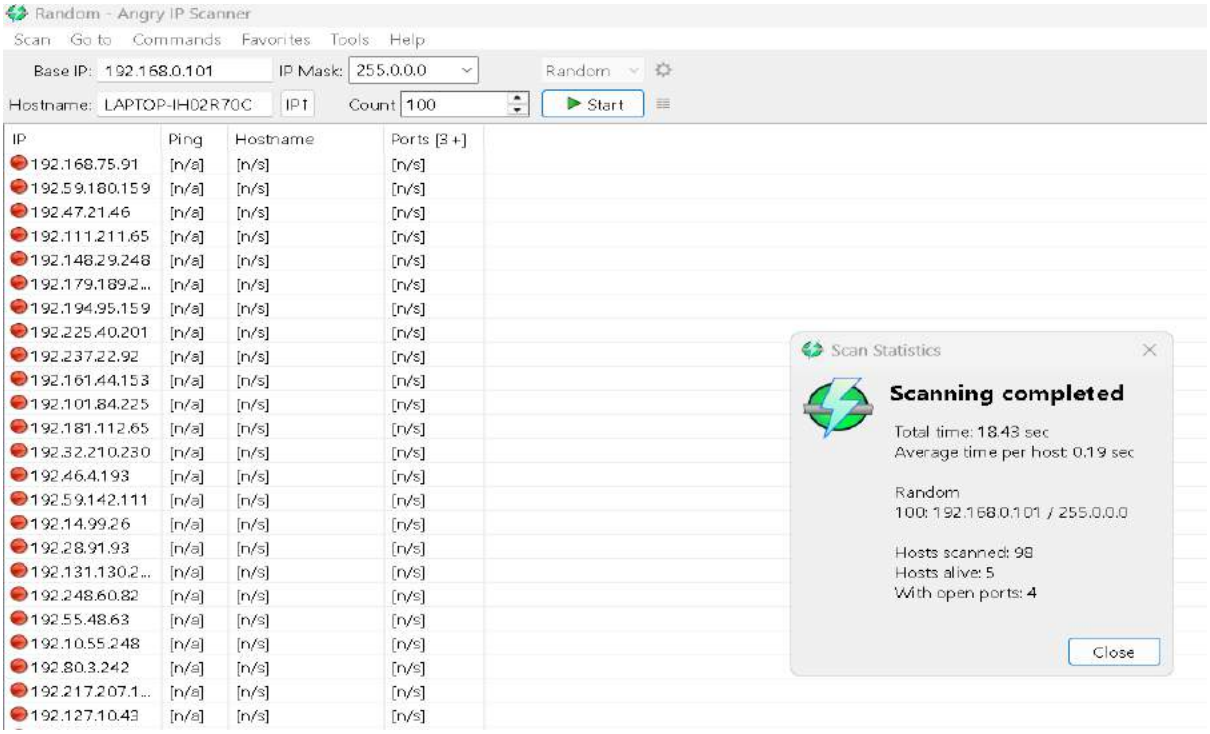
Step:- open the angry Ip scanner software



Step2: - scan for the Ip range



Ste3: - Scan for the random Ip

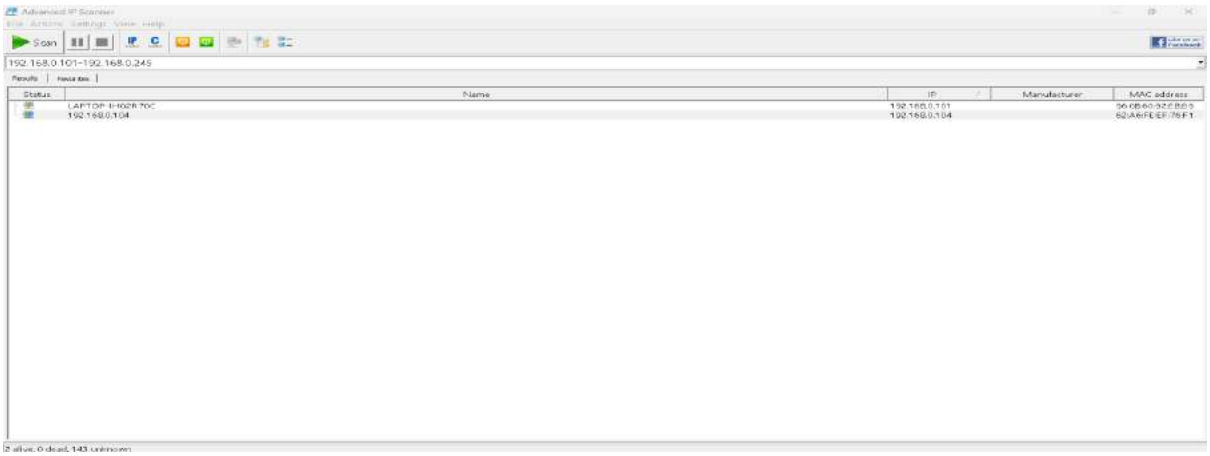


Points to note: - Red dot indicates that the host does not exists anymore, Blue dot indicates that the host is alive but is not active currently and Green dot indicates that the host is alive as well as it is currently active.

2) Advance IP Scanner

Step1:- Open the advance Ip scanner software

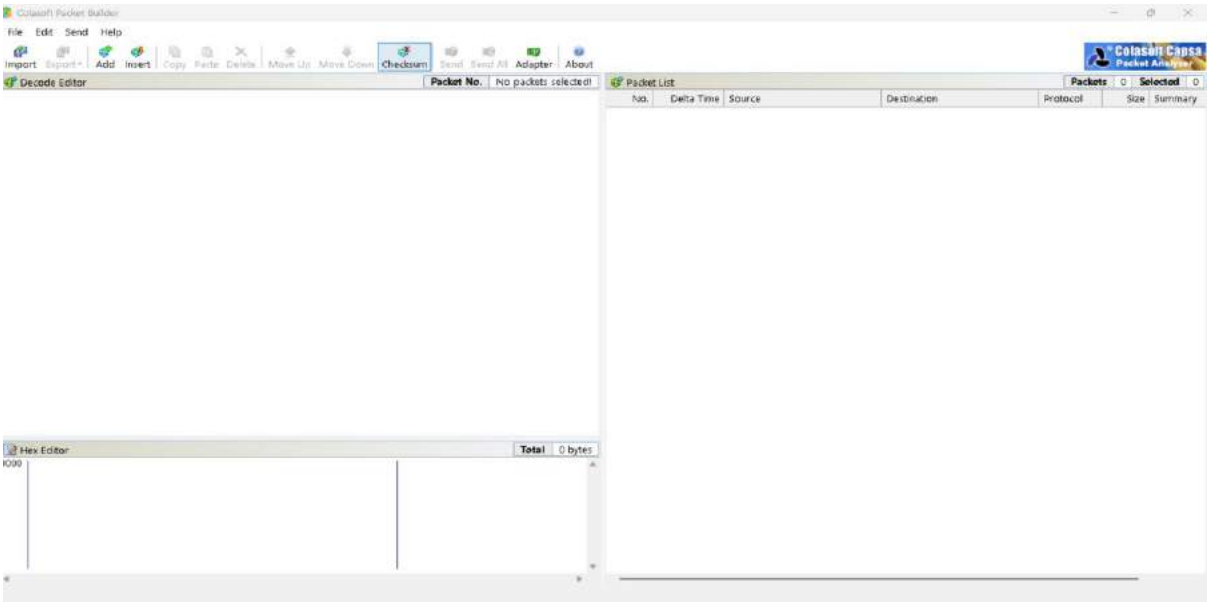
Step2: - now give the Ip address which you want to scan. You can give the range or else you can scan for the single Ip address



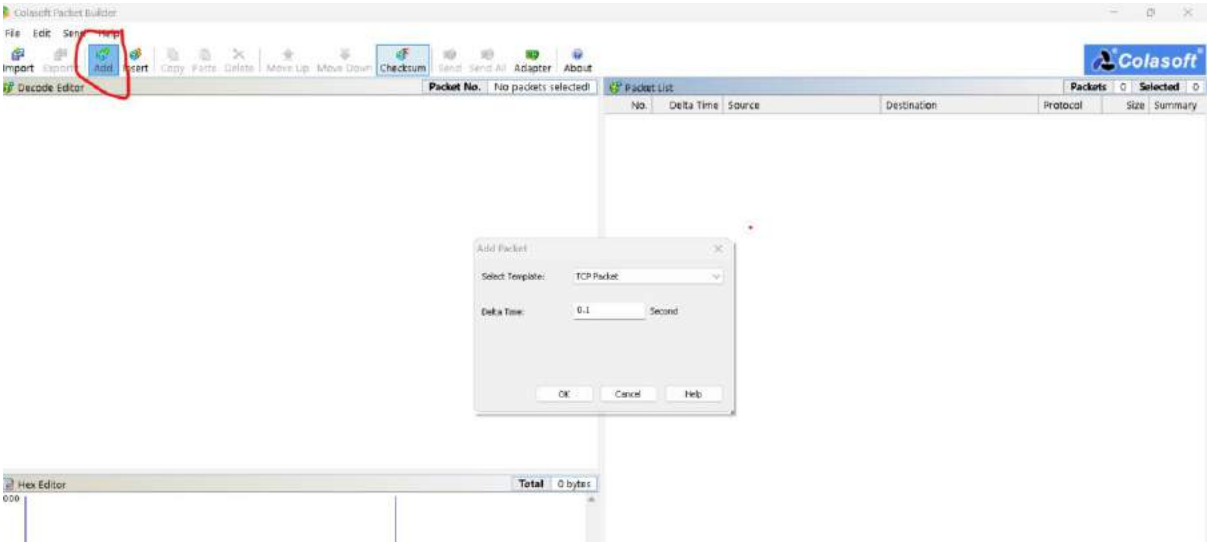
3)Colasoft Packet Builder

ColaSoft Packet Builder is a network performance testing tool that is designed to test the reliability and performance of network devices. It allows users to create and send custom packets through the network, and to analyse the responses received by devices.

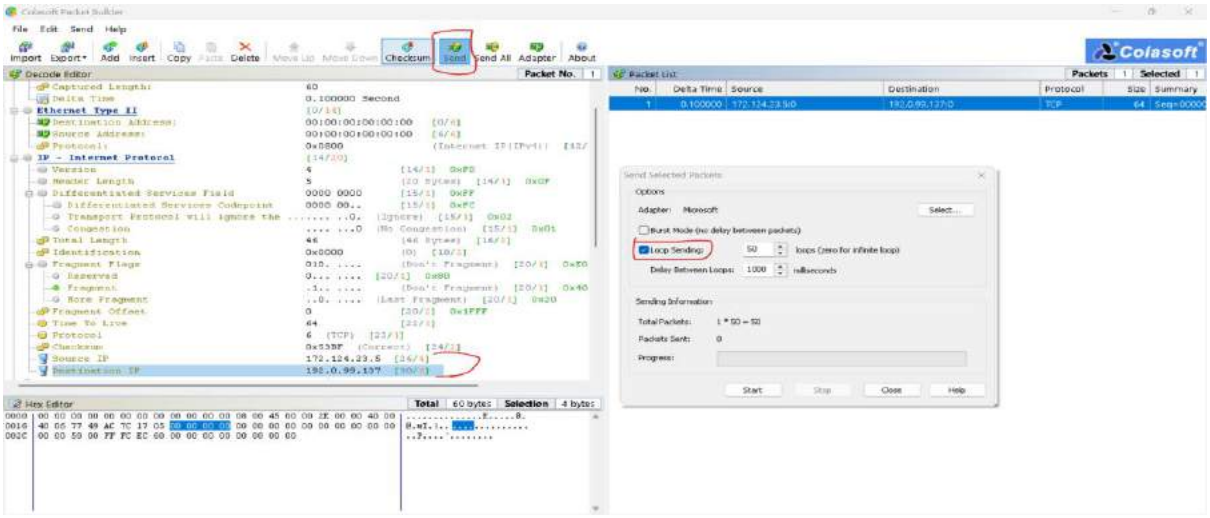
Step1: - Open the colasoft software

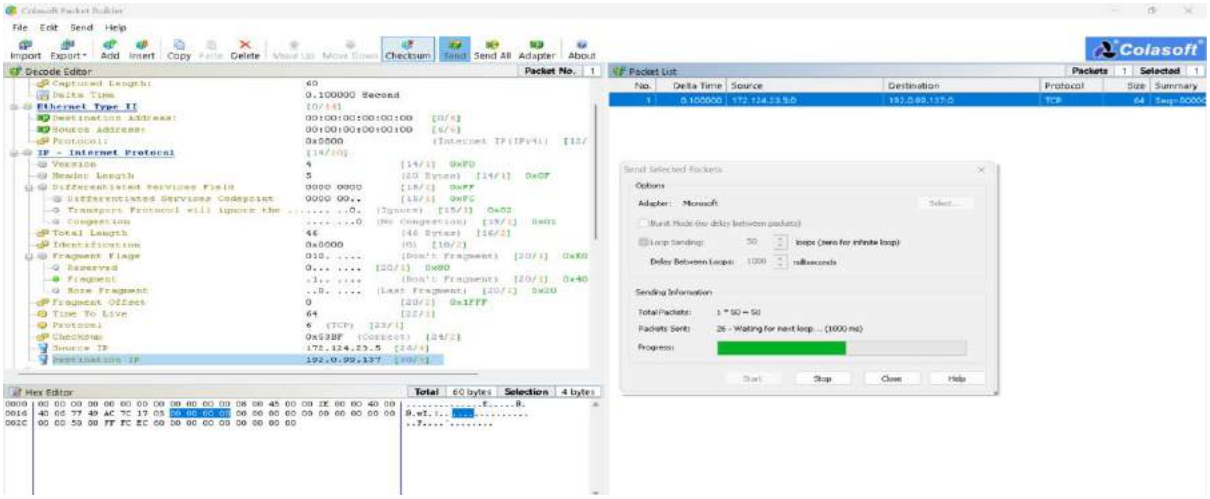


Step2:- click on the add option – select templet and click ok

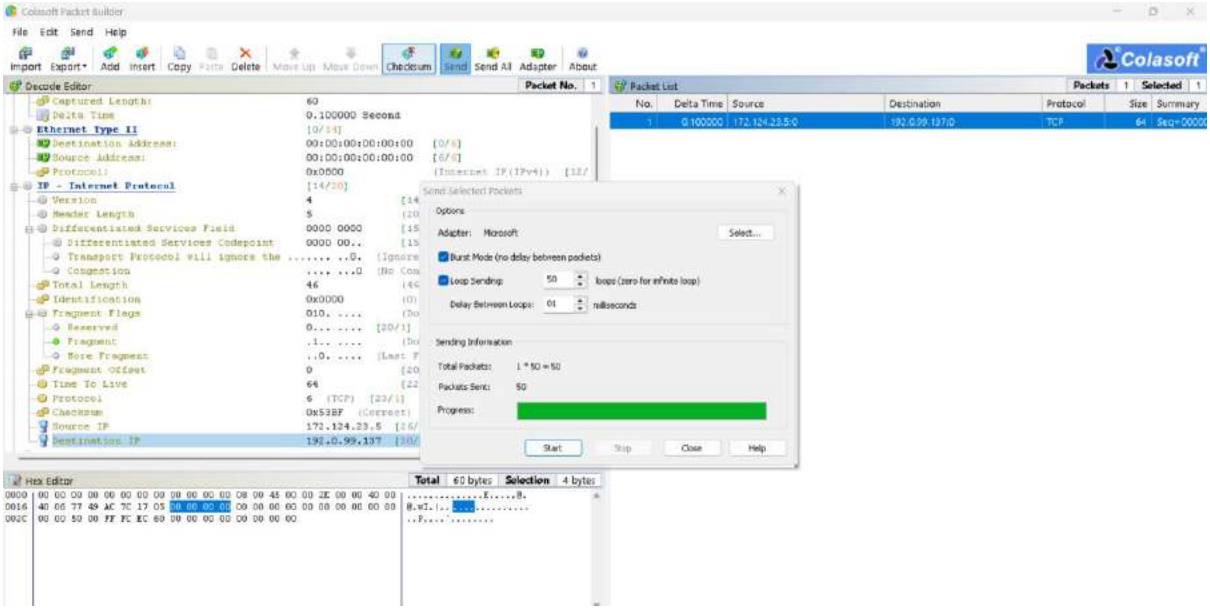


Step3:- now give the source IP and Destination IP of your choice-> then click on send option-> then select the loop sending and click on start.





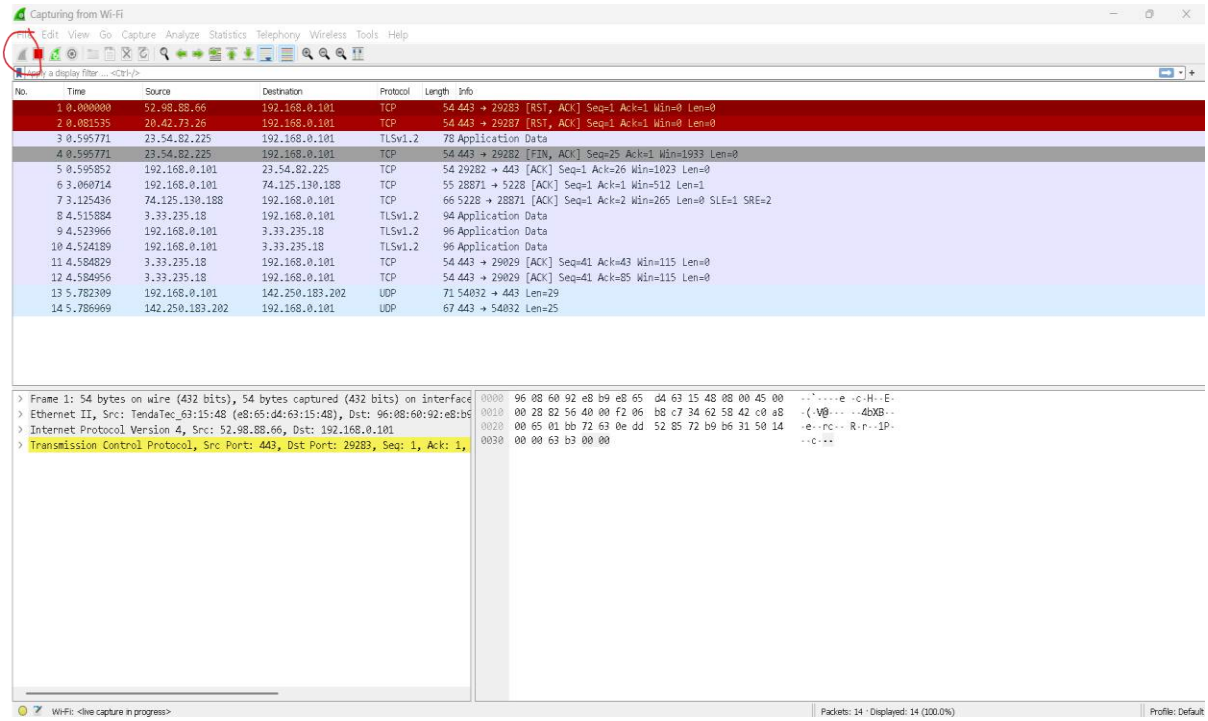
Step4: - You can also use the burst mode



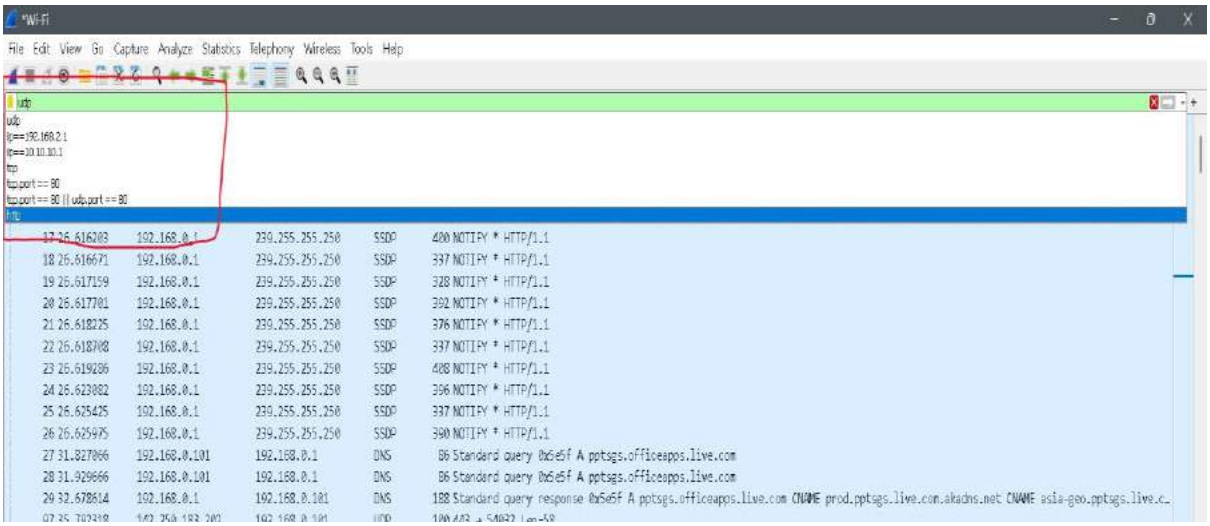
4) Wireshark

Wireshark is a popular network protocol analyser and packet capture tool. It allows you to capture and inspect data traveling on a computer network in real-time.

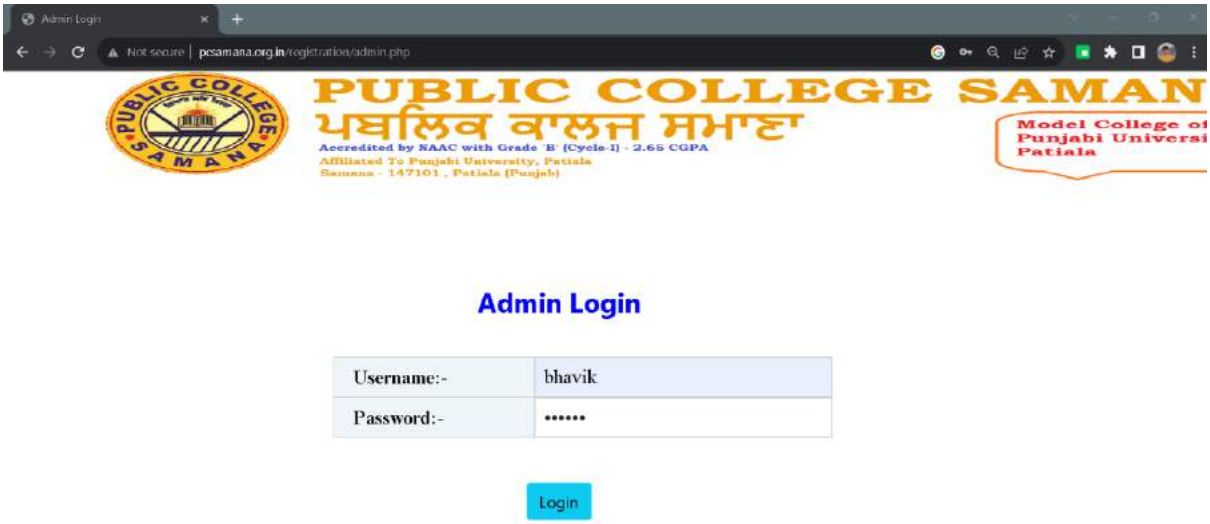
Step: -1 Open the Wireshark software and click on start. This will scan all the traffics which is travelling in your network.



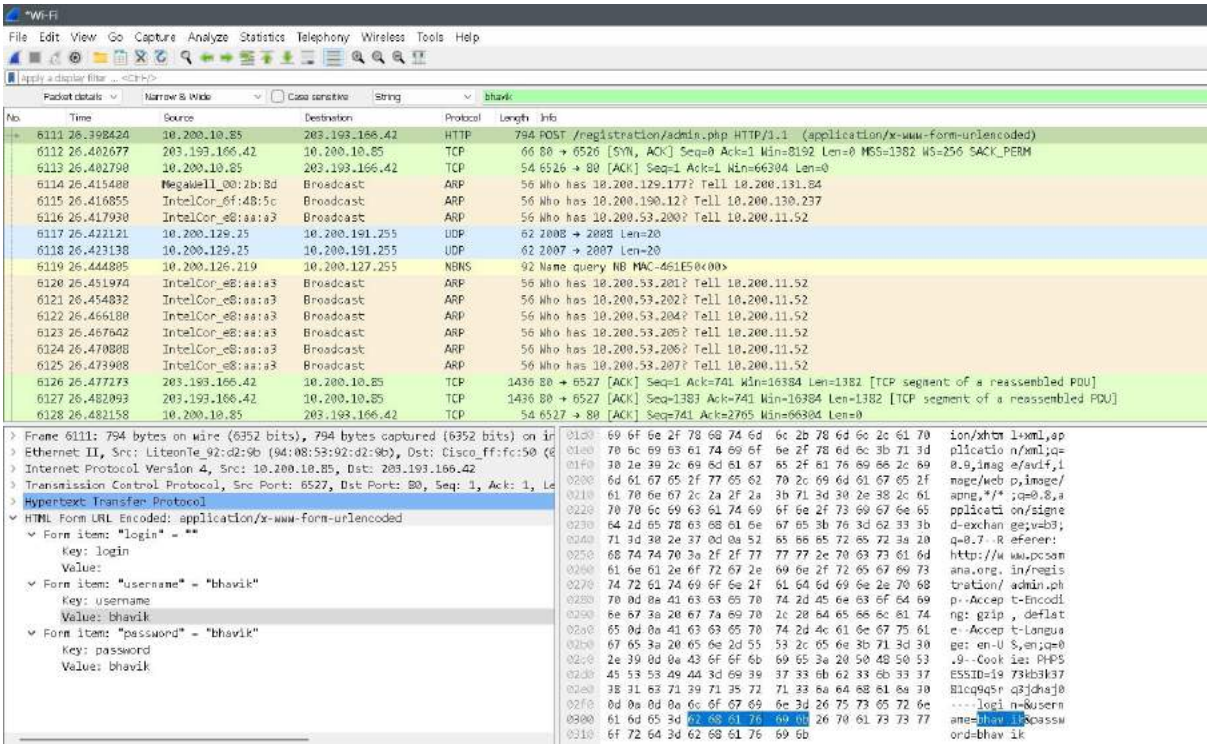
Step2: - Now you can use different filters



STEP3: - In browser search for inurl:admin.php and open any website which has http -> and try toh login using random username and password -> the packet send by that website will be spoofed by the wireshark tool.



Apply the filter using ctrl-f

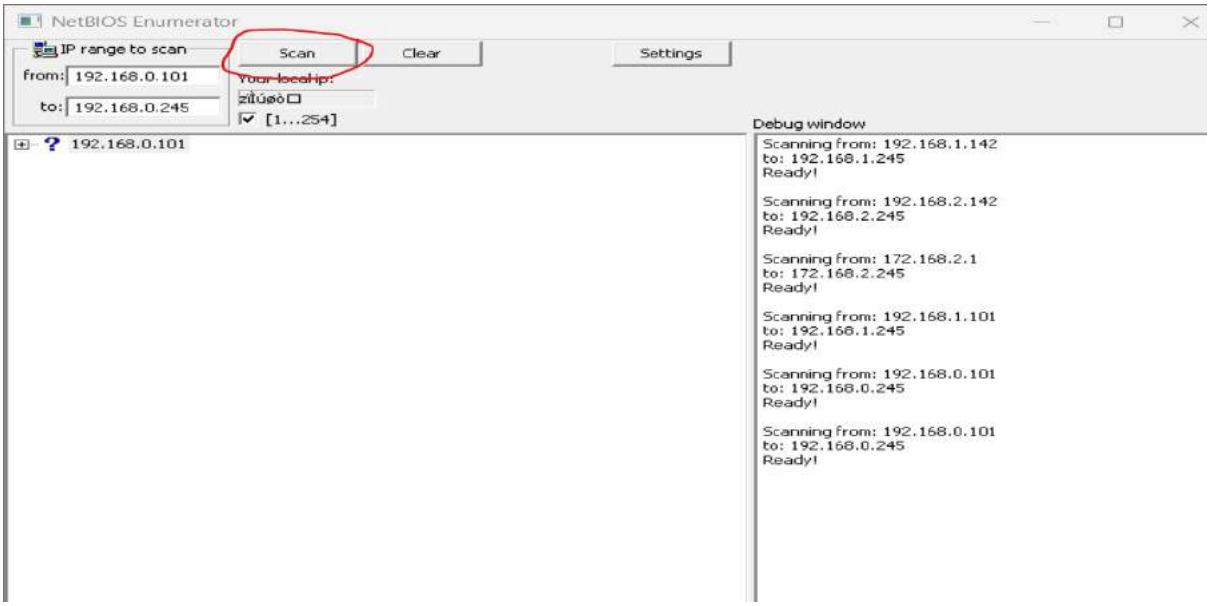


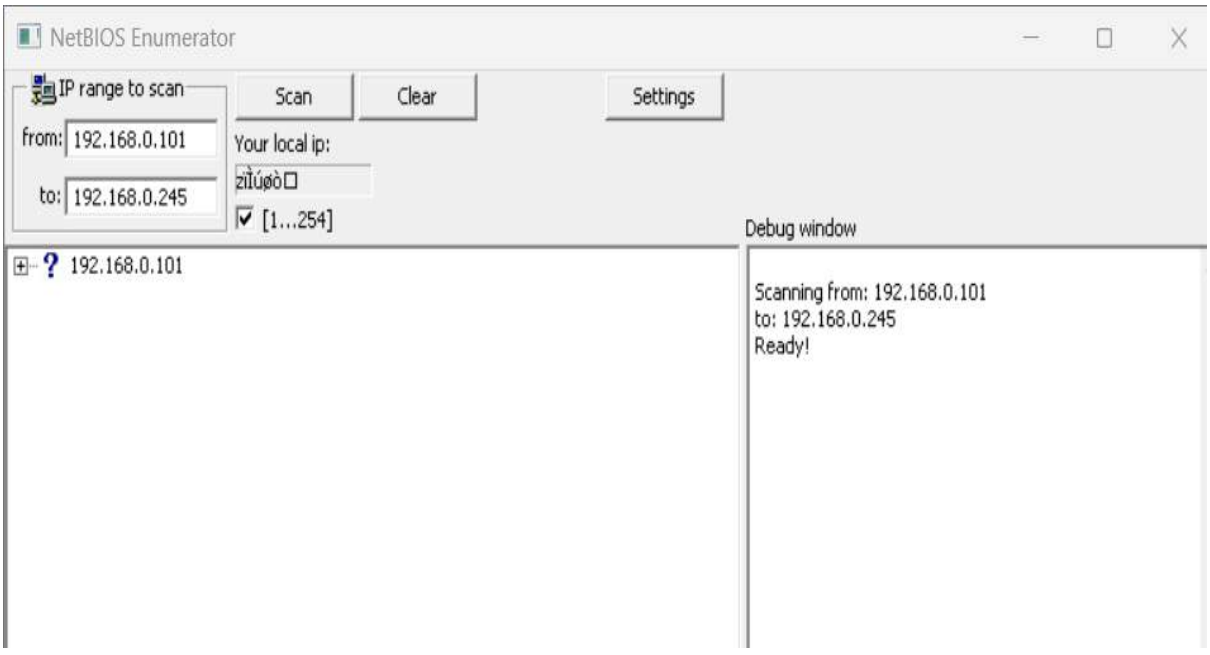
Practical 3

1) NetBIOS Enumerator

NetBIOS is an acronym for Network Basic Input/Output System. It provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network. As strictly an API, NetBIOS is not a networking protocol.

Step1: - pen the netbios enumeration tool -> enter the ip range you want to scan and press scan.

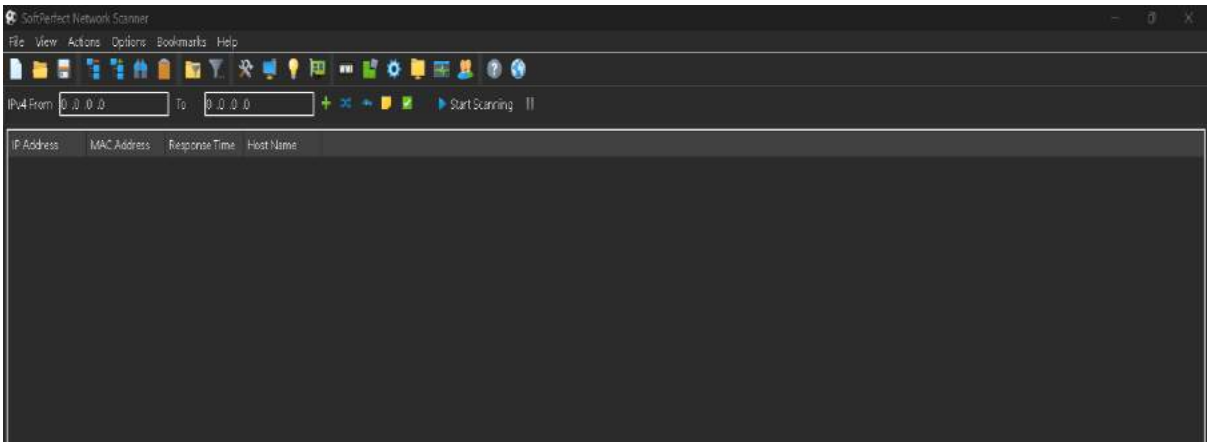


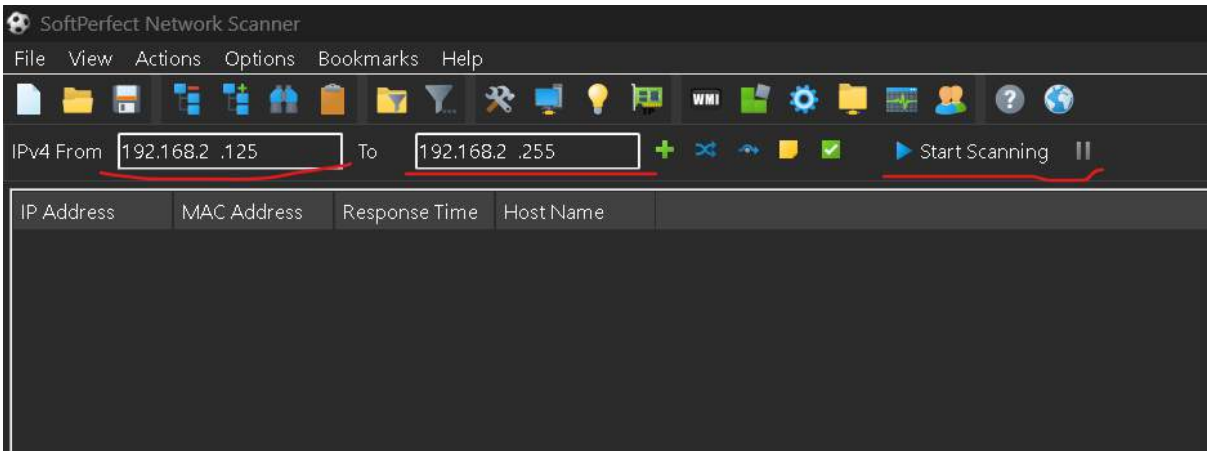


2) SoftPerfect Network Scanner

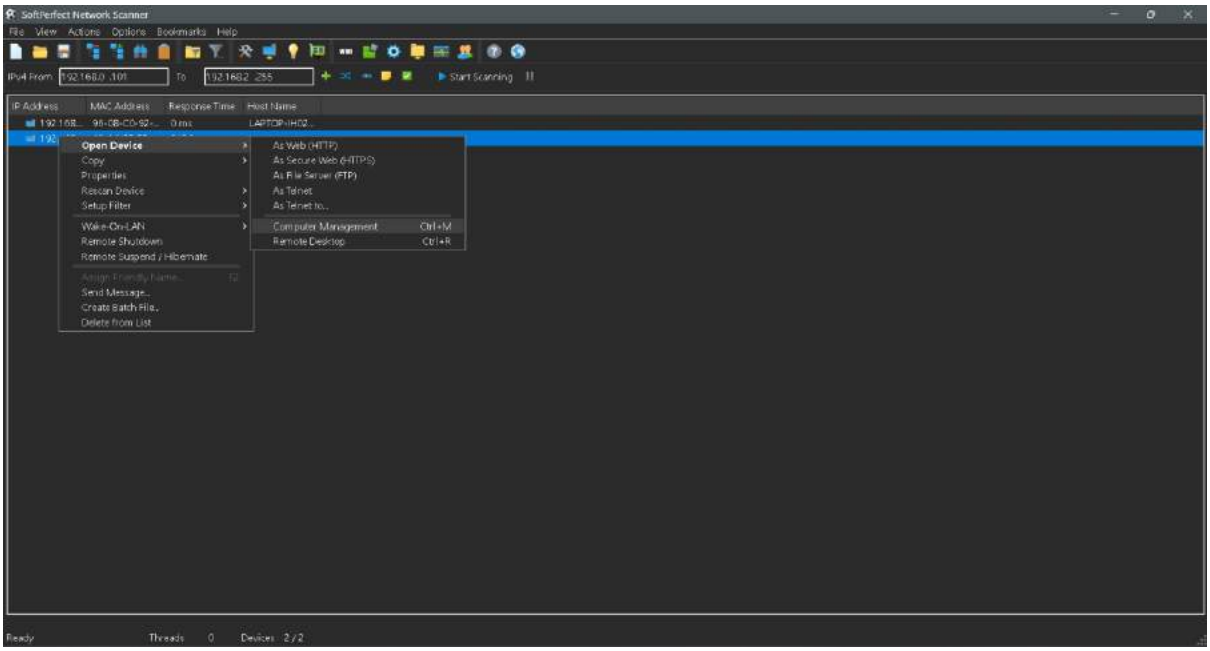
SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices via WMI, SNMP, HTTP, SSHand PowerShell. It also scans for remote services, registry, files and performance counters.

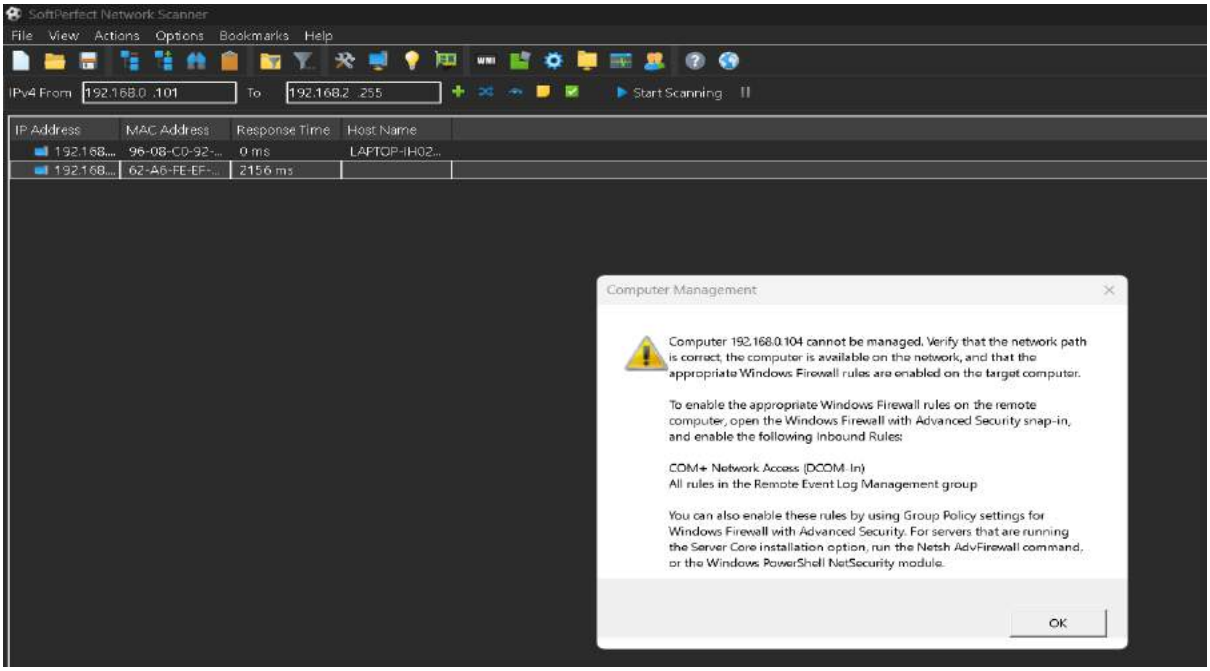
Step1: -Open the SoftPerfect Network Scanner tool -> then entre the ip address range and click on start.





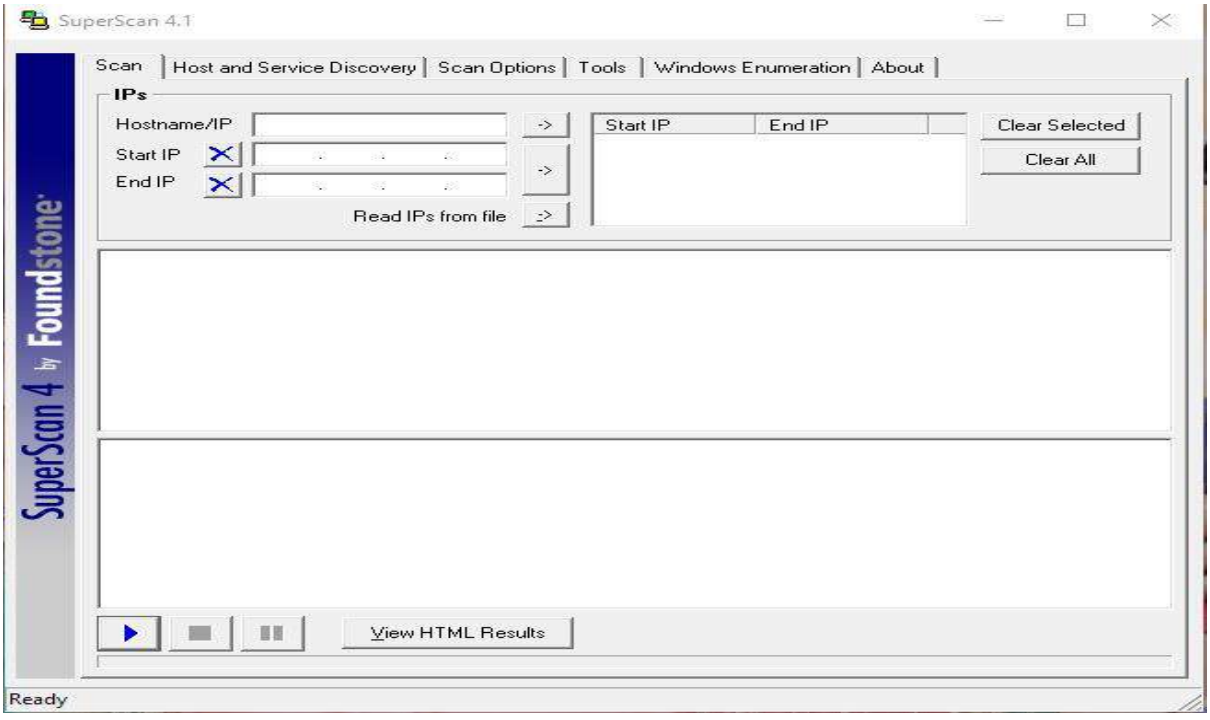
Step 2: - Right click on the IP address click on “Open computer” option and click on “ComputerManagement” in that.



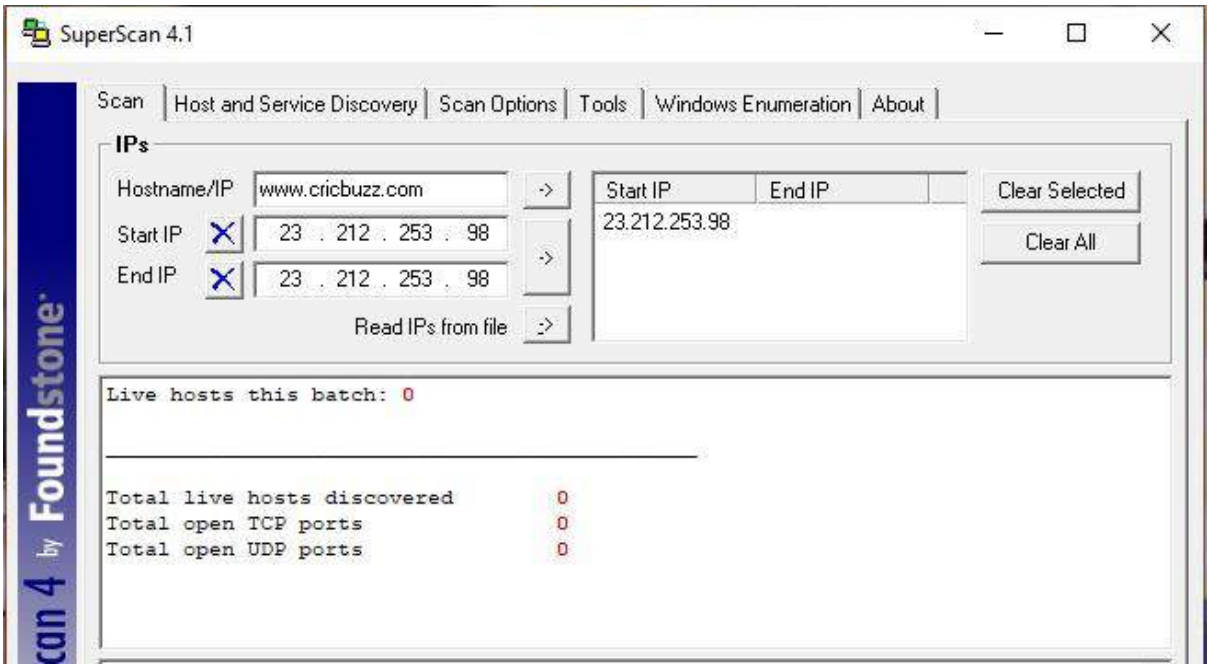


3) Superscan

Step1: - open the super scan tool.



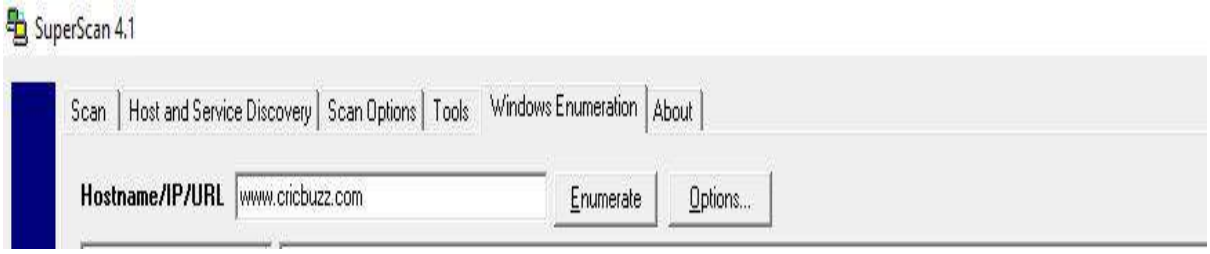
Step2: -Entre the range of ip address you want scan h scan it. And you can also entre the url .




```
The IP list contains 1 entries
Service TCP ports: 179
Service UDP ports: 88
Packet delay: 10
Discovery passes: 1
ICMP pinging for host discovery: Yes
Host discovery ICMP timeout: 2000
TCP banner grabbing timeout: 8000
UDP banner grabbing timeout: 8000
Service scan passes: 1
Hostname resolving passes: 1
Full connect TCP scanning for service scanning: No
Service scanning TCP timeout: 4000
Service scanning UDP timeout: 2000
TCP source port: 0
UDP source port: 0
Enable hostname lookup: Yes
Enable banner grabbing: Yes
```

```
Scan started: 11/06/23 21:03:20

-------- Scan of 1 hosts started --------
Scanning 1 machines with 1 remaining.
-------- Host discovery pass 1 of 1 --------
Host discovery ICMP (Echo) scan (1 hosts)...
*** ICMP host discovery encountered a problem and was unable to continue (Winsock error 10051)
0 new machines discovered with ICMP (Echo)
Host discovery ICMP (Echo) scan (1 hosts)...
*** ICMP host discovery encountered a problem and was unable to continue (Winsock error 10051)
0 new machines discovered with ICMP (Echo)
Host discovery ICMP (Echo) scan (1 hosts)...
*** ICMP host discovery encountered a problem and was unable to continue (Winsock error 10051)
0 new machines discovered with ICMP (Echo)
Reporting scan results...
-------- Scan done --------
```

Step3: -now go to windows enumeration -> entre the url crizzbuz.com -> enumeration



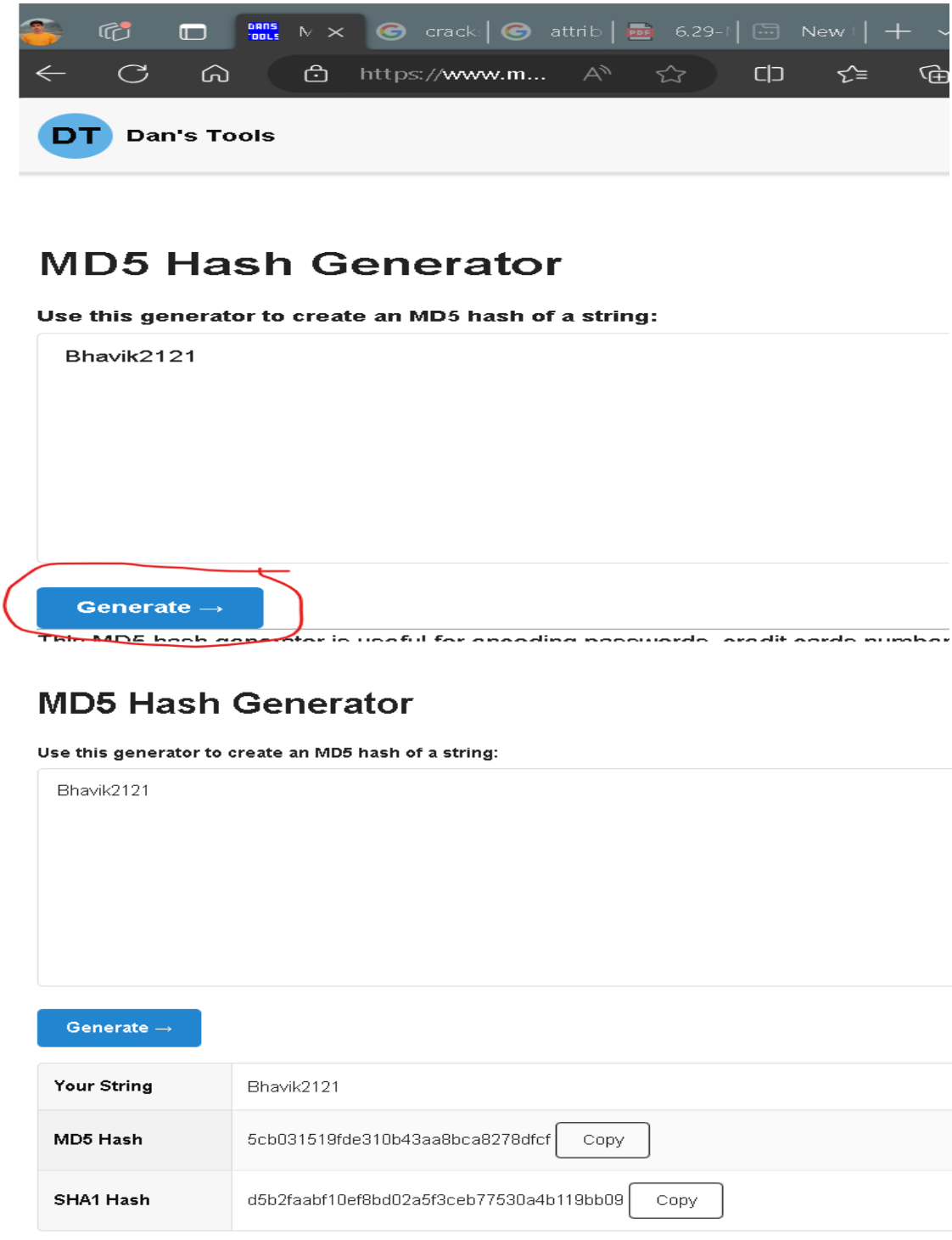

```
NetBIOS information on 23.212.253.98

Attempting a NULL session connection on 23.212.253.98

MAC addresses on 23.212.253.98

Workstation/server type on 23.212.253.98

Users on 23.212.253.98

Groups on 23.212.253.98

RPC endpoints on 23.212.253.98

Password and account policies on 23.212.253.98

Shares on 23.212.253.98

Domains on 23.212.253.98

Remote time of day on 23.212.253.98

Logon sessions on 23.212.253.98
```

```
Drives on 23.212.253.98

Trusted Domains on 23.212.253.98

Remote services on 23.212.253.98

Remote registry items on 23.212.253.98


Enumeration complete
```

Practical 4

1) Password cracker

Step 1: - Open MD5 Hash Generator-> type a password->Click on Generate and then copy the MD5Hash string of it.

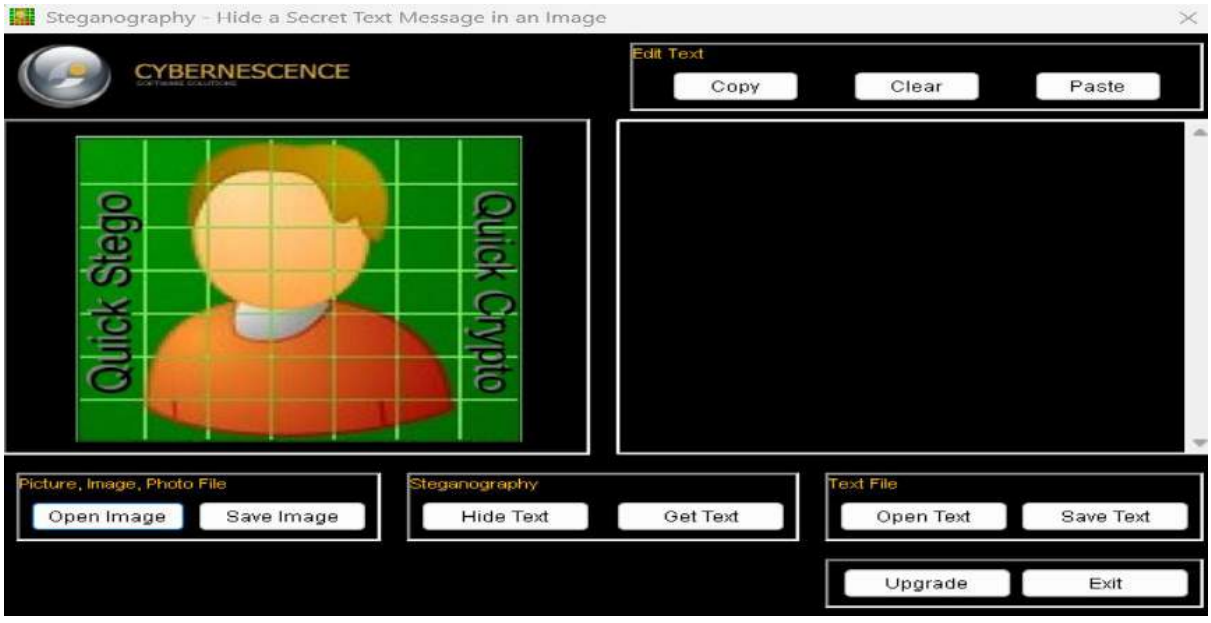


step2: - Now open CrackStation and paste the MD5Hash String -> click on Crack Hashes. In the result column you will be able to see the password which you have typed.

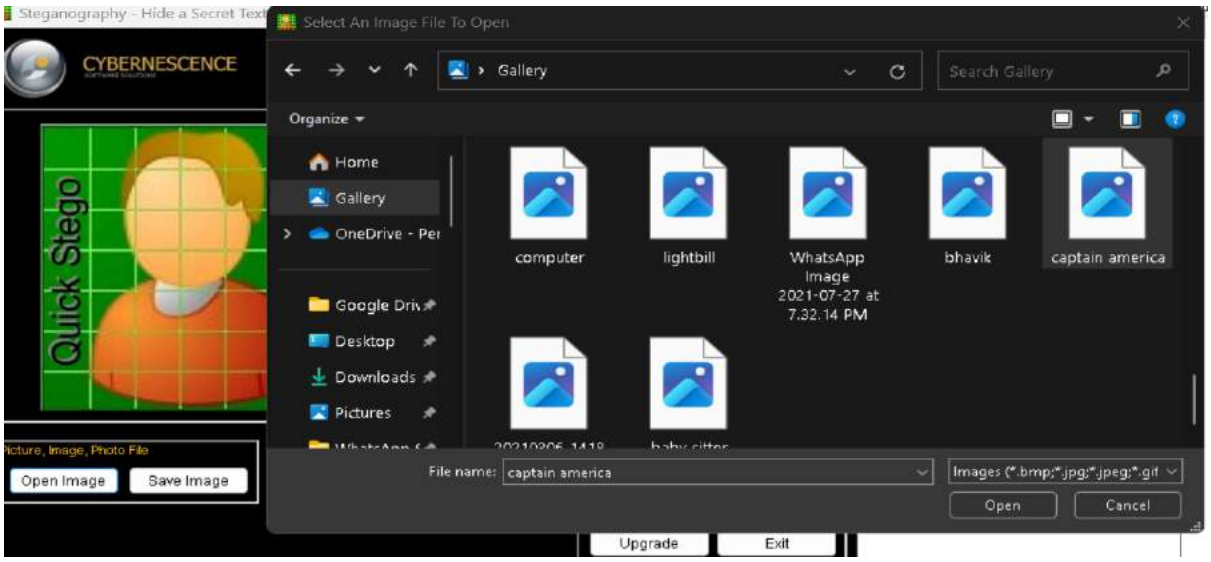
2) Quickstego

QuickStego is use for Steganography . Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

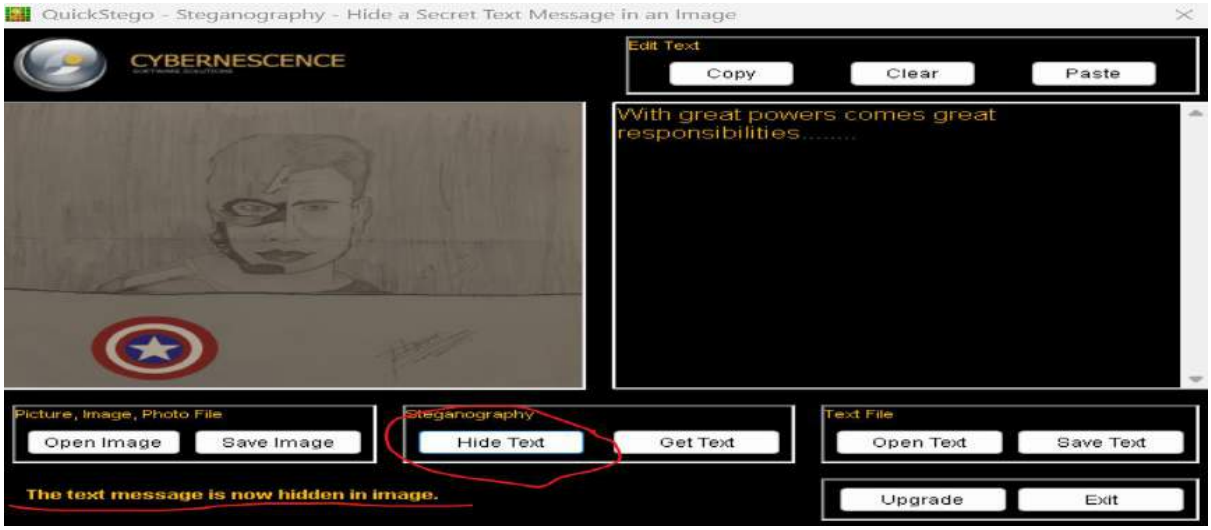
Step 1: - Open the Quickstego tool.



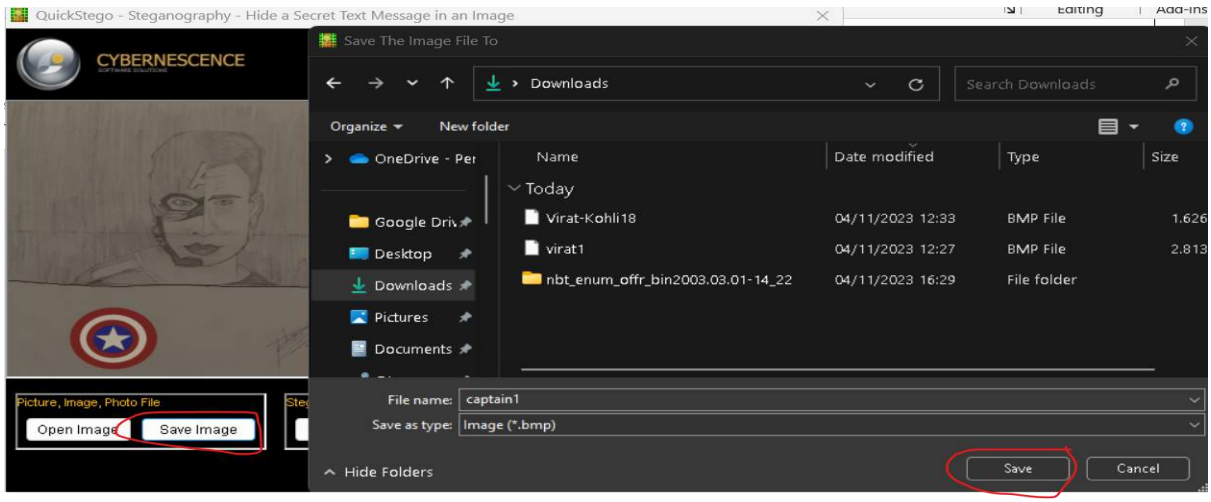
Step 2 : Open an Image-> Write some text->click on Hide Text and then on save the image.



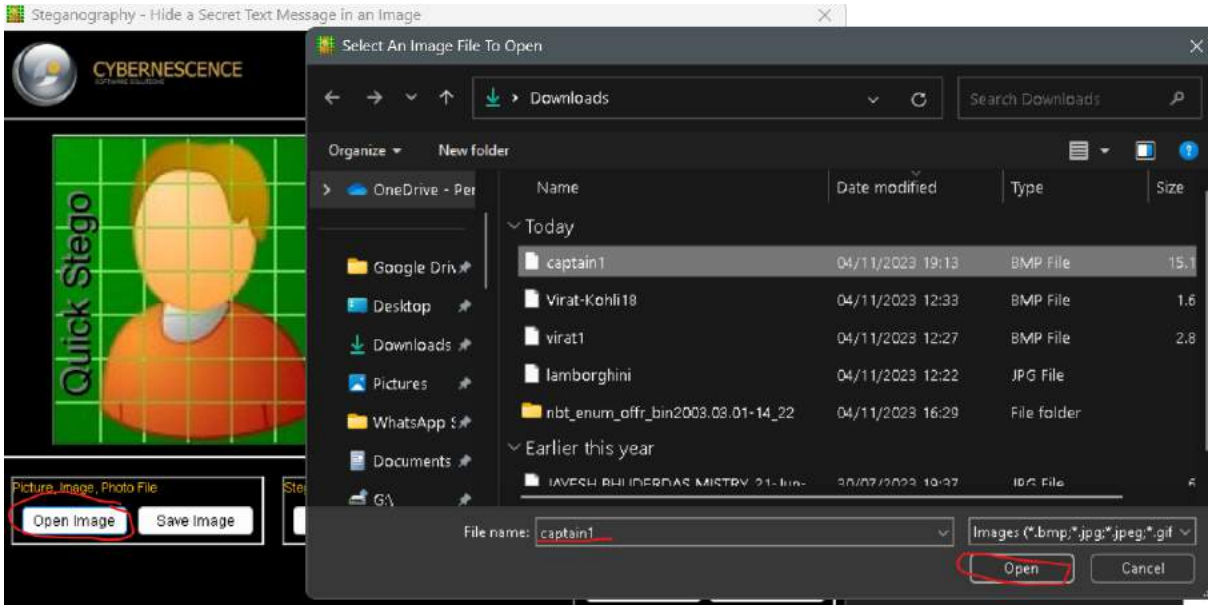
Write and hide



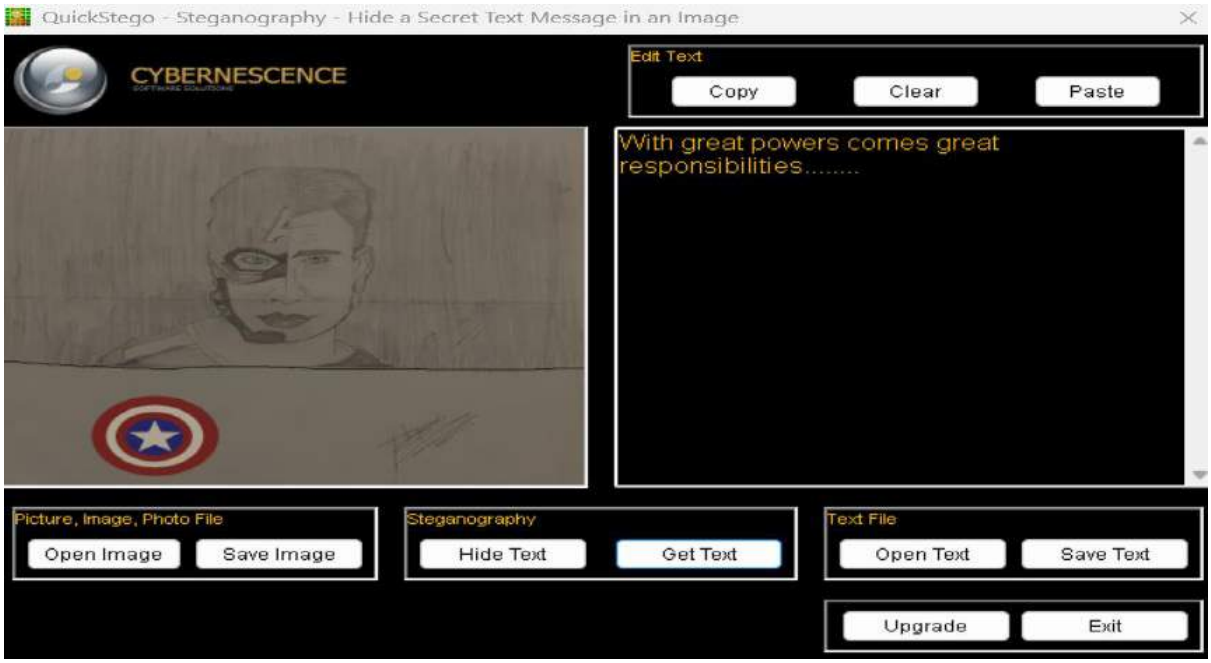
Save image



Step 3: - Again, open QuickStego and open the saved image.

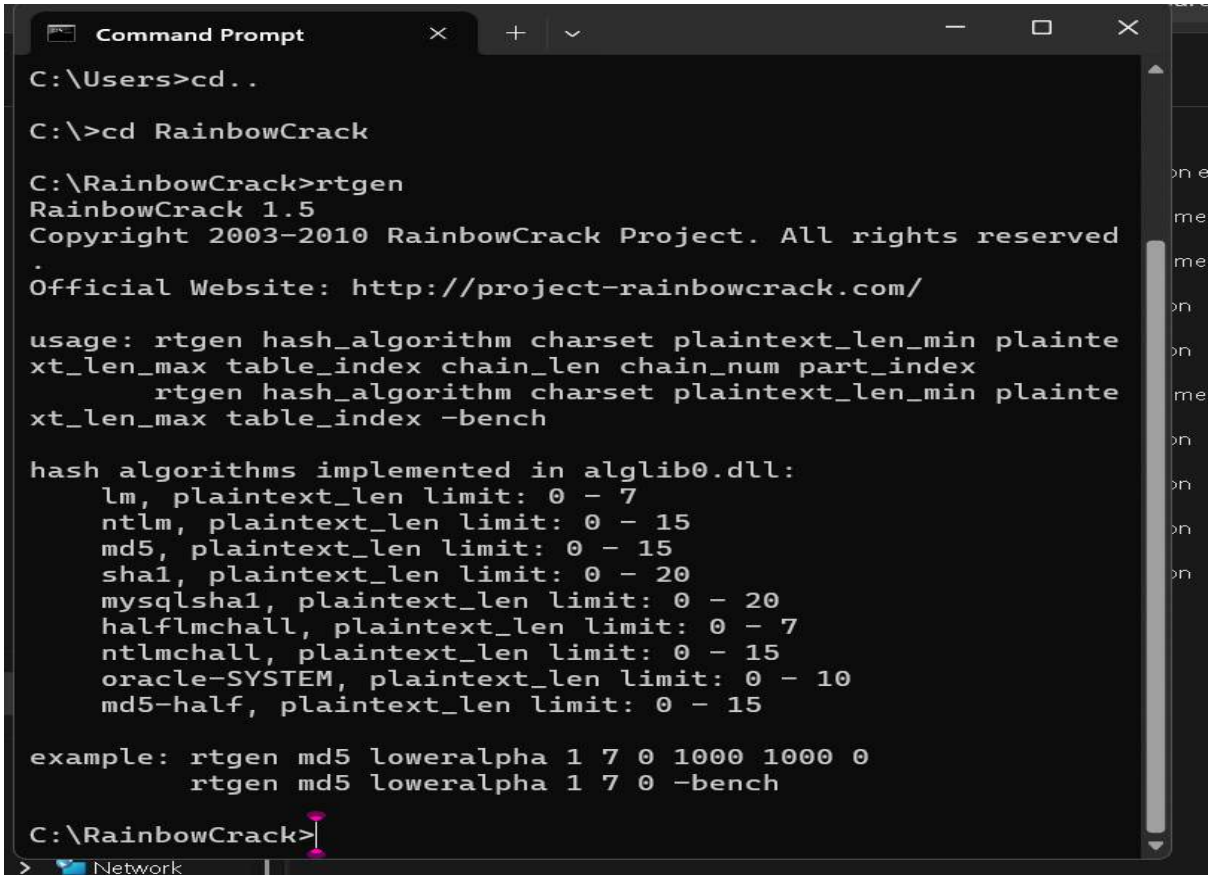


Step4: - click on Get text

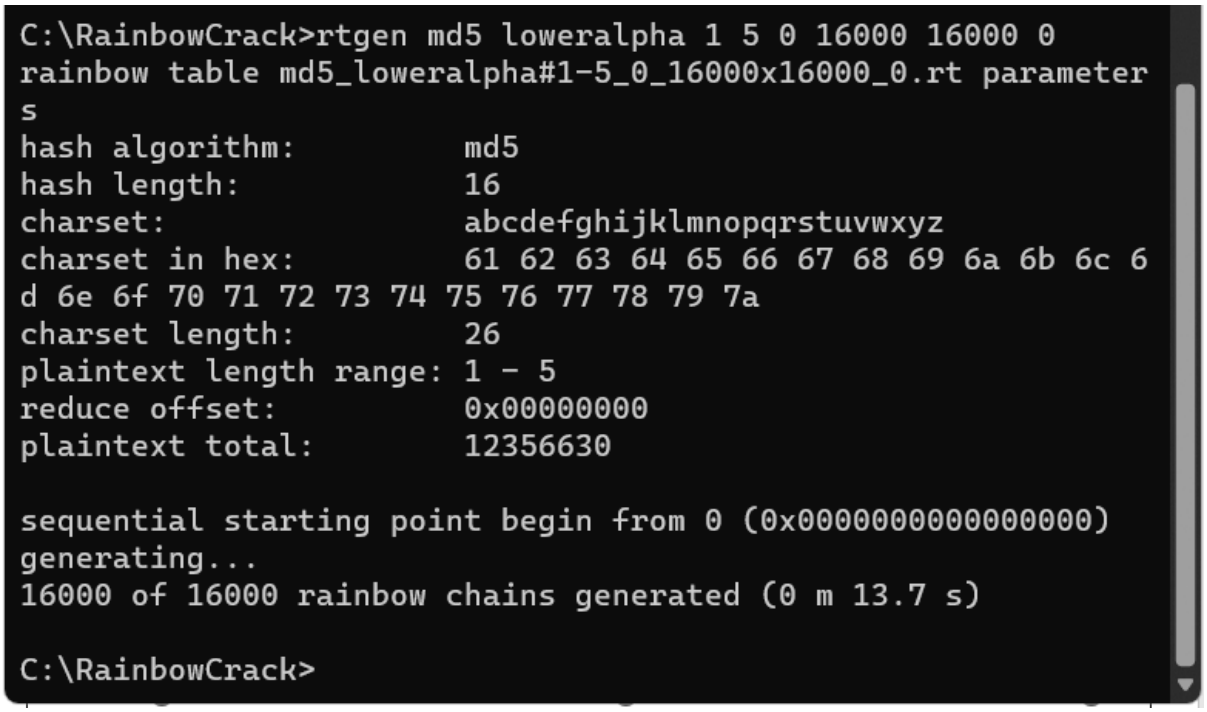


3) Rainbow Crack

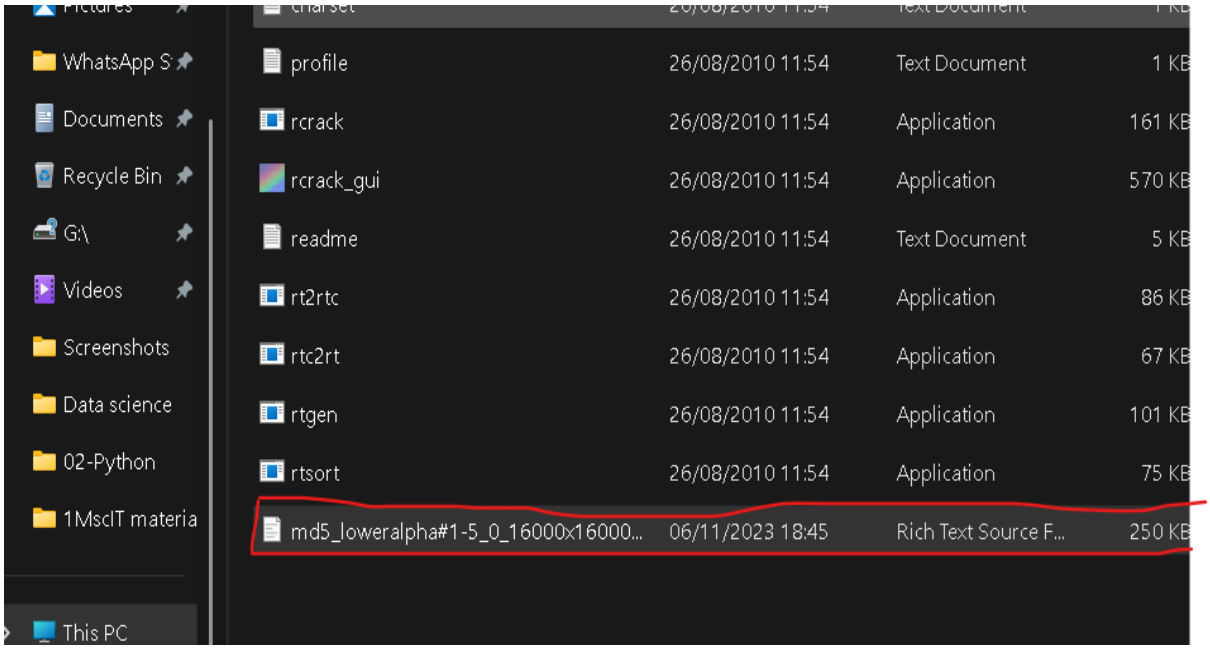
Step 1: -save the rainbow cracker file in c drive-> Open cmd. -> Go to the rainbow cracker path and type the command rtgen.



Step 2: - Now Generate rainbow table. Type the command in cmd **->rtgen md5 loweralpha 1 5 0 16000 16000 0**

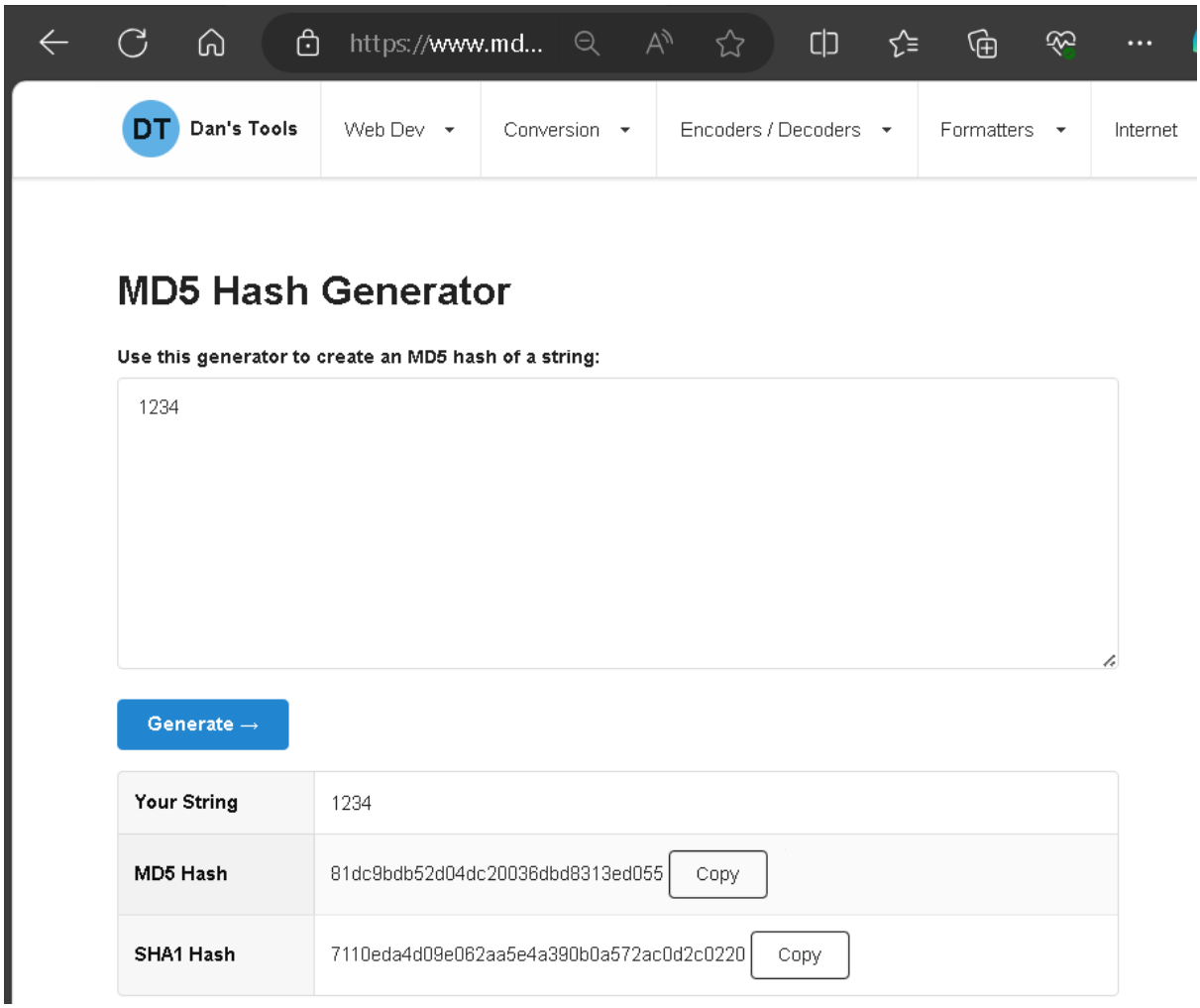


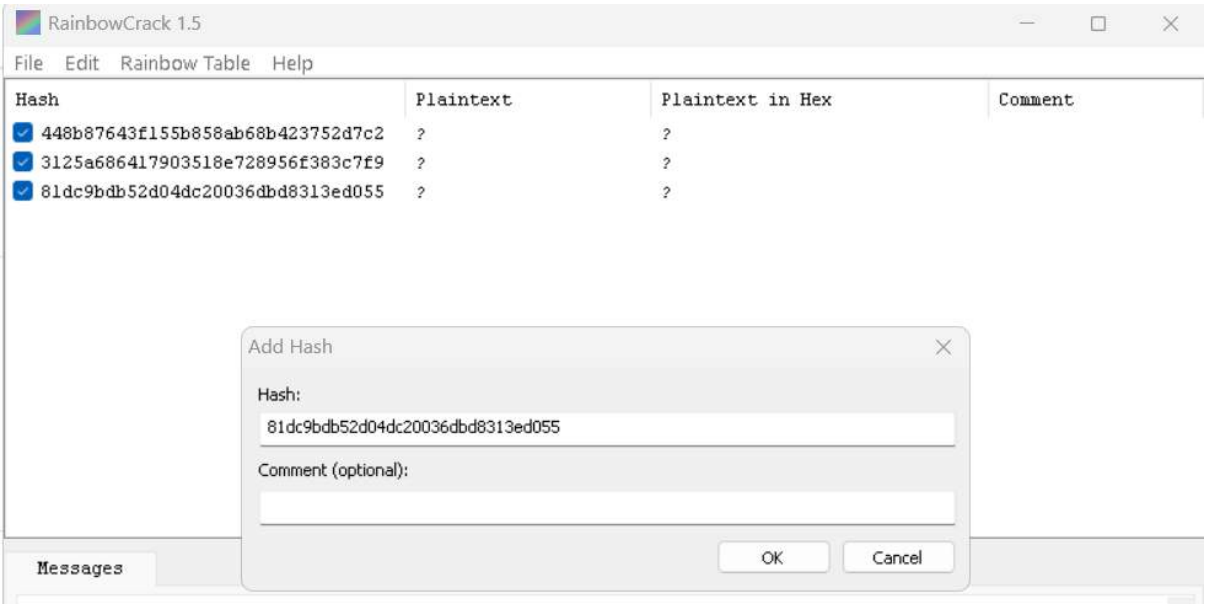
Step 3: You can find the new file in the rainbow crack folder.



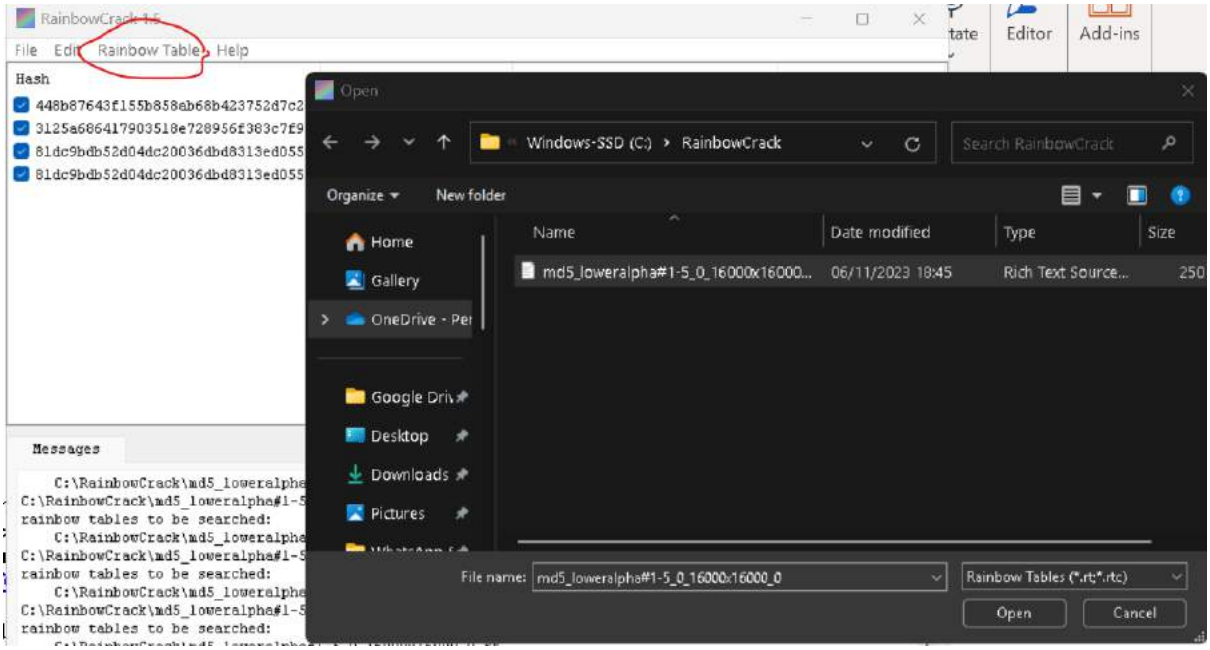
Step4:-open rcrack_gui

Step5: - go to hash generator generate any hash -> copy it -> and paste in the add hash .

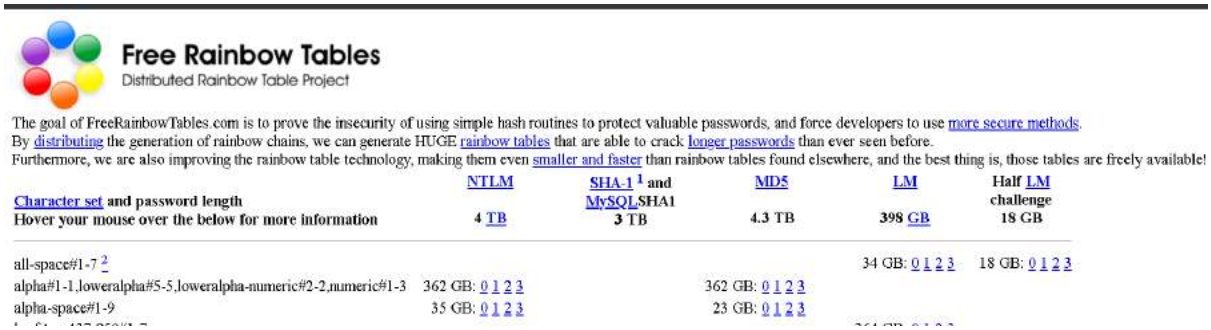




Step6: - after adding you have to go to -> raindow table-> search raindow tables->and add your table .

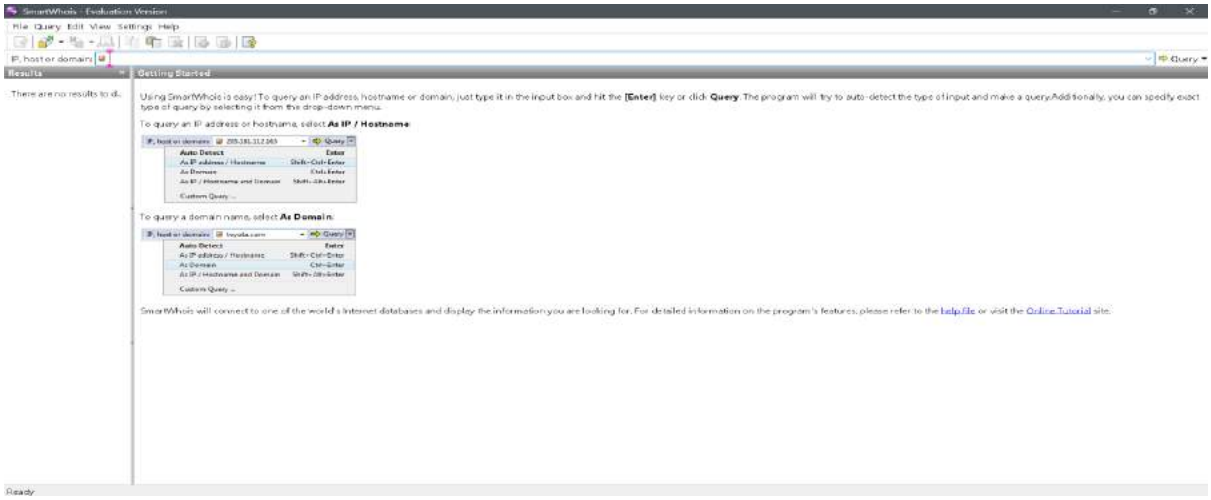


You can Download free rainbow table from here

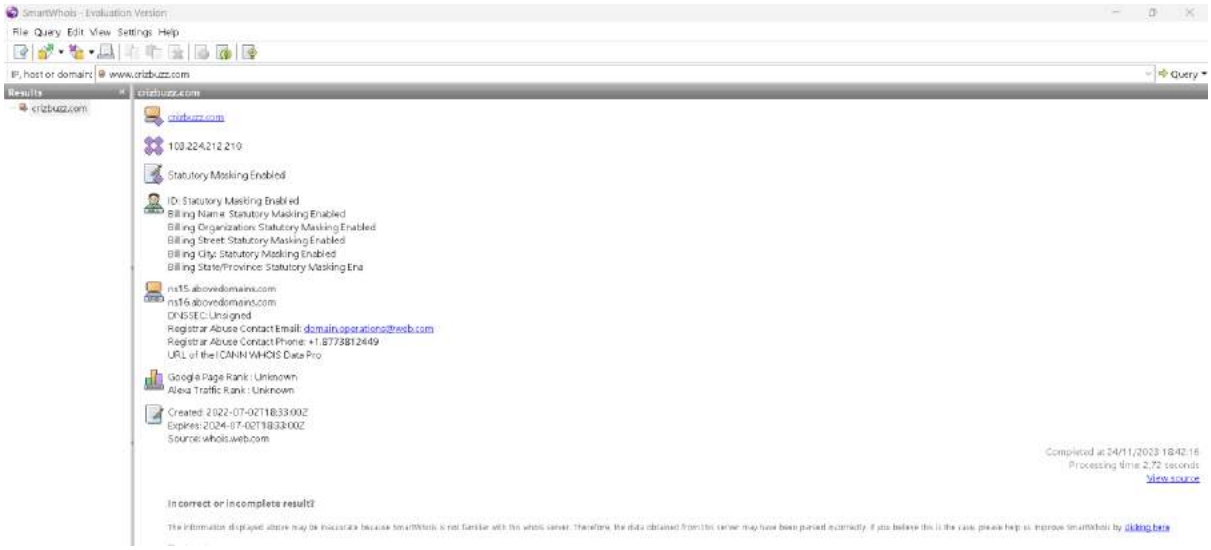


Smart whois

Setp1: Download and open the software

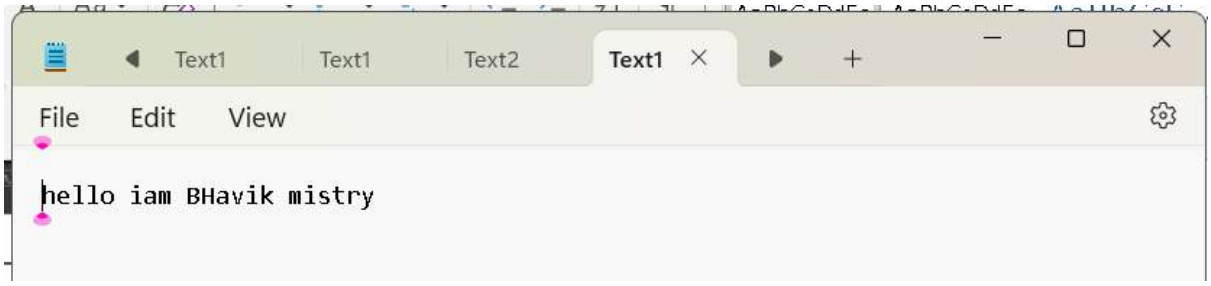


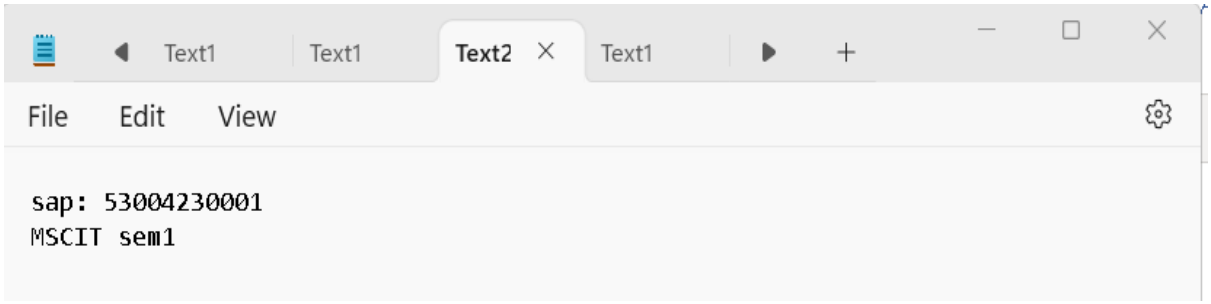
Step2: Entre any ip, or domain name



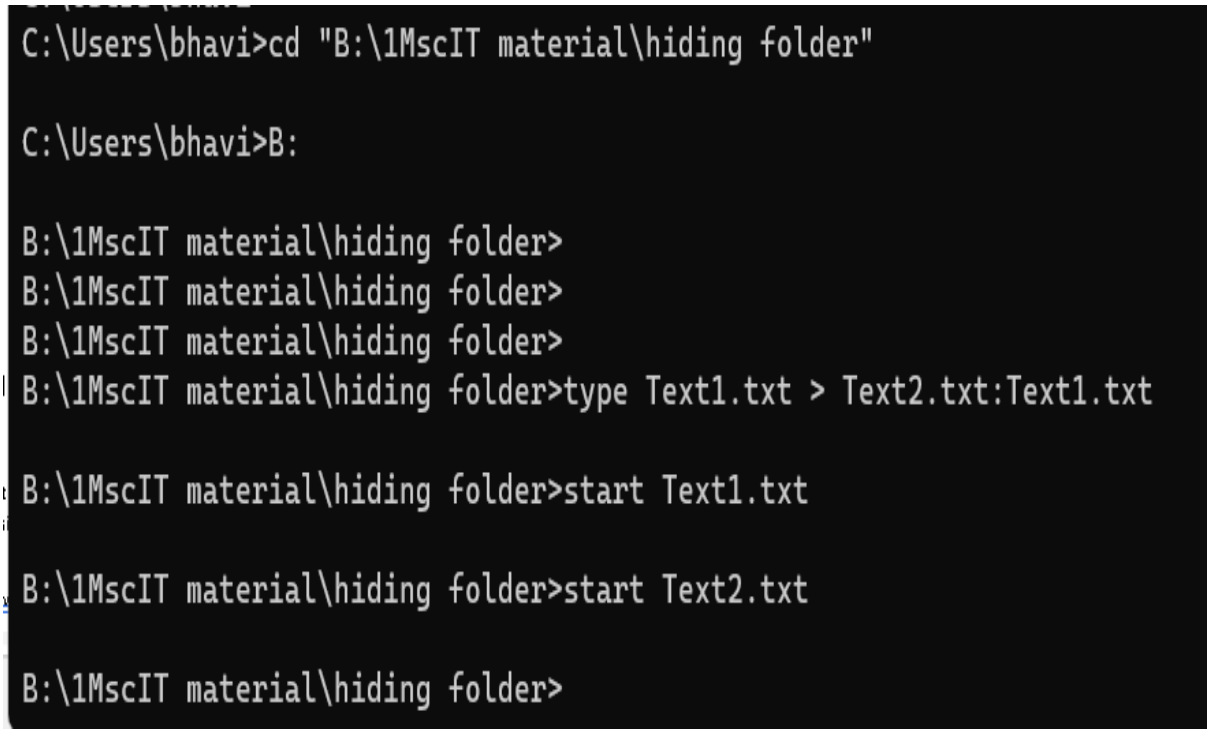
4) ADS Stream

Step 1 : For hiding one file in another file we are using this method. Create two notepad file and save them as .txt file.

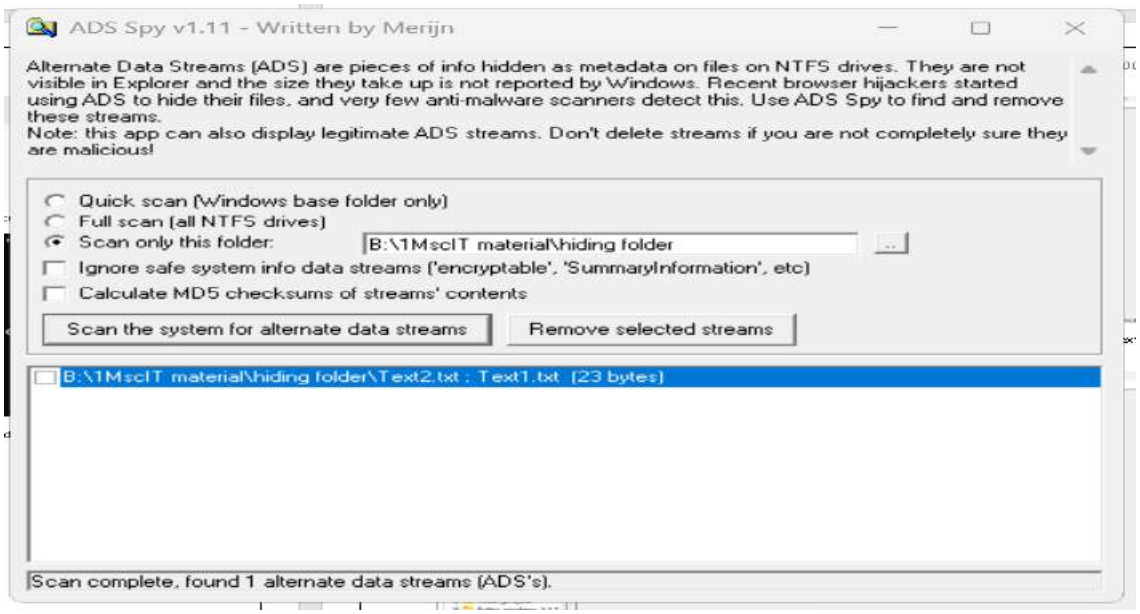




Step 2: Open command prompt on the same folder and type following commands.



Step 3: For checking we are using ADS Spy .We can see that one file is hide in another file and still its size is same.


ADS Spy v1.11 - Written by Merijn
Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!
Quick scan (Windows base folder only)
Full scan (all NTFS drives)
Scan only this folder:
B:\1MscIT material\hiding folder
Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
Calculate MD5 checksums of streams' contents
Scan the system for alternate data streams
Remove selected streams
B:\1MscIT material\hiding folder\Text2.txt : Text1.txt [23 bytes]
Scan complete, found 1 alternate data streams (ADS's).

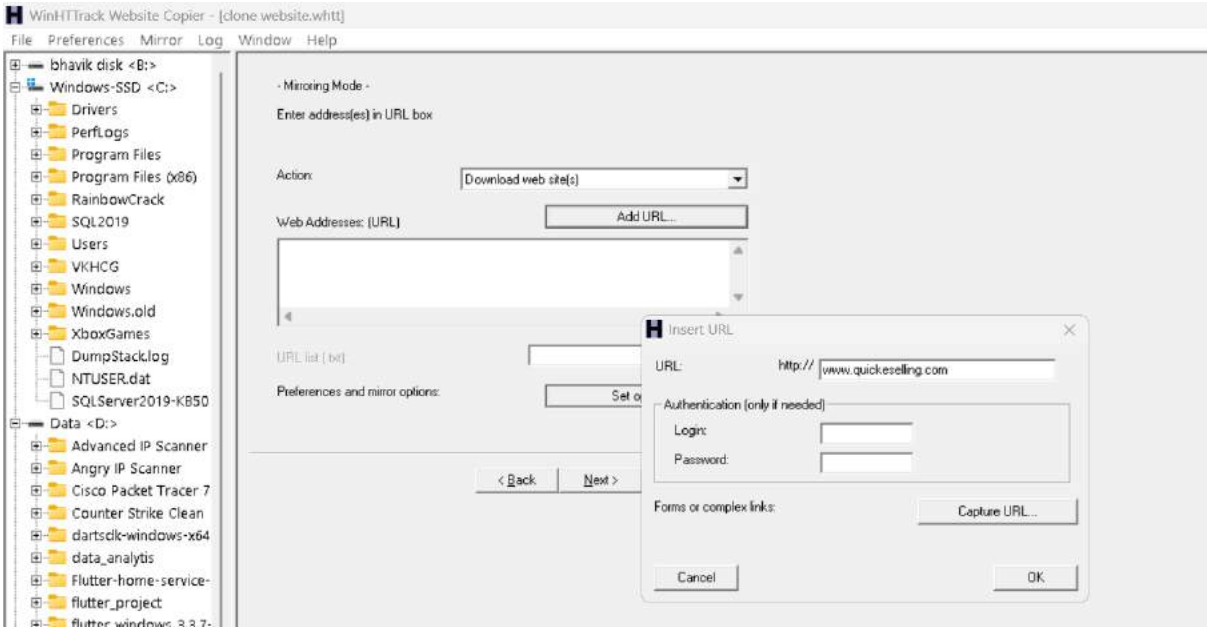
Practical 5

1) HTTrack Website Copier

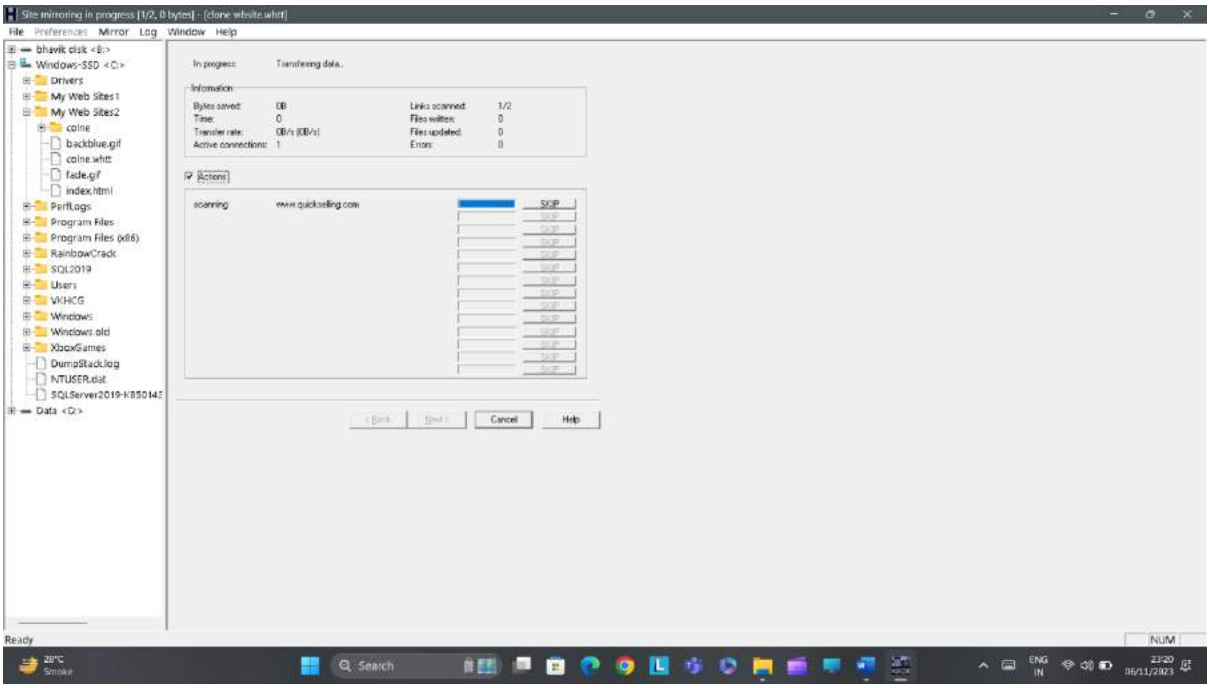
HTTrack is a free and easy-to-use offline browser utility. It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.

Step 1: -Install and open the HTTrack Website Copier software.-> click next

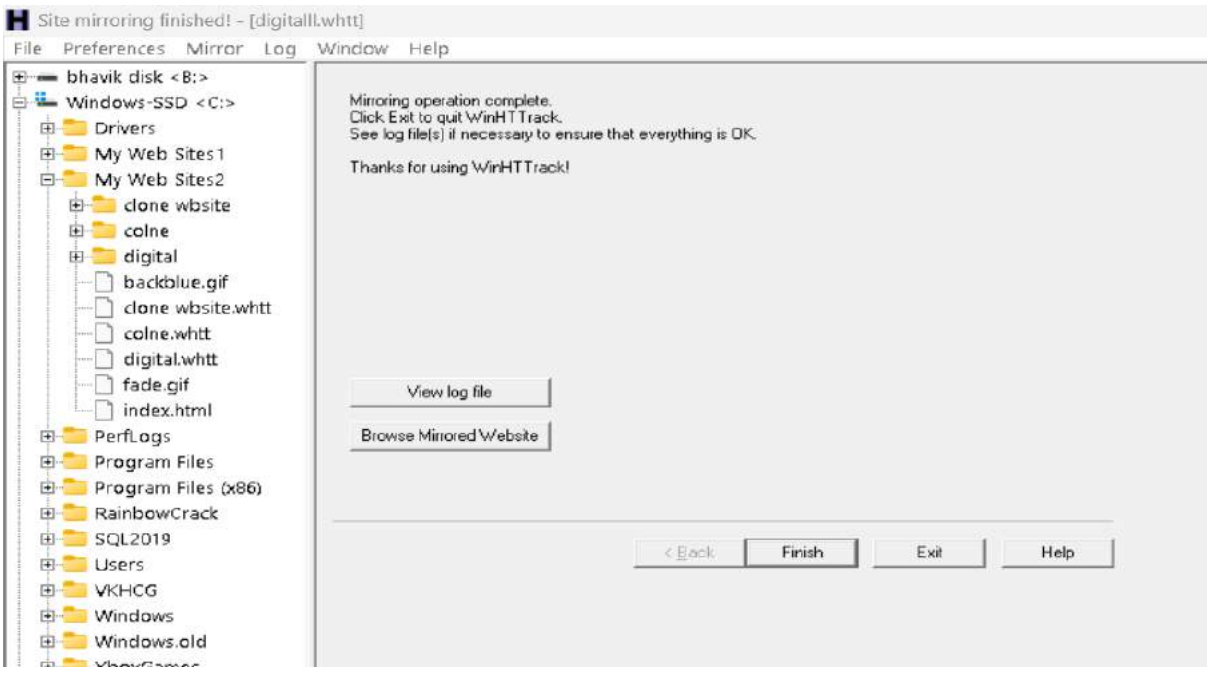
Step 2: - Enter the Project Name along with the path.->Now enter Web Address ->and click on next &then Finish.

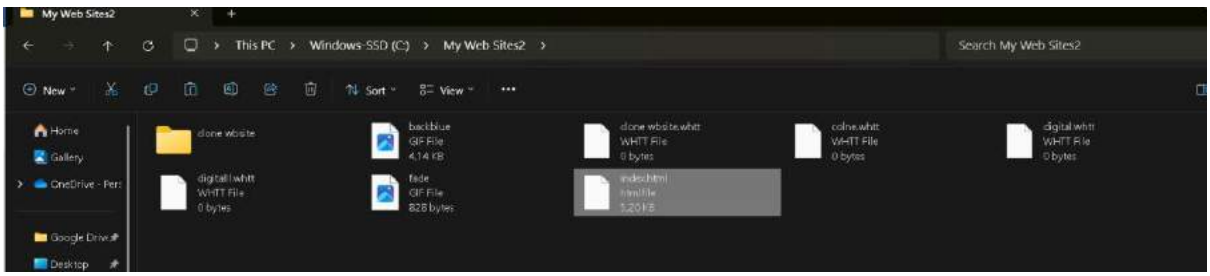


Step 3: -Now we can see that the website is downloading the data.



Step 4: -After completing it will look like this.





Practical 6

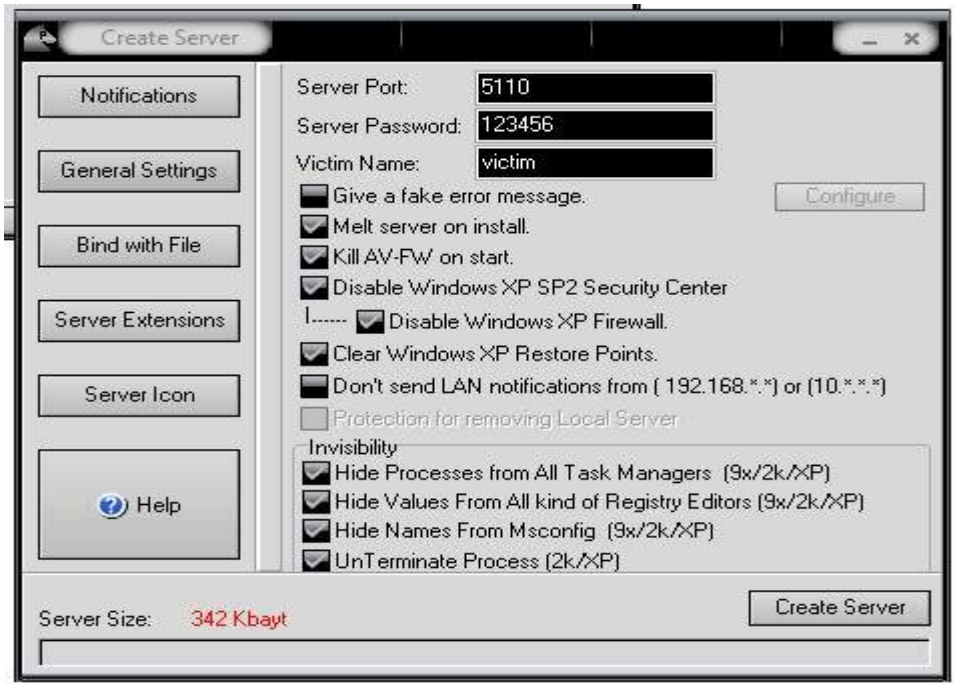
Trojan

1) Prorat

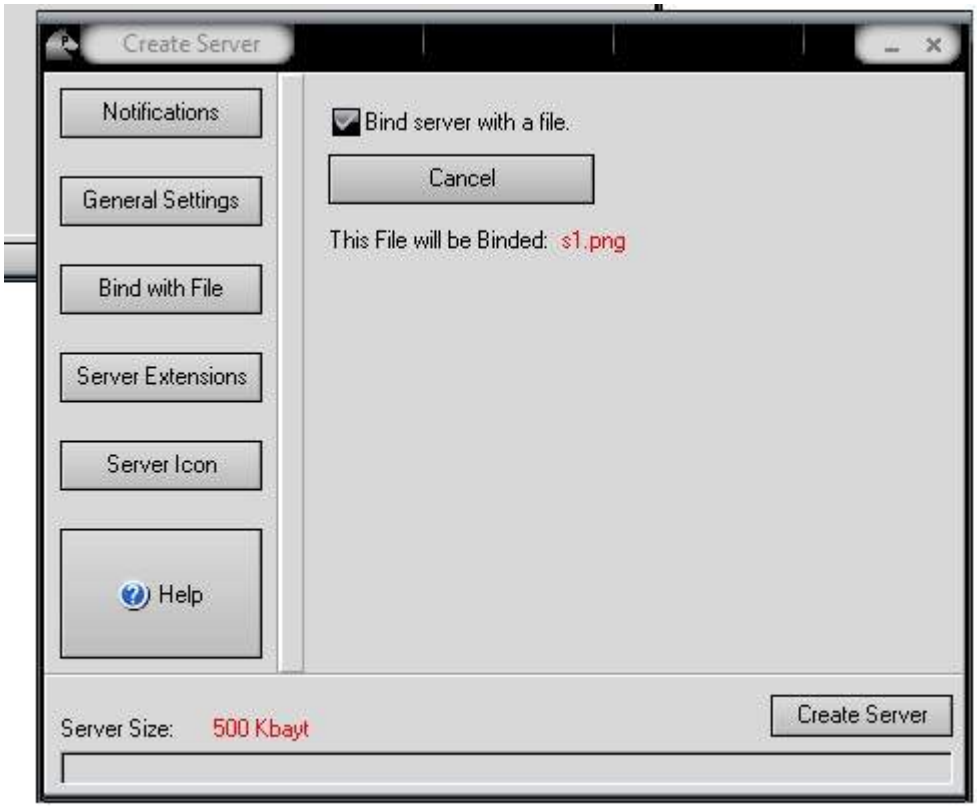
PRORAT is a family of backdoors that serves as a remote administration tool (RAT). Variants of this malware family first appeared in 2005. It opens random ports to establish connection with a remote attacker. Once a connection is established, the remote attacker can execute commands such as creating/opening/closing/deleting files, monitoring visited websites, and retrieving system information among others

Step1: - Open the Prorat tool. For oping the tool you have to disable all the anti-viruses software and windows defender.

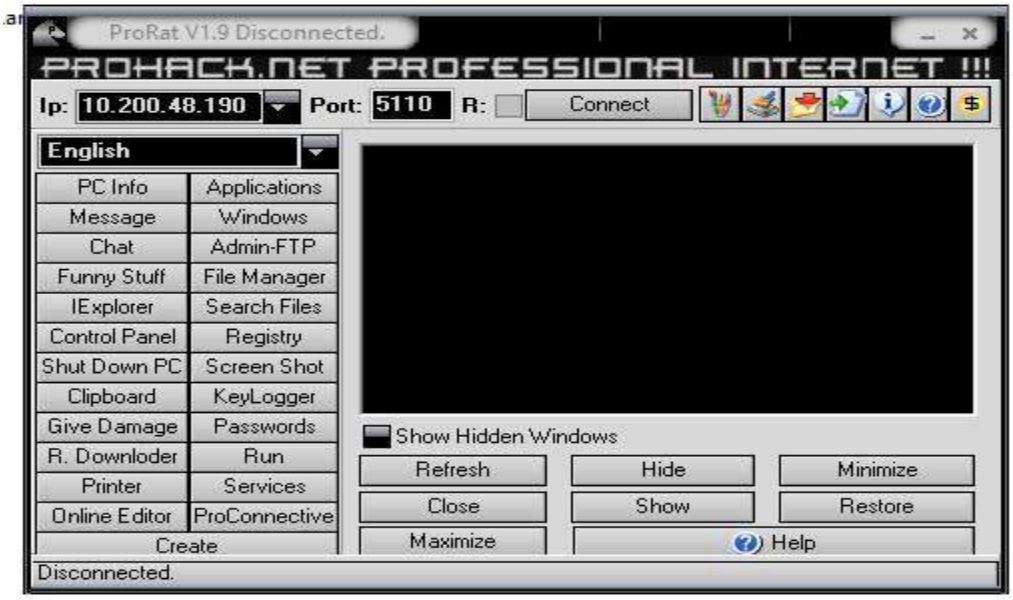
Step2: -Click on 'Create' to create the server.



Step3: - Bind server with a file you want.



Step4: - Enter the ip address of the victim machine -> click on connect

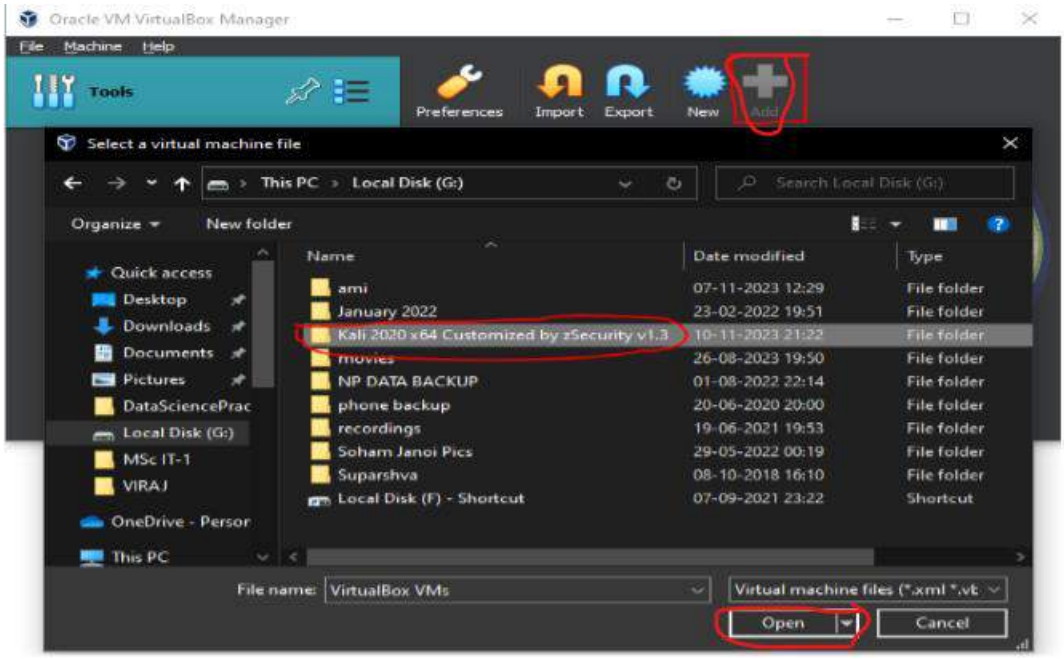


Practical

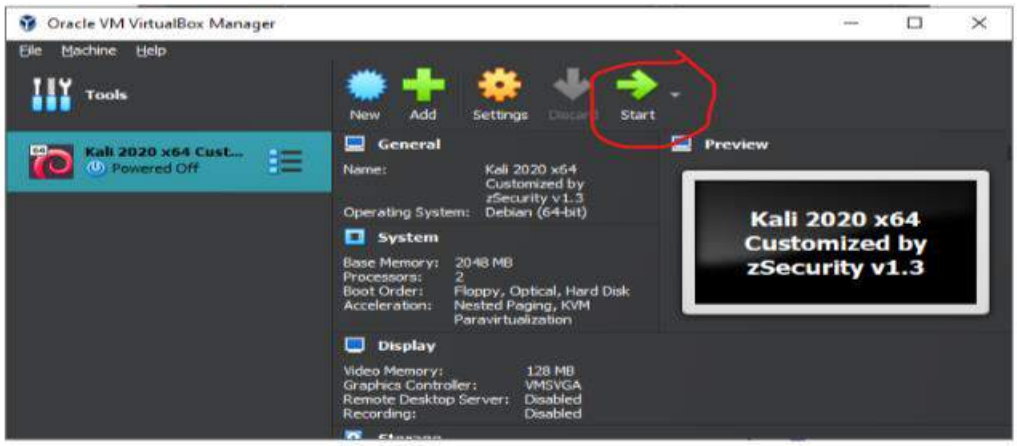
1) Virtual Machine and kali

Step 1:- Download and Install Virtual Box in your device.

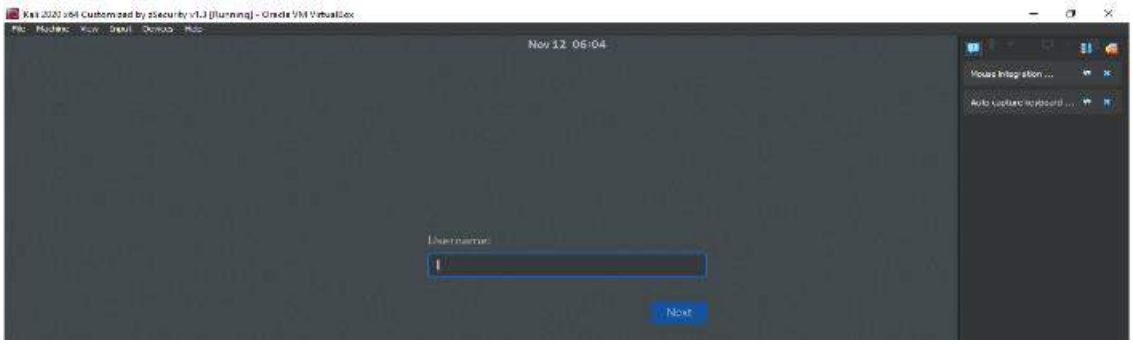
Step 2:- Now click on Add button and select the file as shown in the figure



Step 3:- Once you have added the file, click on the start button to start Kali



Step 4:- Now enter the username as ‘root’ and password as ‘toor’.

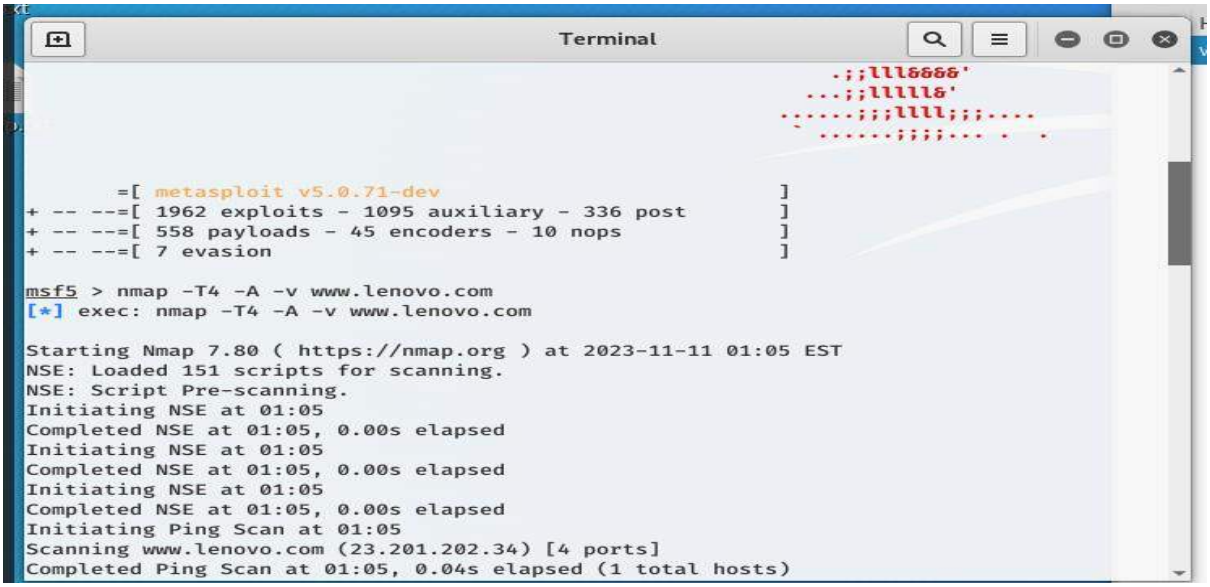


This is the window that will appear once you’ve entered the username and password.

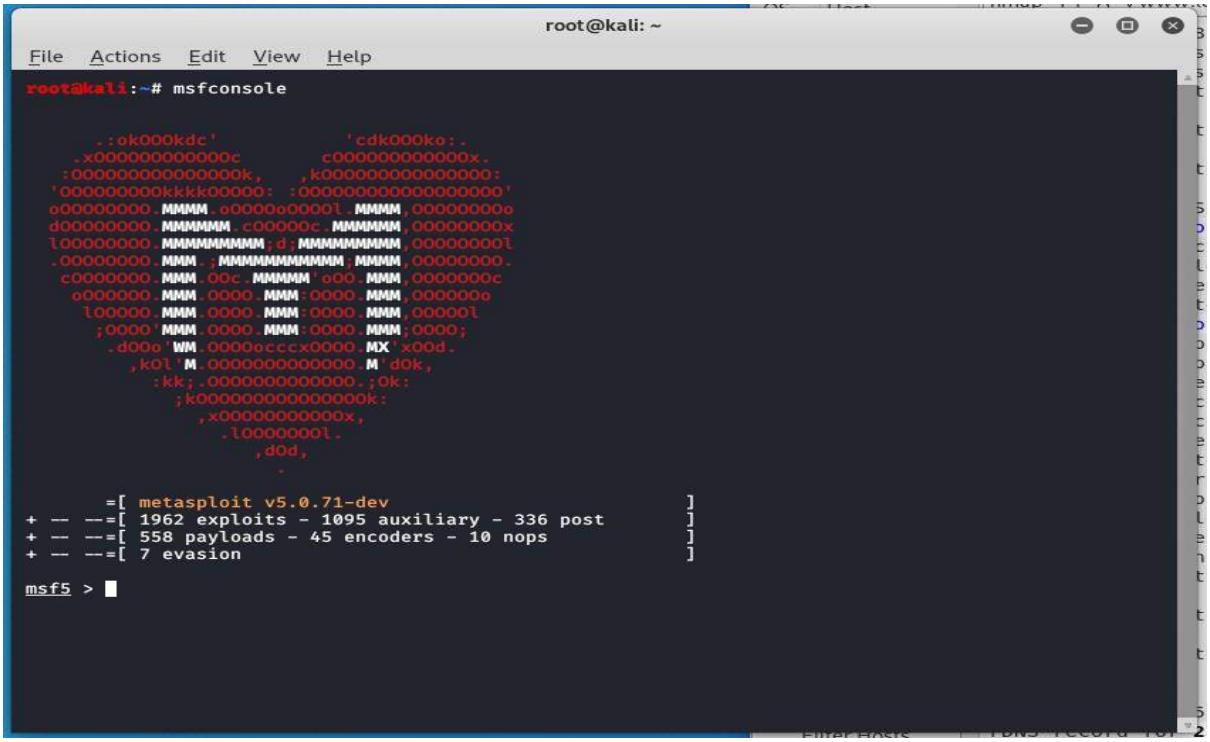
2)Metasploit

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.

Step1: Open kali Linux->open Metasploit tool -> then entre the command “nmap -T4 -A -v www.lenovo.com”



Step 2: Type the command “msfconsole” to launch a Metasploit framework

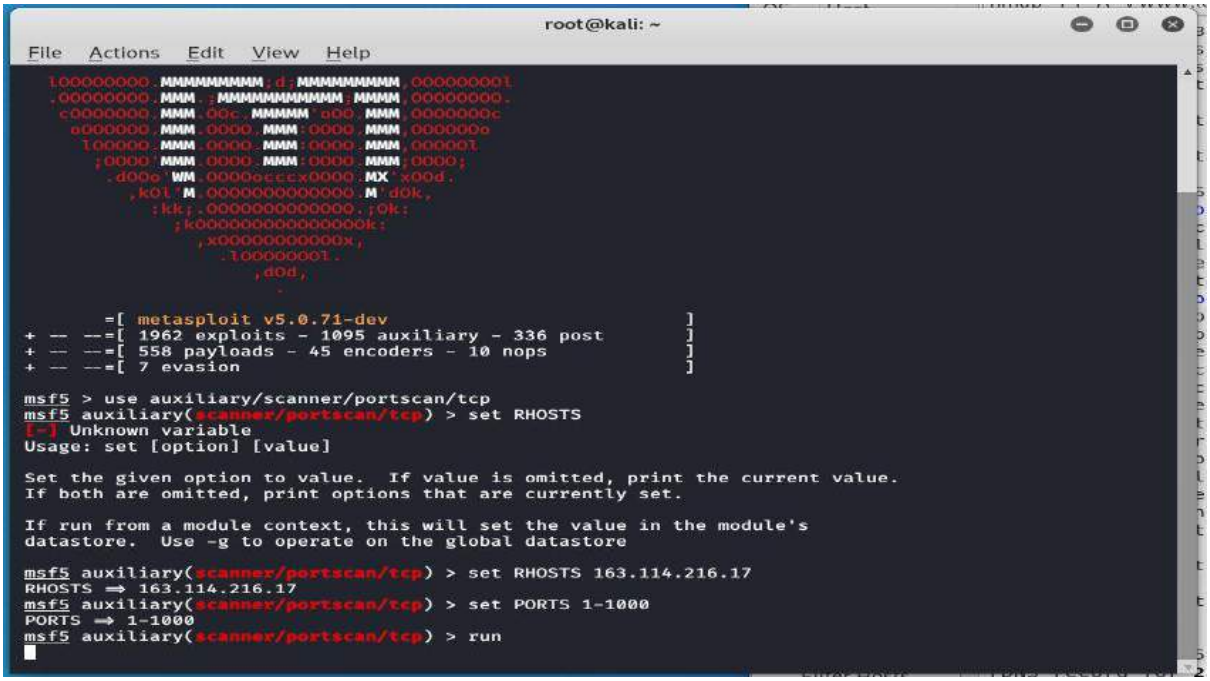


Step 3 : Enter the command “use auxiliary/scanner/portsscan/tcp-> Enter the command “show options”

Step 4 : Enter the following commands msf auxiliary(scanner/portscan/tcp) > set RHOST 163.114.216

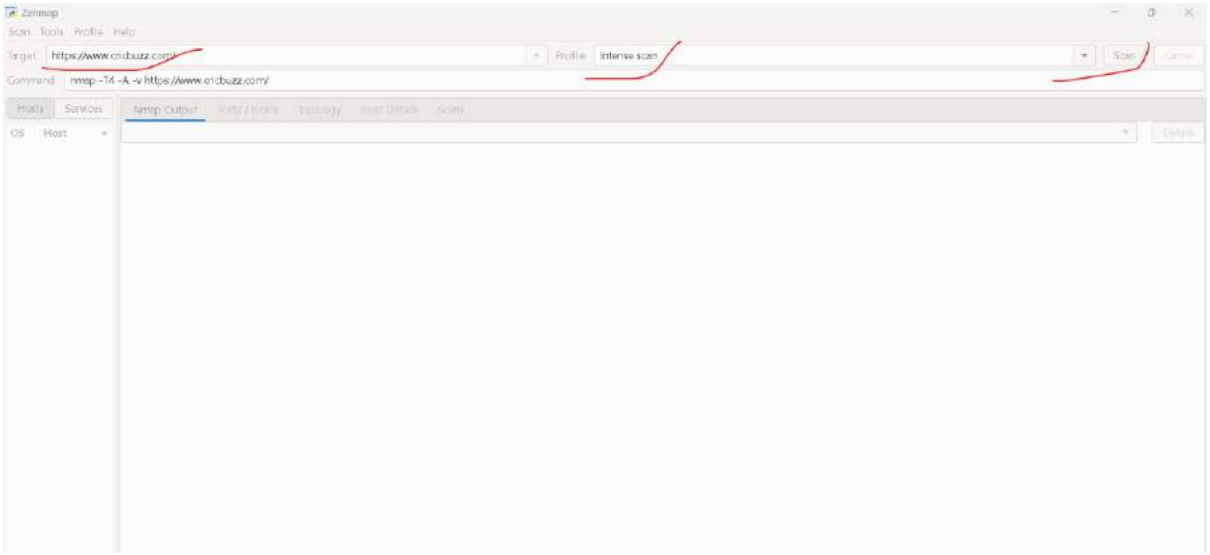
>Set PORTS 1-1000

> run



3) Nmap/Zenmap

Step1: Enter Domain name in the (Target) field and select (Intense scan) from the profile and click on Scan.
Eg: https://www.cricbuzz.com



Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -T4 -A -v www.cricbuzz.com

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-24 19:05 India Standard Time
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Initiating Ping Scan at 19:05
Scanning www.cricbuzz.com (23.46.9.19) [4 ports]
Completed Ping Scan at 19:05, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:05
Completed Parallel DNS resolution of 1 host. at 19:05, 0.01s elapsed
Initiating SYN Stealth Scan at 19:05
Scanning www.cricbuzz.com (23.46.9.19) [1000 ports]
Discovered open port 80/tcp on 23.46.9.19
Discovered open port 443/tcp on 23.46.9.19
Completed SYN Stealth Scan at 19:05, 10.88s elapsed (1000 total ports)
Initiating Service scan at 19:05
Scanning 2 services on www.cricbuzz.com (23.46.9.19)
Completed Service scan at 19:06, 12.18s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.cricbuzz.com (23.46.9.19)
Retrying OS detection (try #2) against www.cricbuzz.com (23.46.9.19)
Initiating Traceroute at 19:06
Completed Traceroute at 19:06, 3.06s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 19:06
Completed Parallel DNS resolution of 4 hosts. at 19:06, 0.01s elapsed
NSE: Script scanning 23.46.9.19.
Initiating NSE at 19:06
Completed NSE at 19:06, 5.26s elapsed
Initiating NSE at 19:06
Completed NSE at 19:06, 0.23s elapsed
Initiating NSE at 19:06
Completed NSE at 19:06, 0.00s elapsed
Nmap scan report for www.cricbuzz.com (23.46.9.19)
Host is up (0.013s latency).
Other addresses for www.cricbuzz.com (not scanned): 23.46.9.98 23.46.9.105
rDNS record for 23.46.9.19: a23-46-9-19.deploy.static.akamaitechnologies.com
```

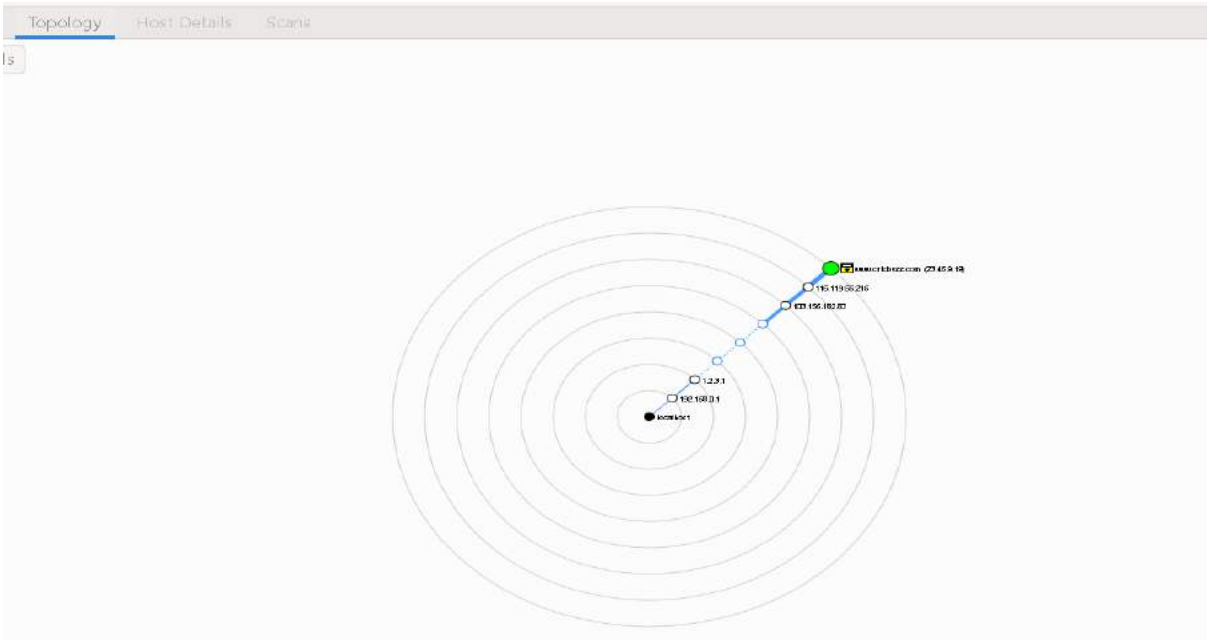
```
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-06-17T00:00:00
| Not valid after:  2024-06-19T23:59:59
| MD5:   24b6:a0d9:7d24:452d:f042:9455:33f9:a3f8
|_SHA-1: 55ad:80f4:8629:1f40:1213:f800:87fa:568a:1a7d:6778
|_http-title: Live Cricket Score, Schedule, Latest News, Stats &amp;amp; Videos ...
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Device type: general purpose
Running (JUST GUESSING): Linux 5.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:5.0
Aggressive OS guesses: Linux 5.0 (87%), Linux 5.0 - 5.4 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 11.110 days (since Mon Nov 13 16:28:36 2023)
Network Distance: 8 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 53/tcp)
HOP RTT       ADDRESS
1   14.00 ms 192.168.0.1
2   16.00 ms 1.2.3.1
3   ...5
6   27.00 ms 103.156.182.83
7   31.00 ms 116.119.55.215
8   35.00 ms a23-46-9-19.deploy.static.akamaitechnologies.com (23.46.9.19)

NSE: Script Post-scanning.
Initiating NSE at 19:06
Completed NSE at 19:06, 0.00s elapsed
Initiating NSE at 19:06
Completed NSE at 19:06, 0.00s elapsed
Initiating NSE at 19:06
Completed NSE at 19:06, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.19 seconds
           Raw packets sent: 2076 (93.660KB) | Rcvd: 61 (3.920KB)
```

Ports/Hosts

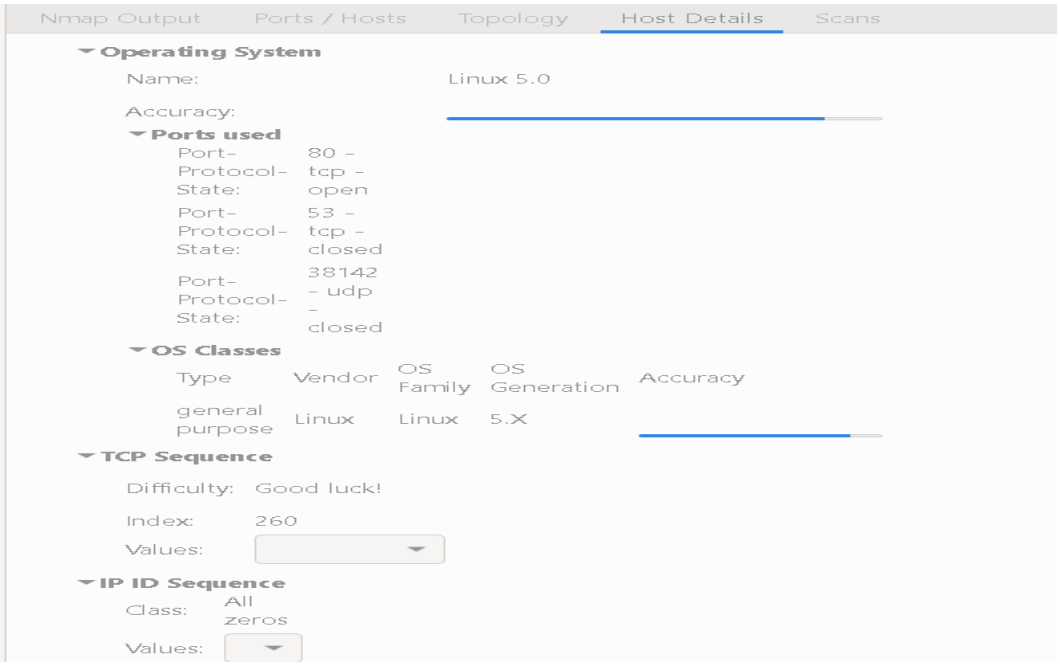
Nmap Output Ports / Hosts Topology Host Details Scans

Port	Protocol	State	Service	Version
53	tcp	closed	domain	
80	tcp	open	http	AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
443	tcp	open	http	AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)

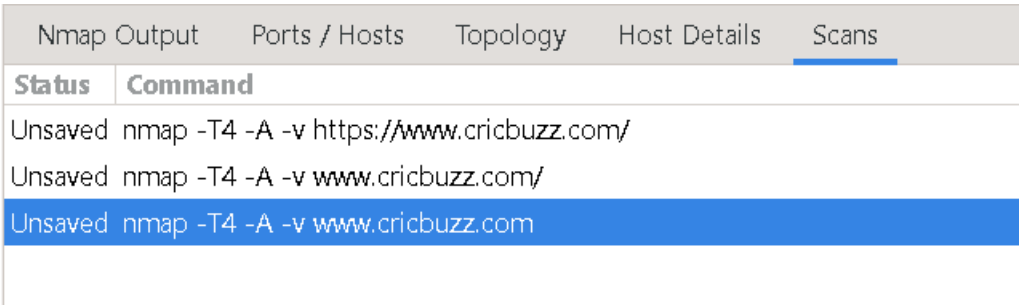
Topology



Host Details



Scans



CommandInfo

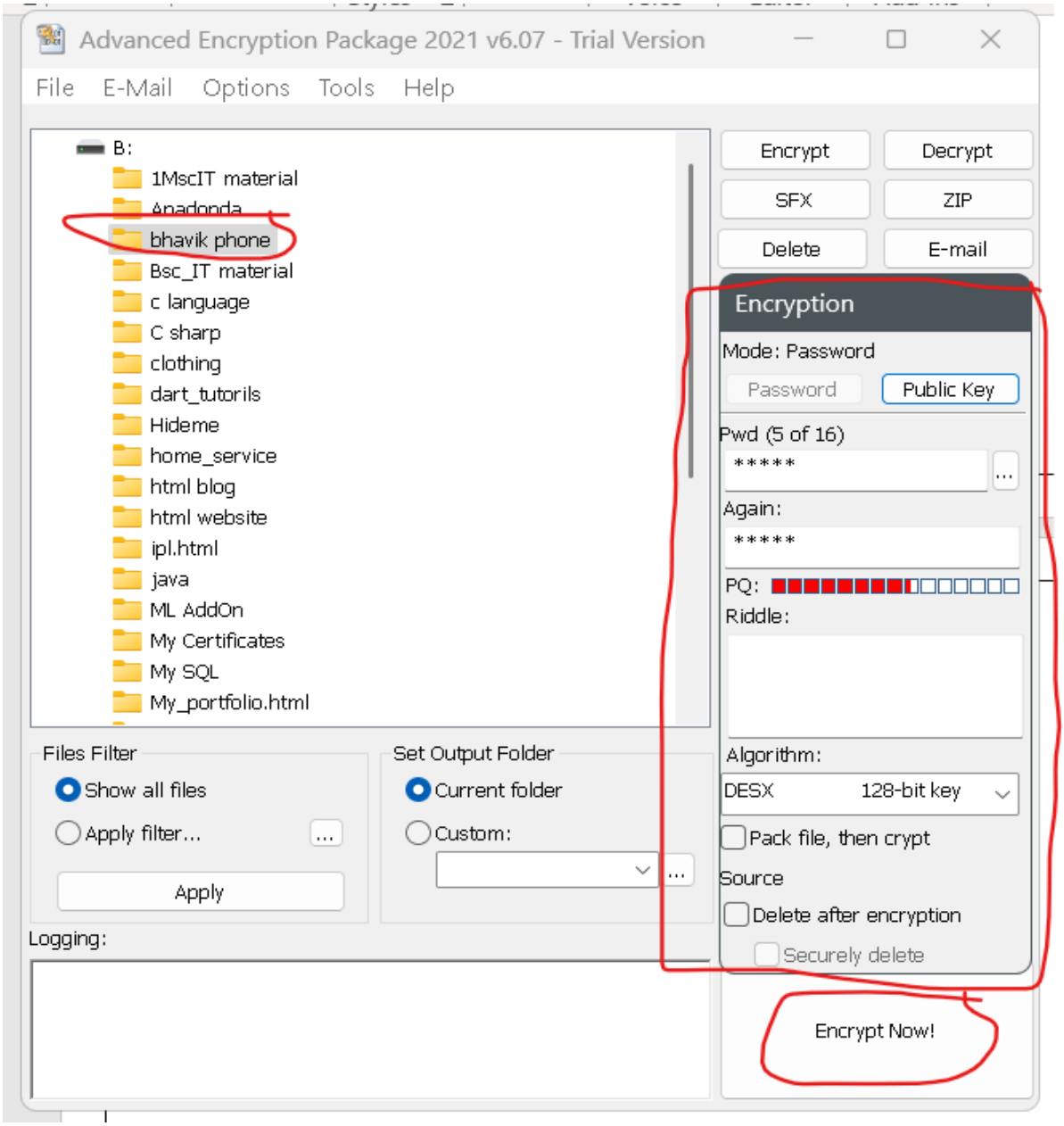
Practical

Cryptography

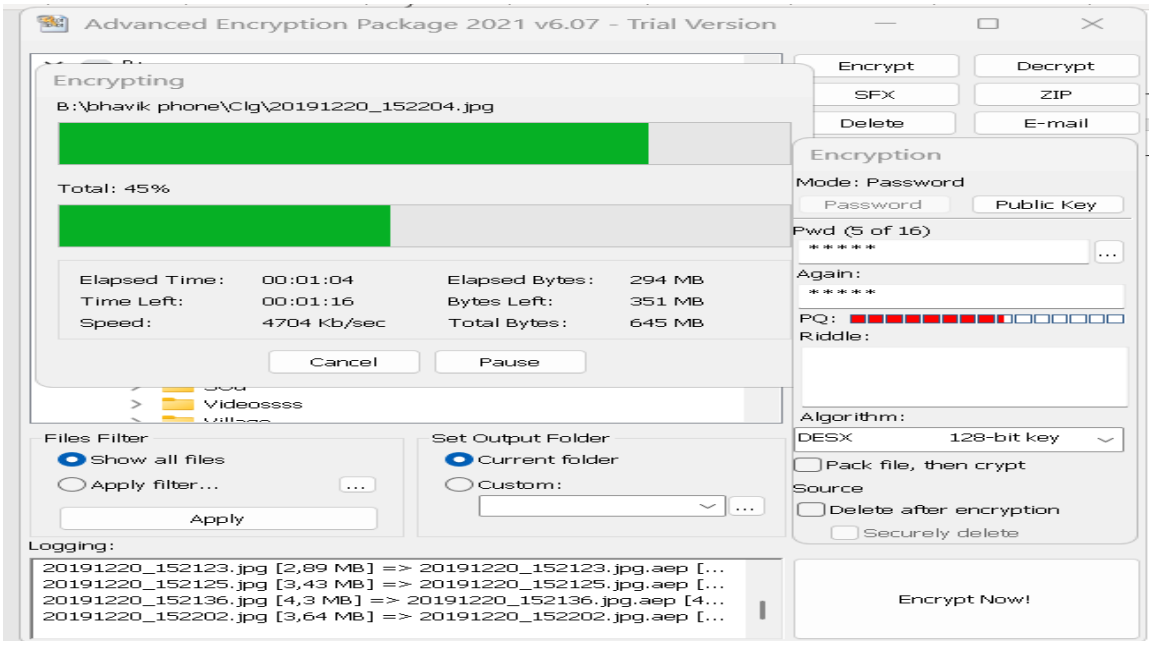
1)Advance Encryption Package

Advanced Encryption Package: AEP is an award-winning feature-rich encryption software program that encrypts, decrypts, shreds, and makes zip files or sfx.exe files. It allows users to carry out secure file transfers, batch folder encryptions, send encrypted emails, as well as carry out encrypted backups in the cloud. The software works well with Windows 10/11.

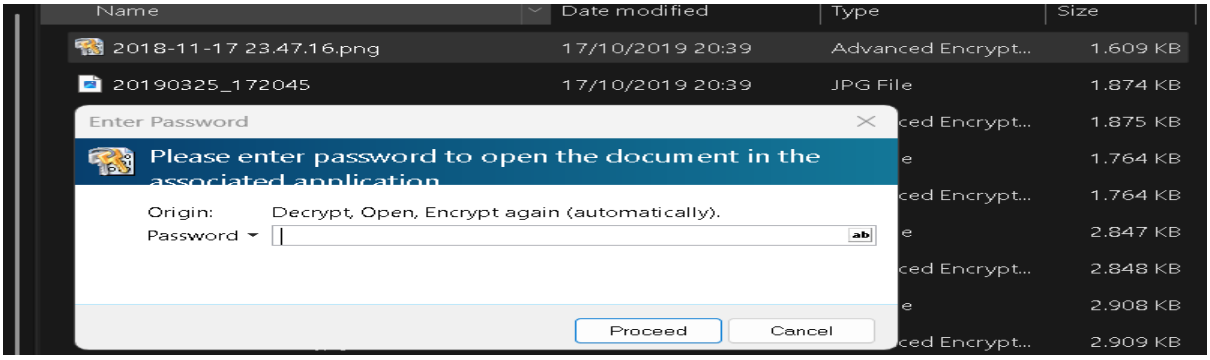
Step 1: Open AEP Software-> Select the file for Encryption-> Enter the password , confirm it and click on Encrypt Now!



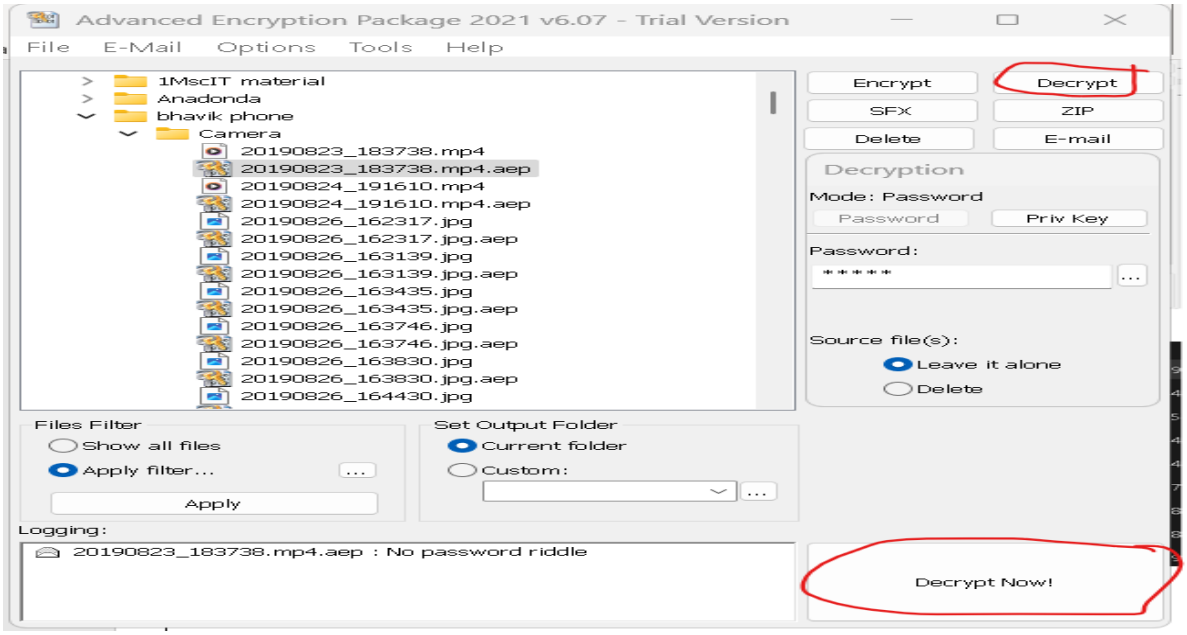
Step 2: As we can below see an encrypted file has been created



Step 3: Now enter the password for opening the file.



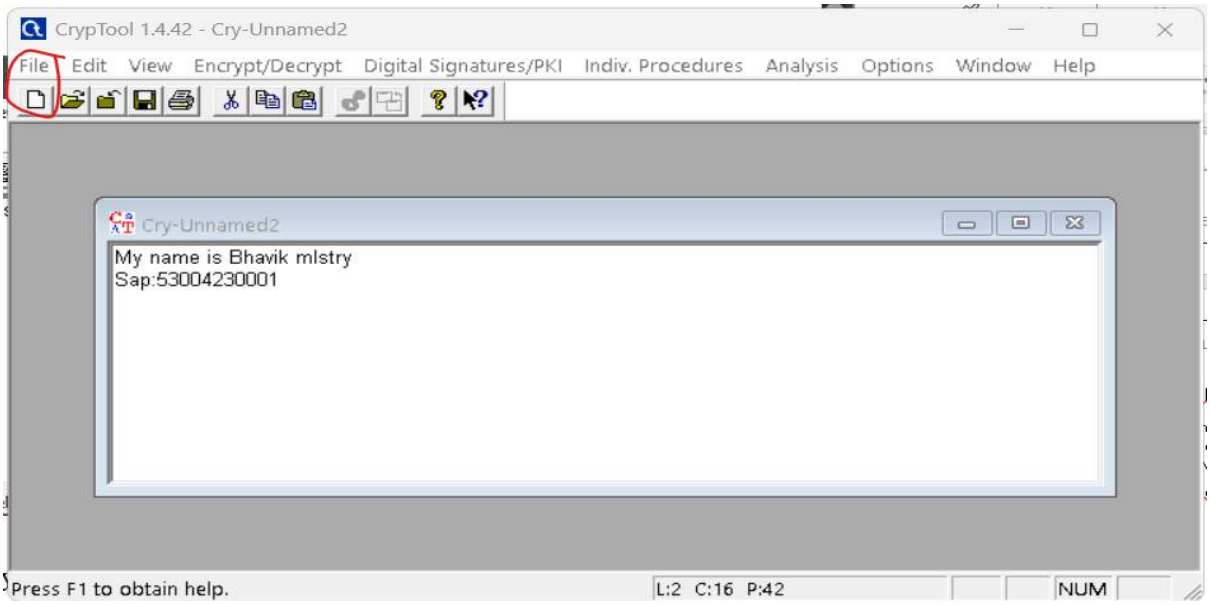
Step 4 : Follow the same steps for Decryption.



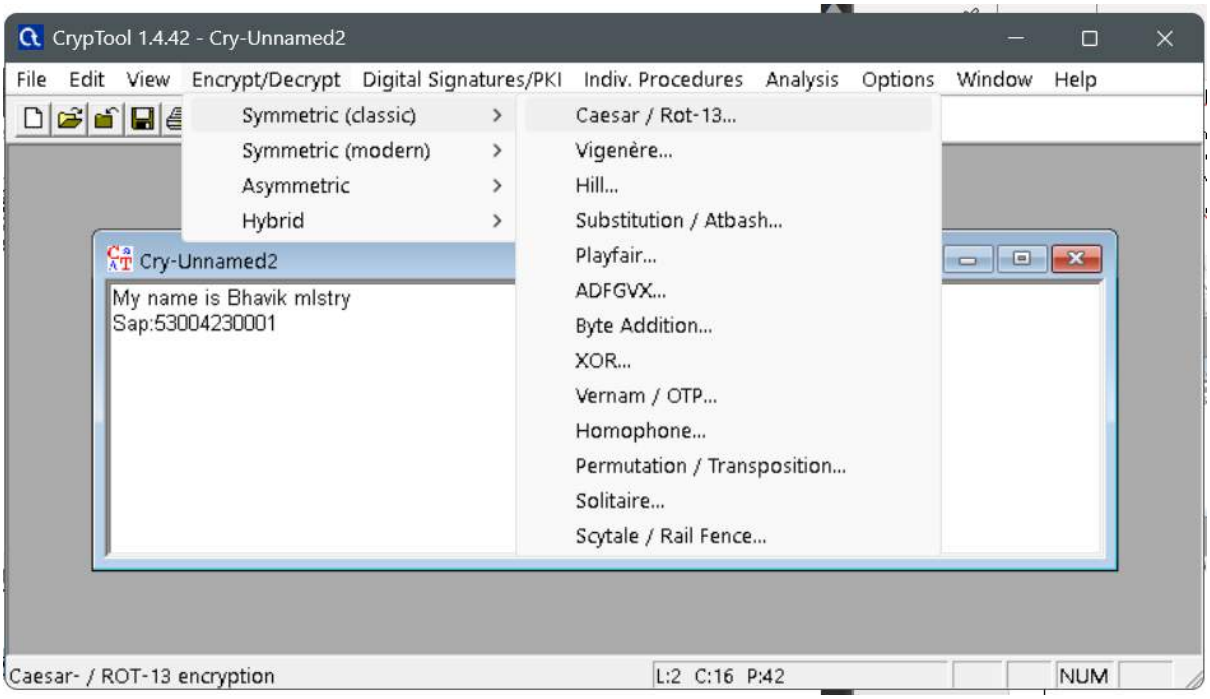
2) CrypTool

CrypTool is an open-source project that is a free e-learning software for illustrating cryptographic and cryptanalytic concepts. According to "Hakin9", CrypTool is worldwide the most widespread e-learning software in the field of cryptology.

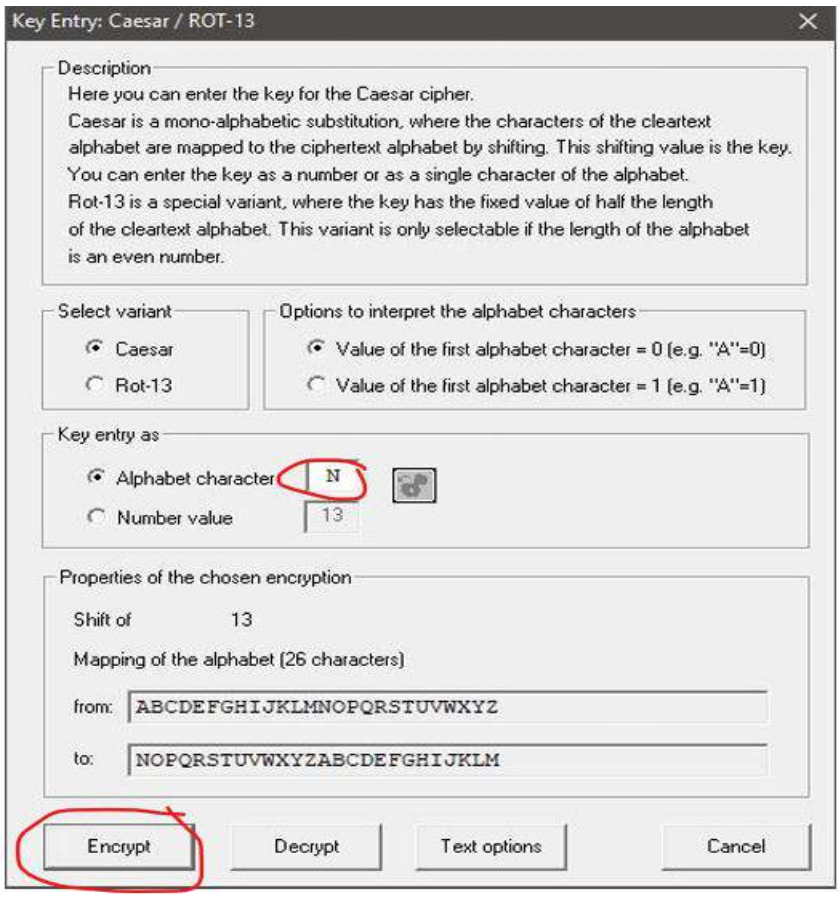
Step 1: Start CrypTool and go to File-> New to create a new empty file. Enter some Text in this file.->save it.



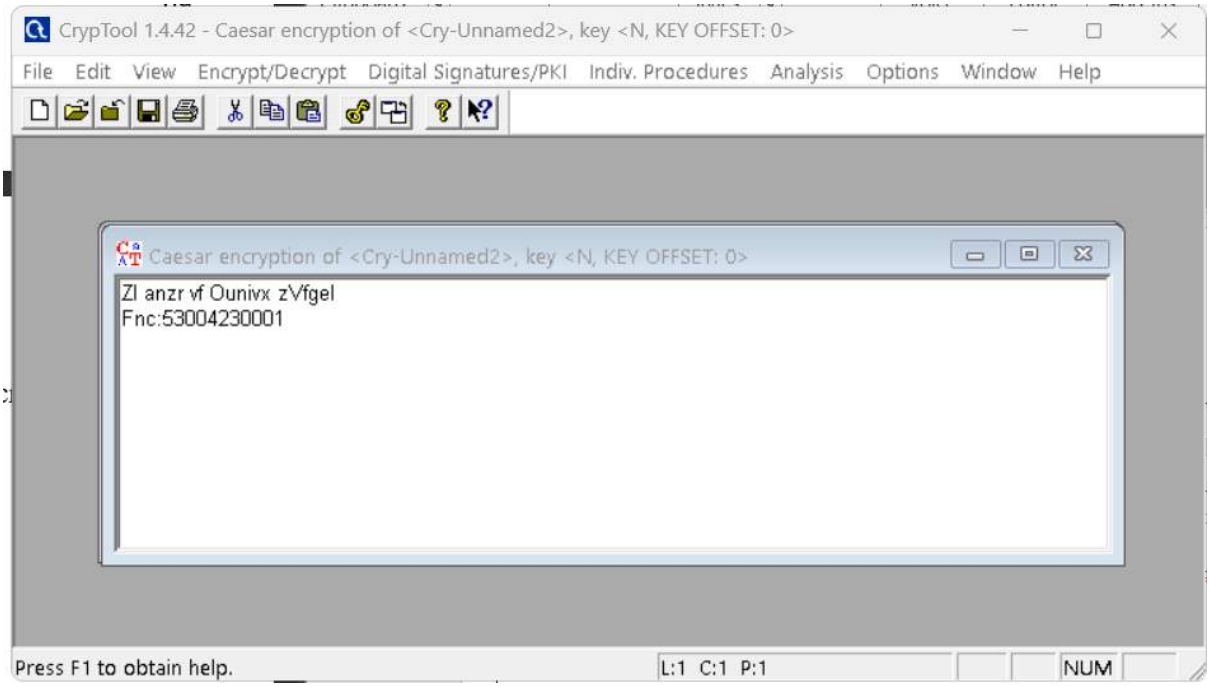
Step 2: Goto Encrypt/Decrypt->Symmetric(classic)-> Caesar/Rot-13.



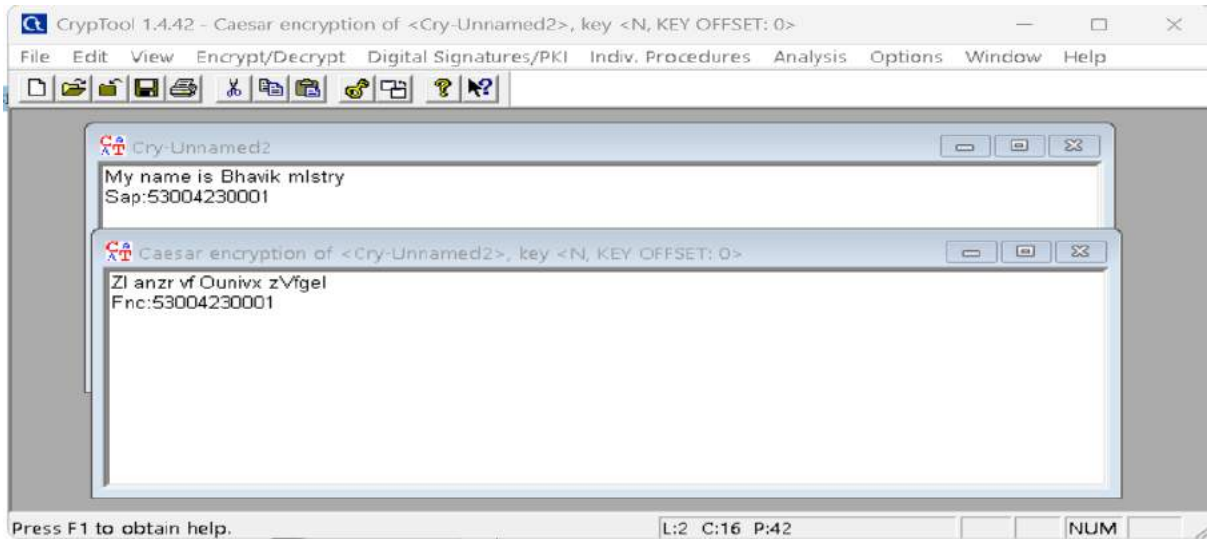
Step 3: Enter the alphabet character to be replaced. Entering N here will replace A by N, B by O and so on. Meaning a shift of 13 character along the alphabet. Click on Encrypt.



Step 4 : Given below is the Encrypted Text.



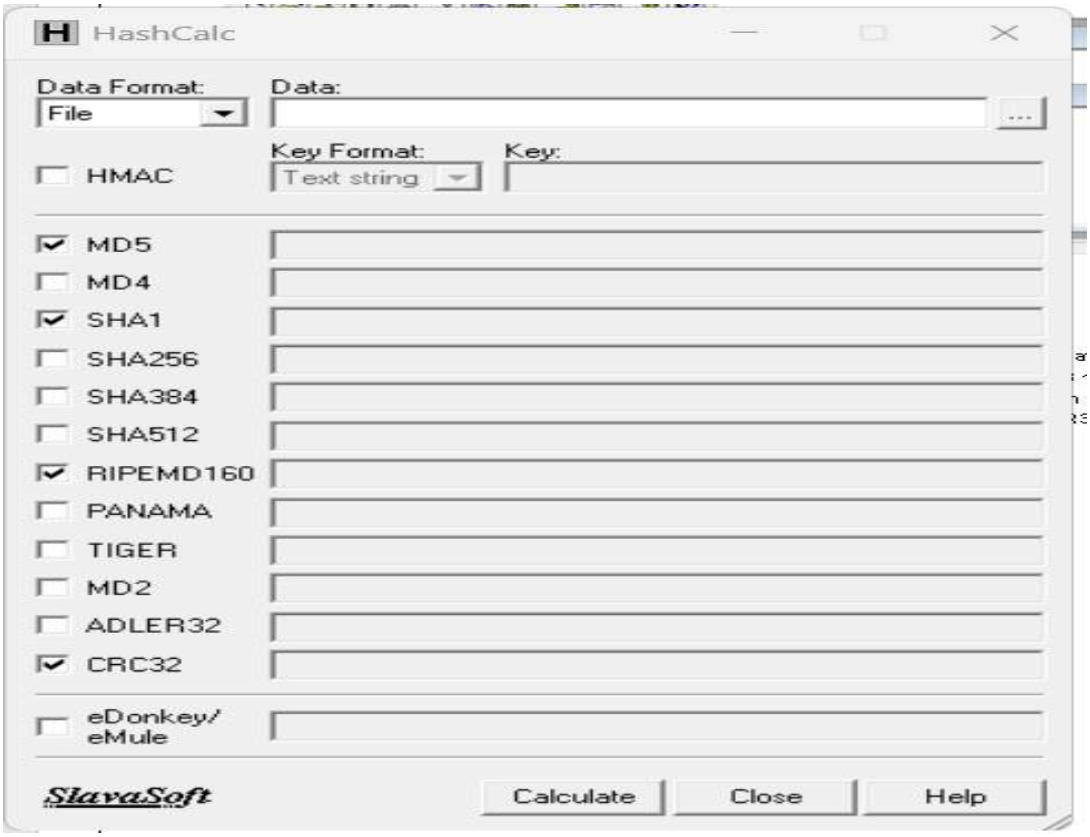
Step 5 : Performing the same steps and clicking on Decrypt, allows us to Decrypt the Encrypted Text.



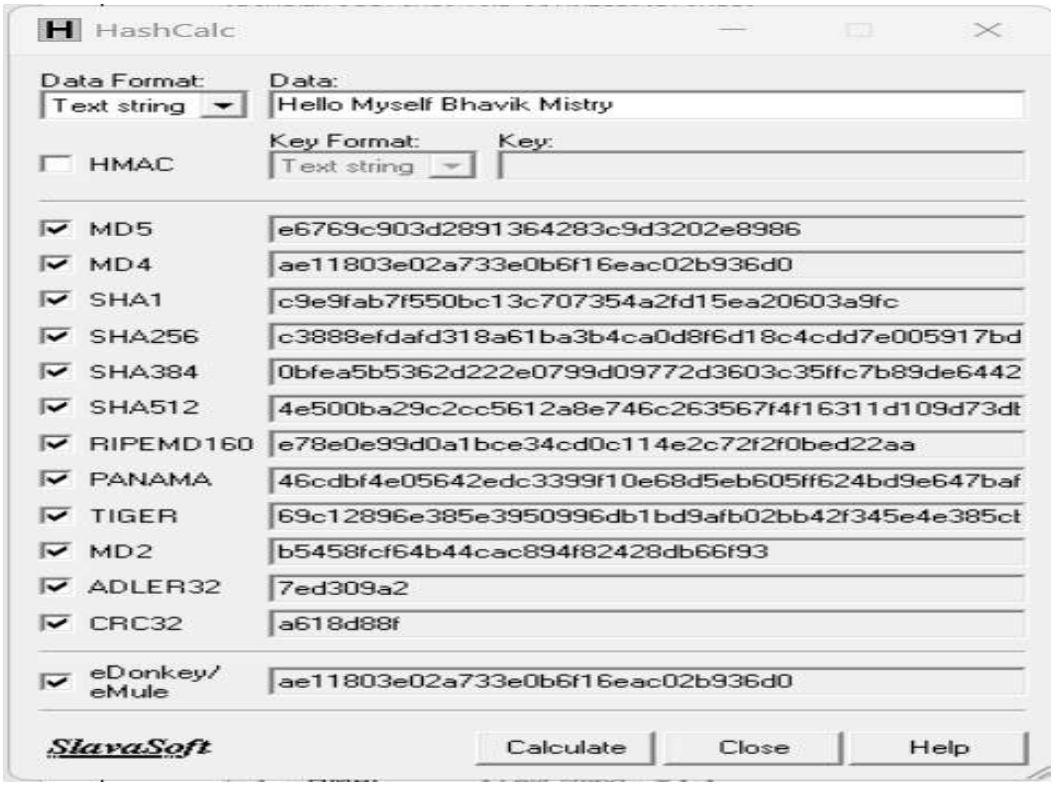
3) HashCalc

HashCalc is a free-of-charge desktop utility that allows you to easily calculate hashes, checksums, and HMAC values for texts, hex strings, and other file types. It presents the 13 most popular hash and checksum algorithms for computation that you can freely choose from. This includes MD2, MD4, MD5, SHA-1, SHA-2 (256, 384, 512), RIPEMD-160, PANAMA, TIGER, ADLER32, and CRC32

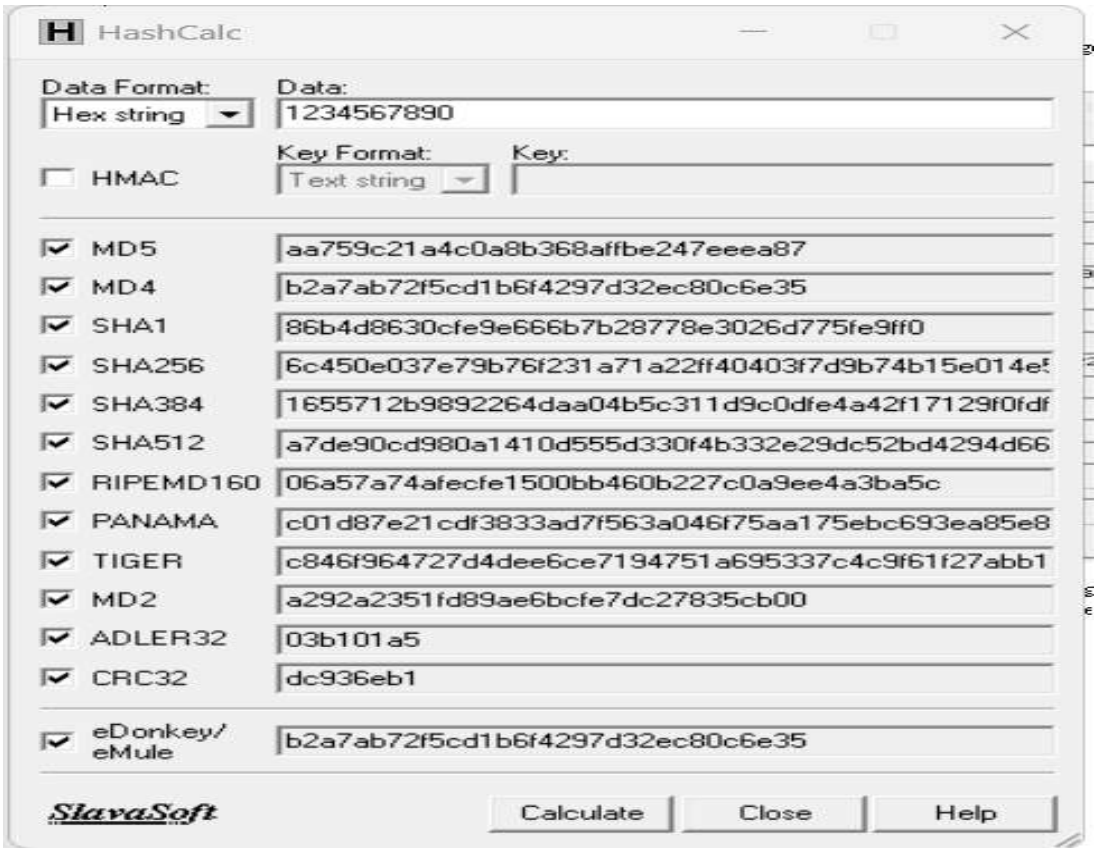
Step 1: Install and Open HashCalc.



Step 2: In Data Format, browse and select Text string. Choose the Hash algorithms you want to use to generate hashes and click on Calculate to generate the respective hashes.



Step 3 : In Data Format, browse and select Hex string. Choose the Hash algorithms you want to use to generate hashes and click on Calculate to generate the respective hashes.



Step 4: In Data Format, browse and select the file using the file browser. Choose the Hash algorithms you want to use to generate hashes and click on Calculate to generate the respective hashes.

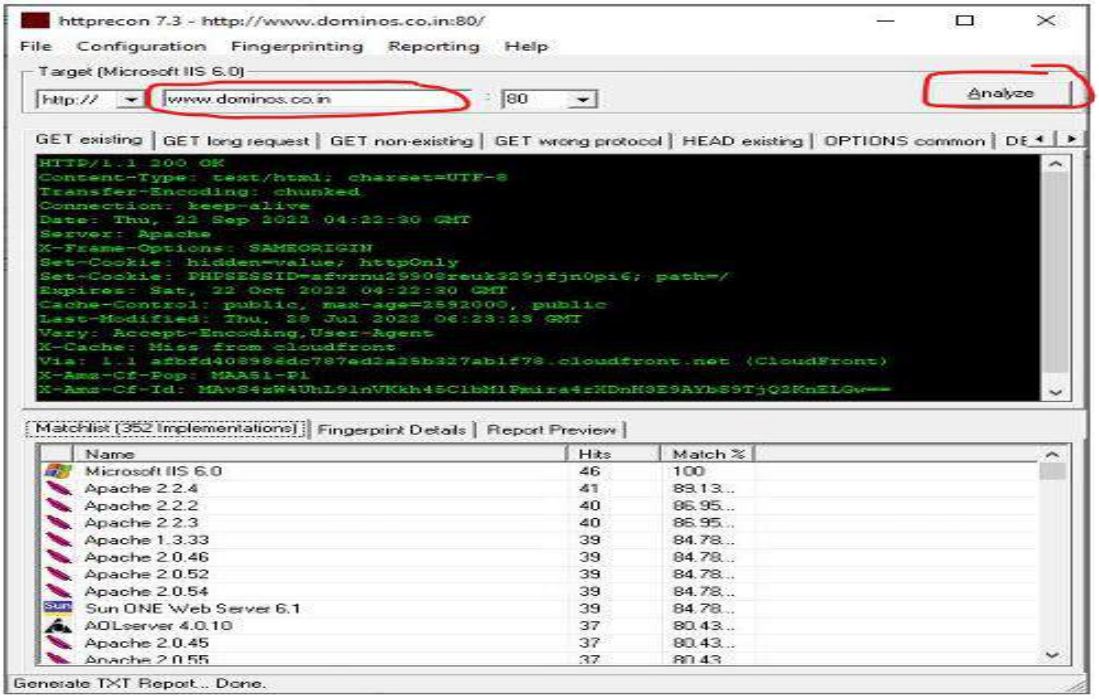
Practical

Webserver vulnerability/attack

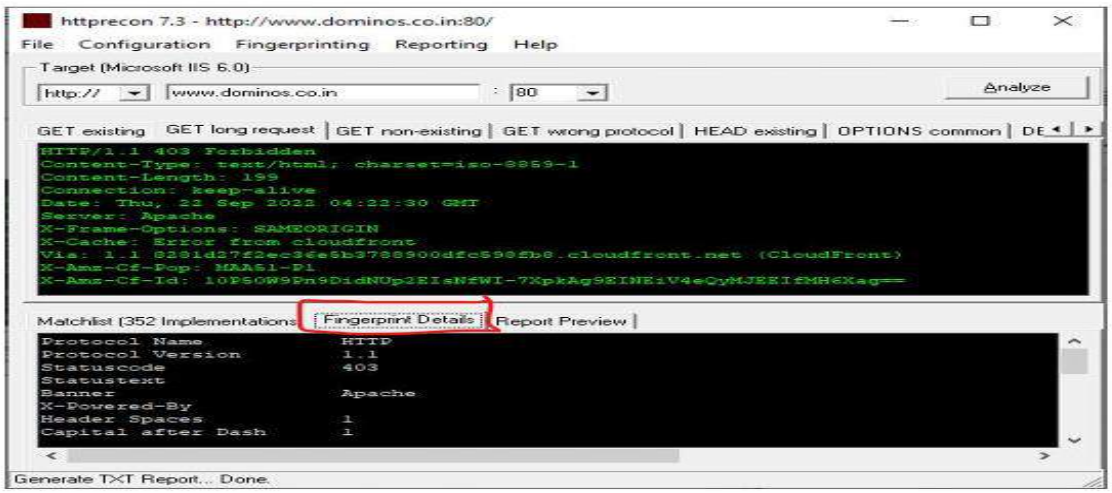
1) Httprecon

Httprecon is a Windows software, designed for highly accurate identification of some http implementations. It can be defined as one of the best tools for fingerprinting the web server, becoming the successor to the equally famous and now outdated httPrint . This tool simplifies and automates the fingerprinting process. Traditional approaches such as banner grabbing, enumeration of the status code and analysis of header orders are use.

Step 1: Open Httprecon software -> Enter URL or IP address and cllick on Analyze.



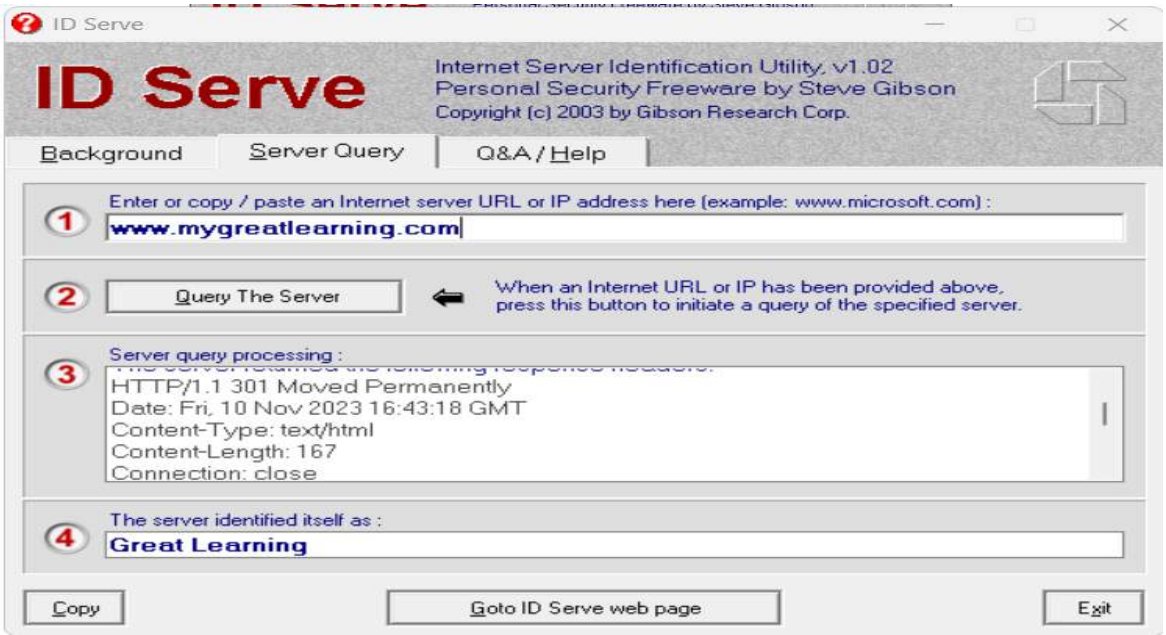
Step 2: Now Click on Fingerprint Details to get the Protocol name, Protocol version, etc.

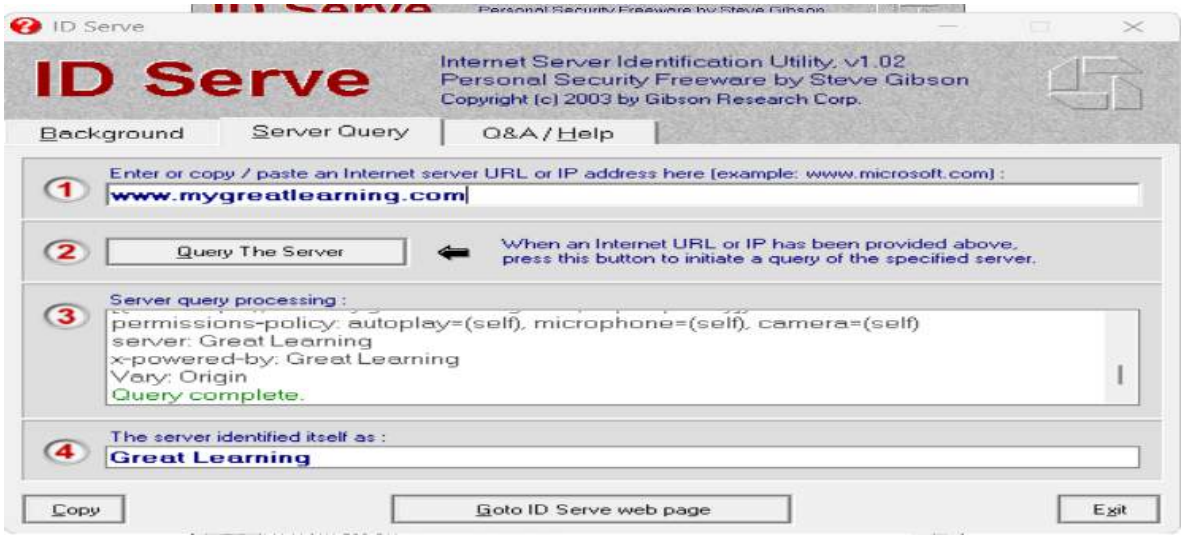


3) ID Serve

A. ID Serve : ID Serve is a freeware by Steve Gibson is essentially a security investigation tool. Its main function is to examine the workings of the Web server. This program also gives information in the operating platform of the server. The probe can also reveal useful information on other information such as cookie values and reverse DNS information.

Steps: Open ID Serve software -> Enter URL or IP address and click on Query the Server.




ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A / Help
Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :
www.mygreatlearning.com
Query The Server
When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.
Server query processing :
permissions-policy: autoplay=(self), microphone=(self), camera=(self)
server: Great Learning
x-powered-by: Great Learning
Vary: Origin
Query complete.
The server identified itself as :
Great Learning
Copy
Goto ID Serve web page
Exit

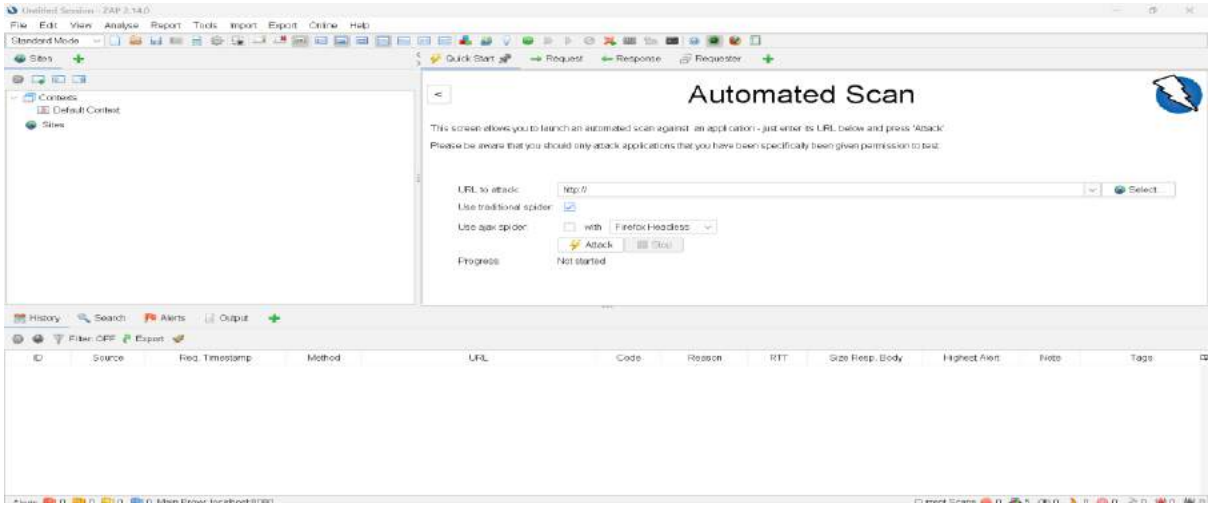
Practical

Session Hijacking

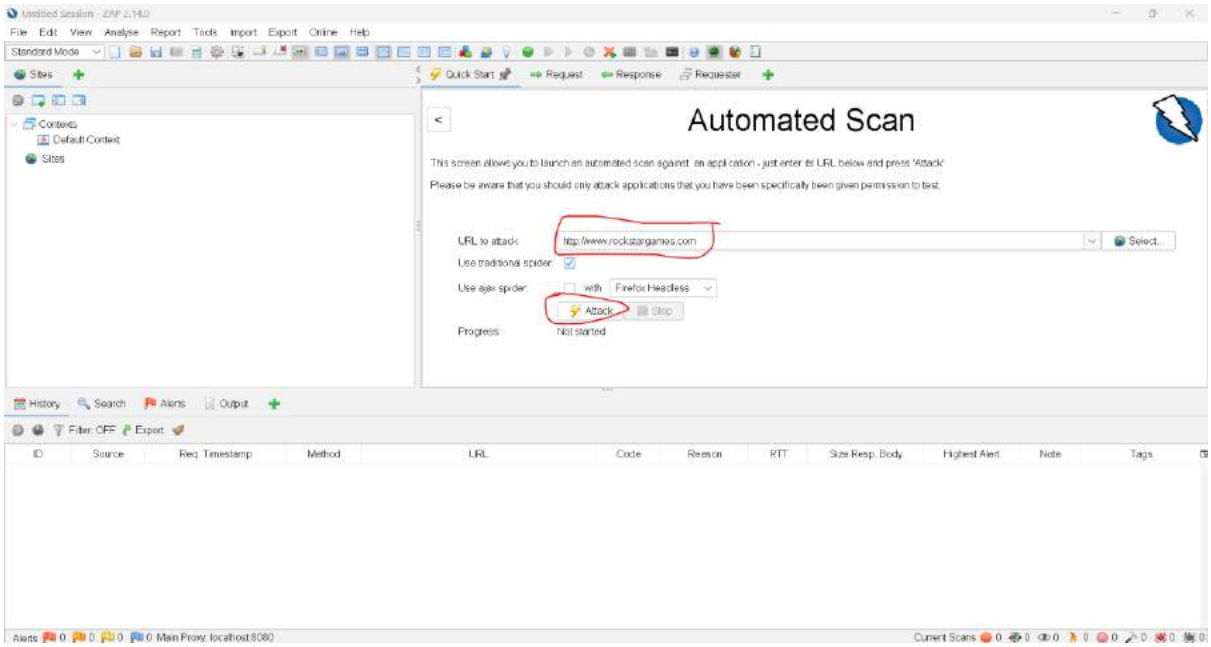
ZAP:

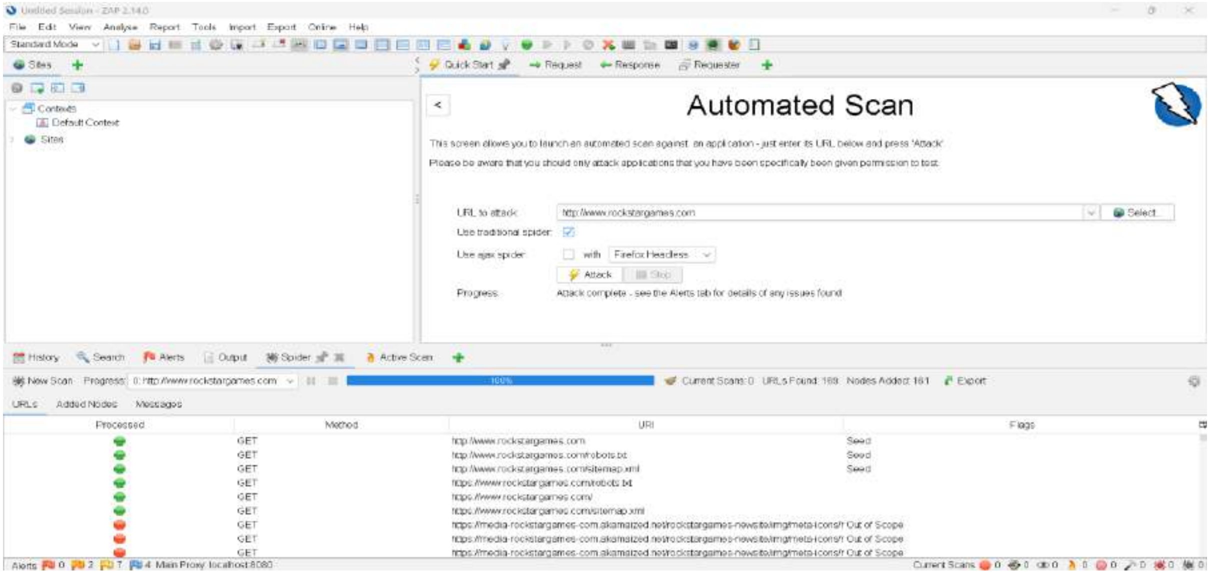
OWASPZAP (short for Zed Attack Proxy) is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers. It is one of the most active Open Web Application Security Project (OWASP) projects and has been given Flagship status When used as a proxy server it allows the user to manipulate all of the traffic that passes through it, including traffic using HTTPS

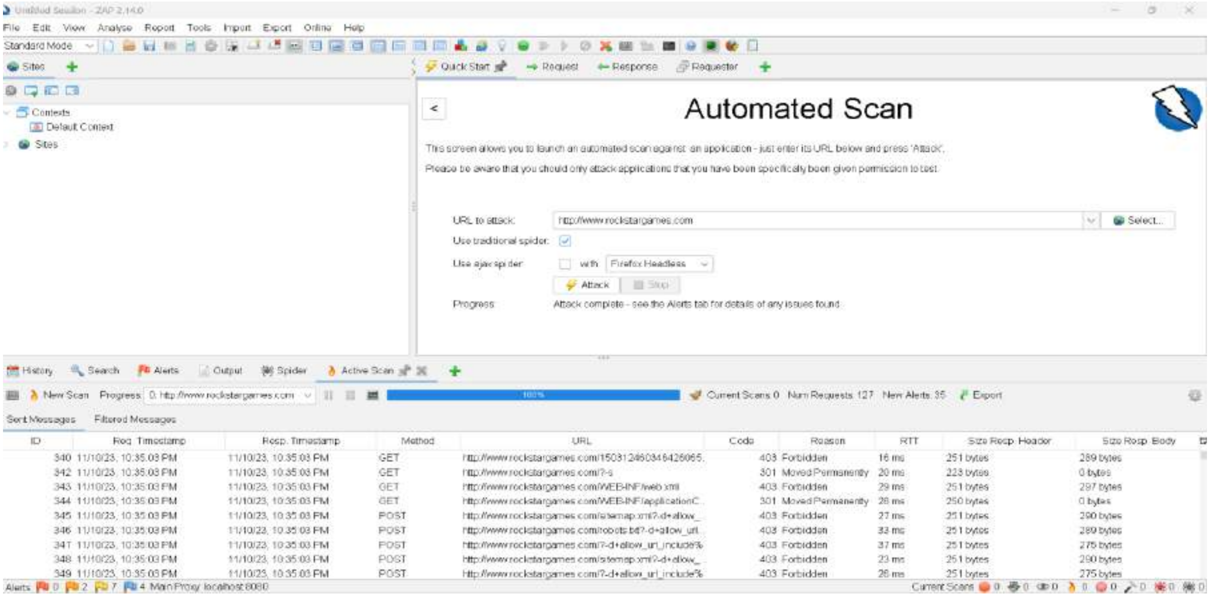
Step 1: Download and Install ZAP.

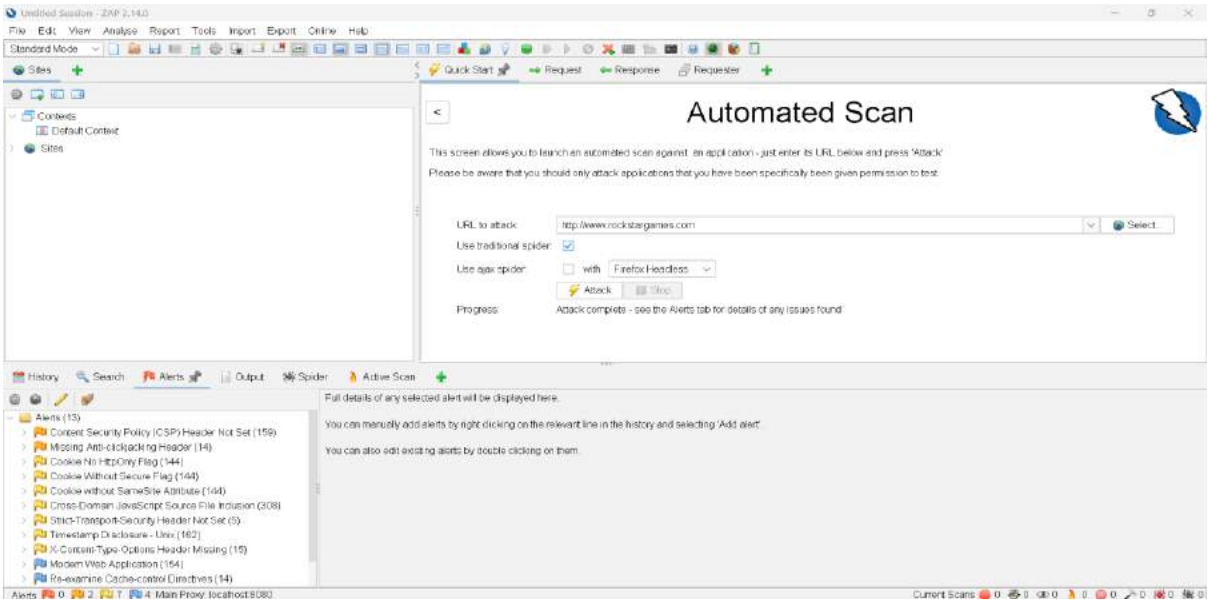


Step 2: In the URL to attack text box-> enter the full URL of the web application you want to attack-> Click the Attack.

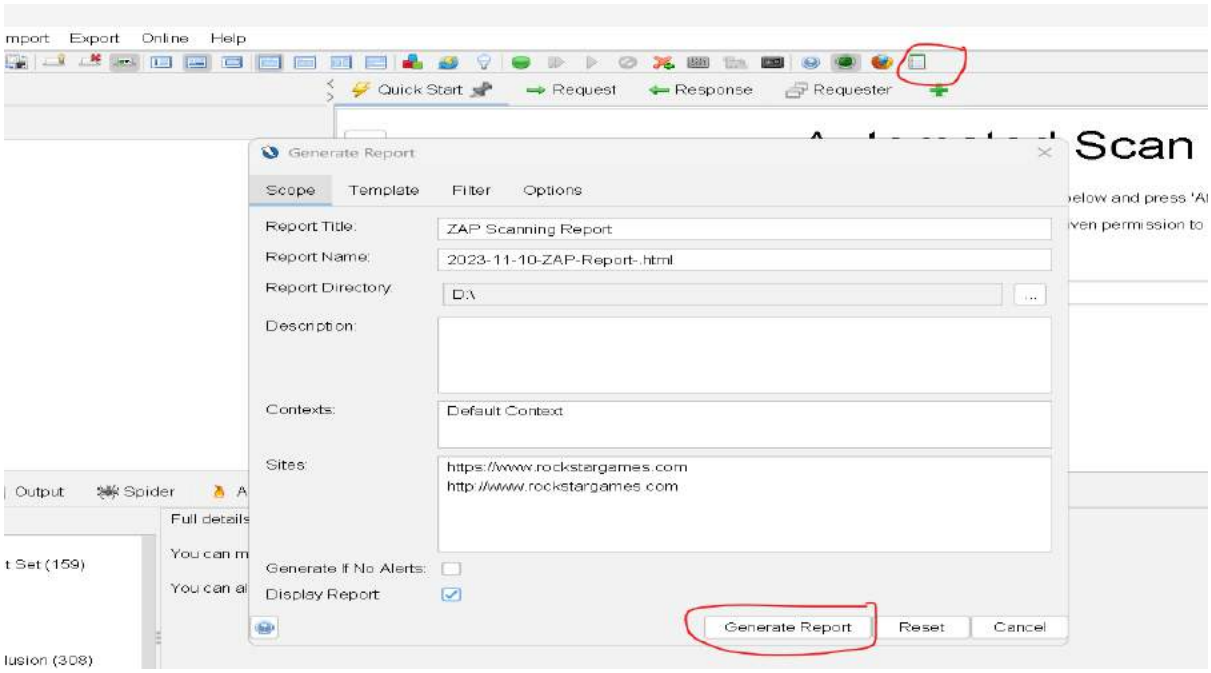


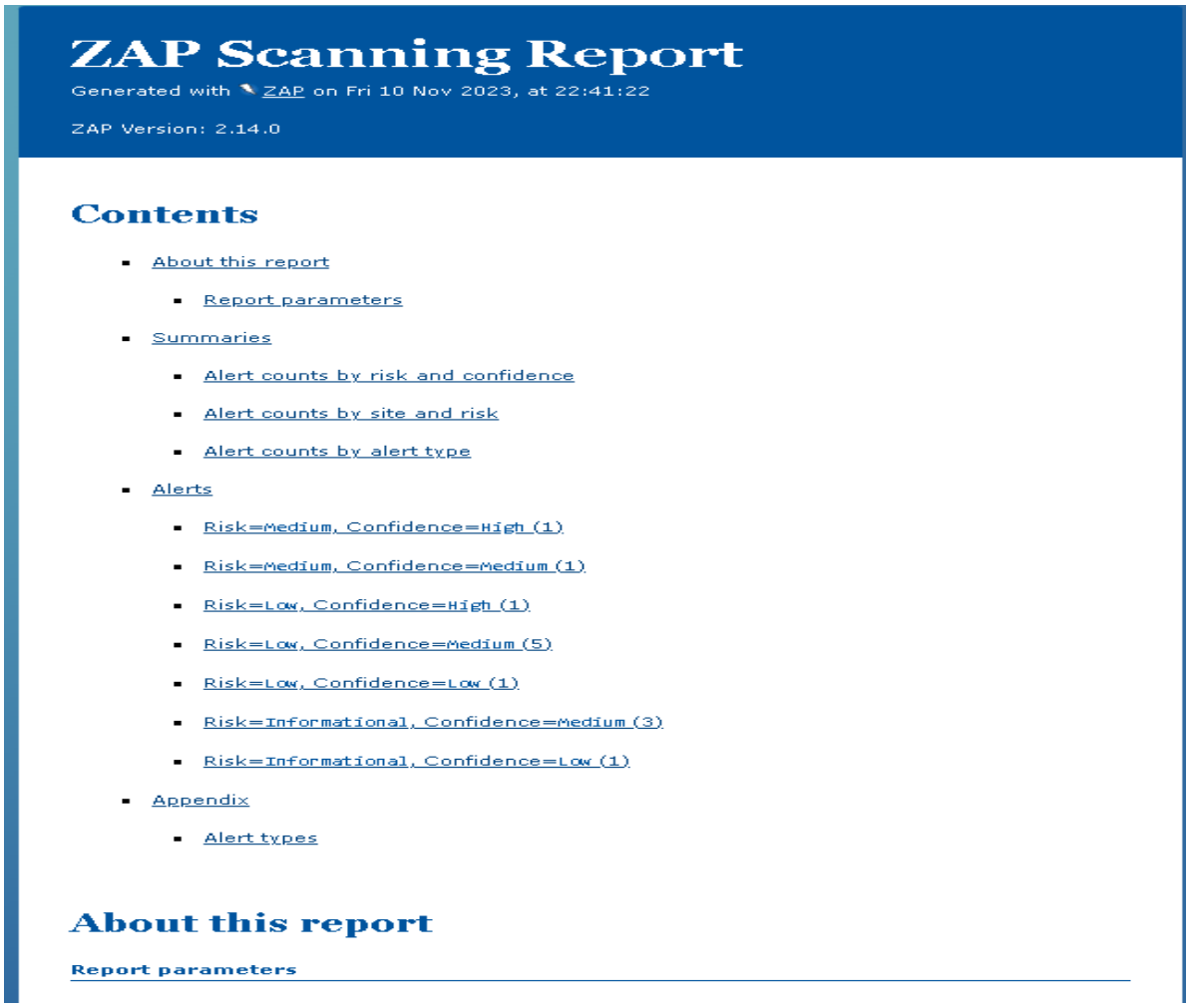

Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://www.rockstargames.com
Use traditional spider:
Use ajax spider:
Attack
Progress:
Attack complete - see the Alerts tab for details of any issues found


Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://www.rockstargames.com
Progress:
Attack complete - see the Alerts tab for details of any issues found


Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://www.rockstargames.com
Progress:
Attack complete - see the Alerts tab for details of any issues found
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.

Step 3 : After successful running of the tool, you can download reports in formats such as HTML, XML, and Markdown by navigating ZAP tool-> Report.





ZAP Scanning Report

Generated with ZAP on Fri 10 Nov 2023, at 22:41:22

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
- Alerts
  - Risk=Medium, Confidence=High (1)
  - Risk=Medium, Confidence=Medium (1)
  - Risk=Low, Confidence=High (1)
  - Risk=Low, Confidence=Medium (5)
  - Risk=Low, Confidence=Low (1)
  - Risk=Informational, Confidence=Medium (3)
  - Risk=Informational, Confidence=Low (1)
- Appendix
  - Alert types

About this report

Report parameters

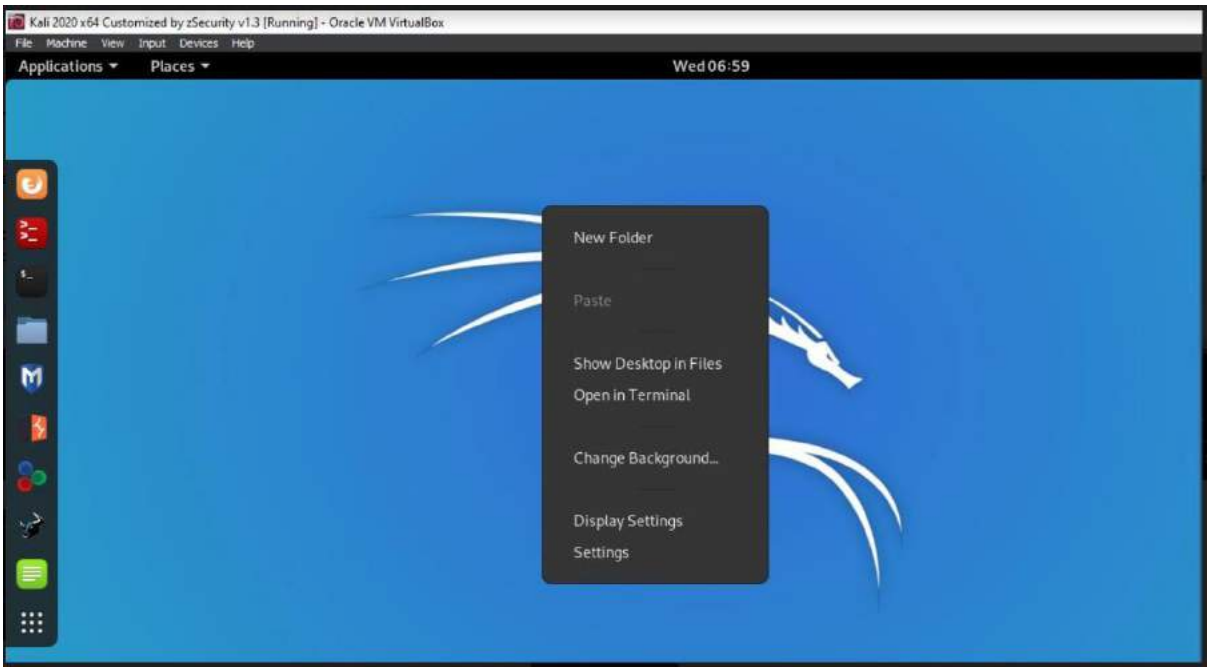
Practical

Denial of Service and Kali Linux

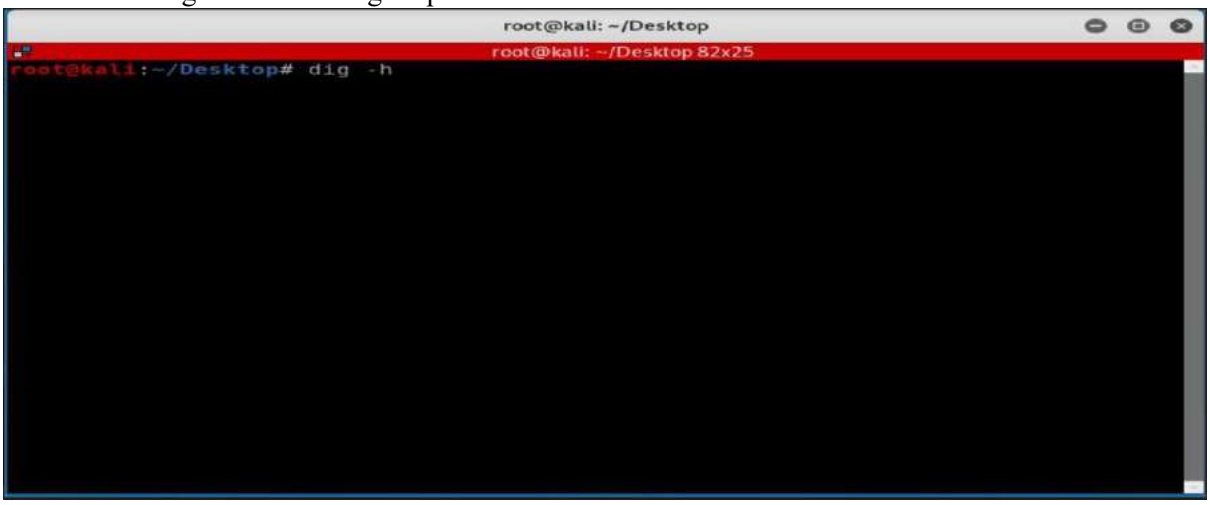
1) DoSHTTP

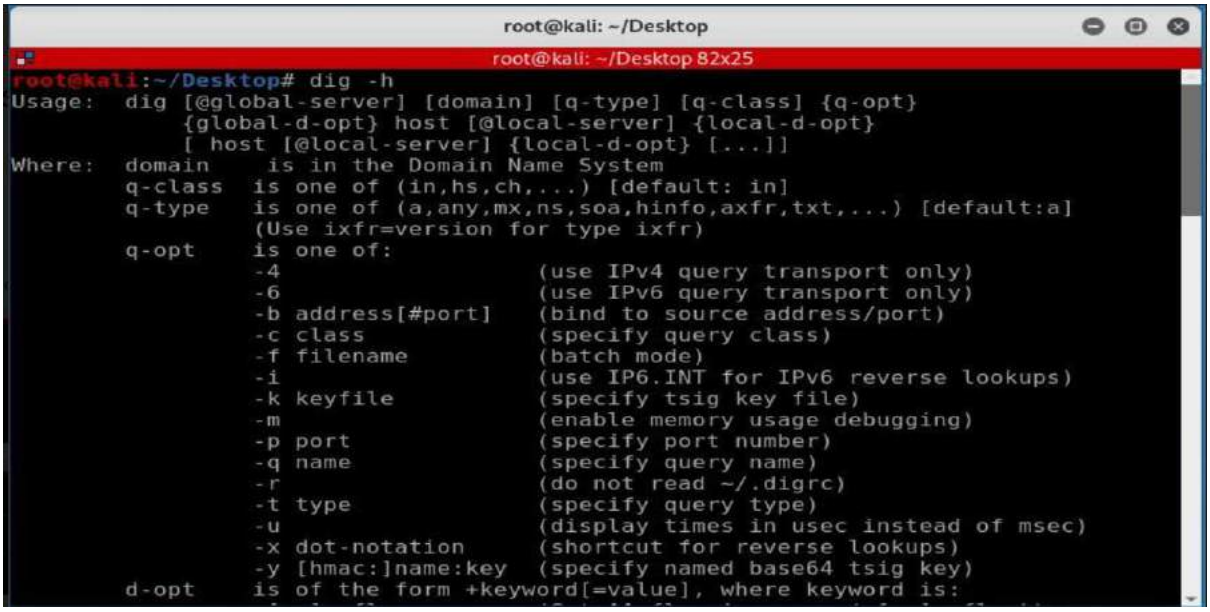
DoSHTTP is an easy to use and powerful HTTP Flood Denial of Service (DoS) Testing Tool for Windows. DoSHTTP includes URL Verification, HTTP Redirection, Port Designation, Performance Monitoring and Enhanced Reporting. DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP Flood. DoSHTTP can be used simultaneously on multiple clients to emulate a Distributed Denial of Service (DDoS) attack

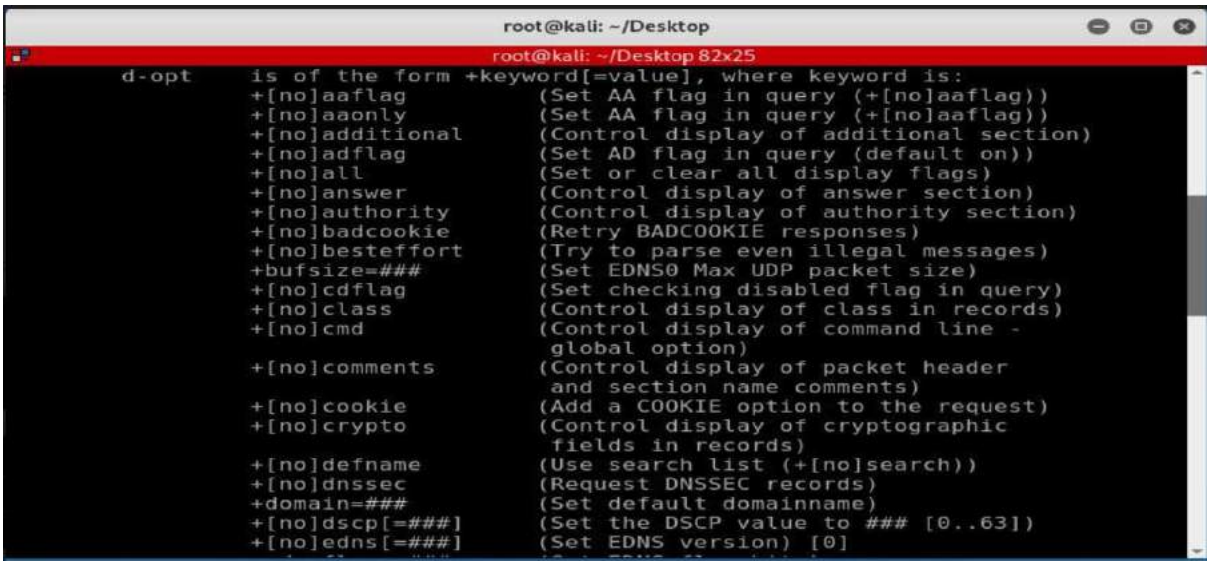
Step 1:- In Kali Linux, right click and select open in terminal

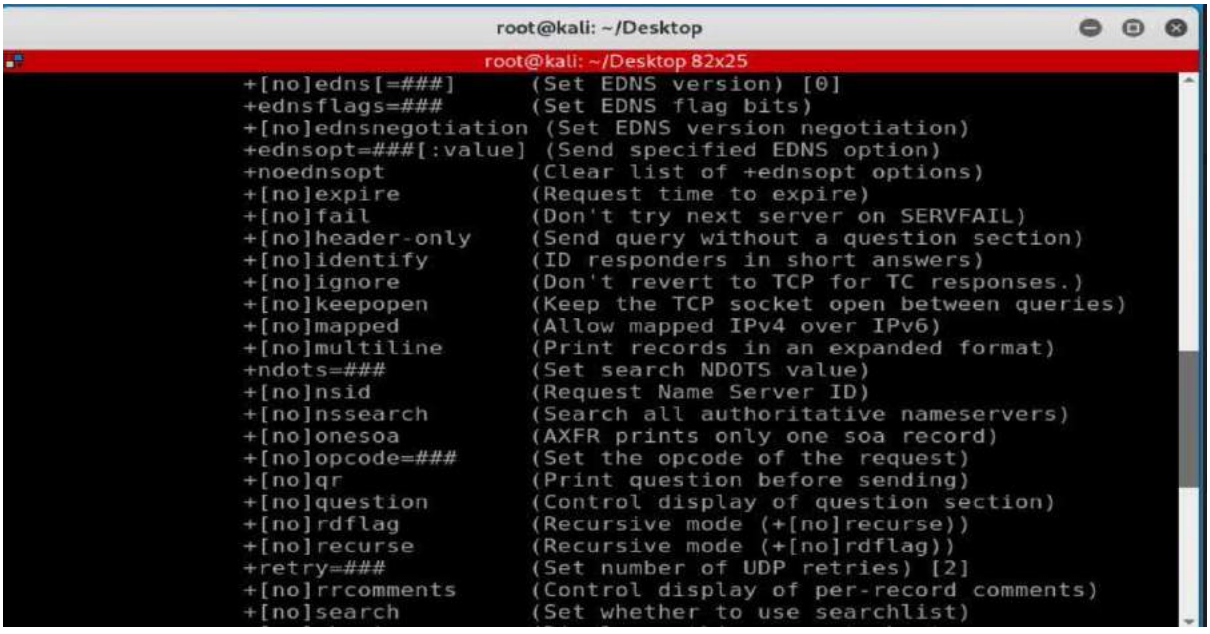


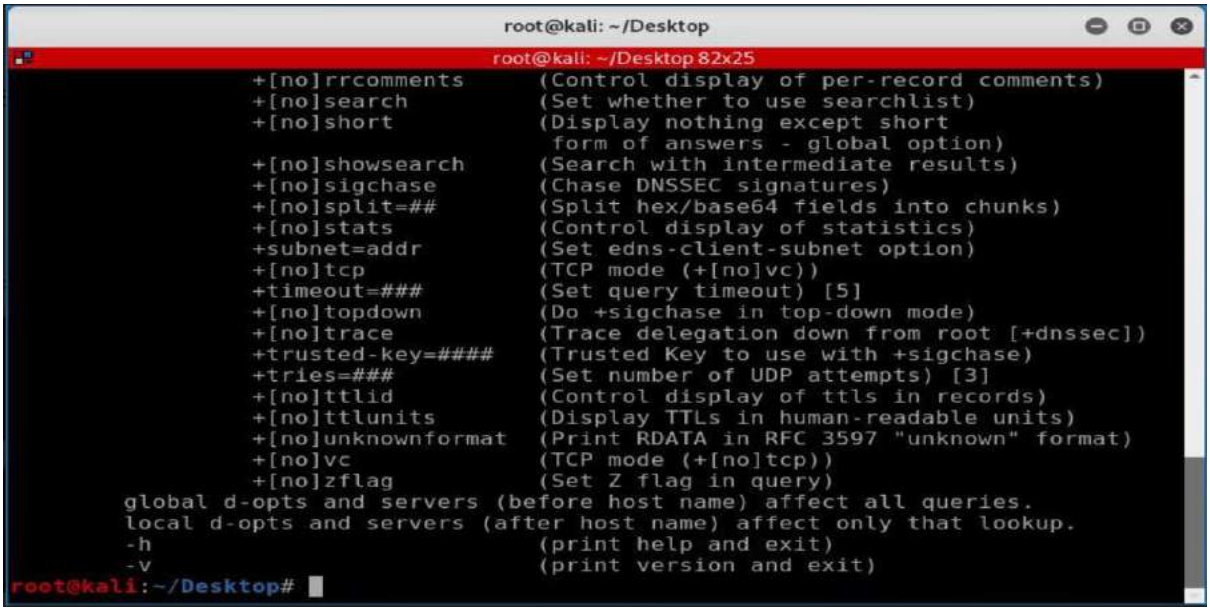
Step 2:- Now in the terminal window enter the command dig –h and press enter. You will get the following output.



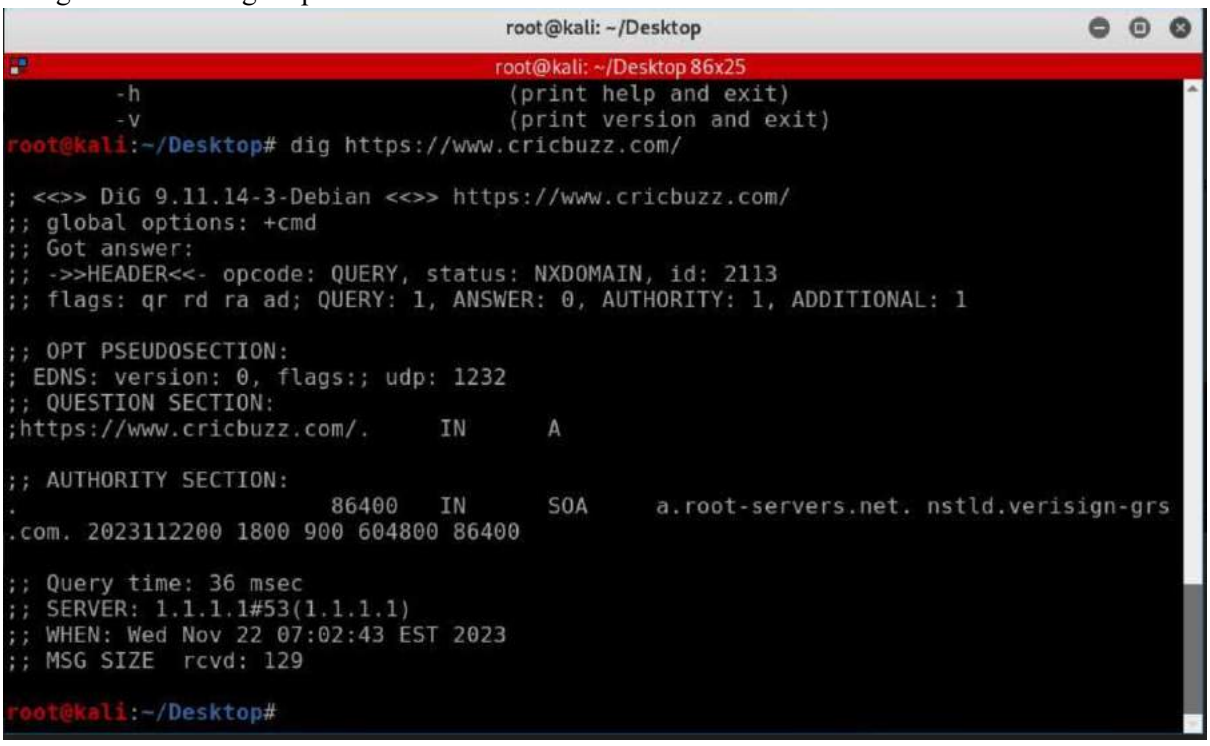

root@kali: ~/Desktop
root@kali: ~/Desktop 82x25
root@kali:~/Desktop# dig -h
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
{global-d-opt} host [@local-server] {local-d-opt}
[host [@local-server] {local-d-opt} [...]]
Where: domain is in the Domain Name System
q-class is one of (in,hs,ch,...) [default: in]
q-type is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
(Use ixfr=version for type ixfr)
q-opt is one of:
-4 (use IPv4 query transport only)
-6 (use IPv6 query transport only)
-b address[#port] (bind to source address/port)
-c class (specify query class)
-f filename (batch mode)
-i (use IP6.INT for IPv6 reverse lookups)
-k keyfile (specify tsig key file)
-m (enable memory usage debugging)
-p port (specify port number)
-q name (specify query name)
-r (do not read ~/.digrc)
-t type (specify query type)
-u (display times in usec instead of msec)
-x dot-notation (shortcut for reverse lookups)
-y [hmac:]name:key (specify named base64 tsig key)
d-opt is of the form +keyword[=value], where keyword is:


root@kali: ~/Desktop
root@kali: ~/Desktop 82x25
d-opt is of the form +keyword[=value], where keyword is:
+[no]aaflag (Set AA flag in query (+[no]aaflag))
+[no]aaonly (Set AA flag in query (+[no]aaflag))
+[no]additional (Control display of additional section)
+[no]adflag (Set AD flag in query (default on))
+[no]all (Set or clear all display flags)
+[no]answer (Control display of answer section)
+[no]authority (Control display of authority section)
+[no]badcookie (Retry BADCOOKIE responses)
+[no]besteffort (Try to parse even illegal messages)
+bufsize=### (Set EDNS0 Max UDP packet size)
+[no]cdflag (Set checking disabled flag in query)
+[no]class (Control display of class in records)
+[no]cmd (Control display of command line -
global option)
+[no]comments (Control display of packet header
and section name comments)
+[no]cookie (Add a COOKIE option to the request)
+[no]crypto (Control display of cryptographic
fields in records)
+[no]defname (Use search list (+[no]search))
+[no]dnssec (Request DNSSEC records)
+domain=### (Set default domainname)
+[no]dscp[=###] (Set the DSCP value to ### [0..63])
+[no]edns[=###] (Set EDNS version) [0]


root@kali: ~/Desktop
root@kali: ~/Desktop 82x25
+[no]edns[=###] (Set EDNS version) [0]
+ednsflags=### (Set EDNS flag bits)
+[no]ednsnegotiation (Set EDNS version negotiation)
+ednsopt=###[:value] (Send specified EDNS option)
+noednsopt (Clear list of +ednsopt options)
+[no]expire (Request time to expire)
+[no]fail (Don't try next server on SERVFAIL)
+[no]header-only (Send query without a question section)
+[no]identify (ID responders in short answers)
+[no]ignore (Don't revert to TCP for TC responses.)
+[no]keepopen (Keep the TCP socket open between queries)
+[no]mapped (Allow mapped IPv4 over IPv6)
+[no]multiline (Print records in an expanded format)
+ndots=### (Set search NDOTS value)
+[no]nsid (Request Name Server ID)
+[no]nssearch (Search all authoritative nameservers)
+[no]onesoa (AXFR prints only one soa record)
+[no]opcode=### (Set the opcode of the request)
+[no]qr (Print question before sending)
+[no]question (Control display of question section)
+[no]rdflag (Recursive mode (+[no]recurse))
+[no]recurse (Recursive mode (+[no]rdflag))
+retry=### (Set number of UDP retries) [2]
+[no]rrcomments (Control display of per-record comments)
+[no]search (Set whether to use searchlist)



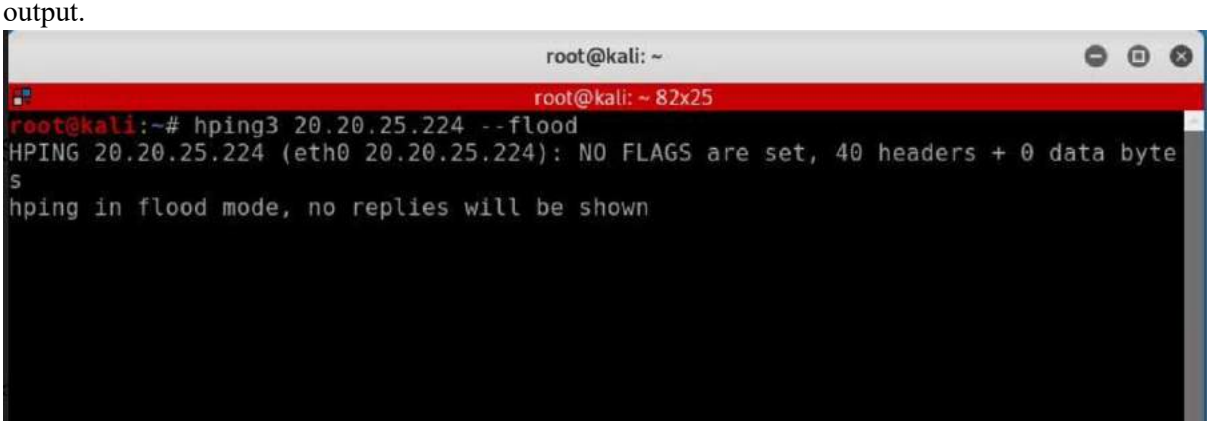
Step 3:- Now enter the command dig and the website link and press enter, you will get the following output.



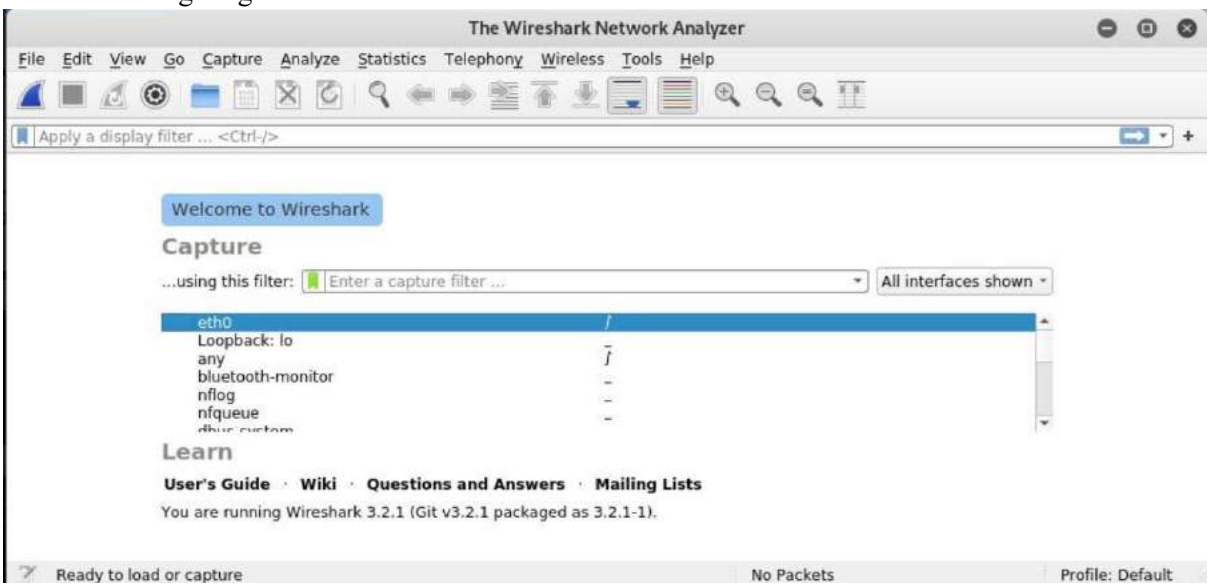
3) Hping3

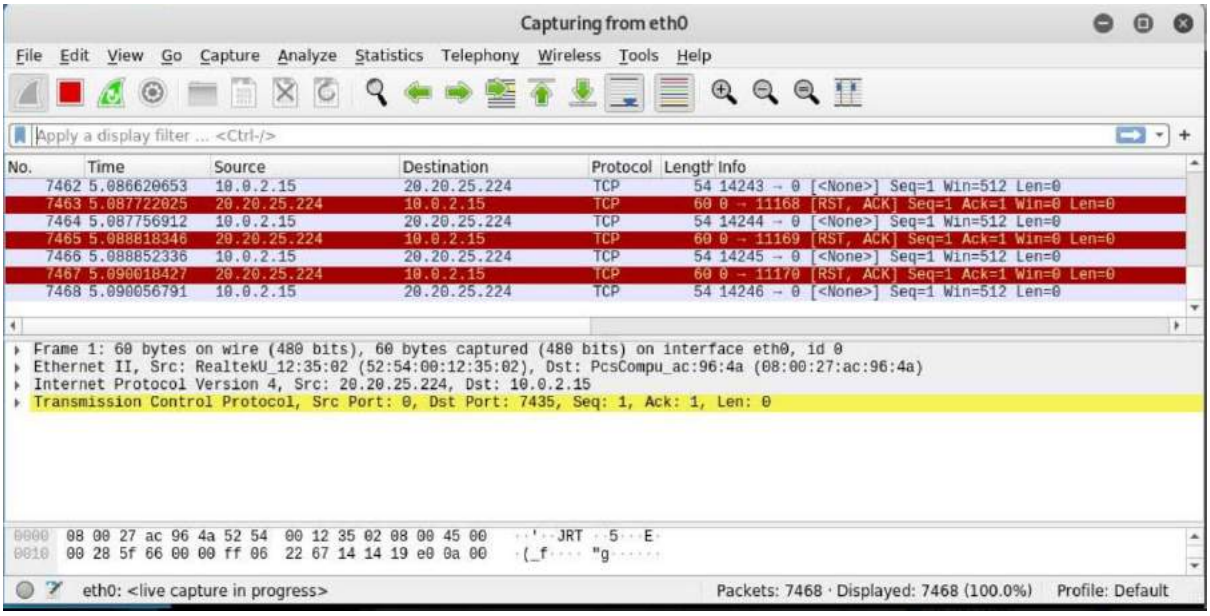
Hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols.

Step 1:- In Kali Linux, open the terminal and enter the command 'hping3 20.20.24.224--flood' and press enter, you will get the following output.



Step 2:- Now go to Applications and run Wireshark, select etho0 as interface as shown in the figure given below.




Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
7462 5.086620653 10.0.2.15 20.20.25.224 TCP 54 14243 → 0 [<None>] Seq=1 Win=512 Len=0
7463 5.087722025 20.20.25.224 10.0.2.15 TCP 60 0 → 11168 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7464 5.087756912 10.0.2.15 20.20.25.224 TCP 54 14244 → 0 [<None>] Seq=1 Win=512 Len=0
7465 5.088818346 20.20.25.224 10.0.2.15 TCP 60 0 → 11169 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7466 5.088852336 10.0.2.15 20.20.25.224 TCP 54 14245 → 0 [<None>] Seq=1 Win=512 Len=0
7467 5.090018427 20.20.25.224 10.0.2.15 TCP 60 0 → 11170 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7468 5.090056791 10.0.2.15 20.20.25.224 TCP 54 14246 → 0 [<None>] Seq=1 Win=512 Len=0
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_ac:96:4a (08:00:27:ac:96:4a)
Internet Protocol Version 4, Src: 20.20.25.224, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 0, Dst Port: 7435, Seq: 1, Ack: 1, Len: 0
0000 08 00 27 ac 96 4a 52 54 00 12 35 02 08 00 45 00
0010 00 28 5f 66 00 00 ff 06 22 67 14 14 19 e0 0a 00
eth0: <live capture in progress>
Packets: 7468 · Displayed: 7468 (100.0%)
Profile: Default

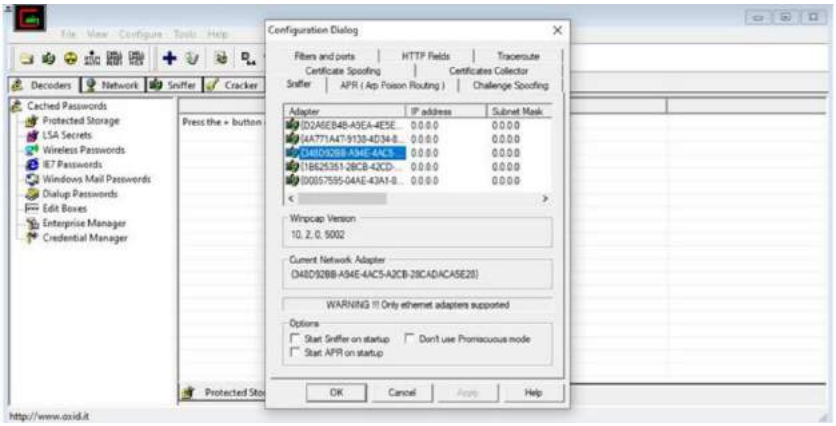
Practical

Network Sniffing.

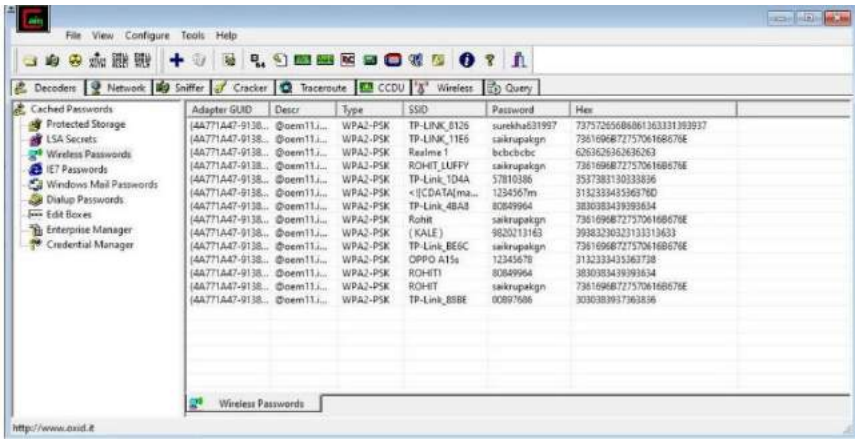
1) Cain & Cabel

Cain and Cabel (often abbreviated to Cain) was a password recovery tool for Microsoft Windows. It could recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attack

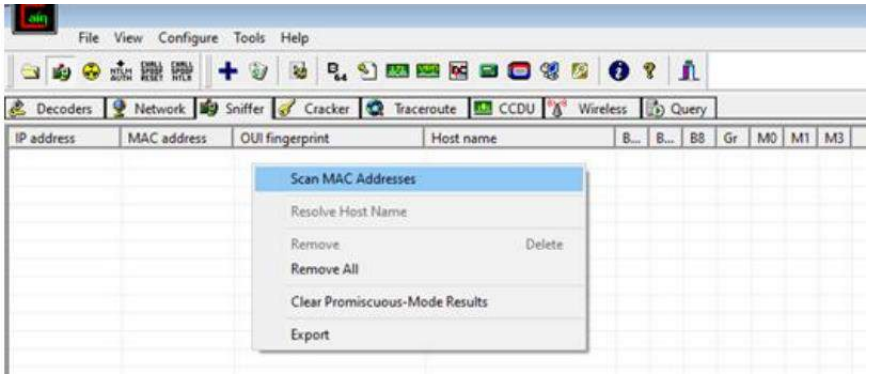
Step1: Open Cain n Abel. Click on configure. Select Adapter

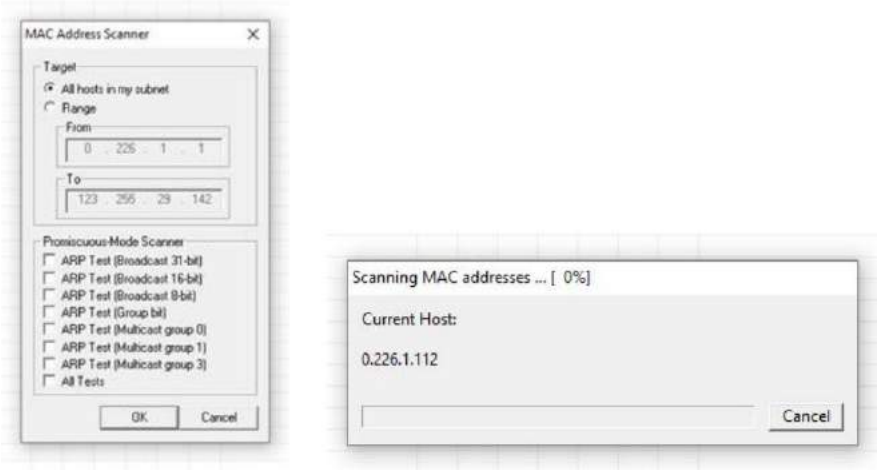


Step2: Go to Wireless password option to get wireless passwords

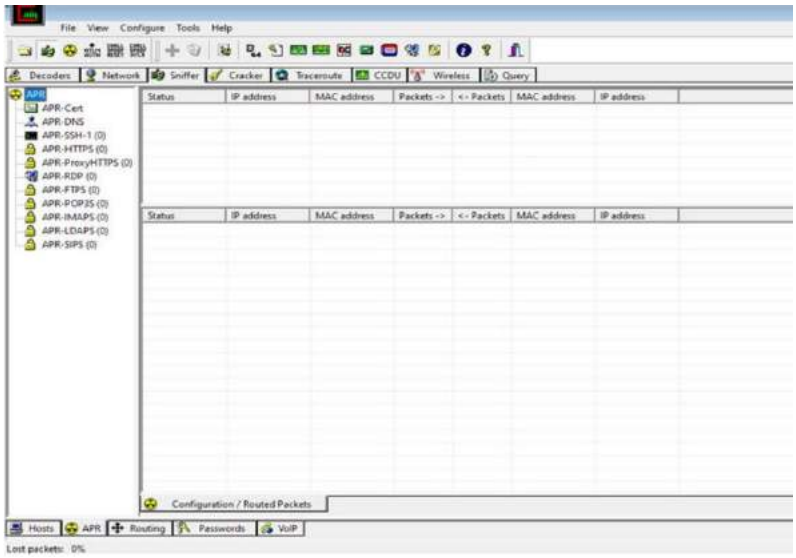


Step3: Activate Sniffer by clicking LAN Card Icon. Right click on sniffer list and choose scan MAC address. Select all tests

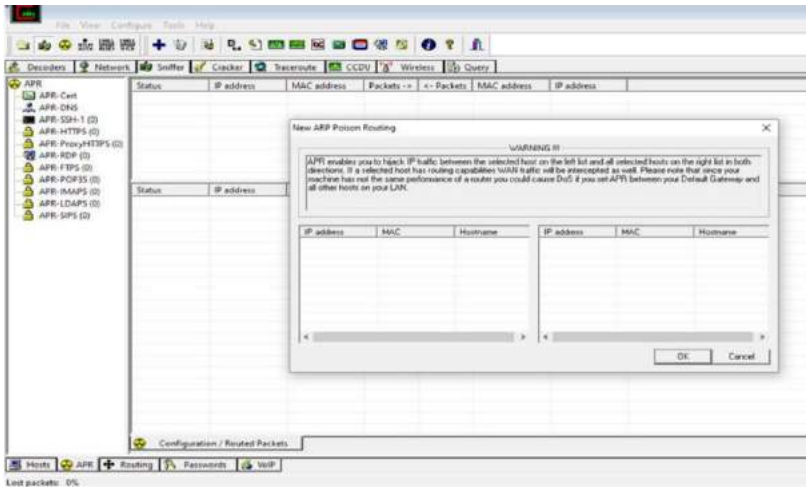




Step4: Activate apr. Click apr tab and click add to list.



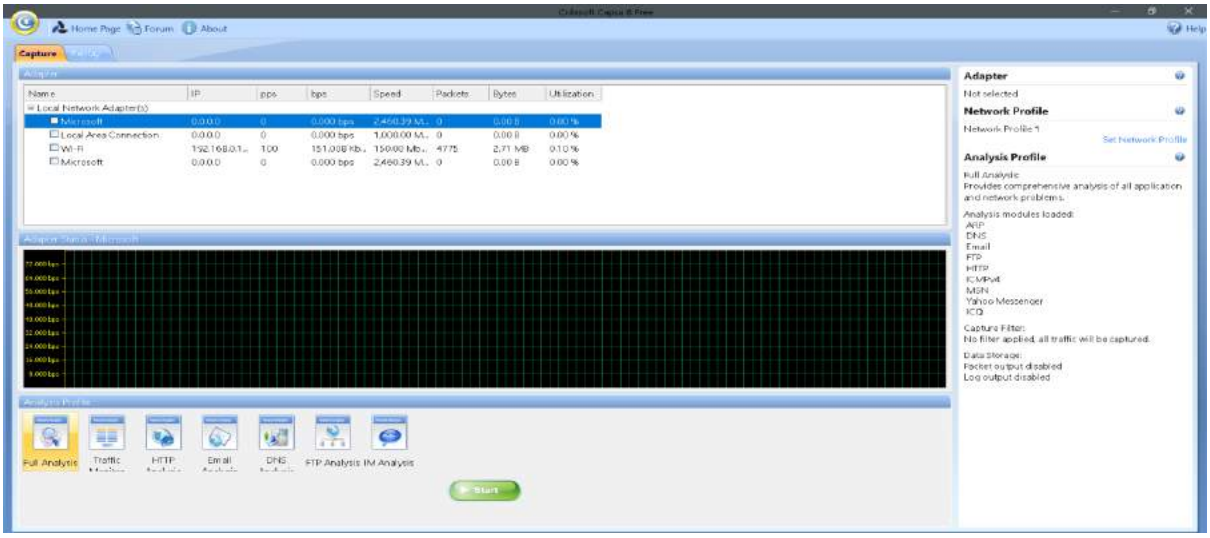
Step5: Choose machines between which you want to poison.



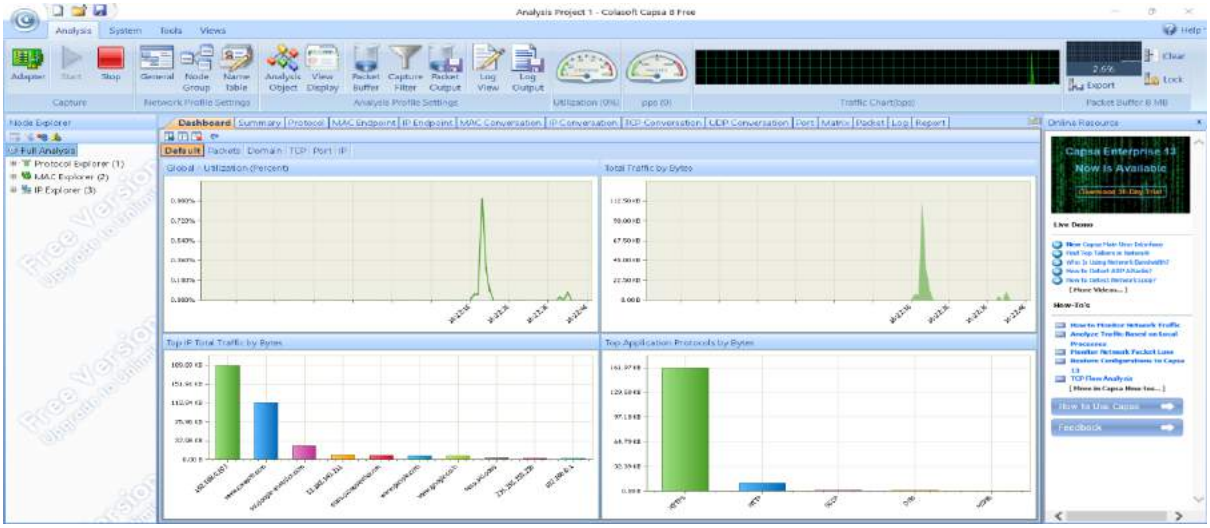
2) Caspa free Network Analyser

Capsa Free is a network analyzer freeware for Ethernet monitoring, troubleshooting and analysis. It provides users with great experience to learn how to monitor network activities, pinpoint network problems, enhance network security

Step 1 : Open Capsa Free Software and click on Full Analysis and then on start.



Step 2 : On the Dashboard you will be able to see total traffic by bytes.



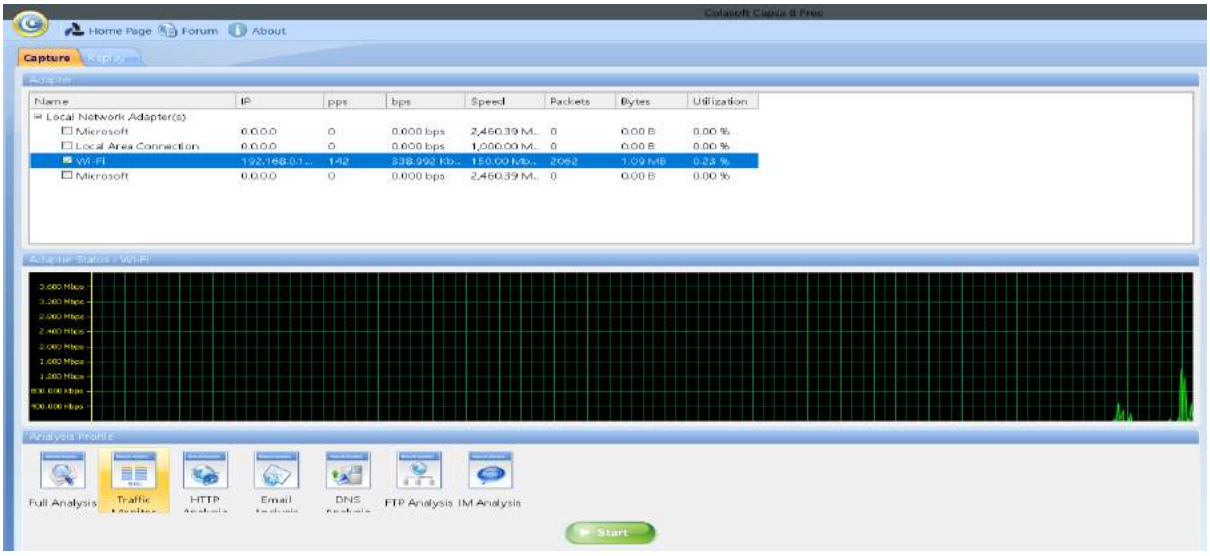
Summary

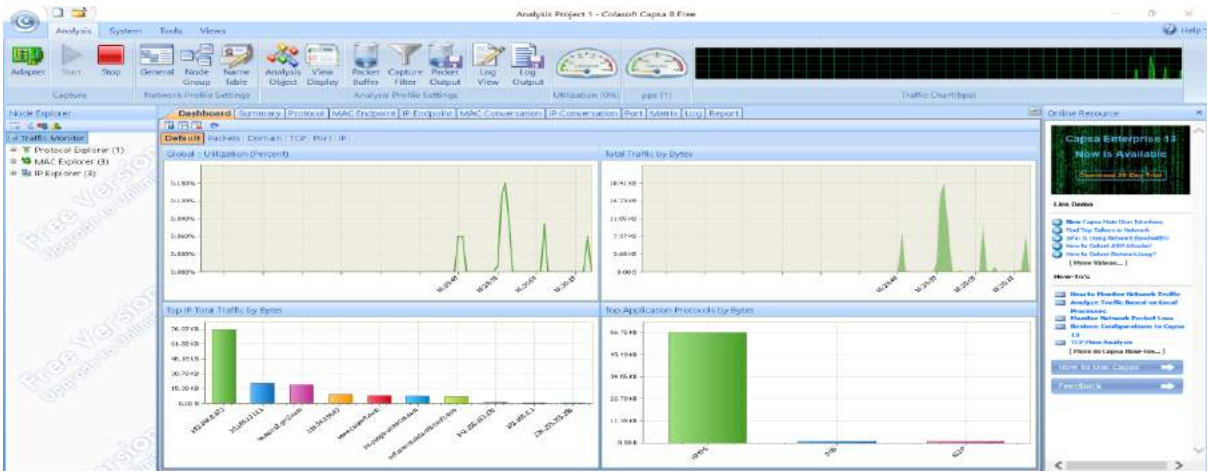
Dashboard | Summary | Protocol | MAC Endpoint | IP Endpoint | MAC Conversation | IP Conversation | TCP Co

Statistics Item					Current Value
Traffic	Bytes	Packets	Utilization	bps	pps
Total	271.88 KB	731	0.003%	3.160 Kbps	4
Broadcast	92.00 B	2	0.000%	0.000 bps	0
Multicast	3.83 KB	20	0.002%	1.768 Kbps	1
Average Packet Size					380.000 Bytes
Pkt Size Distribution	Bytes	Packets	Utilization	bps	pps
<=64	16.46 KB	291	0.001%	1.392 Kbps	3
65-127	12.50 KB	153	0.000%	0.000 bps	0
128-255	10.97 KB	60	0.002%	1.768 Kbps	1
256-511	18.15 KB	50	0.000%	0.000 bps	0
512-1023	37.97 KB	54	0.000%	0.000 bps	0
1024-1517	175.83 KB	123	0.000%	0.000 bps	0
>=1518	0.00 B	0	0.000%	0.000 bps	0
Address					Count
MAC Address					6
IP Address					33
Local IP Address					4
Remote IP Address					29
Protocol					Count
Total Protocols					20
Data Link Layer					4
Network Layer					2
Transport Layer					2
Session Layer					0
Presentation Layer					0
Application Layer					12
Conversation					Count
MAC conversation					5

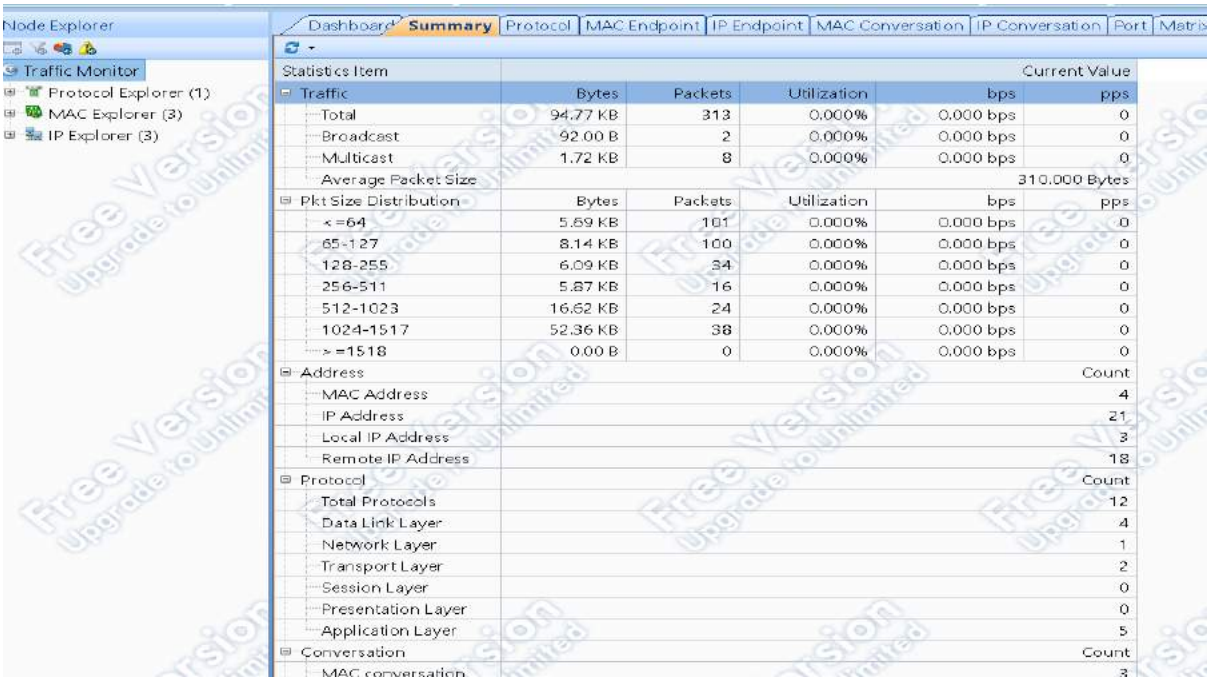
-Fi | Network Profile 1 - Bandwidth - 100Mbps | Inactive 00:02:10 | 731 0 | Ready

Step 3 : Now for Traffice Monitor-> Dashboard.





Summary



Node Explorer

Traffic Monitor

- Protocol Explorer (1)
- MAC Explorer (3)
- IP Explorer (3)

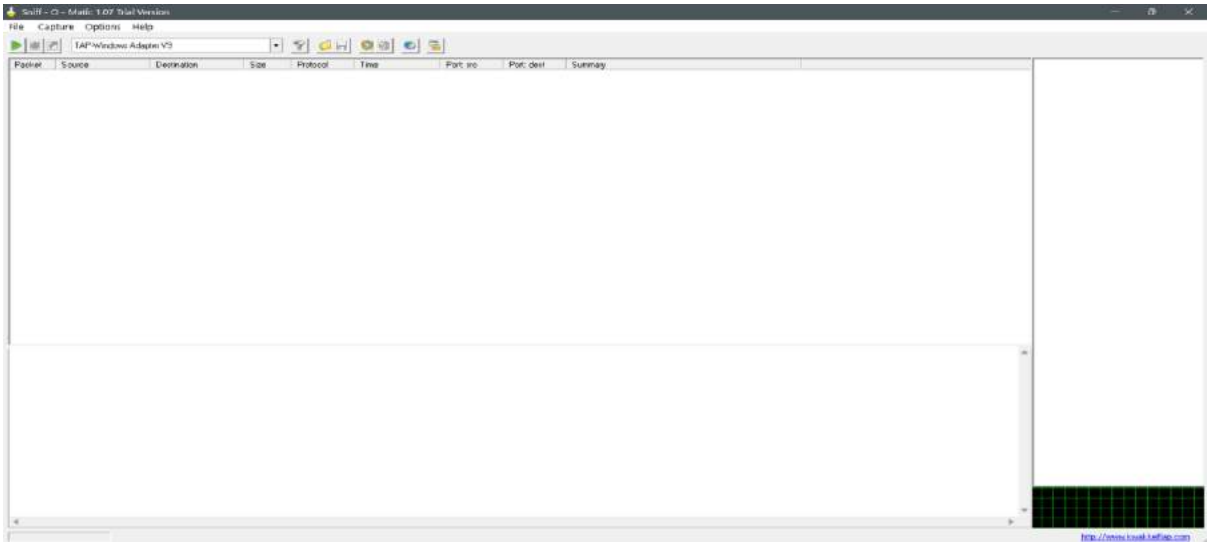
Dashboard | Summary | Protocol | MAC Endpoint | IP Endpoint | MAC Conversation | IP Conversation | Port | Matrix

Statistics Item					Current Value
Traffic	Bytes	Packets	Utilization	bps	pps
Total	94.77 KB	313	0.000%	0.000 bps	0
Broadcast	92.00 B	2	0.000%	0.000 bps	0
Multicast	1.72 KB	8	0.000%	0.000 bps	0
Average Packet Size					310.000 Bytes
Pkt Size Distribution	Bytes	Packets	Utilization	bps	pps
<=64	5.69 KB	101	0.000%	0.000 bps	0
65-127	8.14 KB	100	0.000%	0.000 bps	0
128-255	6.09 KB	34	0.000%	0.000 bps	0
256-511	5.87 KB	16	0.000%	0.000 bps	0
512-1023	16.62 KB	24	0.000%	0.000 bps	0
1024-1517	52.36 KB	38	0.000%	0.000 bps	0
>=1518	0.00 B	0	0.000%	0.000 bps	0
Address					Count
MAC Address					4
IP Address					21
Local IP Address					3
Remote IP Address					18
Protocol					Count
Total Protocols					12
Data Link Layer					4
Network Layer					1
Transport Layer					2
Session Layer					0
Presentation Layer					0
Application Layer					5
Conversation					Count
MAC conversation					3

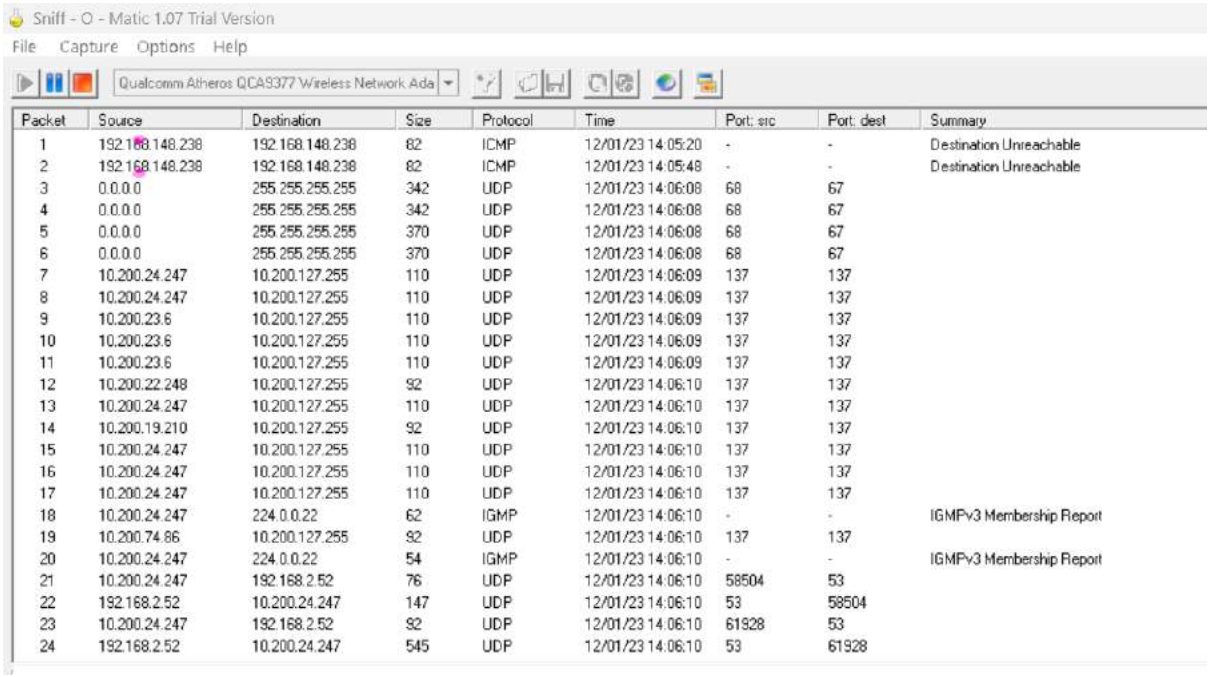
3) Sniff-o-matic

Sniff- O- Matic is a network protocol analyzer and packet sniffer with a clear and intuitive interface. It captures network traffic and enables you to analyze the data. Sniff- O- Matic is a simple network protocol analyzer and packet sniffer with an easy to use and unsophisticated interface.

Step1: Download and run the Tool



Step2: Now click on play button to start capturing and you will get the details about captured packets.



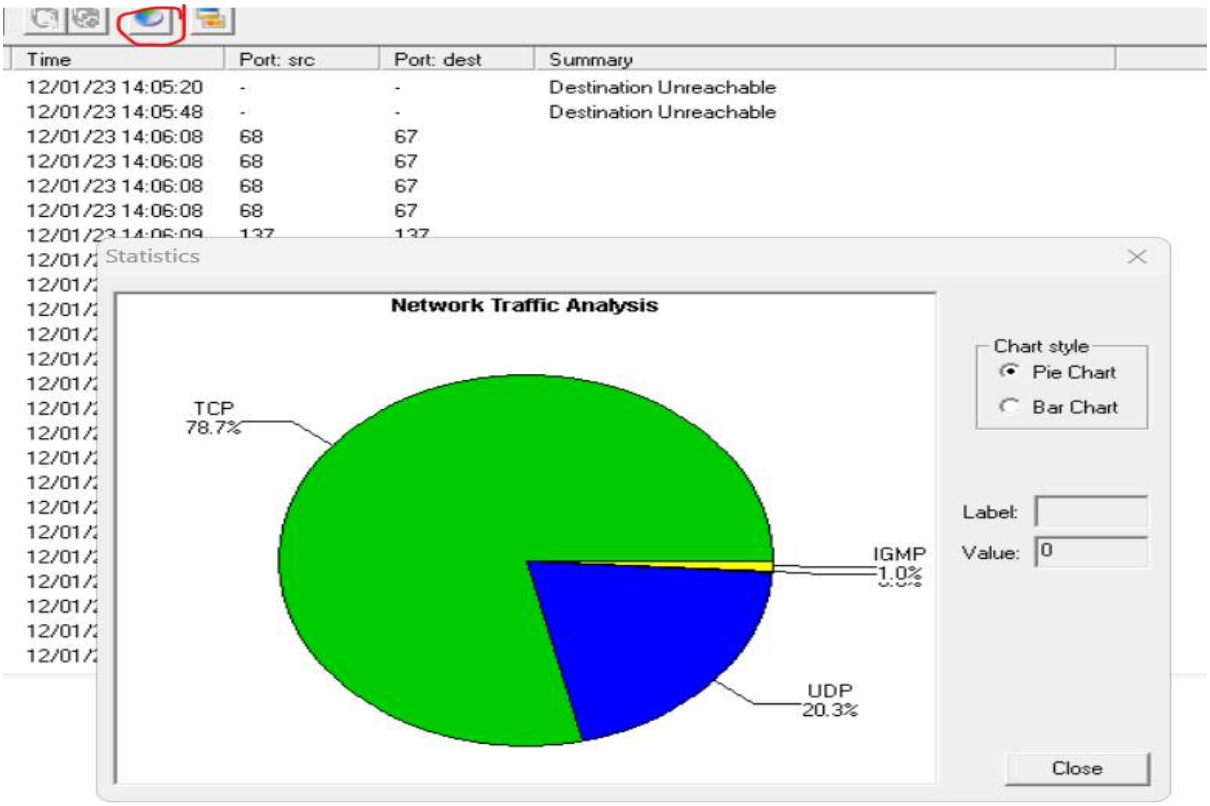
Sniff - O - Matic 1.07 Trial Version

File Capture Options Help

Qualcomm Atheros QCA9377 Wireless Network Ada

Packet	Source	Destination	Size	Protocol	Time	Port: src	Port: dest	Summary
1	192.168.148.238	192.168.148.238	82	ICMP	12/01/23 14:05:20	-	-	Destination Unreachable
2	192.168.148.238	192.168.148.238	82	ICMP	12/01/23 14:05:48	-	-	Destination Unreachable
3	0.0.0.0	255.255.255.255	342	UDP	12/01/23 14:06:08	68	67	
4	0.0.0.0	255.255.255.255	342	UDP	12/01/23 14:06:08	68	67	
5	0.0.0.0	255.255.255.255	370	UDP	12/01/23 14:06:08	68	67	
6	0.0.0.0	255.255.255.255	370	UDP	12/01/23 14:06:08	68	67	
7	10.200.24.247	10.200.127.255	110	UDP	12/01/23 14:06:09	137	137	
8	10.200.24.247	10.200.127.255	110	UDP	12/01/23 14:06:09	137	137	
9	10.200.23.6	10.200.127.255	110	UDP	12/01/23 14:06:09	137	137	
10	10.200.23.6	10.200.127.255	110	UDP	12/01/23 14:06:09	137	137	
11	10.200.23.6	10.200.127.255	110	UDP	12/01/23 14:06:09	137	137	
12	10.200.22.248	10.200.127.255	92	UDP	12/01/23 14:06:10	137	137	
13	10.200.24.247	10.200.127.255	110	UDP	12/01/23 14:06:10	137	137	
14	10.200.19.210	10.200.127.255	92	UDP	12/01/23 14:06:10	137	137	
15	10.200.24.247	10.200.127.255	110	UDP	12/01/23 14:06:10	137	137	
16	10.200.24.247	10.200.127.255	110	UDP	12/01/23 14:06:10	137	137	
17	10.200.24.247	10.200.127.255	110	UDP	12/01/23 14:06:10	137	137	
18	10.200.24.247	224.0.0.22	62	IGMP	12/01/23 14:06:10	-	-	IGMPv3 Membership Report
19	10.200.74.86	10.200.127.255	92	UDP	12/01/23 14:06:10	137	137	
20	10.200.24.247	224.0.0.22	54	IGMP	12/01/23 14:06:10	-	-	IGMPv3 Membership Report
21	10.200.24.247	192.168.2.52	76	UDP	12/01/23 14:06:10	58504	53	
22	192.168.2.52	10.200.24.247	147	UDP	12/01/23 14:06:10	53	58504	
23	10.200.24.247	192.168.2.52	92	UDP	12/01/23 14:06:10	61928	53	
24	192.168.2.52	10.200.24.247	545	UDP	12/01/23 14:06:10	53	61928	

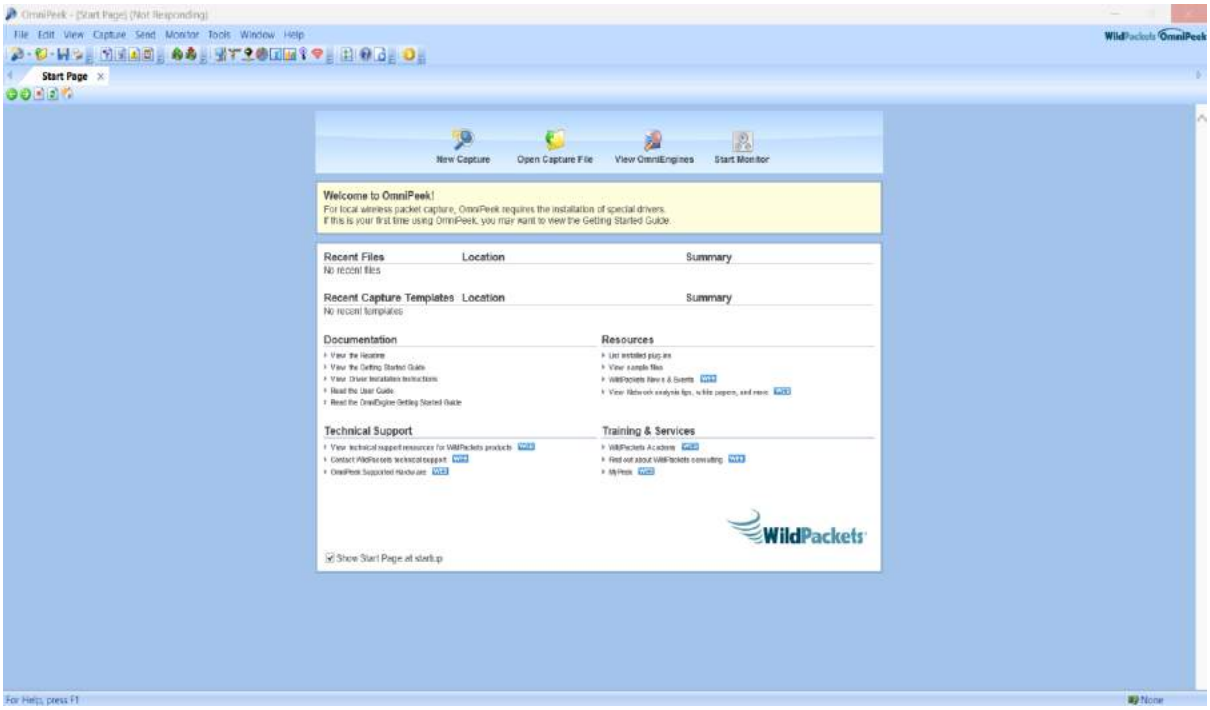
Step3: click on the statistics option.



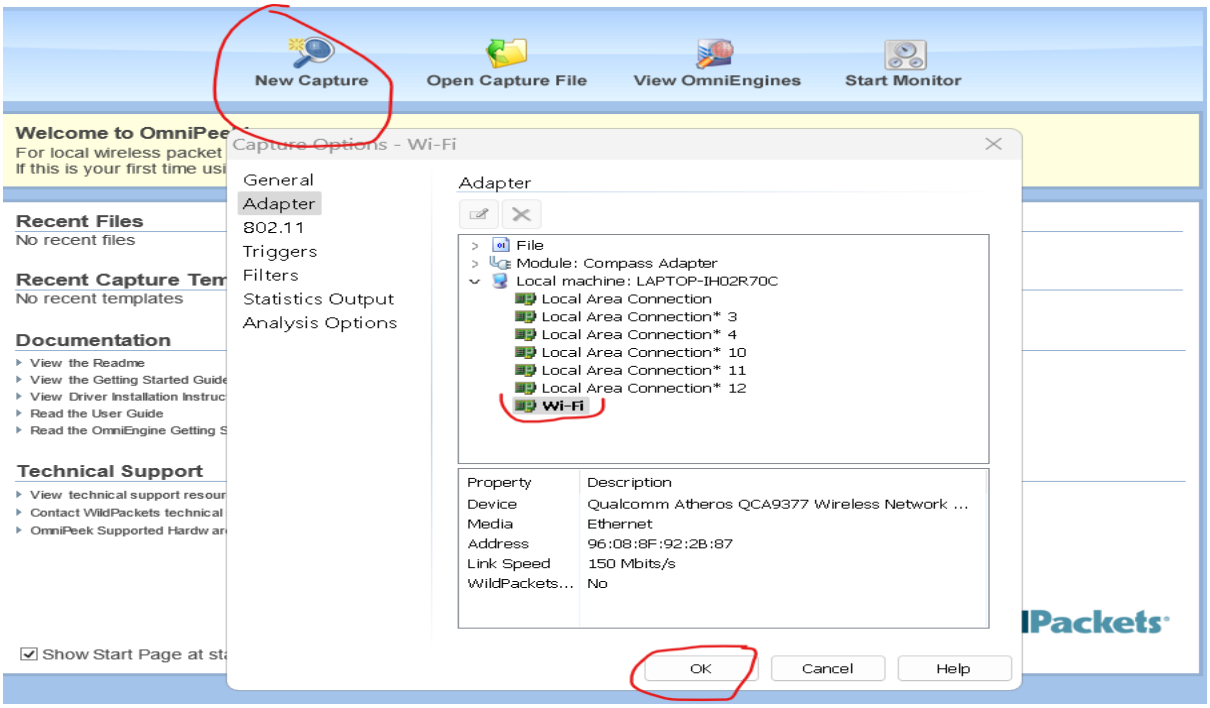
4) OminPeek

Omnipeek is a packet analyzer software tool from Savvius, a LiveAction company,for network troubleshooting and protocol analysis. It supports an application programming interface for plugins

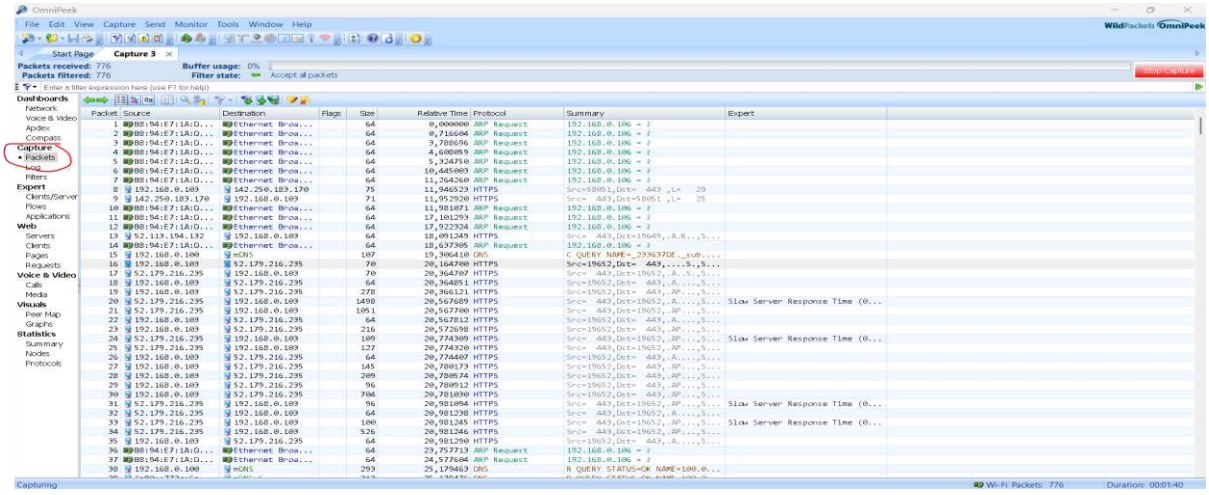
Step 1 : OpenOmnipeek Network Analyzer Software.



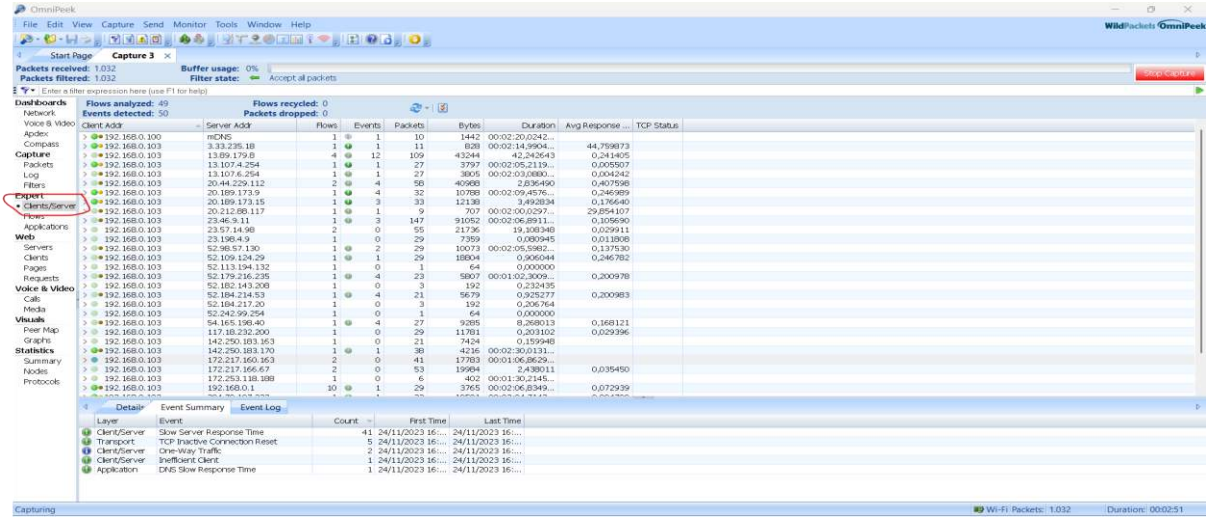
Step 2 : Select Wi-Fi and click on start.



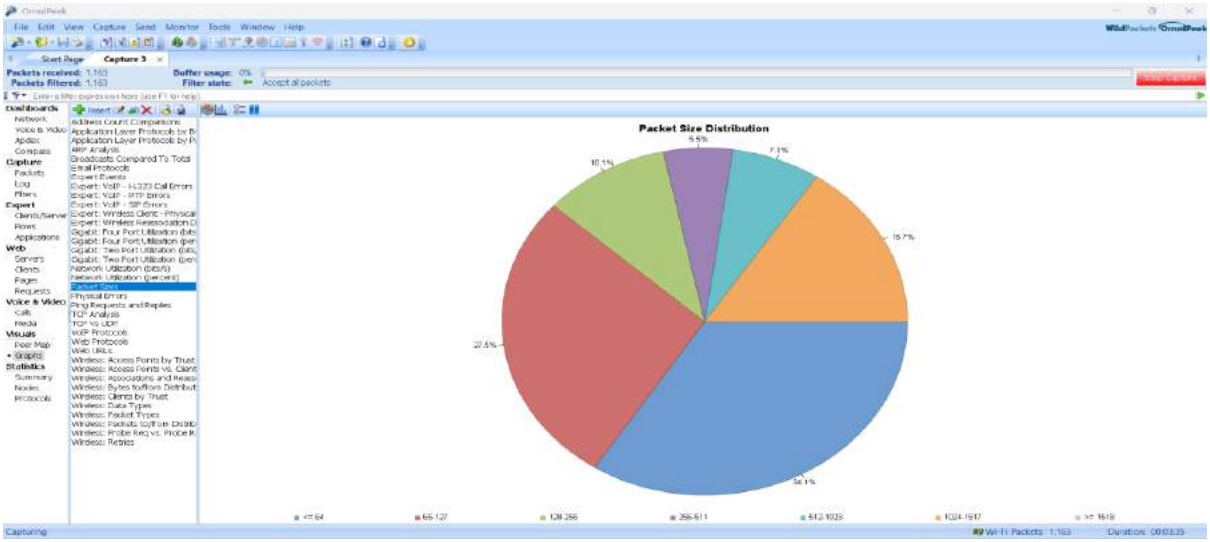
Step 3 : Go to Capture-> Packets to see the source and destination of a traffic.



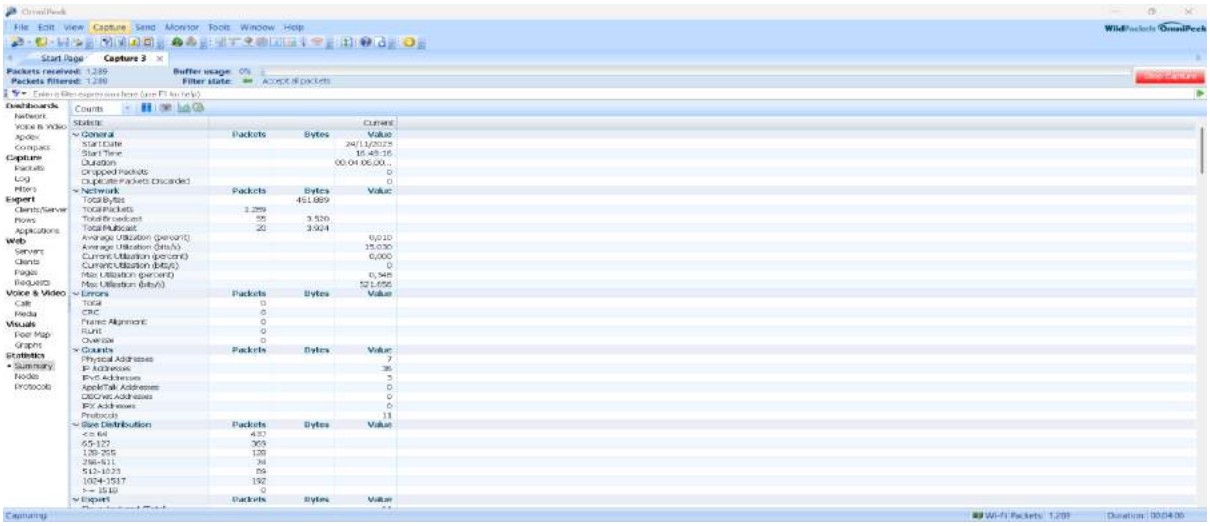
Step 4 : Go to Expert-> Client address and Server address.



Step 5 : Go to Visuals-> Graph.

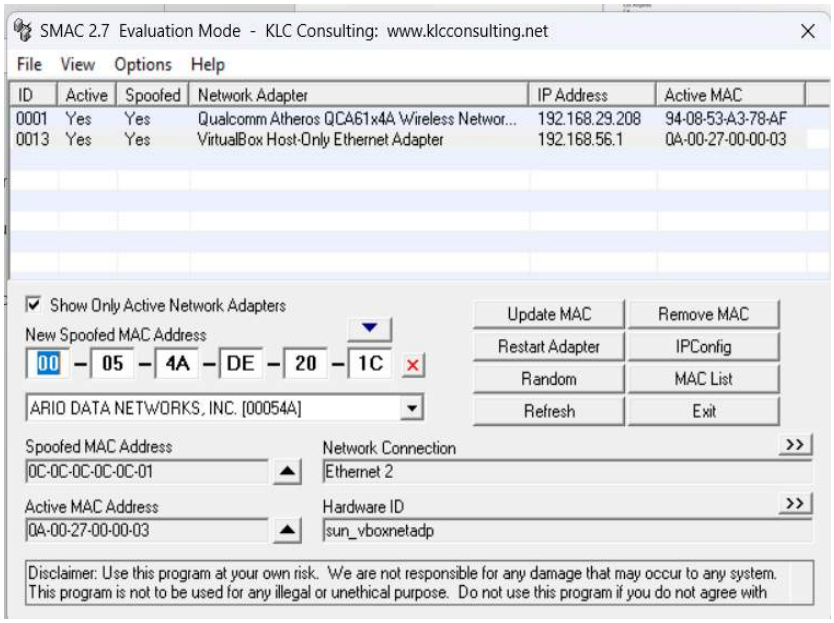


Step 6 : Go to Statistics-> Summary.

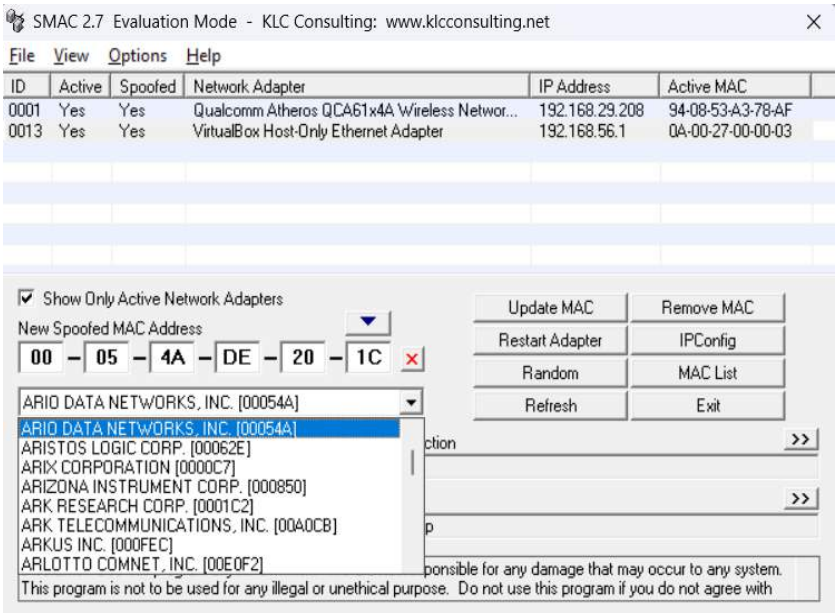


5) SMAC

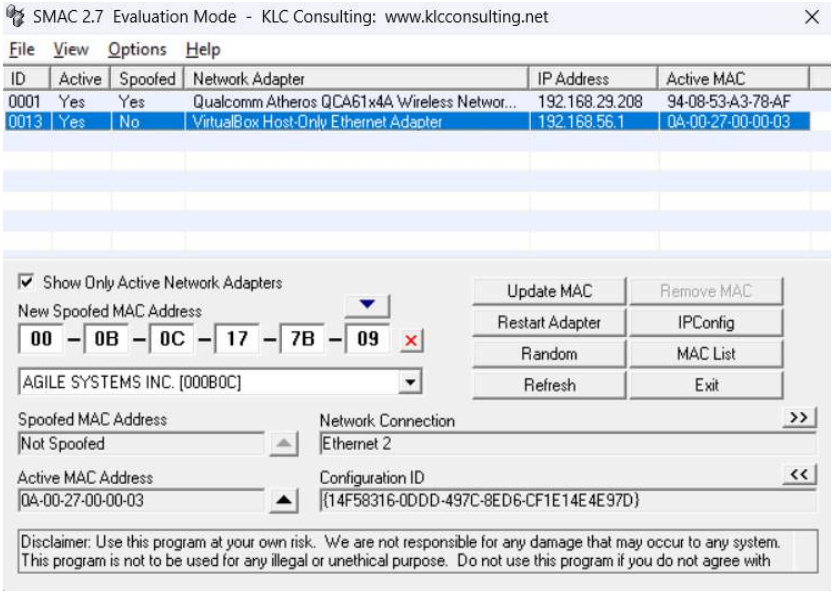
Step 1:Open SMAC, go to options and click on automatically restart adapter. Now select one network adapter. Now either you can manually type in the mac address or click on the arrow to get mac address or click on random to get mac address.



Step2: The dropdown box below the new spoofed mac address displays the network adapter manufacturer associated with the MAC address.



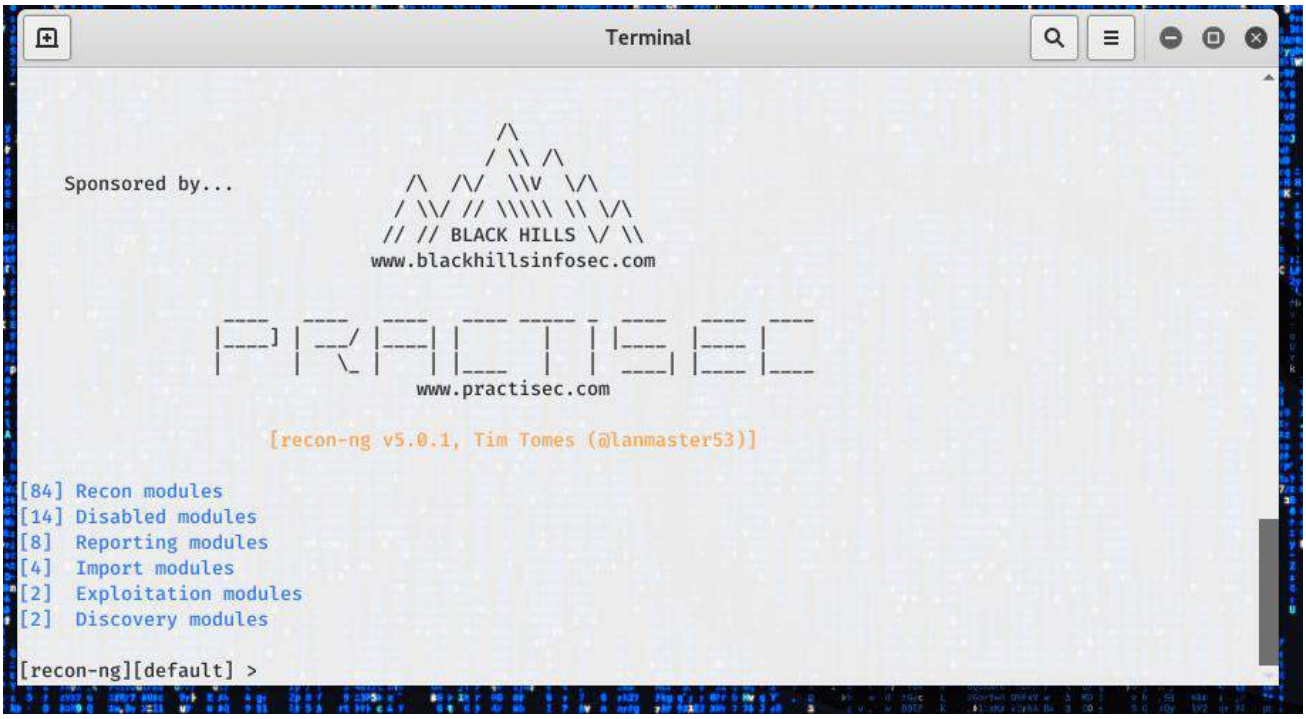
Step3: Now click on Update MAC and also you can remove the mac and you will see the address is not spoofed.



Practical no:

1)Recong-ng
Recon-ng is an open-source framework for conducting reconnaissance and information gathering during the initial phases of penetration testing. It is written in Python and provides a modular and extensible platform for gathering information about a target. Here's a basic guide on how to use Recon-ng

Step1: open kali linux- go to recong-np



Step2: Enter the command to see all the modules available

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

+-------------------------------------------------------------------------------------------+
|                          Path                          | Version |   Status  | Updated   | D | K |
+-------------------------------------------------------------------------------------------+
| discovery/info_disclosure/cache_snoop                  | 1.1     | installed | 2020-10-13 |   |   |
| discovery/info_disclosure/interesting_files            | 1.2     | installed | 2021-10-04 |   |   |
| exploitation/injection/command_injector                | 1.0     | installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter                    | 1.2     | installed | 2019-10-08 |   |   |
| import/csv_file                                        | 1.1     | installed | 2019-08-09 |   |   |
| import/list                                            | 1.1     | installed | 2019-06-24 |   |   |
| import/masscan                                         | 1.0     | installed | 2020-04-07 |   |   |
| import/nmap                                            | 1.1     | installed | 2020-10-06 |   |   |
| recon/companies-contacts/bing_linkedin_cache           | 1.0     | installed | 2019-06-24 |   | * |
| recon/companies-contacts/censys_email_address          | 2.0     | disabled  | 2021-05-11 | * | * |
| recon/companies-contacts/pen                           | 1.1     | installed | 2019-10-15 |   |   |
| recon/companies-domains/censys_subdomains              | 2.0     | disabled  | 2021-05-10 | * | * |
| recon/companies-domains/pen                            | 1.1     | installed | 2019-10-15 |   |   |
| recon/companies-domains/viewdns_reverse_whois          | 1.1     | installed | 2021-08-24 |   |   |
| recon/companies-domains/whoxy_dns                      | 1.1     | installed | 2020-06-17 |   | * |
| recon/companies-hosts/censys_org                       | 2.0     | disabled  | 2021-05-11 | * | * |
| recon/companies-hosts/censys_tls_subjects              | 2.0     | disabled  | 2021-05-11 | * | * |
| recon/companies-multi/github_miner                     | 1.1     | installed | 2020-05-15 |   | * |
| recon/companies-multi/shodan_org                       | 1.1     | installed | 2020-07-01 | * | * |
| recon/companies-multi/whois_miner                      | 1.1     | installed | 2019-10-15 |   |   |
| recon/contacts-contacts/abc                            | 1.0     | installed | 2019-10-11 | * |   |
| recon/contacts-contacts/mailtester                     | 1.0     | installed | 2019-06-24 |   |   |
```

Step3:we will use “recon/domains-contacts/whois_pocs” module. To load the module use the command ‘modules load (any module name)’

```
[recon-ng][default] > modules load recon/domains-contacts/whois_pocs
[recon-ng][default][whois_pocs] >
```

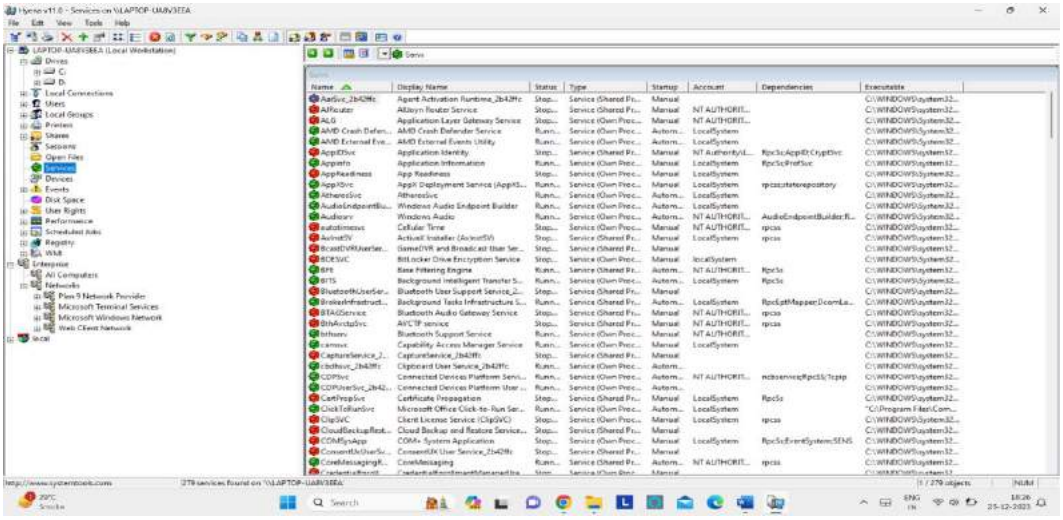
Step4: Once a module is loaded, set the required options using the **set** command ‘options set SOURCE cricbuzz.com’-> Run.

```
[recon-ng][default][whois_pocs] > options set SOURCE Google.com
SOURCE => Google.com
[recon-ng][default][whois_pocs] > run

----------
GOOGLE.COM
----------
[*] URL: http://whois.arin.net/rest/pocs;domain=Google.com
[*] URL: http://whois.arin.net/rest/poc/CREEK14-ARIN
[*] [contact] Alex Creek (alexcreek@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/ABA104-ARIN
[*] [contact] Ari Barkan (ari@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/ABA105-ARIN
[*] [contact] Ari Barkan (ari@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/ZG39-ARIN
[*] [contact] <blank> Google LLC (arin-contact@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/ALS11-ARIN
[*] [contact] Arturo Servin (arturolev@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/BROWN545-ARIN
[*] [contact] Tom Brownlow (brownlow@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/CJC43-ARIN
```

```
-------
SUMMARY
--------
[*] 34 total (7 new) contacts found.
```

2)Hyena

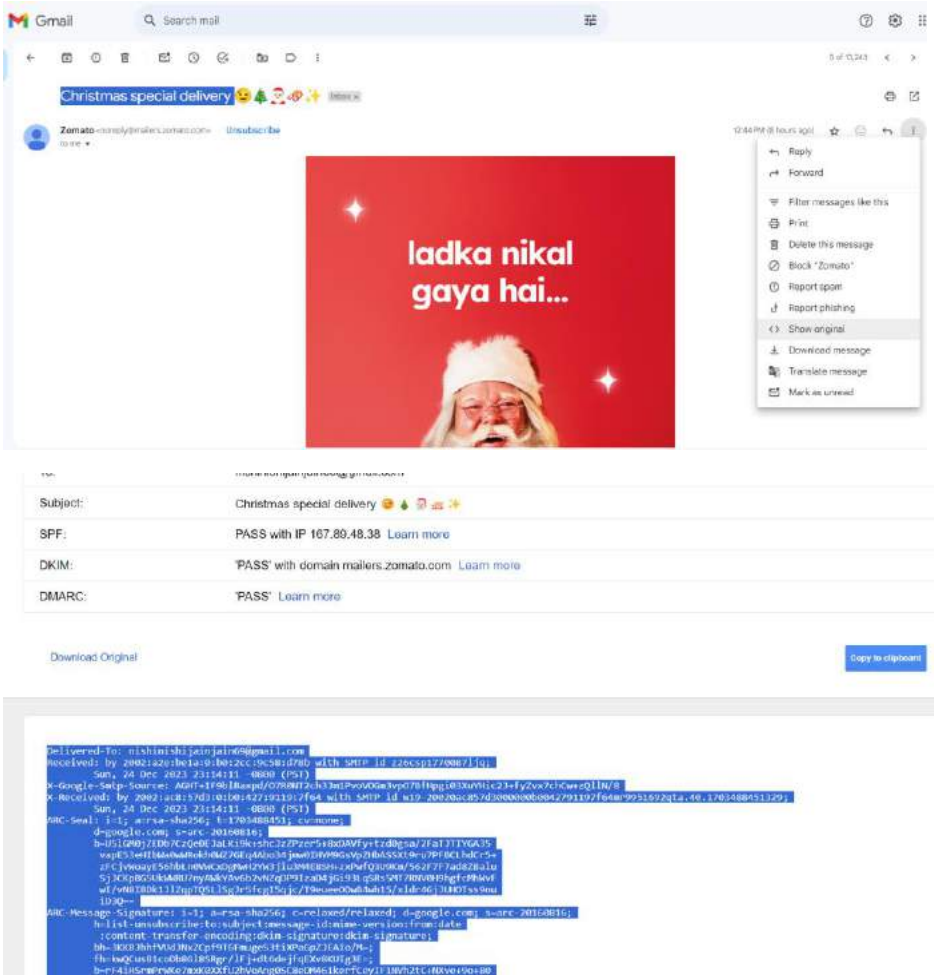
Hyena is designed to both simplify and centralize nearly all of the day-to-day management tasks. Open the software and you can see the directories.



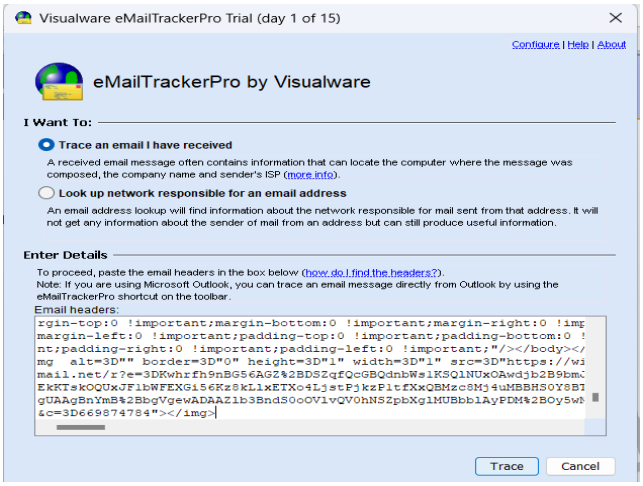
3) EmailTrackerPro

Step1: Open the application and click on I want to trace an email

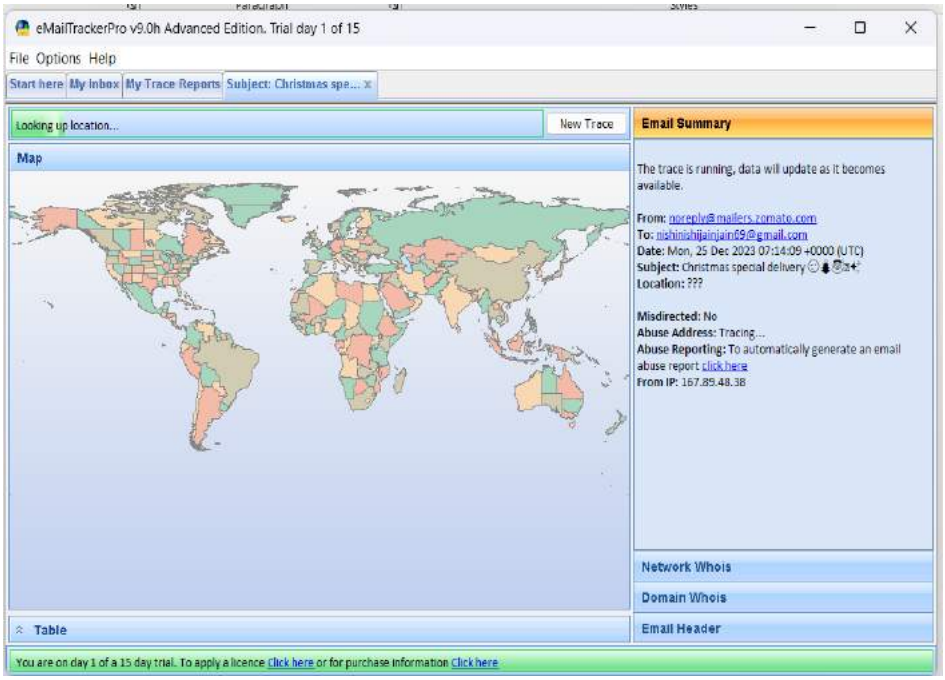
Step2: Open any email that you have received, click on 3 dots and select see original



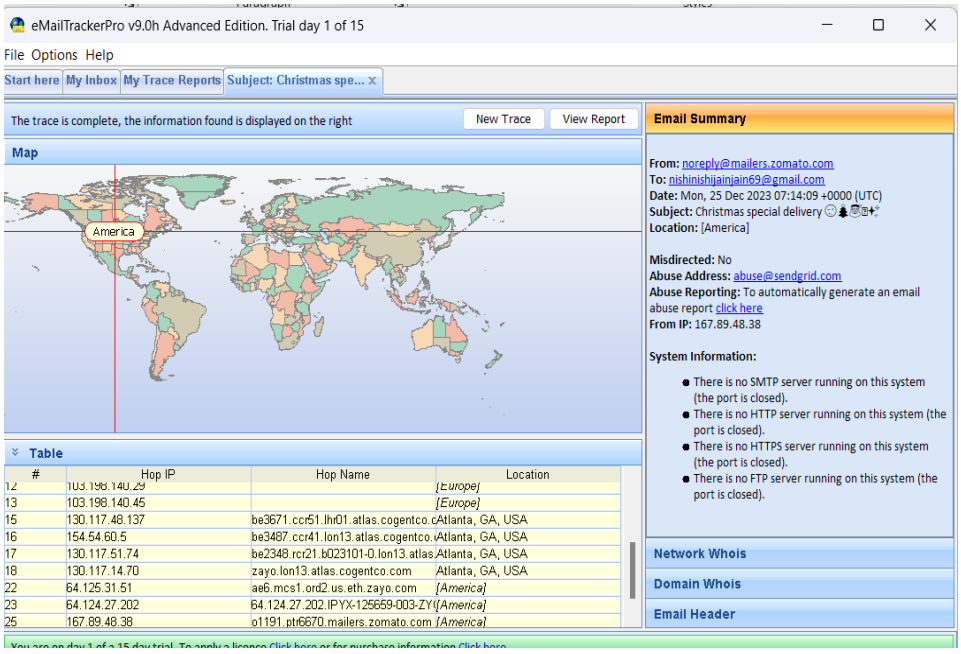
Setp3: Now copy the entire dataset it into the email headers section and click on trace



The trace has started

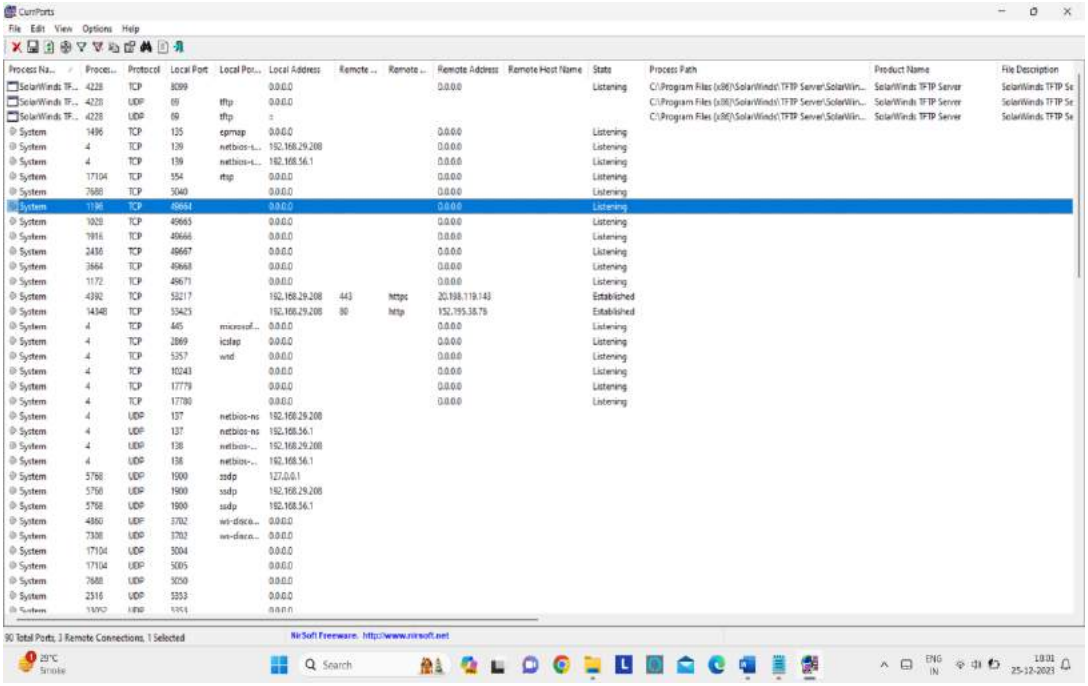


You can see the location, IP and name and network Whois

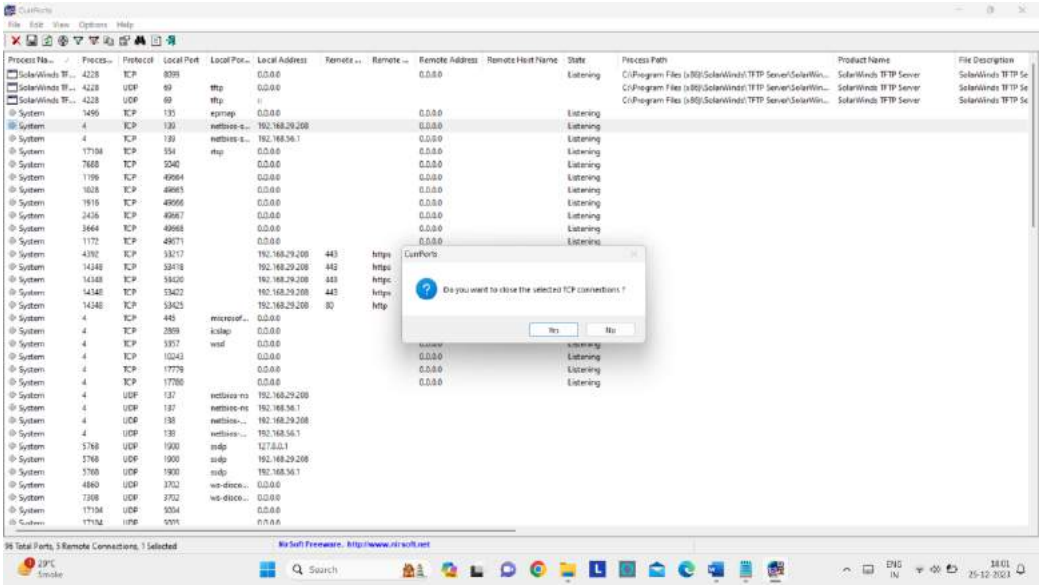


4) Currports

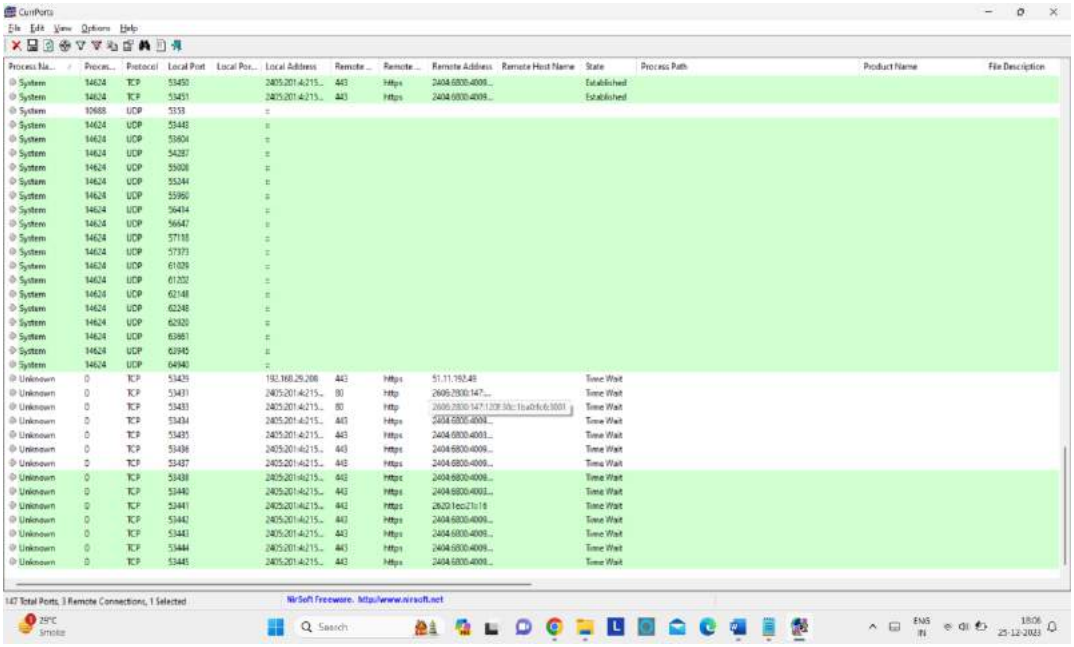
CurrPorts displays the list of all currently opened TCP/IP and UDP ports on your local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it.



In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP ports information to HTML file , XML file, or to tab-delimited text file.



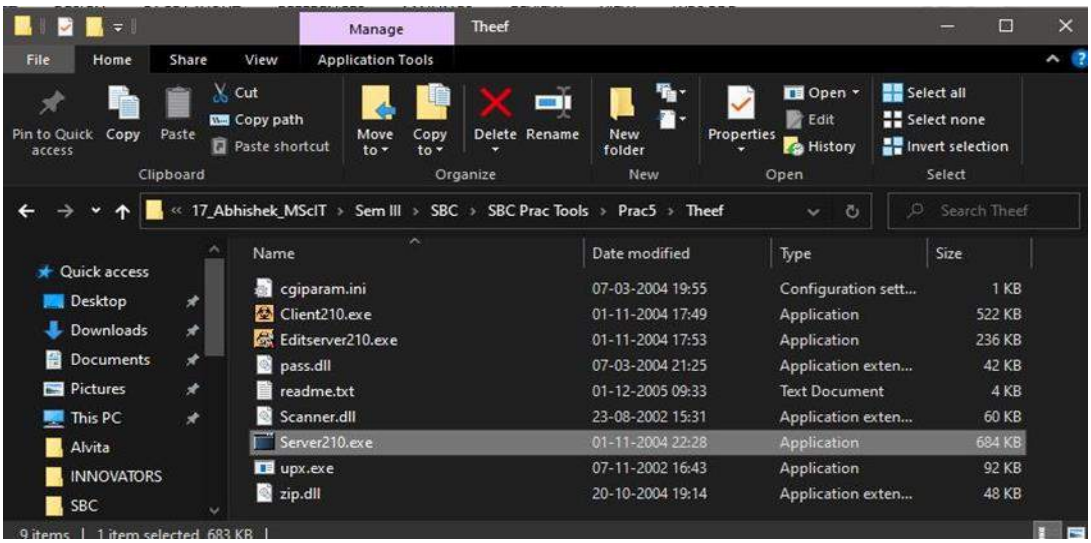
CurrPorts also automatically mark with green color for active TCP/UDP ports owned by applications



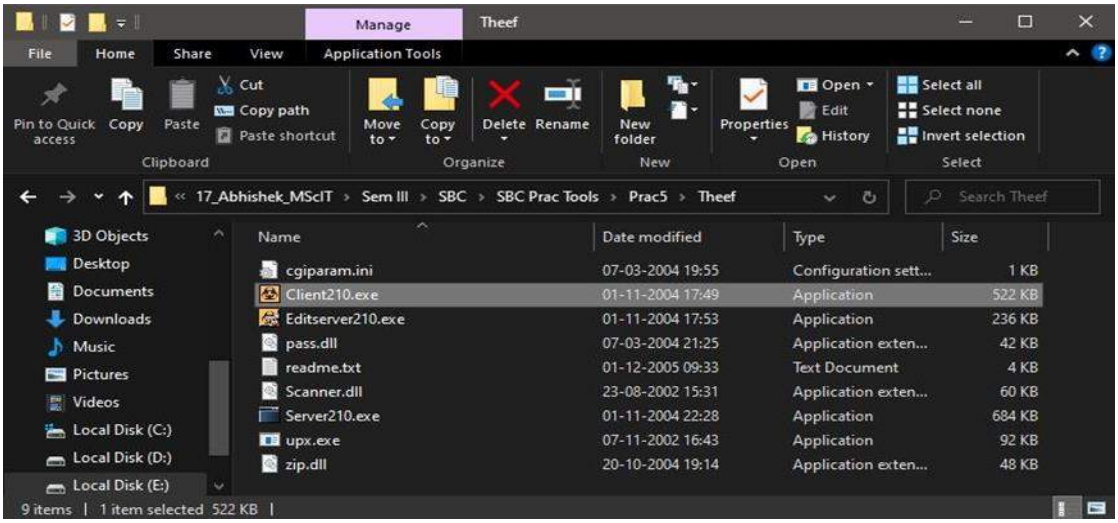
5)Theef

Theef Rat Trojan is a type of malware that is designed to infect computers and steal valuable information such as passwords, personal information, and sensitive data. This malware is known for its ability to become a rootkit, meaning it can hide itself deep within the operating system, making it very difficult for security software to detect.

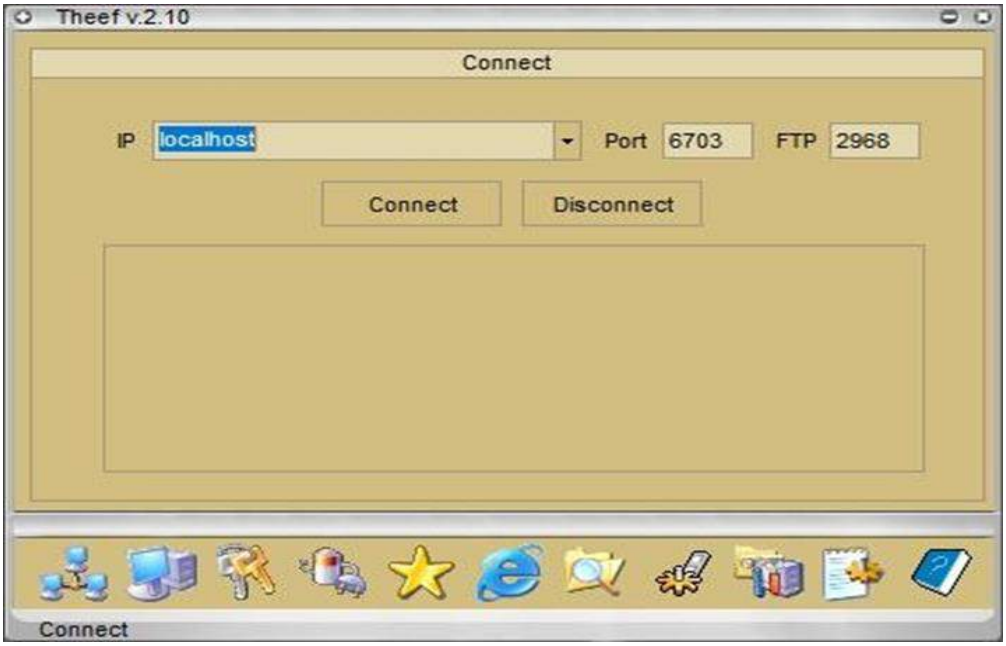
Step 1 : Double-click Server210.exe to run the Trojan.



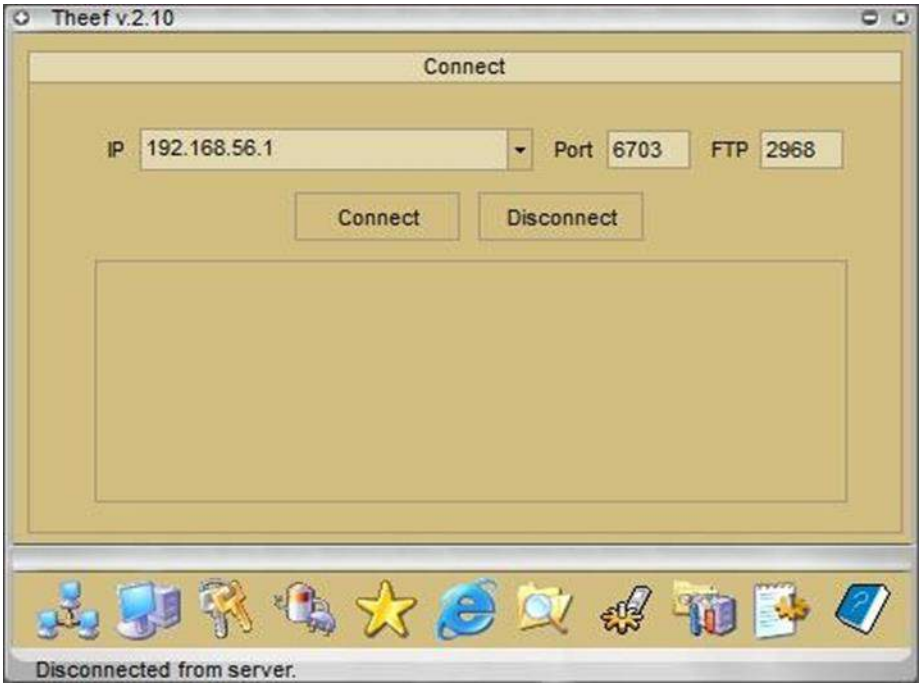
Step2: Double click on Client210.exe to access the victim machine remotely



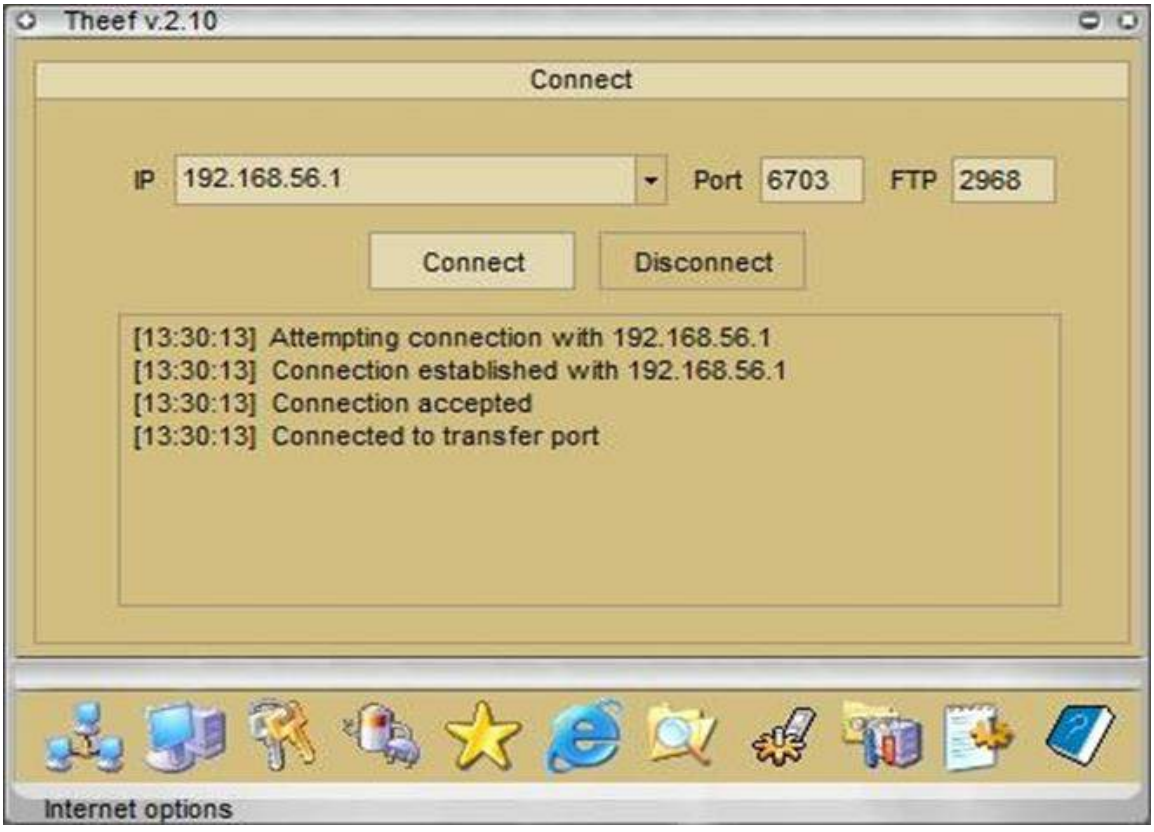
Step3: The main window of theef appears



Step 4 : Enter an IP address in the IP field, and leave the port and FTP fields as theirdefault. And then click on connect button.



Step5: Now we can have access to view the remote machine.



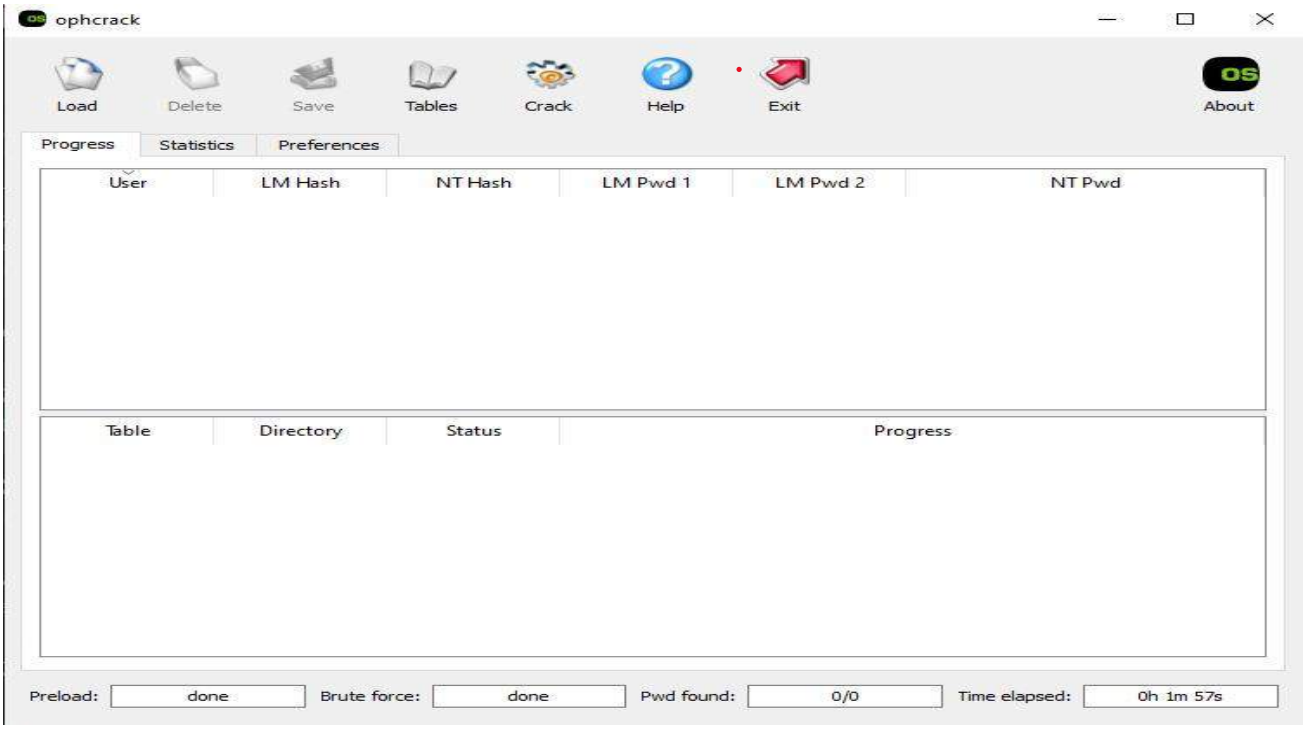
Step 6 : To view the computer information, click the computer icon at the bottom of thewindow. In Computer

Information, you are able to view PC Details, OS Info, Home, andNetwork by clicking on their respective buttons.

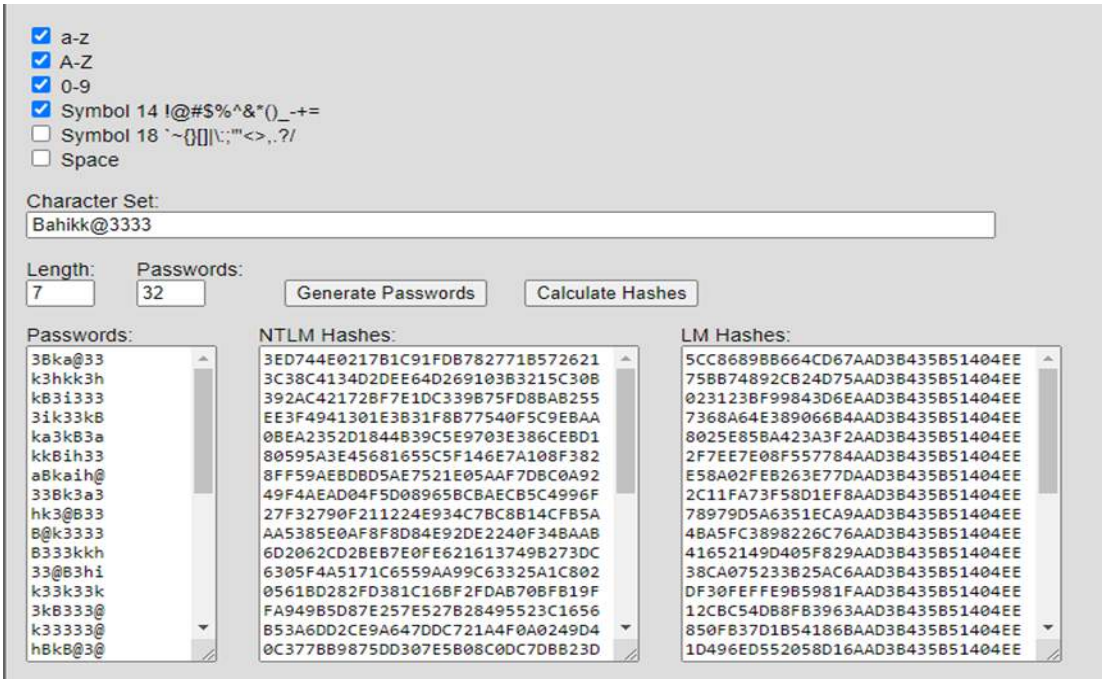
6)ophcrack

Ophcrack is an open-source password recovery tool that is designed to recover encrypted and protected password files from Windows systems. This tool works by analyzing the behavior of the password hash algorithm and can recover passwords when they're written in known formats, such as HRSMF**, LMNOPQRSTU, SMARTERPWD, and others.

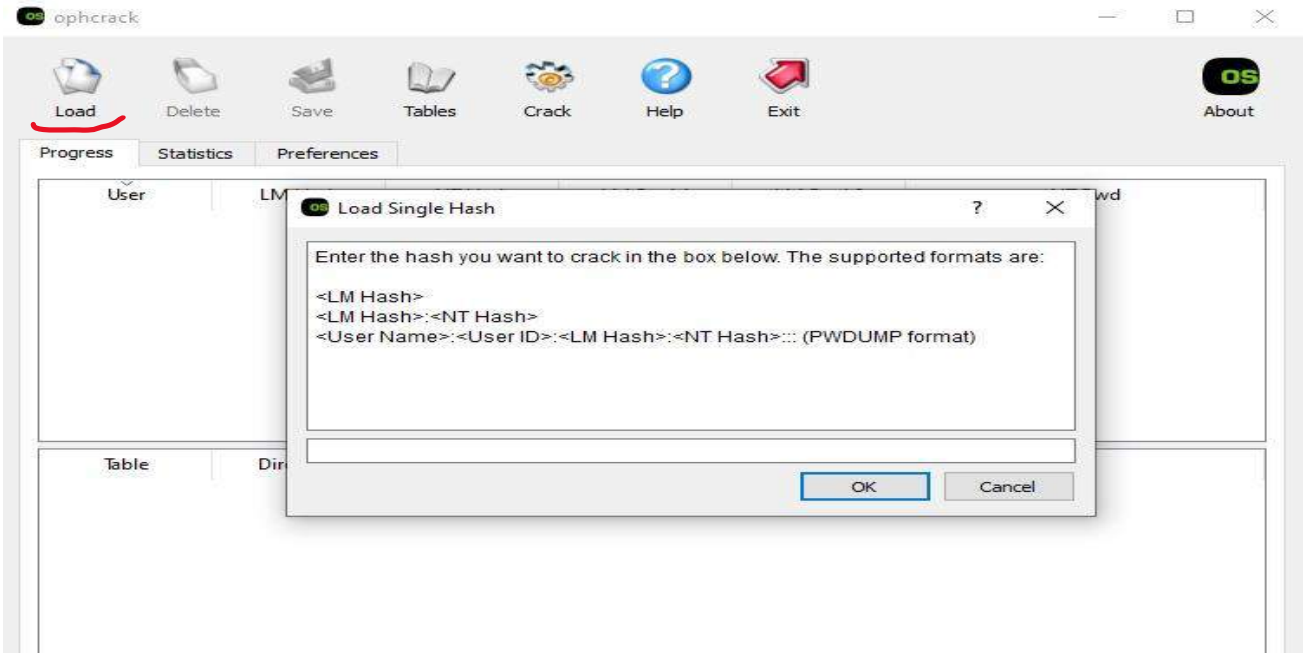
Step 1: Install and Run Ophcrack



Step 2: Now create any password and find LM hashes



Step 3: Now click on 'Load' to enter



Step4: Now click on crack to crack the password