



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)

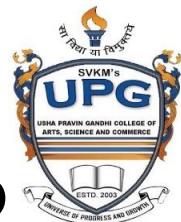
MUMBAI, 400056

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

Practical No.	Description	Page No	Sign
1.	A. Use the following tools to perform footprinting and reconnaissance		
	1) Who.is		
	2) WhatismyIPaddress		
	3) Smart Whois		
	4) Inurl:admin.php		
	5) Live camera footage		
	6) HTTrack		
	7) Tracert		
	8) eMailTracker Pro		
	9) Recon-ng (Using Kali Linux)		
	B. Scan the network using the following tools		
	1) Hping3		
	2) Angry IP Scanner		
	3) Advance IP Scanner		
	4) Colasoft Packet Builder		
	5) Megaping		
	6) DosHTTP		
	7) Kali Linux		
	8) Nmap/Zenmap		
	9) CurrPorts		
	C. Perform DDoS Attack using the following tool		
	1) Metasploit		
2.	A. Perform enumeration using the following tools		

	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:	f.jjqnyqr@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: fjjqnyqr@whoisprivacyprotect.com

Raw Whois Data

```

Domain Name: cricbuzz.com
Registry Domain ID: 317323961_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOMDOMAINS.COM
Updated Date: 2019-02-28T14:07:24.00Z
Creation Date: 2024-04-16T04:27:32.00Z
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: fjjqnyqr@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: fjjqnyqr@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: fjjqnyqr@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/WICP
>>> 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

Hostname	Type	TTL	Priority	Content
cricbuzz.com	SOA	900		ns1.softlayer.com root@cricbuzz.com 2023101901 7200 600 1728000 900
cricbuzz.com	NS	900		ns2.softlayer.com
cricbuzz.com	NS	900		ns1.softlayer.com
cricbuzz.com	A	812		35.200.167.142
cricbuzz.com	MX	900	10	alt4.aspmx.l.google.com
cricbuzz.com	MX	900	10	alt3.aspmx.l.google.com
cricbuzz.com	MX	900	5	alt2.aspmx.l.google.com
cricbuzz.com	MX	900	5	alt1.aspmx.l.google.com
www.cricbuzz.com	A	20		23.212.251.134
www.cricbuzz.com	A	20		23.212.251.137
www.cricbuzz.com	CNAME	789		www.cricbuzz.com-v1.edgekey.net

Diagnosis

```

PING cricbuzz.com (35.200.167.142) 56(84) bytes of data.
64 bytes from 142.167.200.35.bc.googleusercontent.com (35.200.167.142): icmp_seq=1 ttl=54 time=257 ms
64 bytes from 142.167.200.35.bc.googleusercontent.com (35.200.167.142): icmp_seq=2 ttl=54 time=257 ms
64 bytes from 142.167.200.35.bc.googleusercontent.com (35.200.167.142): icmp_seq=3 ttl=54 time=257 ms
64 bytes from 142.167.200.35.bc.googleusercontent.com (35.200.167.142): icmp_seq=4 ttl=54 time=257 ms
64 bytes from 142.167.200.35.bc.googleusercontent.com (35.200.167.142): icmp_seq=5 ttl=54 time=257 ms

--- cricbuzz.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 257.243/257.302/257.349/0.455 ms
  
```

```

traceroute to cricbuzz.com (35.200.167.142), 30 hops max, 60 byte packets
1 ip-10-0-0-14.ec2.internal (10.0.0.14) 0.390 ms 0.354 ms 0.395 ms
2 ec2-3-236-63-45.compute-1.amazonaws.com (3.236.63.45) 58.302 ms ec2-3-236-63-123.compute-1.amazonaws.com (3.236.63.123) 6.752 ms ec2-3-236-63-127.compute-1.amazonaws.com (3.236.63.127) 6.752 ms
3 240.0.224.65 (240.0.224.65) 0.768 ms 240.0.224.98 (240.0.224.98) 0.746 ms 240.0.224.97 (240.0.224.97) 0.810 ms
4 242.2.113.65 (242.2.113.65) 2.374 ms 242.2.113.71 (242.2.113.71) 2.055 ms 242.2.113.69 (242.2.113.69) 1.860 ms
5 240.0.236.2 (240.0.236.2) 1.532 ms 240.0.236.3 (240.0.236.3) 1.590 ms 240.0.236.1 (240.0.236.1) 1.564 ms
6 242.2.212.199 (242.2.212.199) 2.141 ms 242.2.212.67 (242.2.212.67) 1.534 ms 242.2.213.71 (242.2.213.71) 1.717 ms
7 100.100.4.86 (100.100.4.86) 1.465 ms 100.100.36.104 (100.100.36.104) 1.420 ms 100.100.34.86 (100.100.34.86) 1.629 ms
8 72.14.205.158 (72.14.205.158) 1.718 ms 99.82.181.23 (99.82.181.23) 3.794 ms 99.83.115.171 (99.83.115.171) 2.001 ms
9 142.167.200.35.bc.googleusercontent.com (35.200.167.142) 256.800 ms 257.121 ms 256.728 ms
  
```

2) What is my IP Address

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

My IP Address is:
IPv4: [202.134.156.53](#)
IPv6: [Not detected](#)

My IP Information: Your location may be exposed!
ISP: Bulk Assignment
City: Mumbai
Region: Maharashtra
Country: India

[HIDE MY IP ADDRESS NOW](#) [Show Complete IP Details](#)

Location not accurate? [Update My IP Location](#)

Step3: - enter the Ip address

IP Details For: 23.212.251.134

Decimal:	399833990
Hostname:	a23-212-251-134.deploy.static.akamaitechnologies.com
ASN:	20940
ISP:	Akamai Technologies Inc.
Services:	Datacenter
Assignment:	Likely Static IP
Country:	United States
State/Region:	Virginia
City:	Ashburn
Latitude:	39.0395 (39° 2' 22.11" N)
Longitude:	-77.4918 (77° 29' 30.50" W)

[CLICK TO CHECK BLACKLIST STATUS](#)

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from [IP2Location](#) and [IPBlock](#).

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.

The screenshot shows a search results page from a browser. The search query is "inurl:admin.php". The results list several admin panel URLs:

- DMA Softlab: <http://radmandemo.dmasoftlab.com/admin>
- Administration Control Panel**: <https://aisectfi.com/admin>
- Admin Login**: https://www.gita.edu.in/gita/admin/php/_upload
- Index of /gita/admin/php/_upload**: [Index of /gita/admin/php/_upload](https://www.gita.edu.in/gita/admin/php/_upload)
- Acunetix: <https://www.acunetix.com/vulnerabilities/web/color/>
- Collision Testimonials 'admin.php' SQL Injection (3.0)**: [Wordpress Plugin Collision Testimonials is prone to an SQL injection vulnerability because it fails to sufficiently sanitize user-supplied data before using ...](https://www.acunetix.com/vulnerabilities/web/color/)
- Sengamala Thayaar Educational Trust Women's College: <http://www.stet.edu.in/feedback/alumini/admin>
- LOGIN**: [STUDENT FEEDBACK ANALYSIS. ADMIN LOGIN. ADMIN. PASSWORD.](http://www.stet.edu.in/feedback/alumini/admin)
- Scribd: <https://www.scribd.com/doc/Admin-php>
- Admin PHP | PDF | Superuser | Html**: [Admin PHP | PDF | Superuser | Html](https://www.scribd.com/doc/Admin-php)

At the bottom of the browser window, the URL is shown as "Not secure | webapps2.ucalgary.ca/~groupii/html/admin/admin.php".

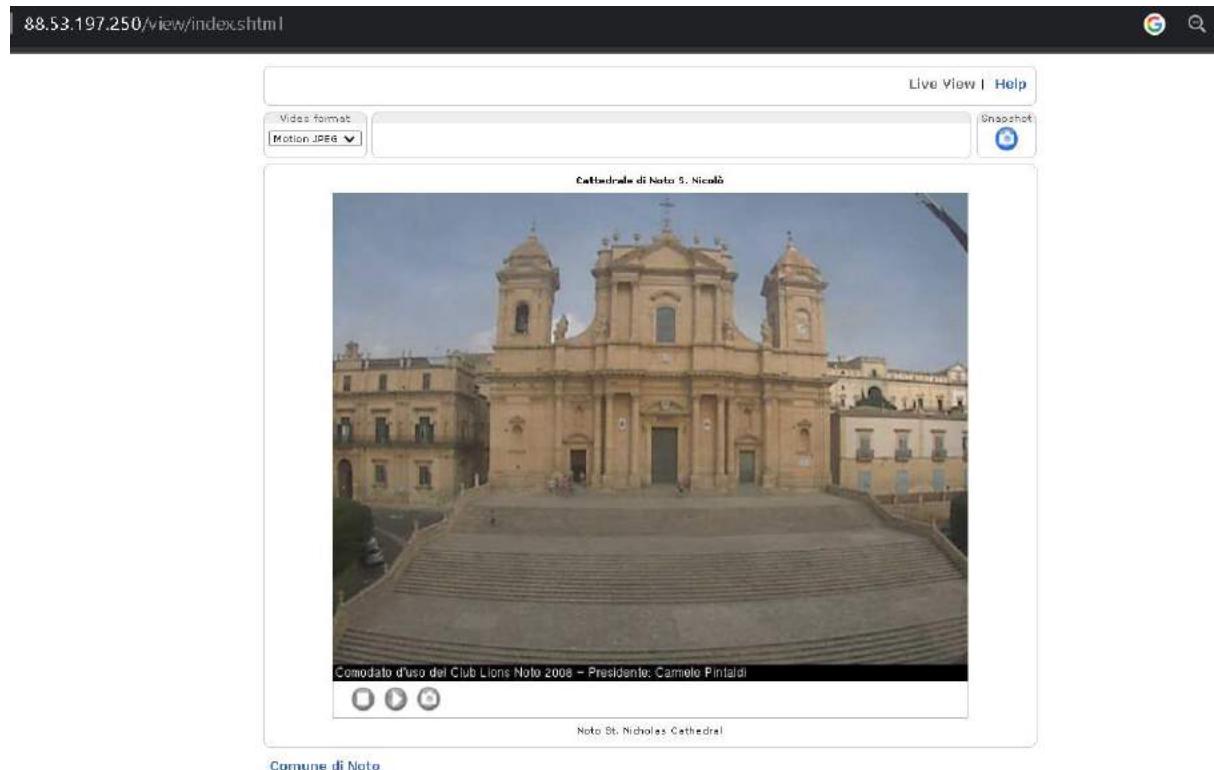
Admin's control panel

Admin shortcuts
Control panel
naming table
edit prototype
new prototype
edit class
edit twintron
edit tandem
do SQL
general
BLAST (admin)
All prototypes
Twintrons
Tandems
Log out

- [backup database to *.sql](#)
- [rebuild blast db](#)
- [add new user](#)
- [empty_dir "/tmp"](#)

4) inurl:index.shtml

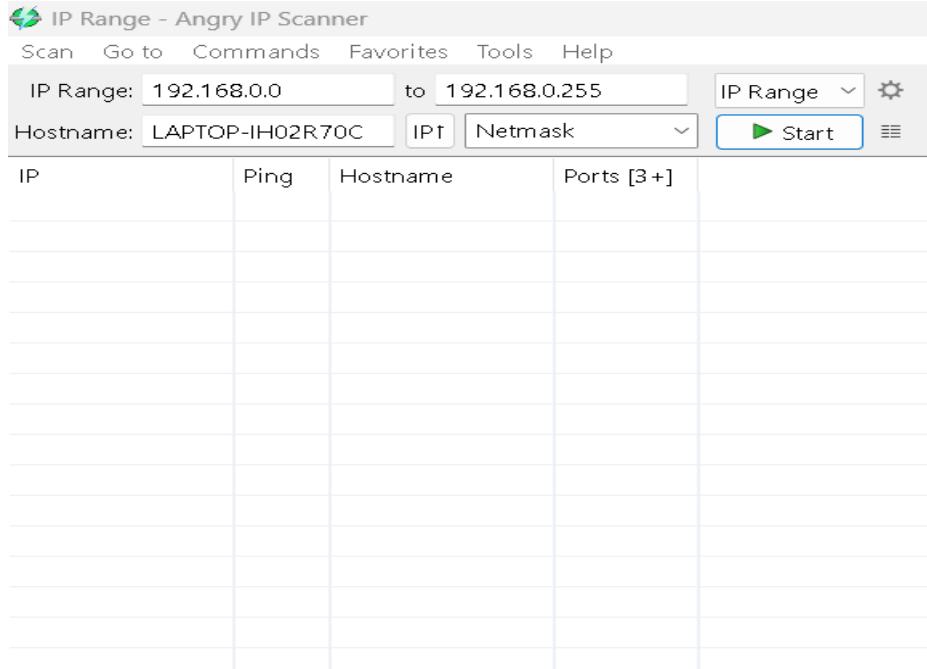
Setp1:- Enter inurl:index.shtml in the browser. It will show you the live view anywhere from the world.



Practical2

1) Angry IP Scanner

Step:- open the angry Ip scanner software

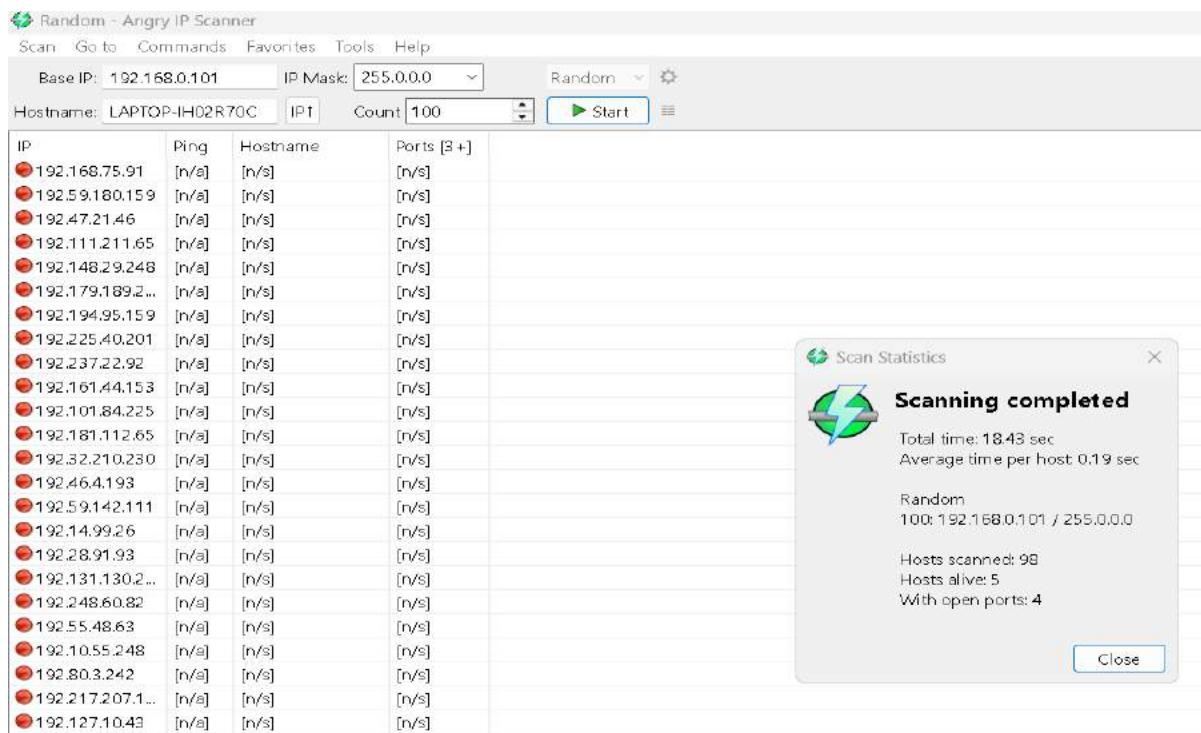


Step2: - scan for the Ip range

The screenshot shows the 'IP Range - Angry IP Scanner' application after a scan has been completed. The 'Scan' tab is selected. The 'IP Range' field contains '192.168.0.0' to '192.168.0.255'. The 'Hostname' field is set to 'LAPTOP-IH02R70C'. The 'Ports' field is set to '[3+]'. The main table displays the scan results for 254 hosts. A 'Scan Statistics' window is overlaid on the interface, showing the following details:

- Scanning completed**
- Total time: 38.34 sec
- Average time per host: 0.15 sec
- IP Range: 192.168.0.0 - 192.168.0.255
- Hosts scanned: 254
- Hosts alive: 4
- With open ports: 1

Step3: - Scan for the random Ip



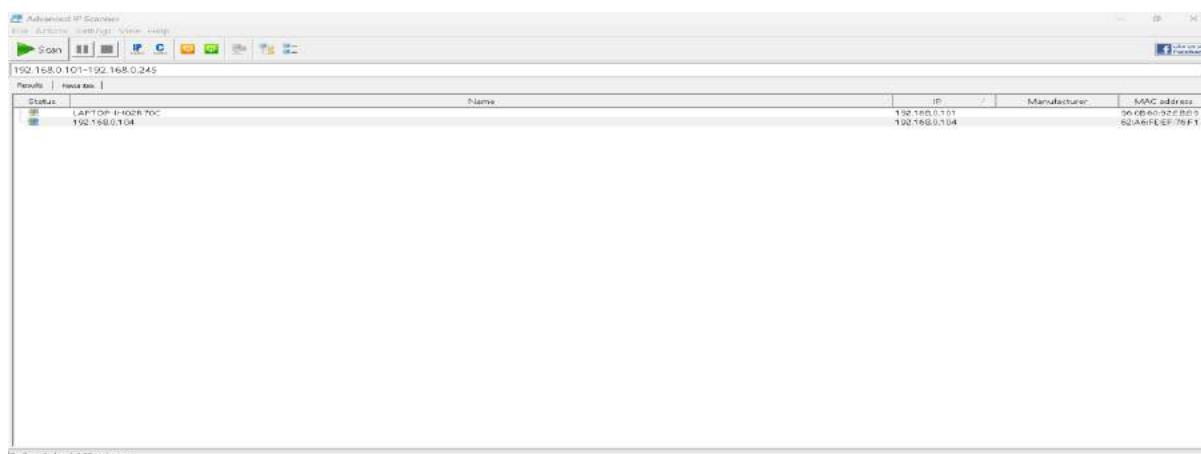
Points to note: - Red dot indicates that the host does not exists anymore, Blue dot indicates that the host is alive but is not active currently and Green dot indicates that the host is alive as well as it is currently active.

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

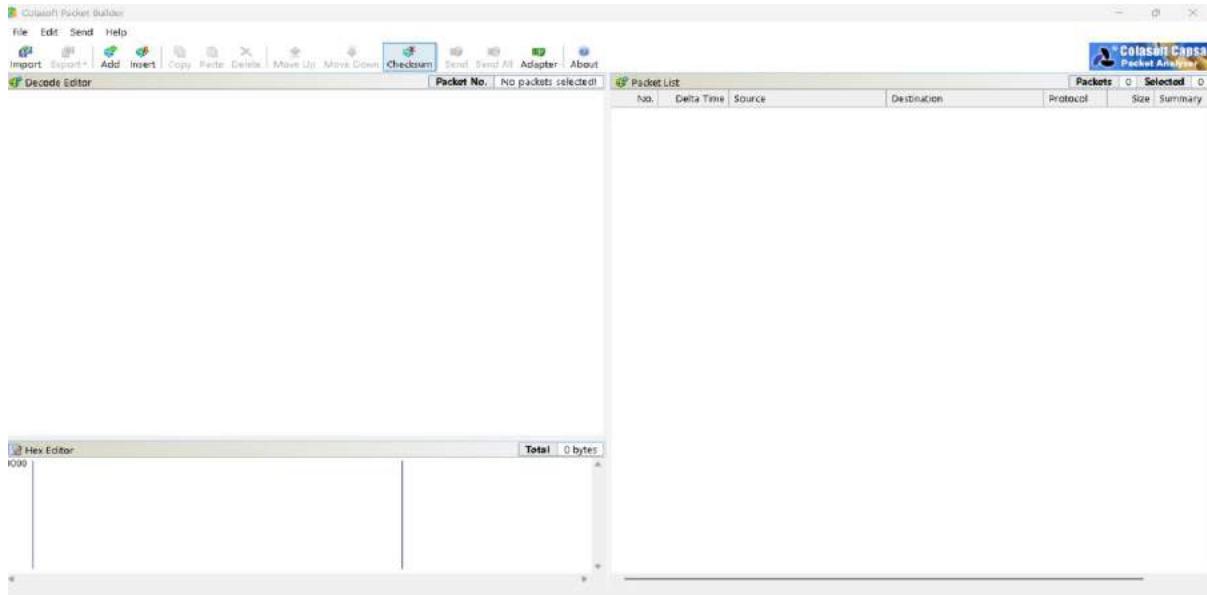




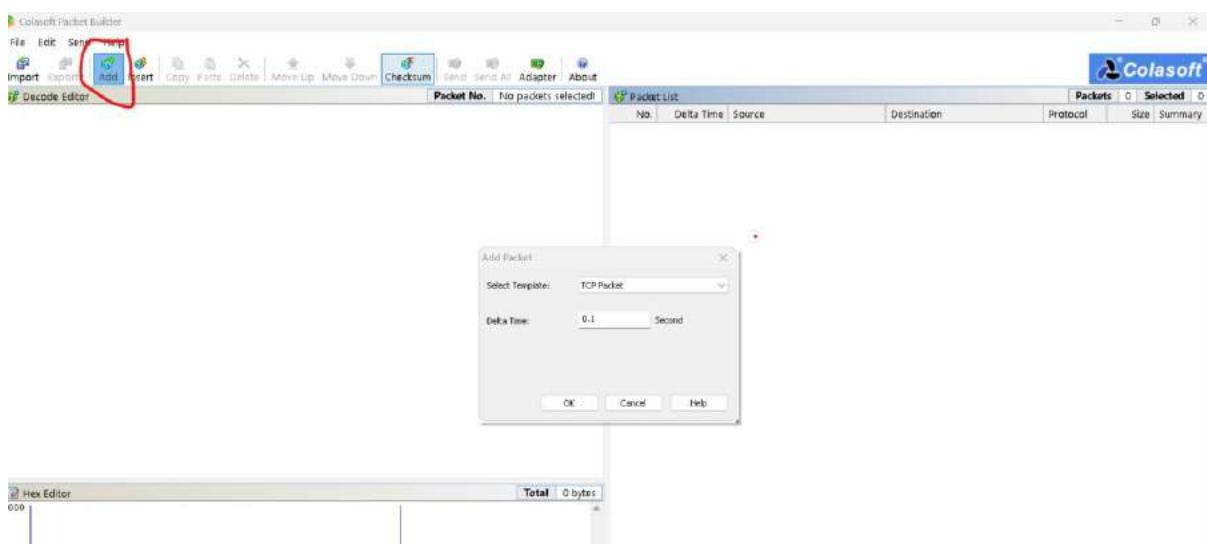
3)Colasoft Packet Builder

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.

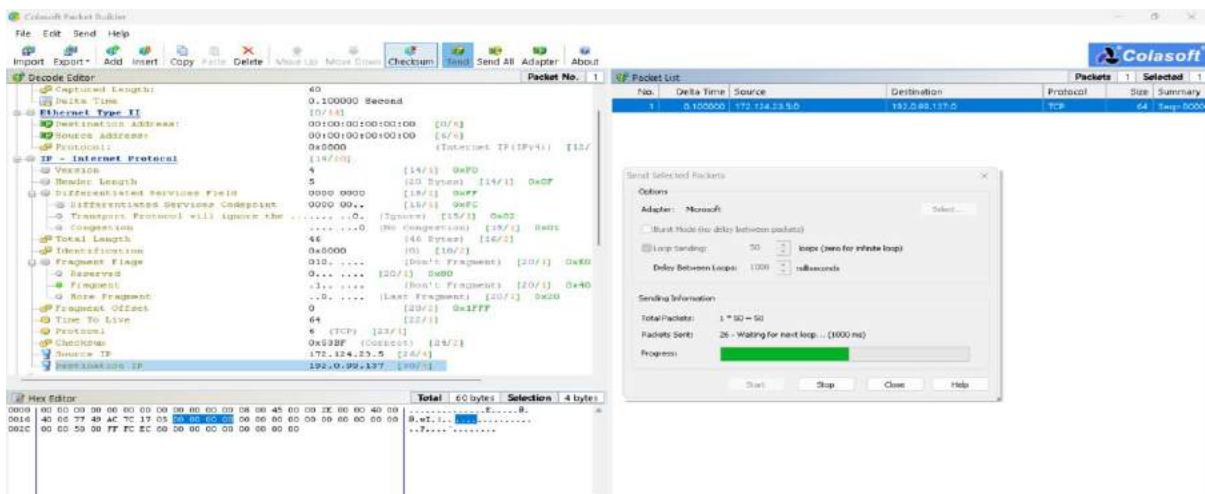
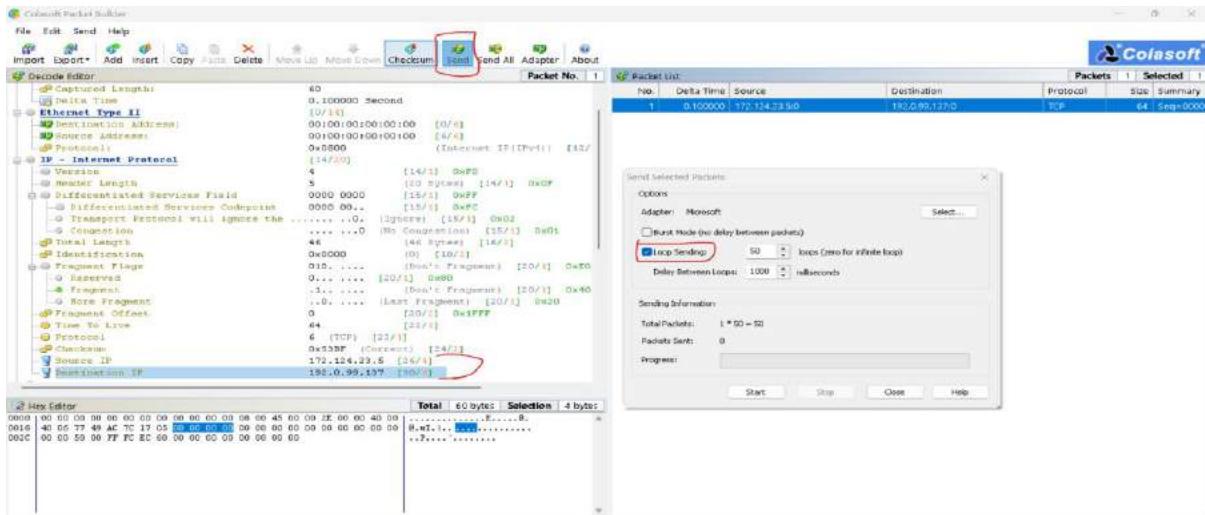
Step1: - Open the colasoft software



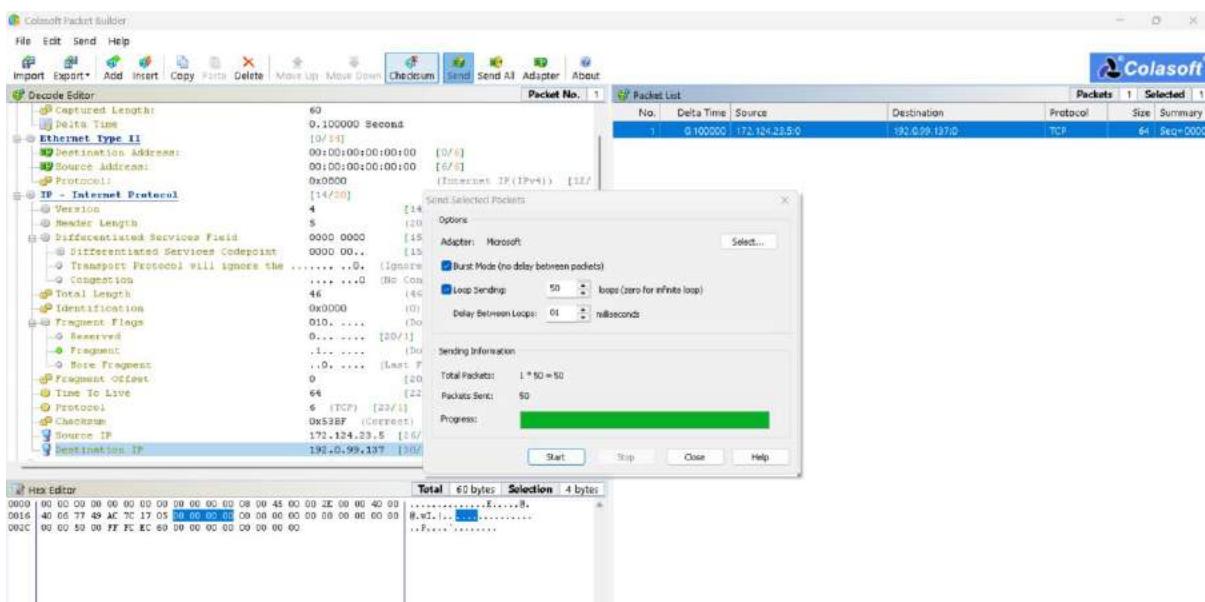
Step2:- click on the add option – select templet and click ok



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.



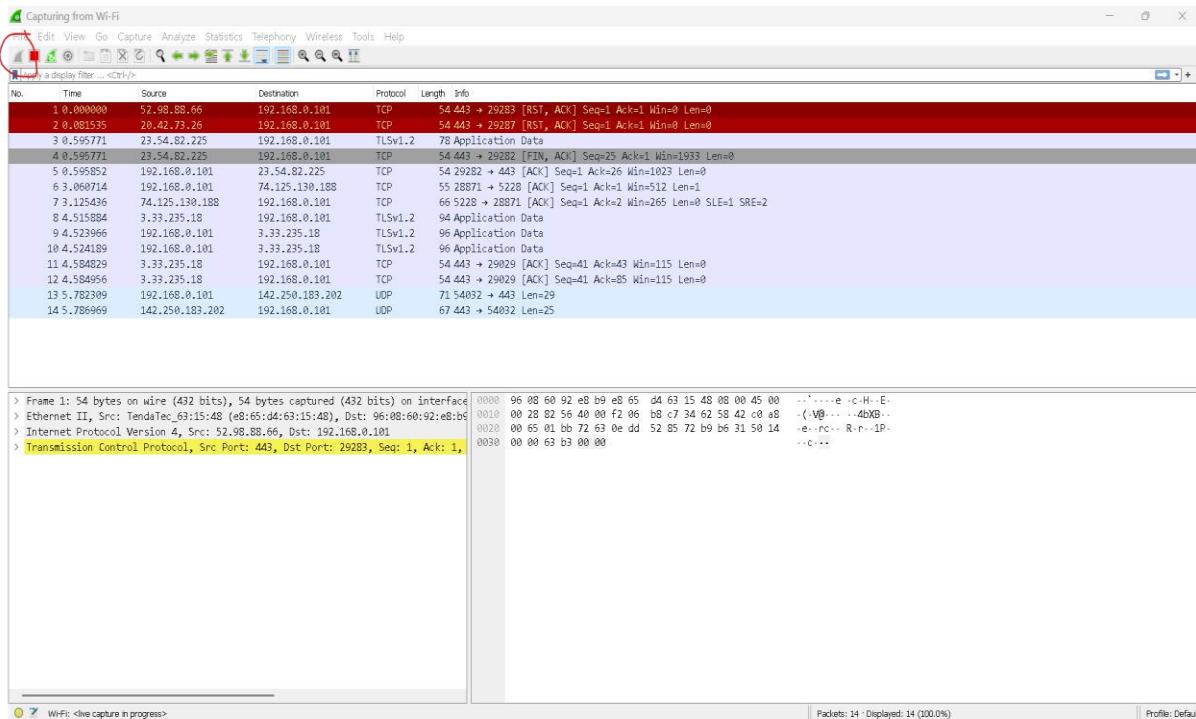
Step4: - You can also use the burst mode



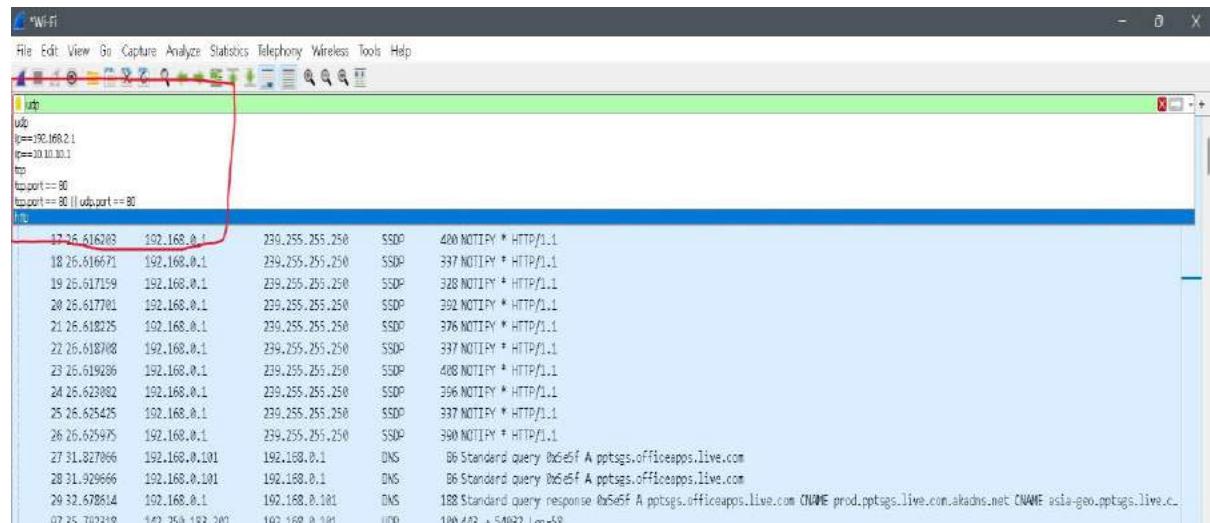
4) Wireshark

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.

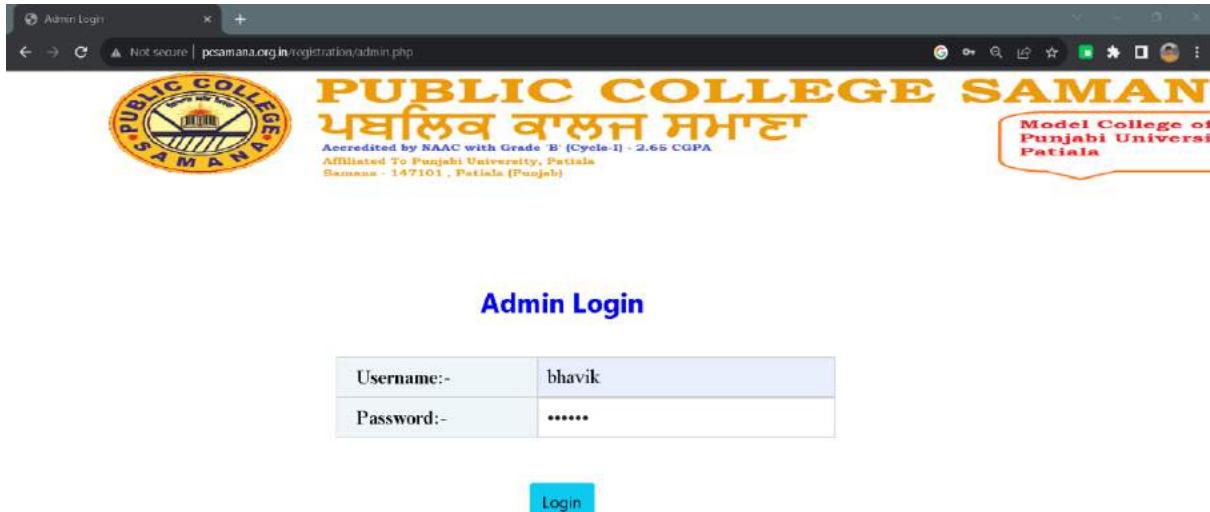
Step: -1 Open the Wireshark software and click on start. This will scan all the traffics which is travelling in your network.



Step2: - Now you can use different filters



STEP3: - In browser search for `inurl:admin.php` and open any website which has `http ->` and try to 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

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <|>>

No	Time	Source	Destination	Protocol	Length	Info
6111	26.398420	10.200.10.85	203.193.166.42	HTTP	794	POST /registration/admin.php HTTP/1.1 (application/x-www-form-urlencoded)
6112	26.402677	203.193.166.42	10.200.10.85	TCP	66	80 → 6526 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1382 WS=256 SACK_PERM
6113	26.402798	10.200.10.85	203.193.166.42	TCP	54	6526 → 80 [ACK] Seq=1 Ack=1 Window=66304 Len=0
6114	26.415480	MegaTel_00:2b:8d	Broadcast	ARP		56 who has 10.200.129.177? Tell 10.200.131.84
6115	26.416855	IntelCor_6f:48:5c	Broadcast	ARP		56 who has 10.200.190.12? Tell 10.200.138.237
6116	26.417930	IntelCor_e6:aa:a3	Broadcast	ARP		56 who has 10.200.53.200? Tell 10.200.11.52
6117	26.422121	10.200.129.25	10.200.191.255	UDP	62	2008 → 2088 Len=20
6118	26.423138	10.200.129.25	10.200.191.255	UDP	62	2007 → 2087 Len=20
6119	26.444805	10.200.126.219	10.200.127.255	NBNS	92	Name query NB MAC-461E50<00>
6120	26.451974	IntelCor_e6:aa:a3	Broadcast	ARP		56 who has 10.200.53.201? Tell 10.200.11.52
6121	26.454832	IntelCor_e6:aa:a3	Broadcast	ARP		56 who has 10.200.53.202? Tell 10.200.11.52
6122	26.466188	IntelCor_e6:aa:a3	Broadcast	ARP		56 who has 10.200.53.204? Tell 10.200.11.52
6123	26.467942	IntelCor_e6:aa:a3	Broadcast	ARP		56 who has 10.200.53.205? Tell 10.200.11.52
6124	26.470888	IntelCor_e6:aa:a3	Broadcast	ARP		56 who has 10.200.53.206? Tell 10.200.11.52
6125	26.473908	IntelCor_e6:aa:a3	Broadcast	ARP		56 who has 10.200.53.207? Tell 10.200.11.52
6126	26.477173	203.193.166.42	10.200.10.85	TCP	1438	80 → 6527 [ACK] Seq=1 Ack=741 Win=16384 Len=1382 [TCP segment of a reassembled PDU]
6127	26.482093	203.193.166.42	10.200.10.85	TCP	1438	80 → 6527 [ACK] Seq=1381 Ack=741 Win=16384 Len=1382 [TCP segment of a reassembled PDU]
6128	26.482158	10.200.10.85	203.193.166.42	TCP	54	6527 → 80 [ACK] Seq=741 Ack=2765 Win=66304 Len=0

> Frame 6111: 794 bytes on wire (6352 bits), 794 bytes captured (6352 bits) on interface
 > Ethernet II, Src: Liteon792:d2:b9 (94:08:53:92:d2:b9), Dst: Cisco_ff:fc:50 (08:00:27:ff:fc:50)
 > Internet Protocol Version 4, Src: 10.200.10.85, Dst: 203.193.166.42
 > Transmission Control Protocol, Src Port: 6527, Dst Port: 80, Seq: 1, Ack: 1, Len: 6352
 > Hypertext Transfer Protocol
 ✓ HTML Form URL Encoded: application/x-www-form-urlencoded
 ▾ Form item: "login" = "
 Key: login
 Value:
 ▾ Form item: "username" = "bhavik"
 Key: username
 Value: bhavik
 ▾ Form item: "password" = "bhavik"
 Key: password
 Value: bhavik

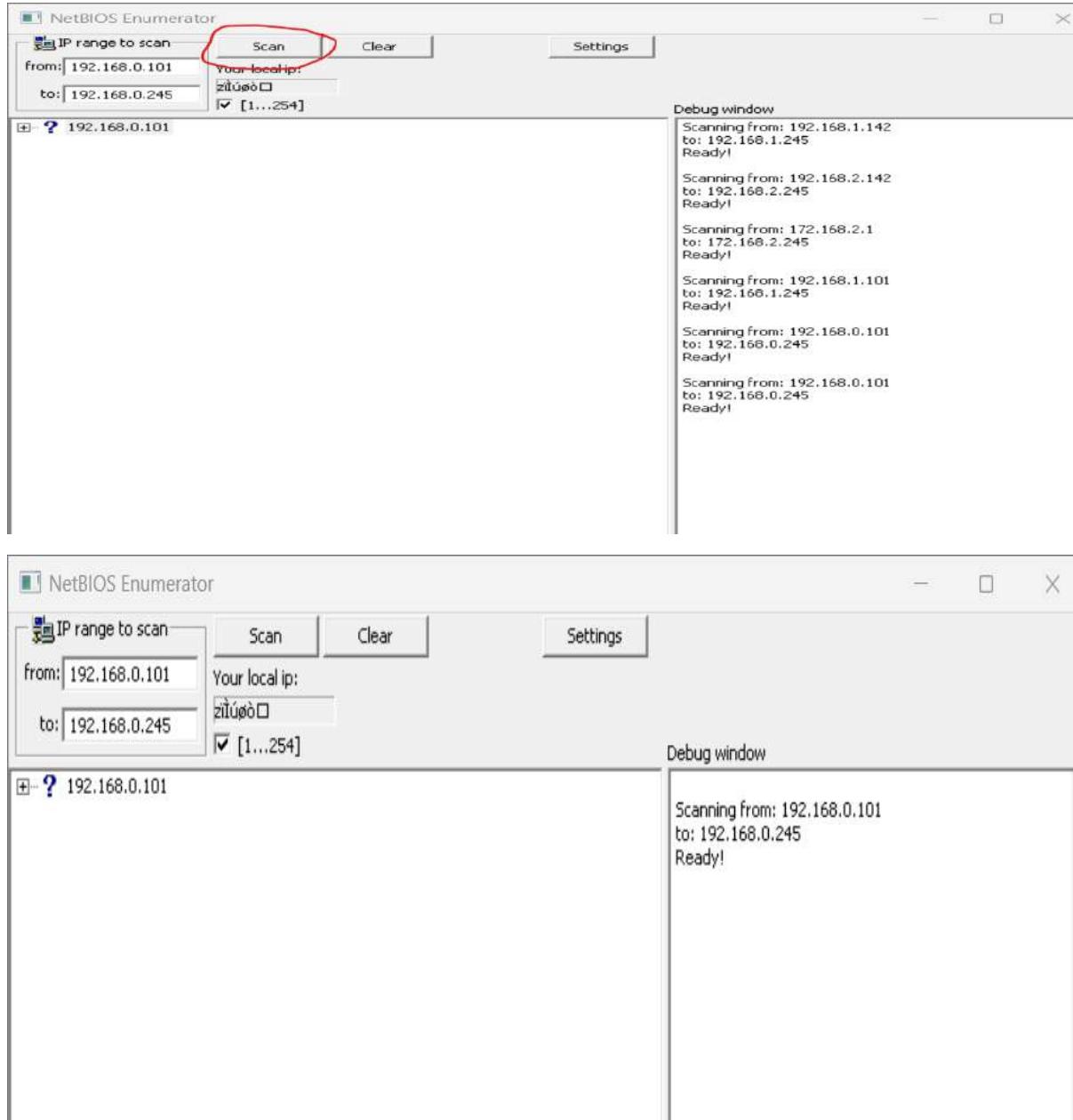
0110: 69 6f 6e 2f 78 69 74 6d 6c 2b 78 64 6c 2c 61 70 ion/xhtml1+xml.ap
 0111: 78 6c 69 63 61 74 69 6f 6e 2f 78 64 6c 3b 71 3d plication/n/xml+ap
 0112: 6d 61 67 65 2f 77 69 62 79 2c 69 64 61 67 65 2f 8.0,image/avif,1
 0210: 48 26 49 2c 63 61 67 65 2f 81 78 69 66 2c 69
 0209: 6d 61 67 65 2f 77 69 62 79 2c 69 64 61 67 65 2f mega/web,p,image/
 0211: 61 78 6c 67 2c 2a 2f 2a 3b 71 3c 30 2c 38 2c 61 apng,*/*;q=0.8,a
 0212: 70 78 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6c 65 pplication/signa
 0213: 64 2d 65 78 63 68 61 6e 67 65 62 76 3d 62 33 3b d-exchan ge;v=b3;
 0214: 71 3d 38 2c 37 0d 0a 52 65 66 65 72 65 72 3d 20 q=0.7 .R eferer:
 0215: 68 74 74 70 3c 2f 2f 77 77 2c 70 63 73 61 6d http://www.pcson
 0216: 61 6e 61 2c 6f 72 67 2e 69 6e 2f 72 65 67 69 73 ana.org.in/regis
 0217: 74 72 61 74 69 6f 6e 2f 61 64 66 69 6e 2c 70 68 tration/admin.ph
 0218: 70 0d 8a 41 63 63 69 70 74 2d 4c 6e 63 6f 64 69 p-Acces t-Encoding
 0219: 6e 67 3a 2c 67 74 69 70 2c 28 64 65 66 6c 61 74 ng:gzip , deflate
 0220: 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 e-Acces t-Language
 0221: 67 65 3a 2c 65 66 2d 55 53 2c 05 6e 3b 71 3d 30 65: en-US;q=0.9
 0222: 2e 39 0d 0a 43 6f 6b 69 65 3a 2c 50 49 50 53 ,9-Cool ie:PHPS
 0223: 45 53 53 29 44 3d 69 39 37 33 6b 62 33 6b 33 37 ESS3219 73kb3k7
 0224: 38 31 63 71 39 71 35 72 71 3c 6a 64 68 61 64 30 Nic945f qjchaj0
 0225: 6d 0d 8d 0a 6c 6f 67 69 6e 3d 26 75 73 65 72 6e ---log in-&usern
 0300: 61 6d 65 3d 62 68 61 76 69 0d 26 70 61 73 73 77 am=bhav ik-&passw
 0310: 6f 72 64 3d 62 68 61 76 69 6b orde=bhav ik

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.

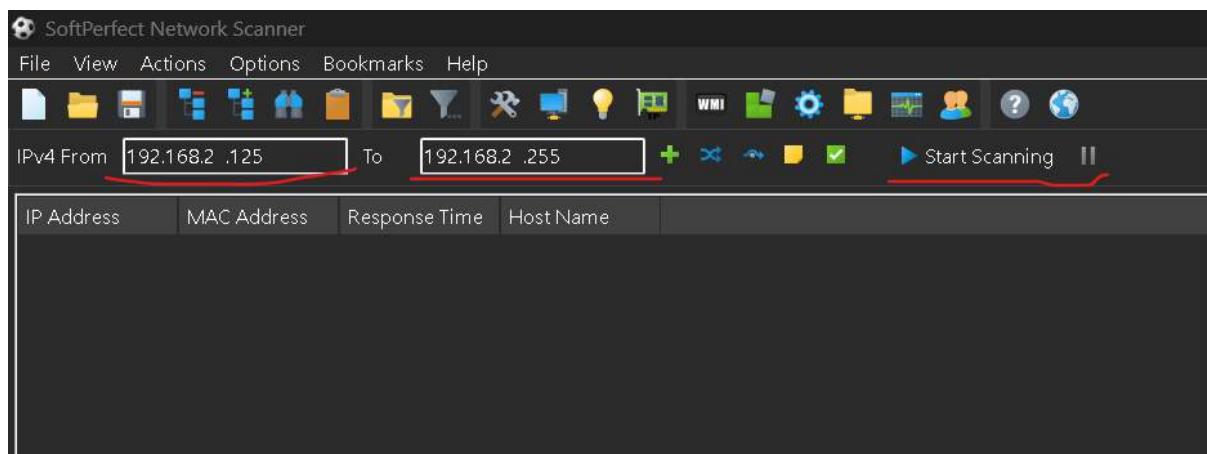
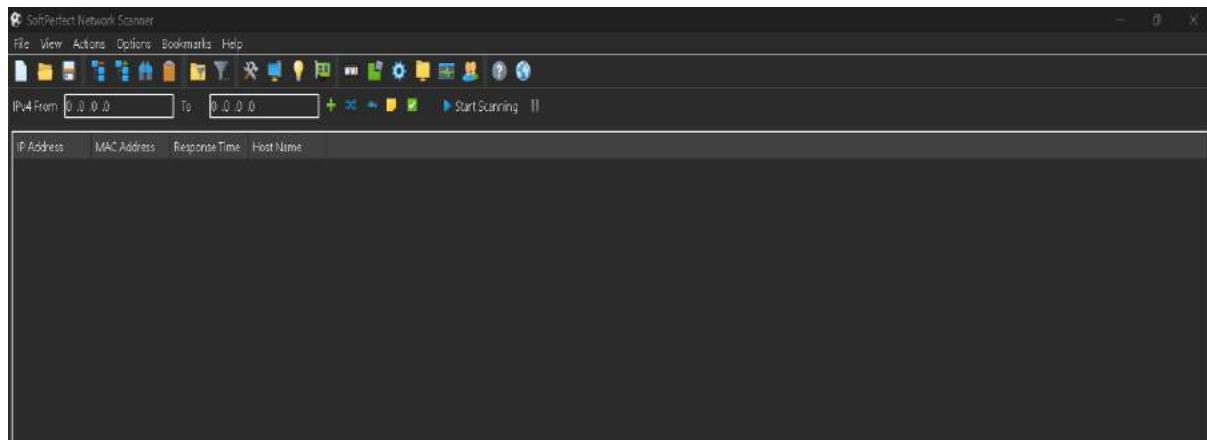
Step1: - pen the netbios enumeration tool -> enter the ip range you want to scan and press scan.



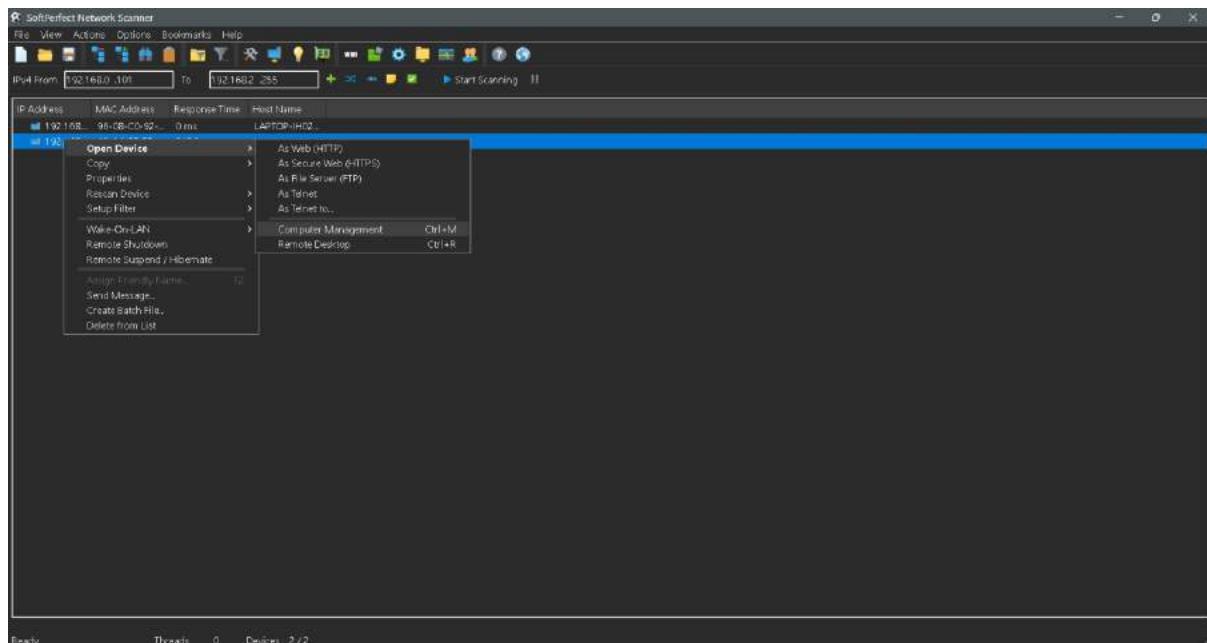
2) SoftPerfect Network Scanner

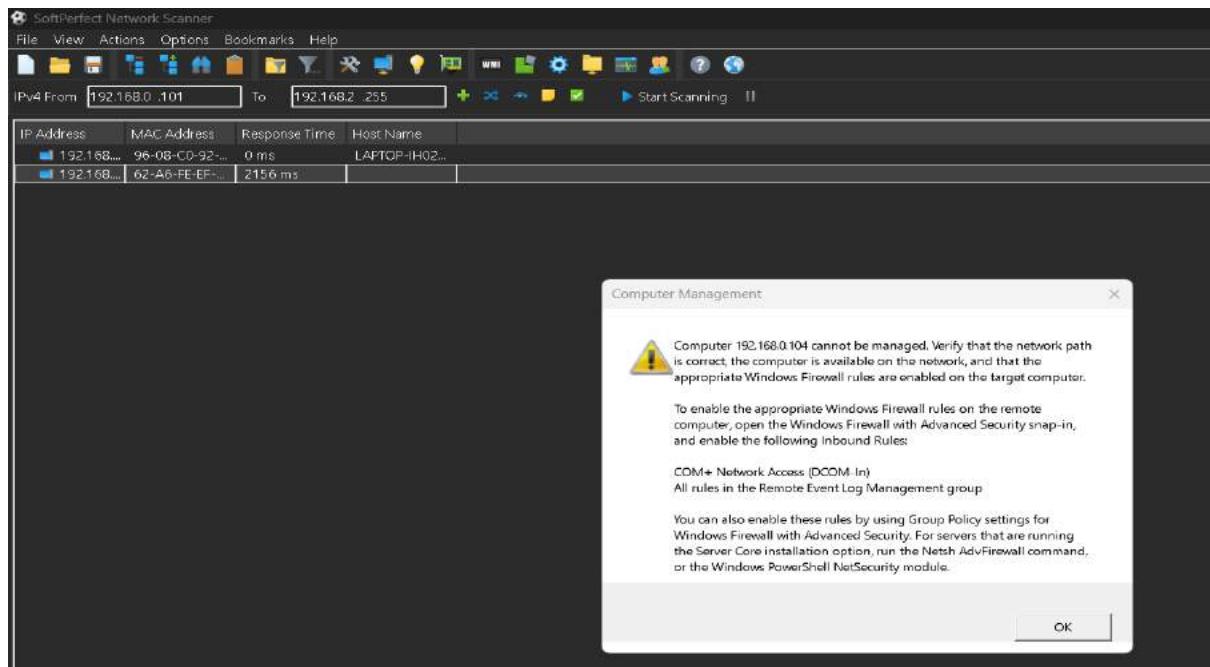
SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices via WMI, SNMP, HTTP, SSH and PowerShell. It also scans for remote services, registry, files and performance counters.

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



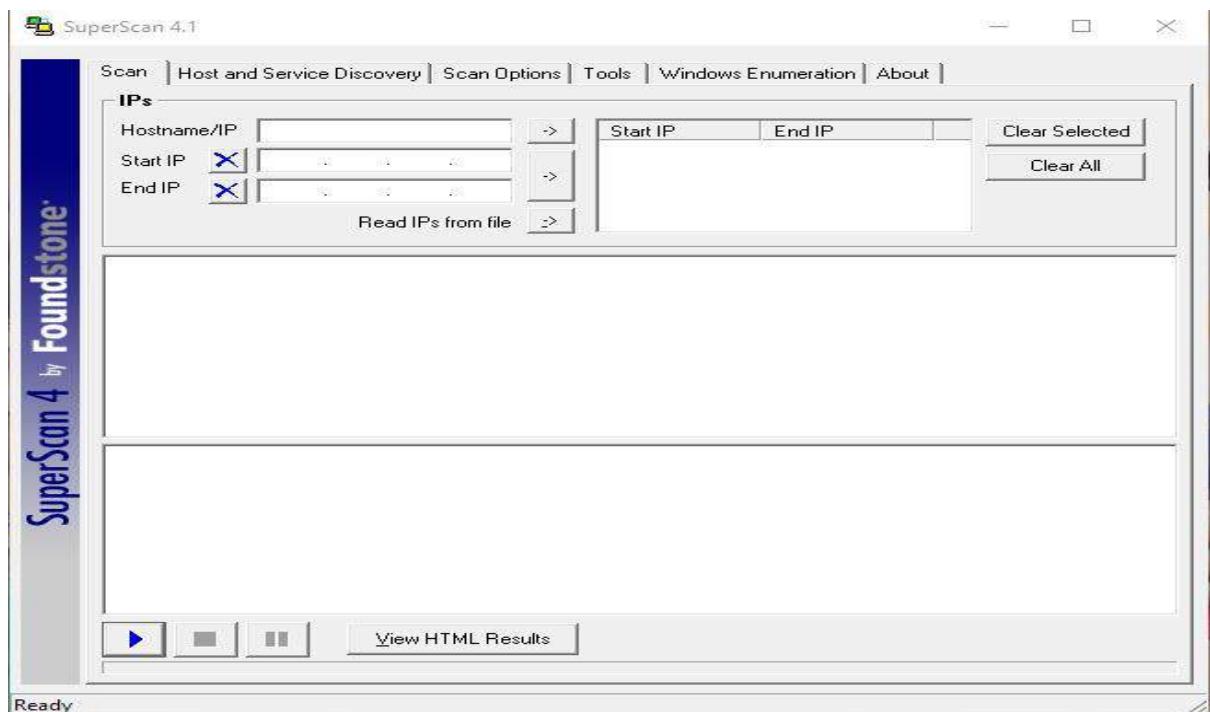
Step 2: - Right click on the IP address click on “Open computer” option and click on “ComputerManagement” in that.



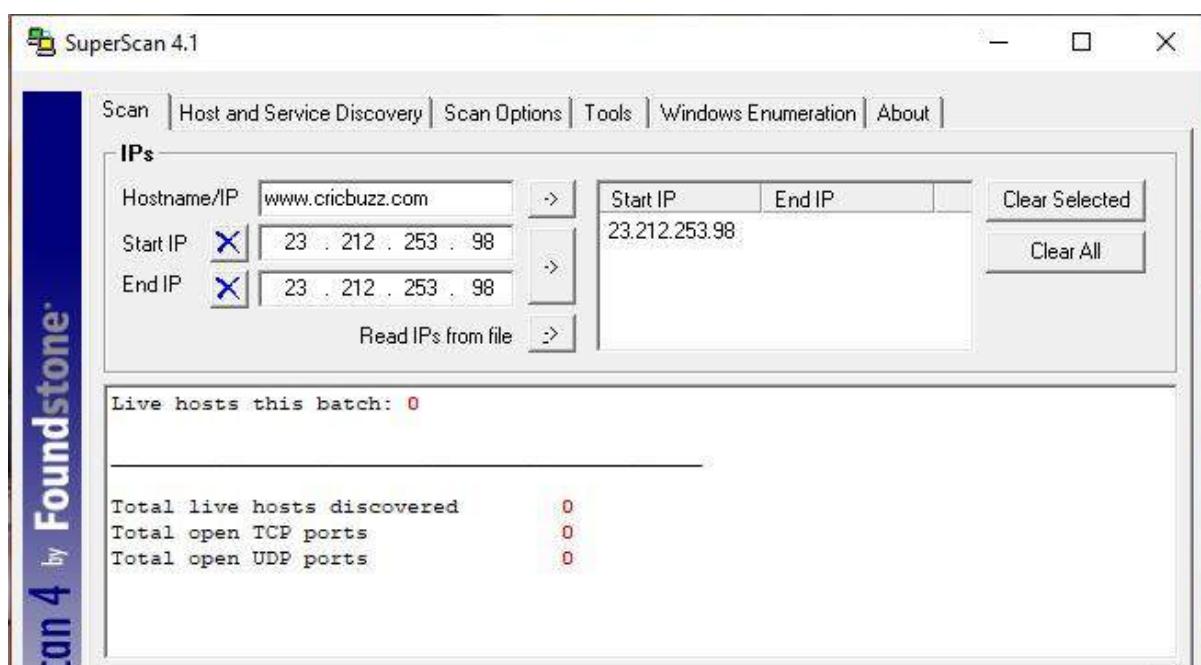


3) Superscan

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 crizzbuzz.com -> enumeration

The screenshot shows the SuperScan 4.1 interface with the following details:

- Toolbar: Scan, Host and Service Discovery, Scan Options, Tools, Windows Enumeration, About.
- Input Field: Hostname/IP/URL: www.cricbuzz.com
- Buttons: Enumerate, Options...

The main window displays the following enumeration results:

- 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

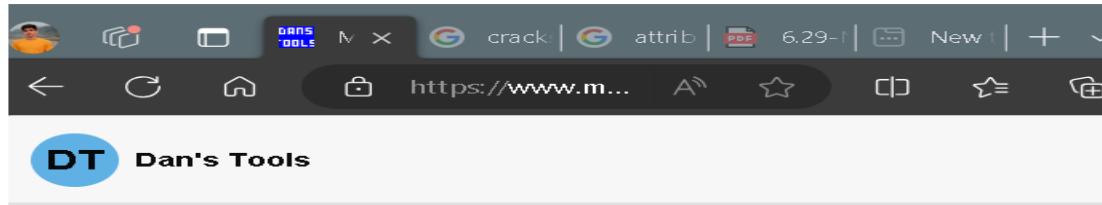
- Drives on 23.212.253.98
- Trusted Domains on 23.212.253.98
- Remote services on 23.212.253.98
- Remote registry items on 23.212.253.98

- 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.



MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Bhavik2121

Generate →

This MD5 hash generator is useful for encoding passwords, credit cards number

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Bhavik2121

Generate →

Your String	Bhavik2121
MD5 Hash	5cb031519fde310b43aa8bca8278dfcf <input type="button" value="Copy"/>
SHA1 Hash	d5b2faabf10ef8bd02a5f3ceb77530a4b119bb09 <input type="button" value="Copy"/>

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.

CrackStation & Password Hashing Security & Defuse Security &

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
scb031519fde310b43aa0bc0a0278dfcf
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha304, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), Qubesv3.1BackupDefaults

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

CrackStation & Password Hashing Security & Defuse Security &

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
scb031519fde310b43aa0bc0a0278dfcf
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha304, sha512, ripemd160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), Qubesv3.1BackupDefaults

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

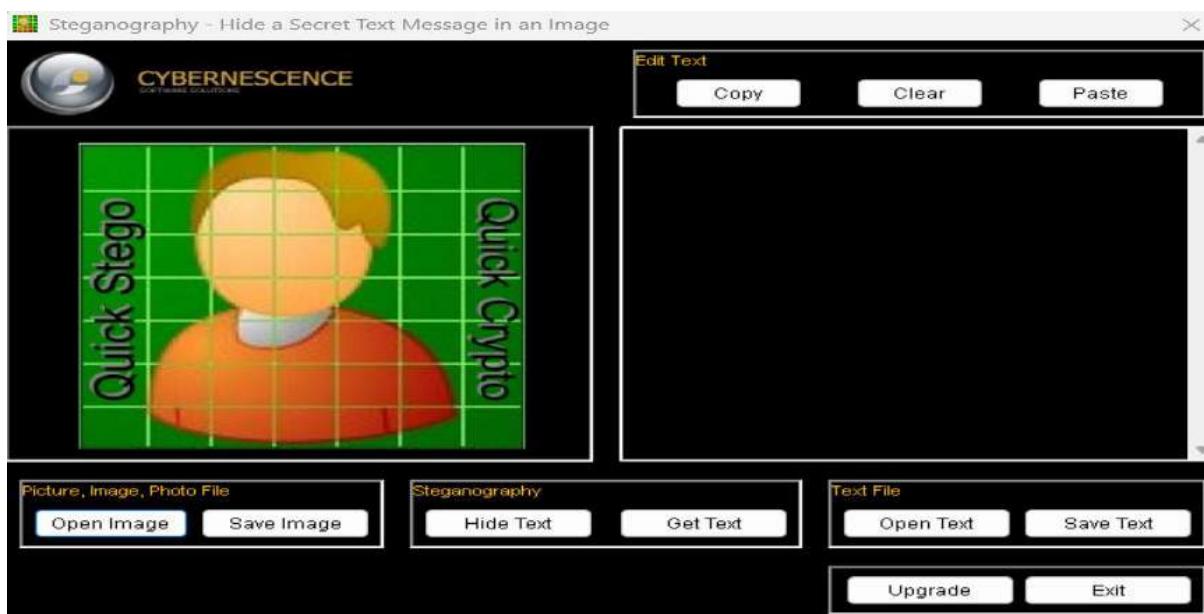
Hash	Type	Result
scb031519fde310b43aa0bc0a0278dfcf	Unknown	Both Found

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

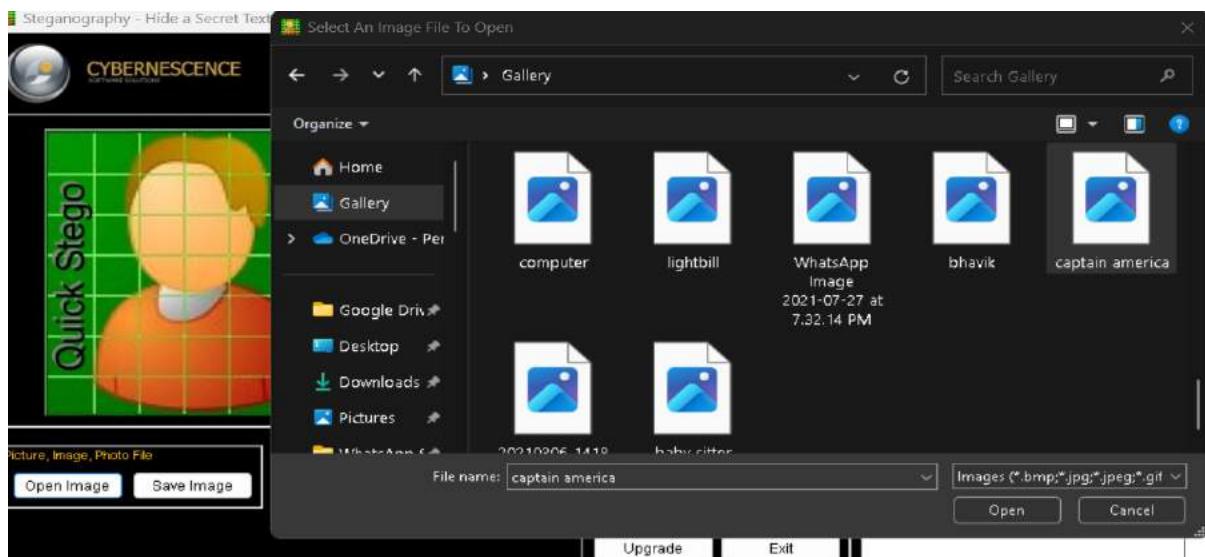
2) Quickstego

QuickStego is used 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.

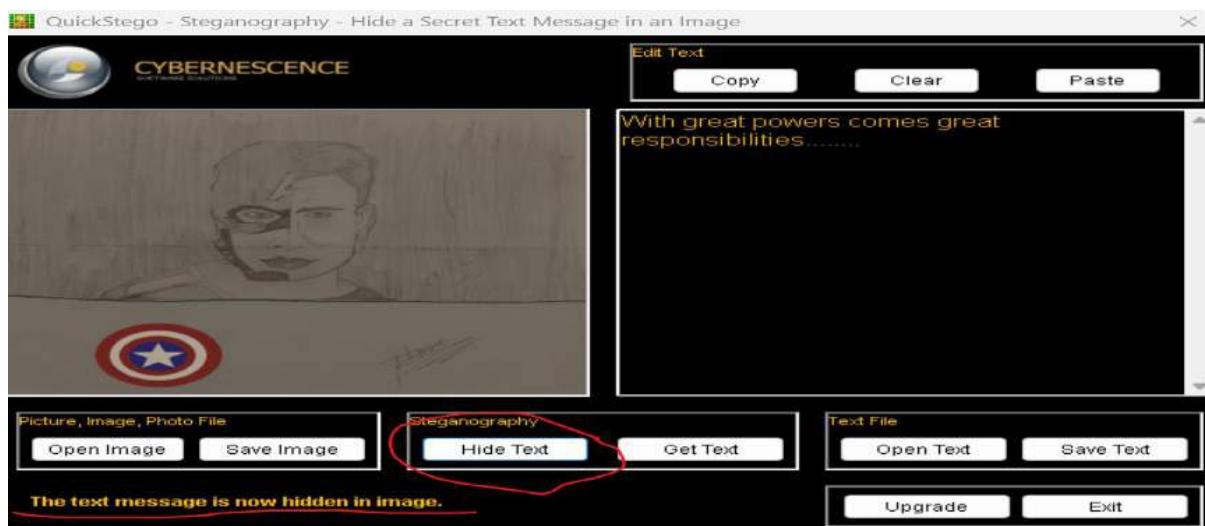
Step 1: - Open the Quickstego tool.



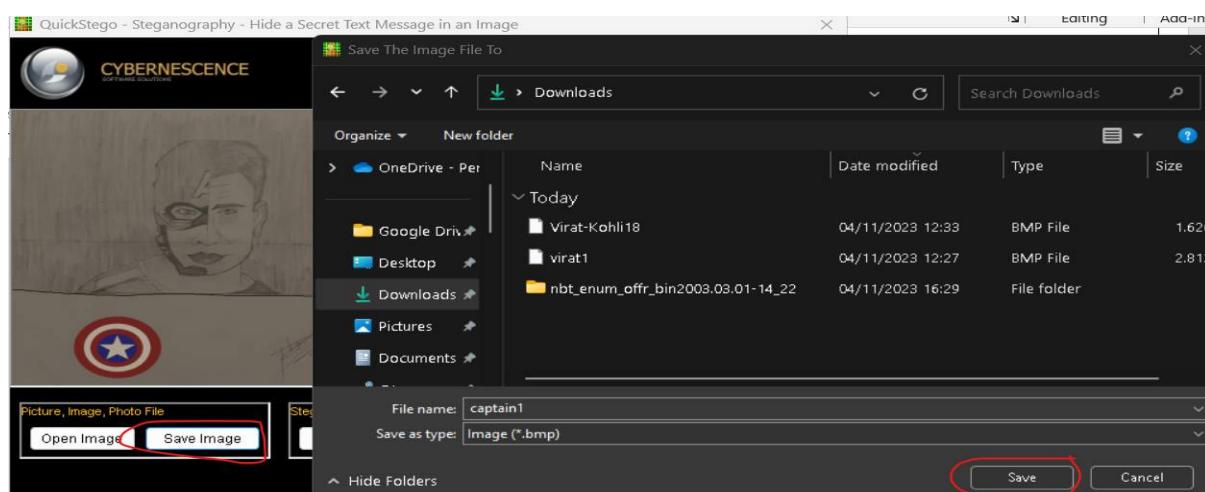
Step 2 : Open an Image-> Write some text->click on Hide Text and then on save the image.



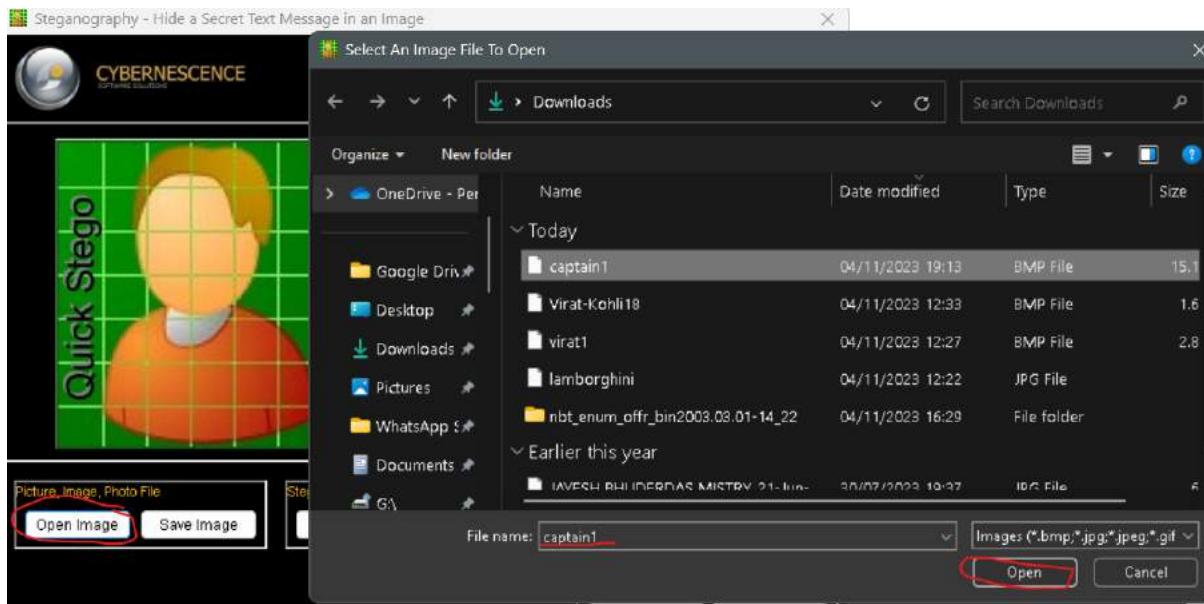
Write and hide



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.

```

Command Prompt
C:\Users>cd..
C:\>cd RainbowCrack
C:\RainbowCrack>rtgen
RainbowCrack 1.5
Copyright 2003-2010 RainbowCrack Project. All rights reserved
.
Official Website: http://project-rainbowcrack.com/
usage: rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index
       rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index -bench

hash algorithms implemented in alglib0.dll:
  lm, plaintext_len limit: 0 - 7
  ntLM, plaintext_len limit: 0 - 15
  md5, plaintext_len limit: 0 - 15
  sha1, plaintext_len limit: 0 - 20
  mysqlsha1, plaintext_len limit: 0 - 20
  halfLMhash, plaintext_len limit: 0 - 7
  ntlmhash, plaintext_len limit: 0 - 15
  oracle-SYSTEM, plaintext_len limit: 0 - 10
  md5-half, plaintext_len limit: 0 - 15

example: rtgen md5 loweralpha 1 7 0 1000 1000 0
          rtgen md5 loweralpha 1 7 0 -bench

C:\RainbowCrack>

```

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

```

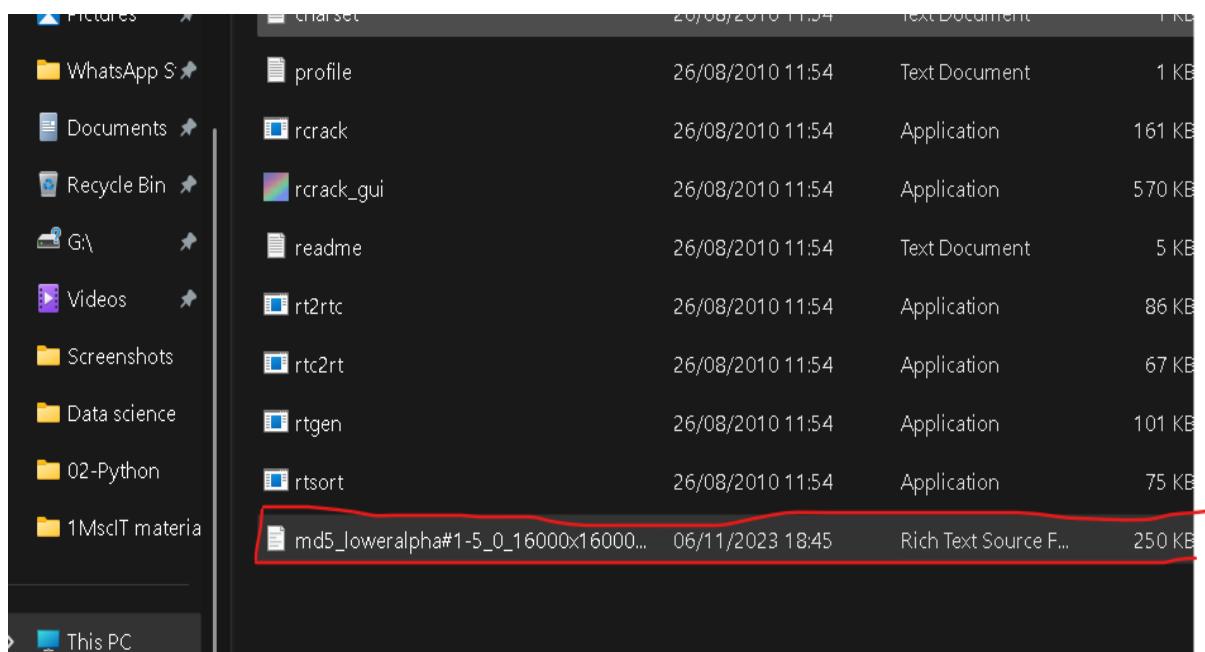
C:\RainbowCrack>rtgen md5 loweralpha 1 5 0 16000 16000 0
rainbow table md5_loweralpha#1-5_0_16000x16000_0.rt parameter
s
hash algorithm:      md5
hash length:        16
charset:            abcdefghijklmnopqrstuvwxyz
charset in hex:    61 62 63 64 65 66 67 68 69 6a 6b 6c 6
d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a
charset length:    26
plaintext length range: 1 - 5
reduce offset:      0x00000000
plaintext total:    12356630

sequential starting point begin from 0 (0x0000000000000000)
generating...
16000 of 16000 rainbow chains generated (0 m 13.7 s)

C:\RainbowCrack>

```

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 .

The screenshot shows a web browser window for 'Dan's Tools'. The URL is https://www.md... The page title is 'MD5 Hash Generator'. A text input field contains the string '1234'. Below it is a blue button labeled 'Generate →'. To the right, there is a table with three rows:

Your String	1234
MD5 Hash	81dc9bdb52d04dc20036dbd8313ed055
SHA1 Hash	7110eda4d09e062aa5e4a390b0a572ac0d2c0220

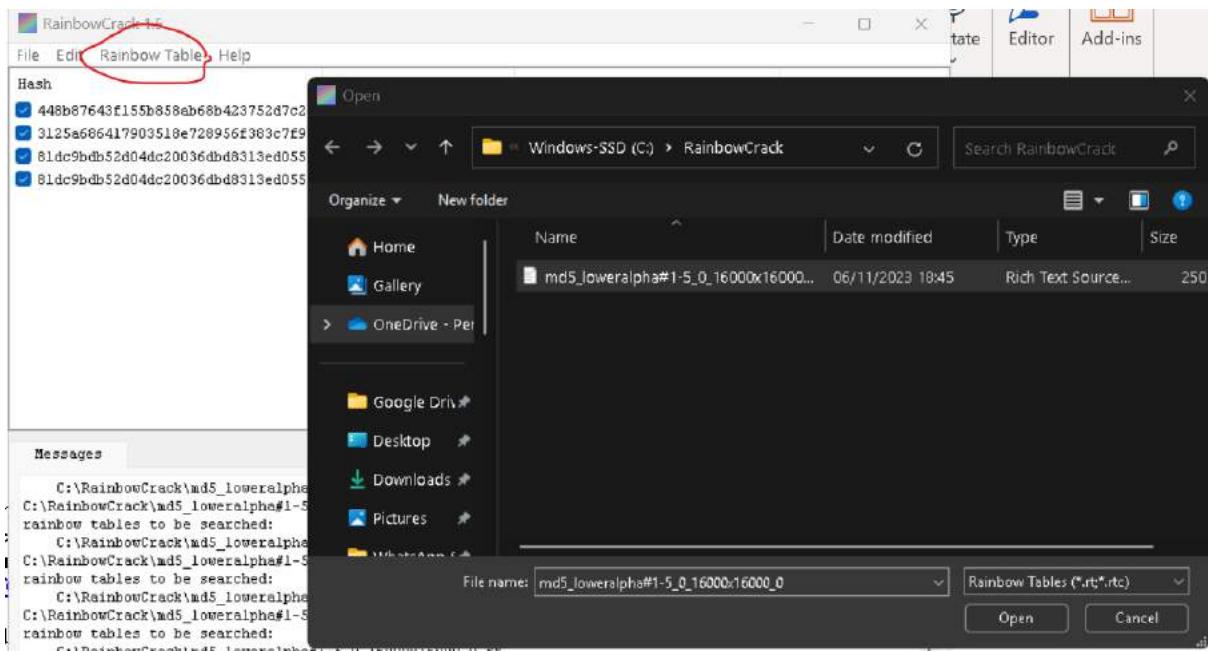
Each hash value has a 'Copy' button next to it.

The screenshot shows the 'RainbowCrack 1.5' application window. The main table has columns: Hash, Plaintext, Plaintext in Hex, and Comment. Three rows are selected, each with a checked checkbox:

Hash	Plaintext	Plaintext in Hex	Comment
448b87643f155b858ab68b423752d7c2	?	?	
3125a686417903518e728956f383c7f9	?	?	
81dc9bdb52d04dc20036dbd8313ed055	?	?	

A modal dialog box titled 'Add Hash' is open in the foreground. It has fields for 'Hash' (containing '81dc9bdb52d04dc20036dbd8313ed055') and 'Comment (optional)'. At the bottom are 'OK' and 'Cancel' buttons.

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



You can Download free rainbow table from here



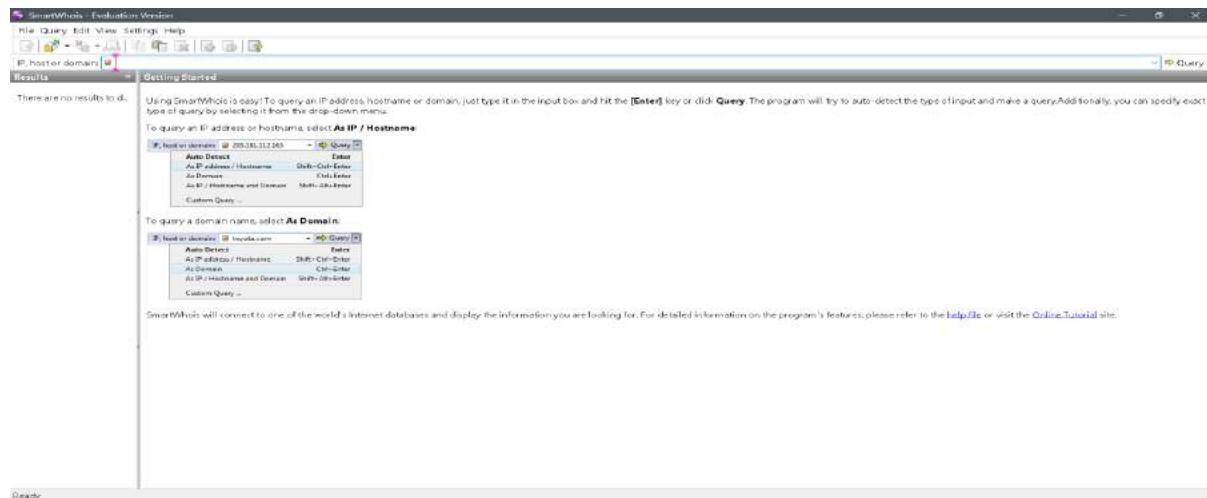
Free Rainbow Tables
Distributed Rainbow Table Project

The goal of FreeRainbowTables.com is to prove the insecurity of using simple hash routines to protect valuable passwords, and force developers to use [more secure methods](#). By [distributing](#) the generation of rainbow chains, we can generate **HUGE rainbow tables** that are able to crack [longer passwords](#) than ever seen before. Furthermore, we are also improving the rainbow table technology, making them even [smaller and faster](#) than rainbow tables found elsewhere, and the best thing is, those tables are freely available!

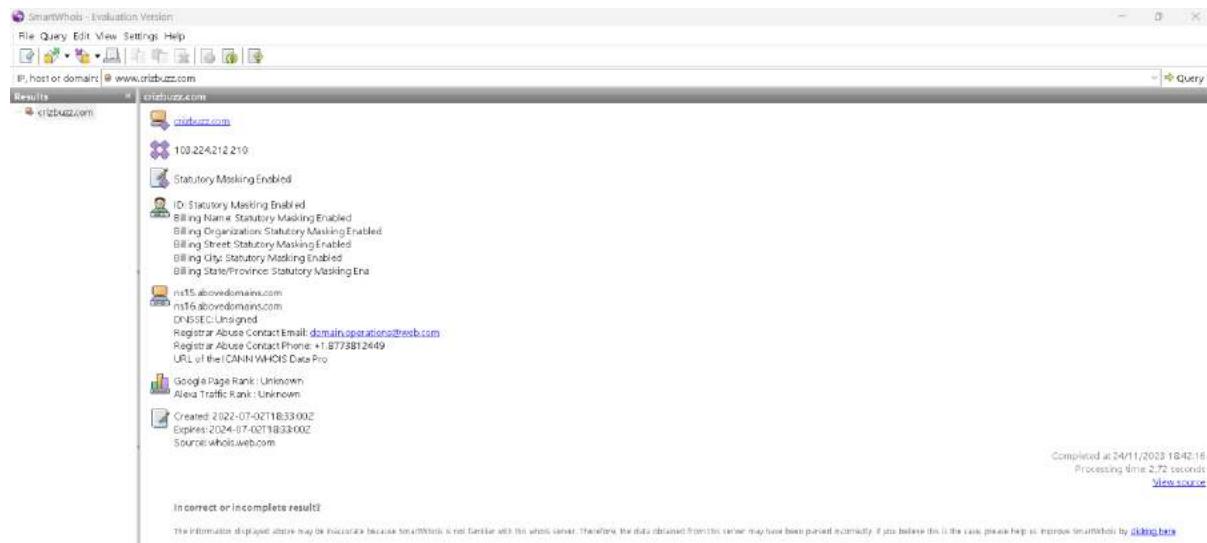
Character set and password length	<u>NTLM</u>	<u>SHA-1¹</u> and MySQL SHA1	<u>MDS</u>	<u>LM</u>	Half <u>LM</u> challenge
Hover your mouse over the below for more information	4 TB	3 TB	4.3 TB	398 GB	18 GB
all-space#1-7 2				34 GB: 0 1 2 3	18 GB: 0 1 2 3
alpha#1-1.loweralpha#5-5.loweralpha-numeric#2-2.numeric#1-3	362 GB: 0 1 2 3				
alpha-space#1-9	35 GB: 0 1 2 3		23 GB: 0 1 2 3		

Smart whois

Step1: Download and open the software

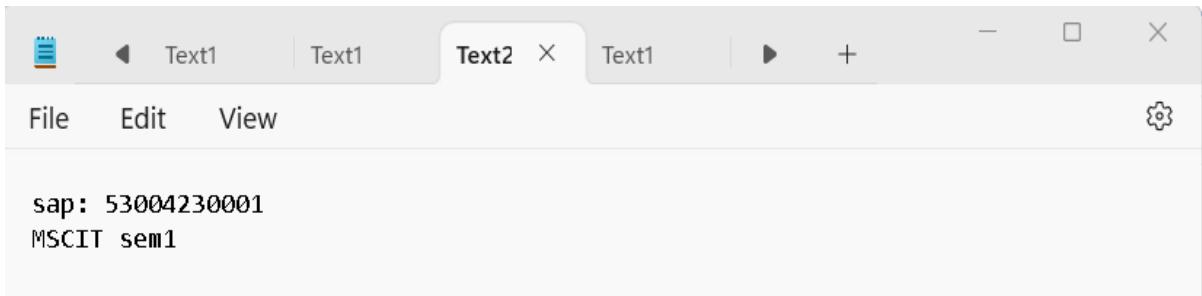
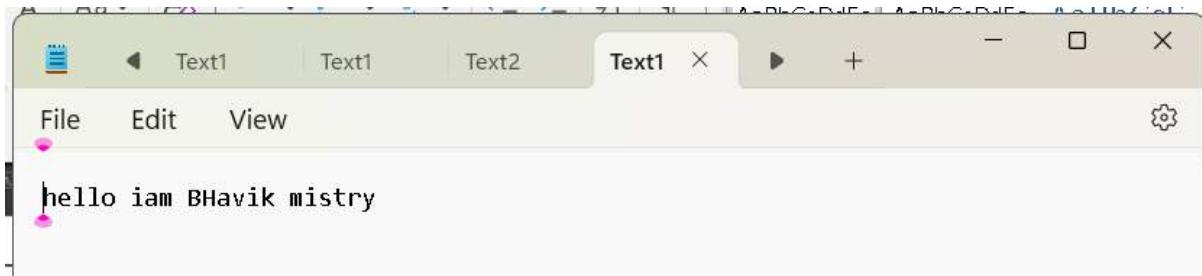


Step2: Enter any ip, or domain name



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.

```
C:\Users\bhavi>cd "B:\1MscIT material\hiding folder"

C:\Users\bhavi>B:

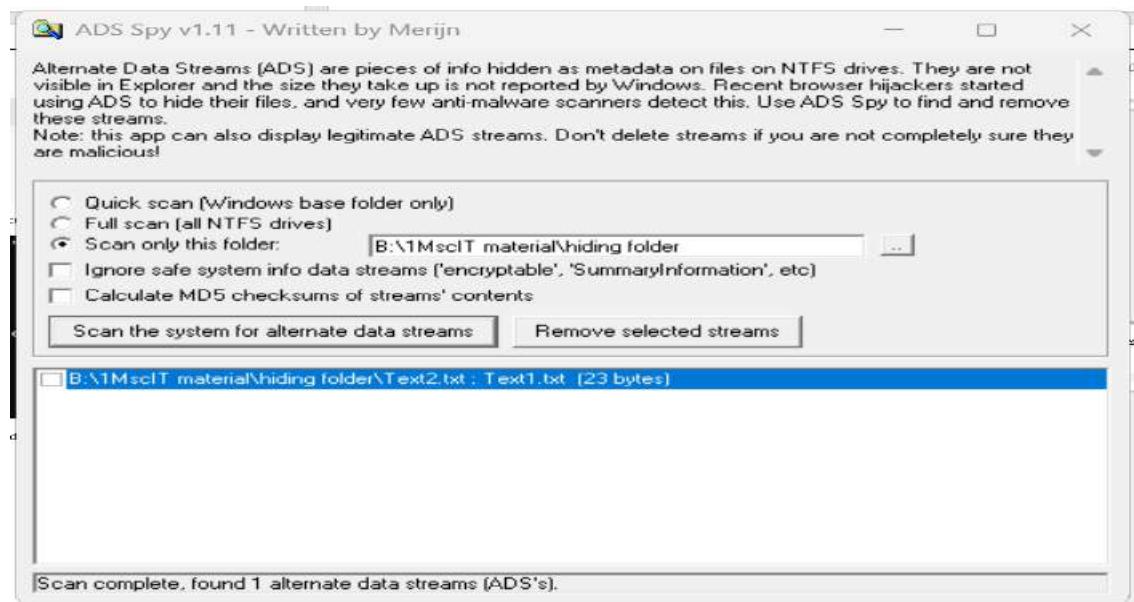
B:\1MscIT material\hiding folder>
B:\1MscIT material\hiding folder>
B:\1MscIT material\hiding folder>
B:\1MscIT material\hiding folder>type Text1.txt > Text2.txt:Text1.txt

B:\1MscIT material\hiding folder>start Text1.txt

B:\1MscIT material\hiding folder>start Text2.txt

B:\1MscIT material\hiding folder>
```

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.

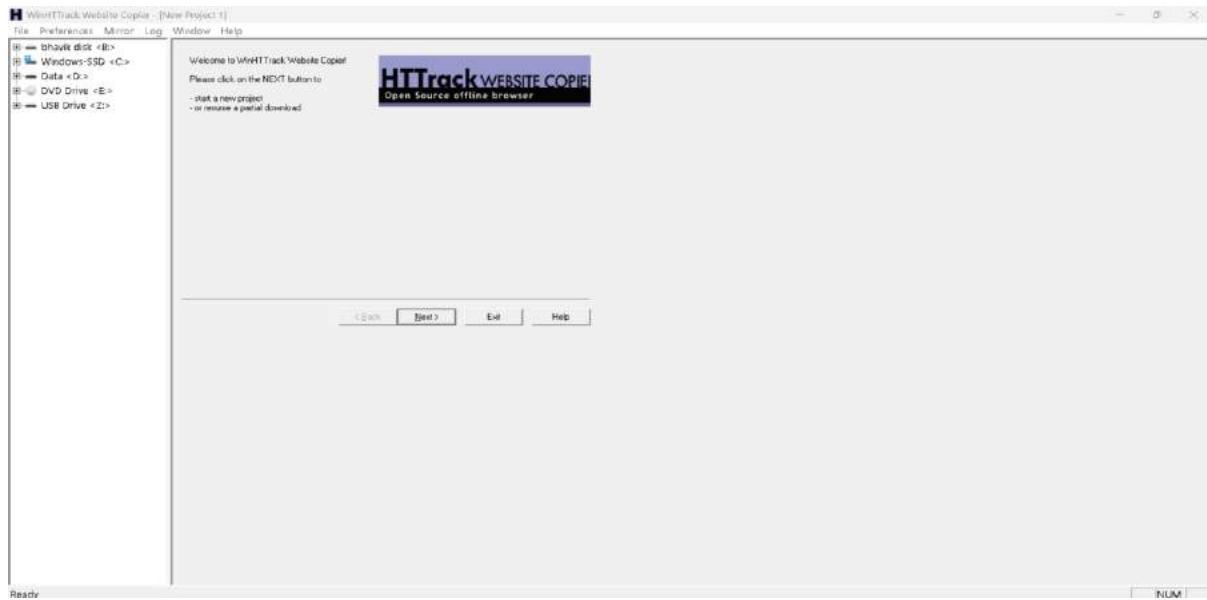


Practical 5

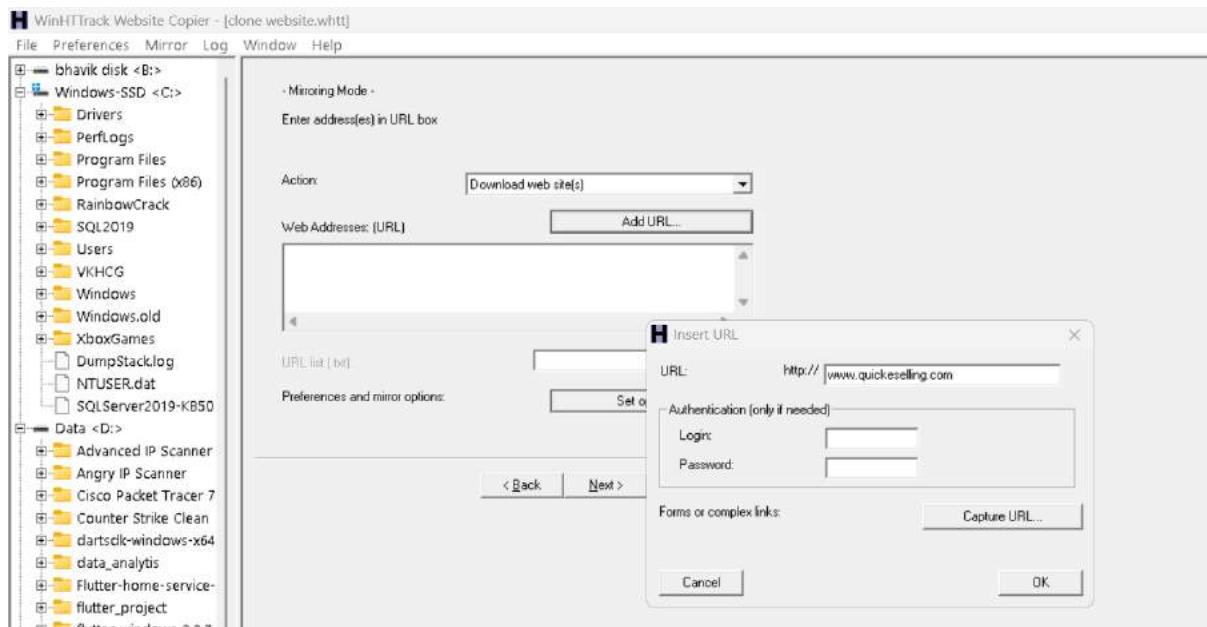
1) HTTrack Website Copier

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.

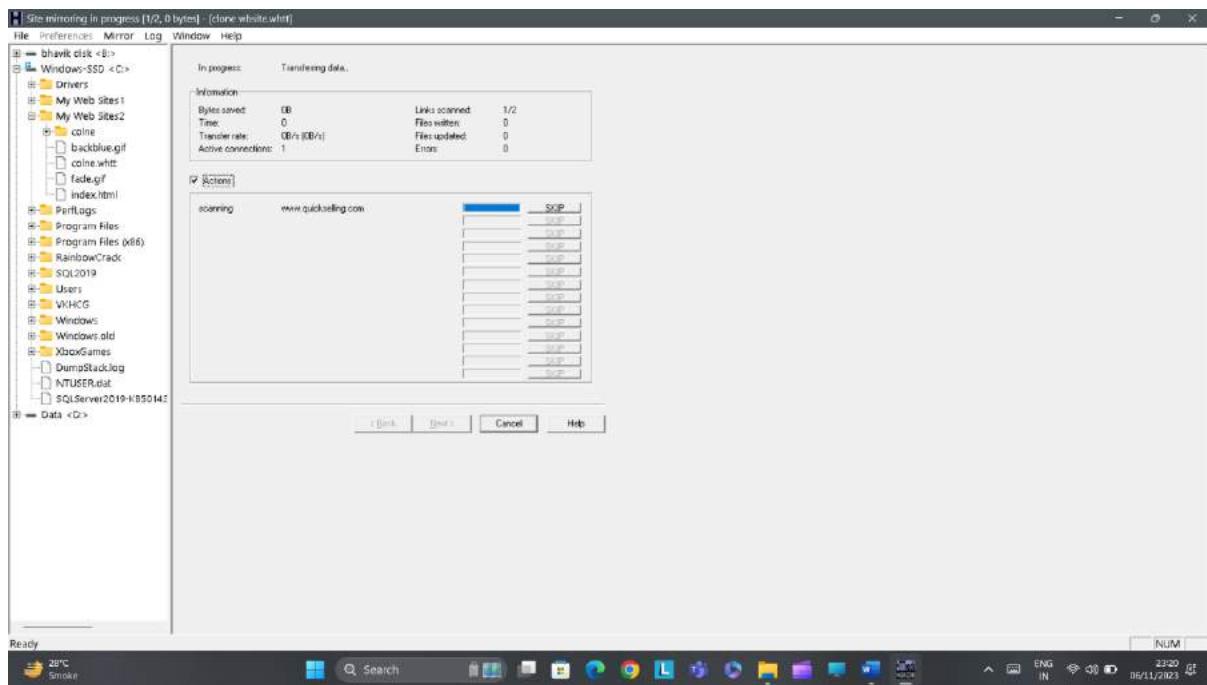
Step 1: -Install and open the HTTrack Website Copier software.-> click next



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

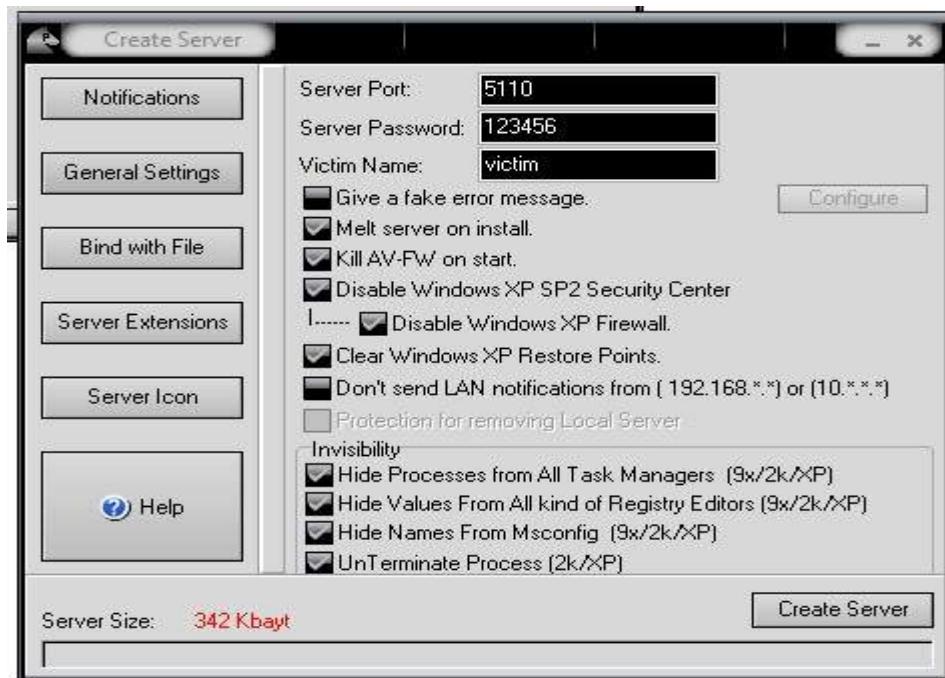
PRORAT is a family of backdoors that serves as a remote administration tool (RAT). Variants of this malware family first appeared in 2005. It opens random ports to establish connection with a remote attacker. Once a connection is established, the remote attacker can execute commands such as creating/opening/closing/deleting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

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



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

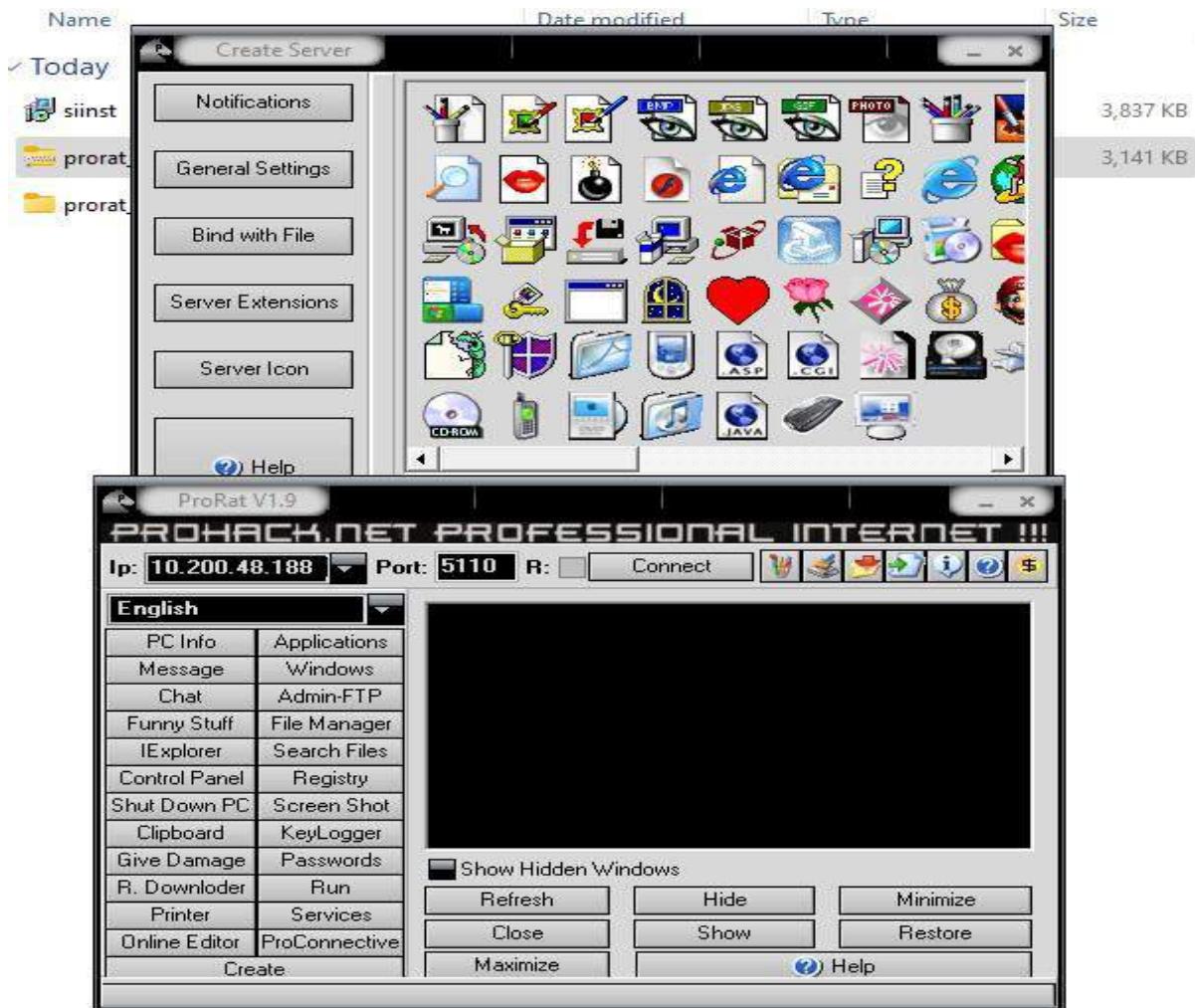




Step3: - Bind server with a file you want.



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



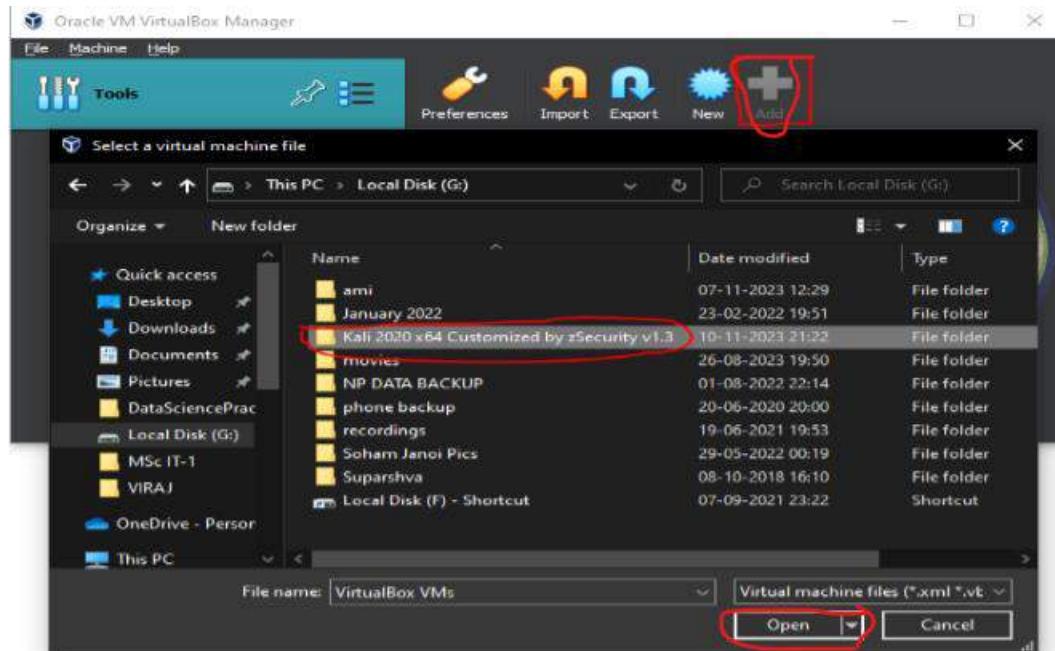
Practical

1) Virtual Machine and kali

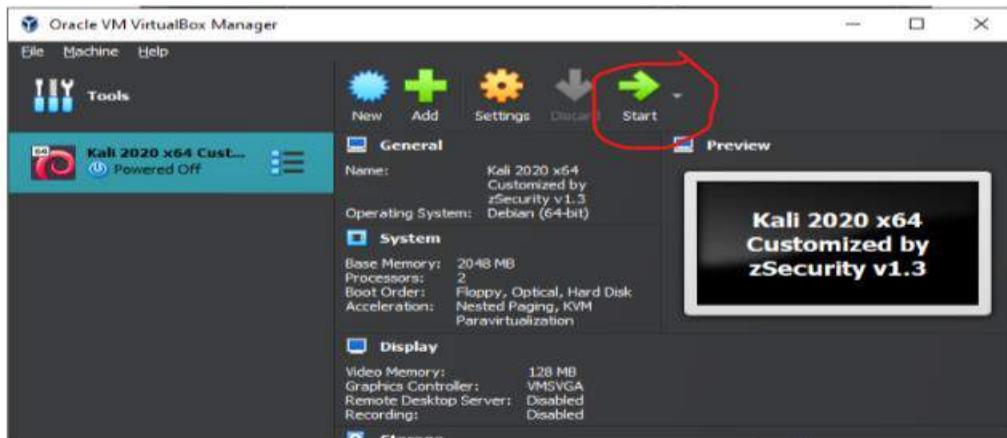
Step 1:- Download and Install Virtual Box in your device.



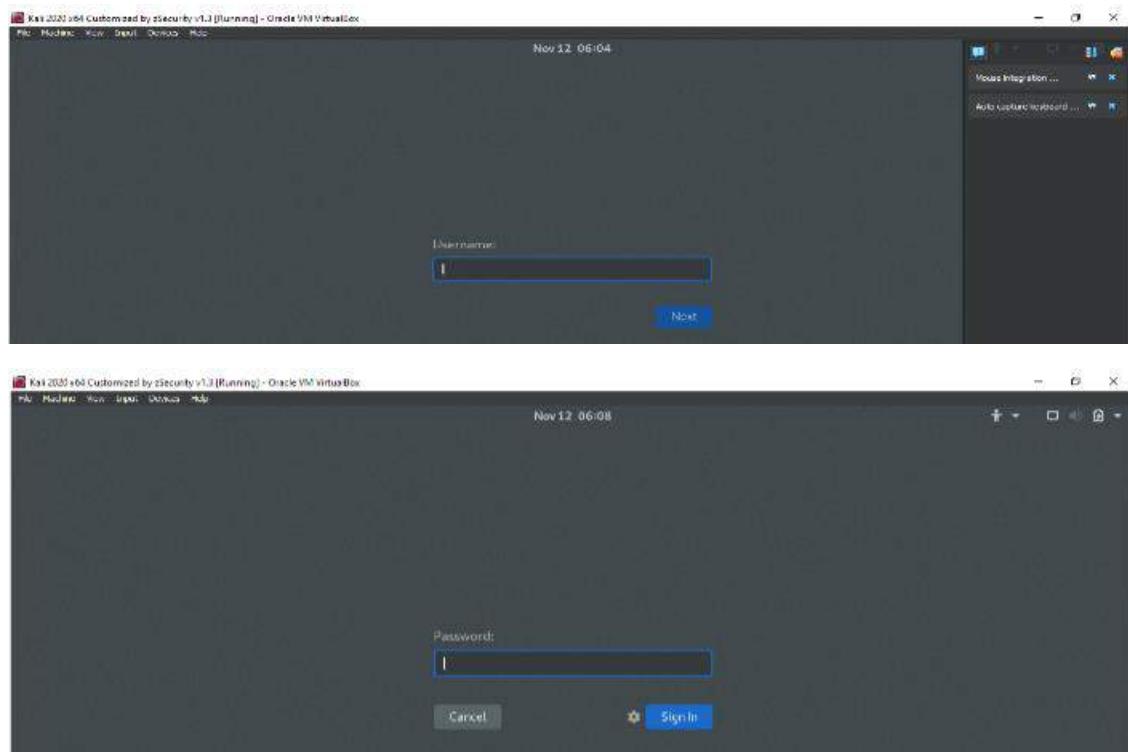
Step 2:- Now click on Add button and select the file as shown in the figure



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”

```

      =[ metasploit v5.0.71-dev
+ -- ---=[ 1962 exploits - 1095 auxiliary - 336 post
+ -- ---=[ 558 payloads - 45 encoders - 10 nops
+ -- ---=[ 7 evasion

msf5 > nmap -T4 -A -v www.lenovo.com
[*] exec: nmap -T4 -A -v www.lenovo.com

Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-11 01:05 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:05
Completed NSE at 01:05, 0.00s elapsed
Initiating NSE at 01:05
Completed NSE at 01:05, 0.00s elapsed
Initiating NSE at 01:05
Completed NSE at 01:05, 0.00s elapsed
Initiating NSE at 01:05
Completed NSE at 01:05, 0.00s elapsed
Initiating Ping Scan at 01:05
Scanning www.lenovo.com (23.201.202.34) [4 ports]
Completed Ping Scan at 01:05, 0.04s elapsed (1 total hosts)

```

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

```

File Actions Edit View Help
root@kali:~# msfconsole

      .:ok000kdc'          'cdk000ko:.
.oooooooooooooo000c  cooooooooooooox.
:oooooooooooooo00k, ,kooooooooooooooo:
'oooooooooooo0kkkko0000: :ooooooooooooooo000'
oooooooooooo MMMM .o0000o0000l MMMM ,00000000
dooooooooo MBBBBB .c0000c .BBBBBB ,0000000x
oooooooooooo MBBBBB .c0000c .BBBBBB ,0000000x
oooooooooooo MBBBBB .c0000c .BBBBBB ,0000000x
loooooooooooo MBBBBBBB ; d MBBBBBBB ,0000000i
.oooooooooooo MBBB ; MBBBBBBB MBBB ,00000000.
coooooooooooo MM .00c .MMMM .o00 .MMMM ,0000000c
oooooooooooo MM .0000 .MM .0000 .MM ,0000000
;oooooooooooo MM .0000 .MM .0000 .MM ,000000
;oooooooooooo MM .0000 .MM .0000 .MM ;0000;
.doooo WM .0000ccccx0000 MX 'x0d.
,k0l M .000000000000 M d0k,
:kk;.000000000000;k:
;k000000000000000k:
,xooooooooooooox,
.1ooooooooool.
,d0d,
.

      =[ metasploit v5.0.71-dev
+ -- ---=[ 1962 exploits - 1095 auxiliary - 336 post
+ -- ---=[ 558 payloads - 45 encoders - 10 nops
+ -- ---=[ 7 evasion

msf5 > 

```

Step 3 : Enter the command “use auxiliary/scanner/portscan/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:1568a:1a7d:6778
|-http-title: Live Cricket Score, Schedule, Latest News, Stats & 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)

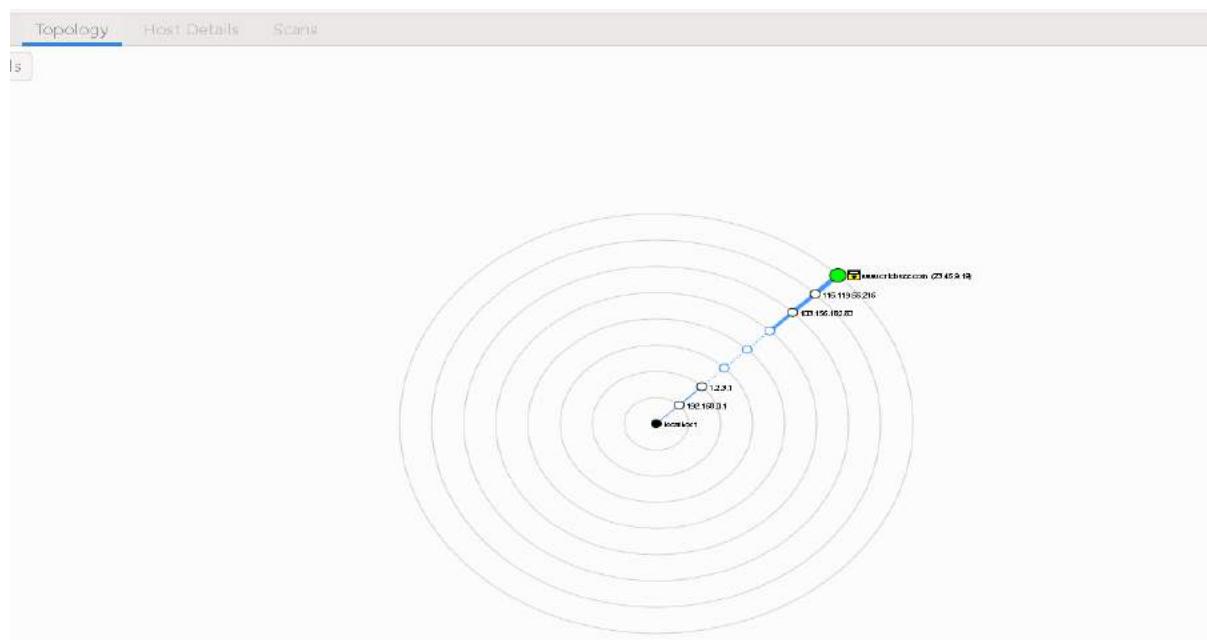
NSE: Script Post-scanning.
Initiating NSE at 19:06
Completed NSE at 19:06, 0.00s elapsed
Initiating NSE at 19:06
Completed NSE at 19:06, 0.00s elapsed
Initiating NSE at 19:06
Completed NSE at 19:06, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please 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

Nmap Output Ports / Hosts Topology **Host Details** Scans

www.cricbuzz.com (23.46.9.19)

Host Status

State:	up
Open ports:	2
Filtered ports:	997
Closed ports:	1
Scanned ports:	1000
Up time:	959862
Last boot:	Mon Nov 13 16:28:36 2023

Addresses

IPv4:	23.46.9.19
IPv6:	Not available
MAC:	Not available

Hostnames

Name:	- www.cricbuzz.com - user
Type:	
Name:	a23-46-9-19.deploy.static.akamaitechnologies.com
-	- PTR

Nmap Output Ports / Hosts Topology **Host Details** Scans

Operating System

Name:	Linux 5.0
Accuracy:	<div style="width: 100%;"> </div>

Ports used

Port-	80 -
Protocol-	tcp -
State:	open
Port-	53 -
Protocol-	tcp -
State:	closed
Port-	38142
Protocol-	- udp
State:	closed

OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
general purpose	Linux	Linux	5.X	<div style="width: 100%;"> </div>

TCP Sequence

Difficulty: Good luck!

Index: 260
Values:

IP ID Sequence

Class: All
Values:

Scans

Nmap Output Ports / Hosts Topology Host Details **Scans**

Status	Command
Unsaved	nmap -T4 -A -v https://www.cricbuzz.com/
Unsaved	nmap -T4 -A -v www.cricbuzz.com/
Unsaved	nmap -T4 -A -v www.cricbuzz.com

CommandInfo

```

Command Info
Command: nmap -T4 -A -v www.cricbuzz.com
Nmap Version: 7.94
Verbosity: 1
Debug level: 0
General Info
Started: November 24, 2023 - 19:05
Finished: November 24, 2023 - 19:06
Hosts up: 1
Hosts down: 0

```

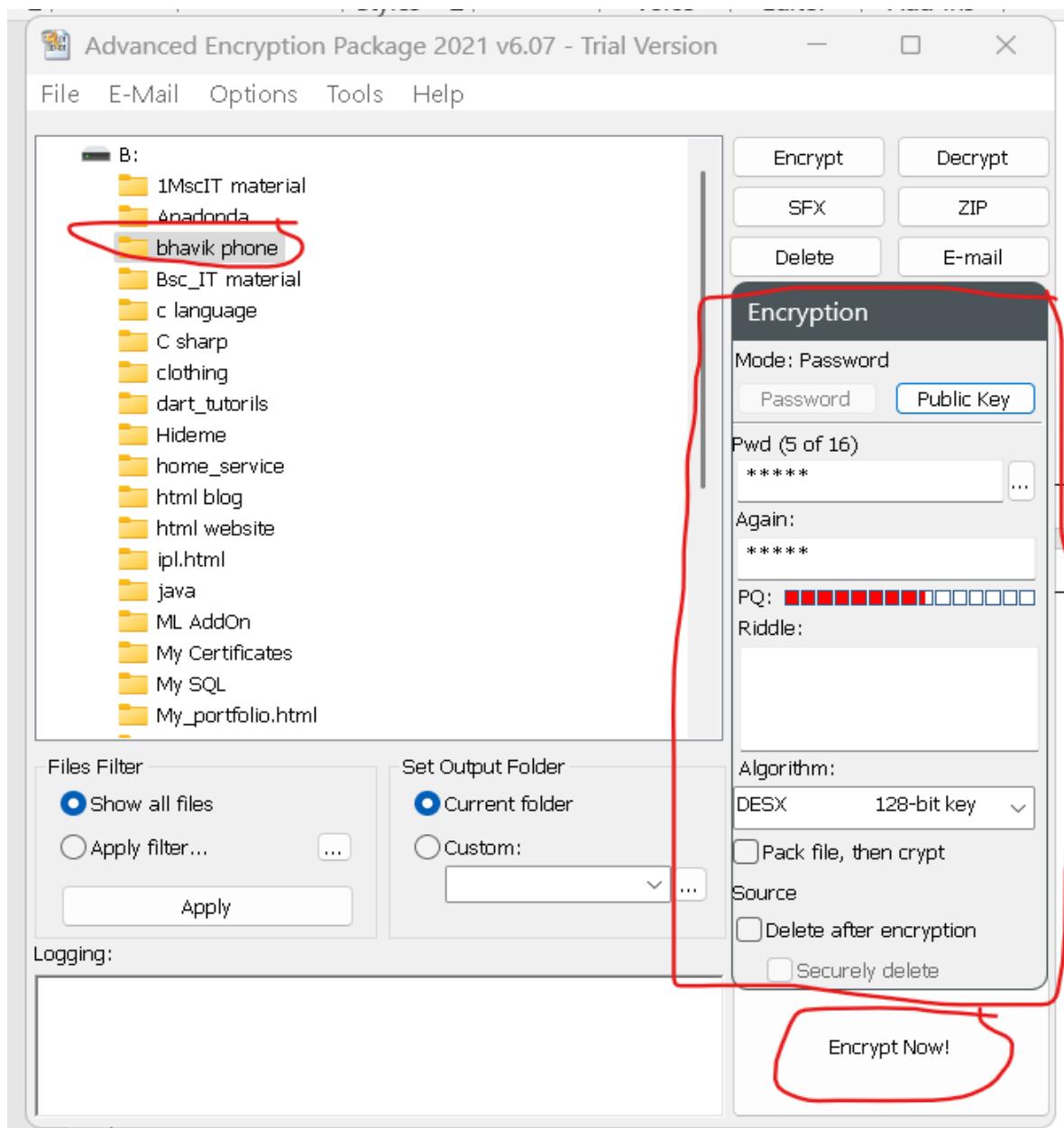
Practical

Cryptography

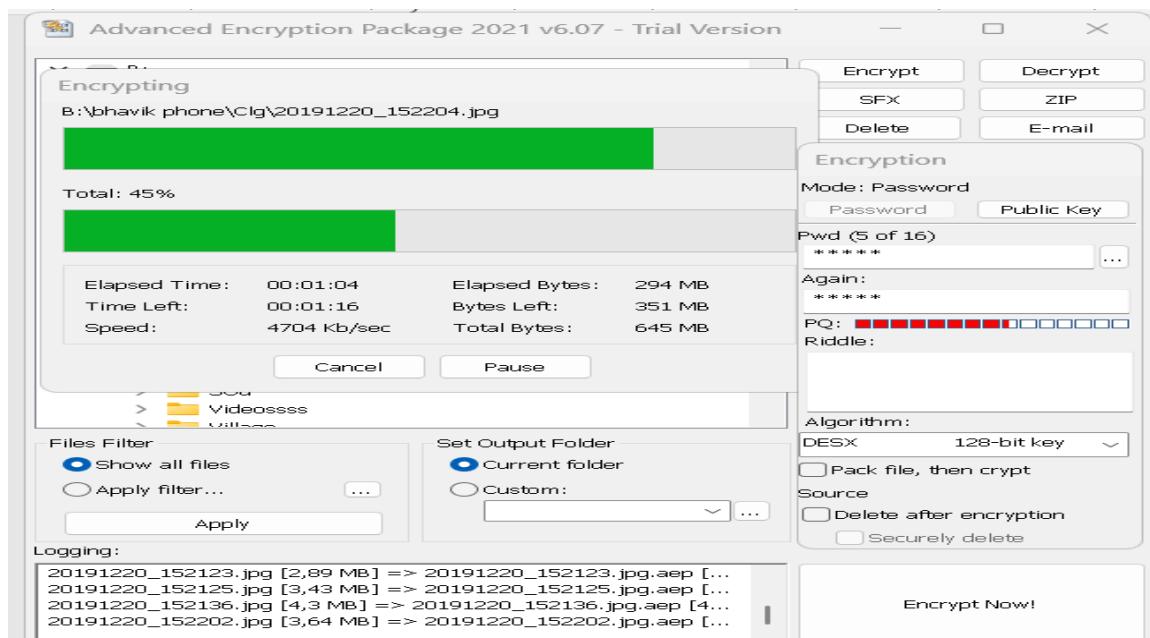
1) Advance Encryption Package

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.

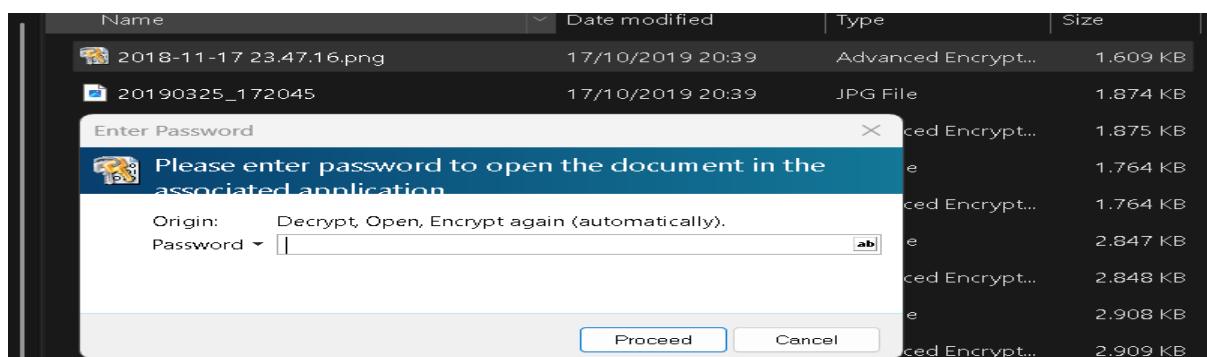
Step 1: Open AEP Software-> Select the file for Encryption-> Enter the password , confirm it and click on Encrypt Now!



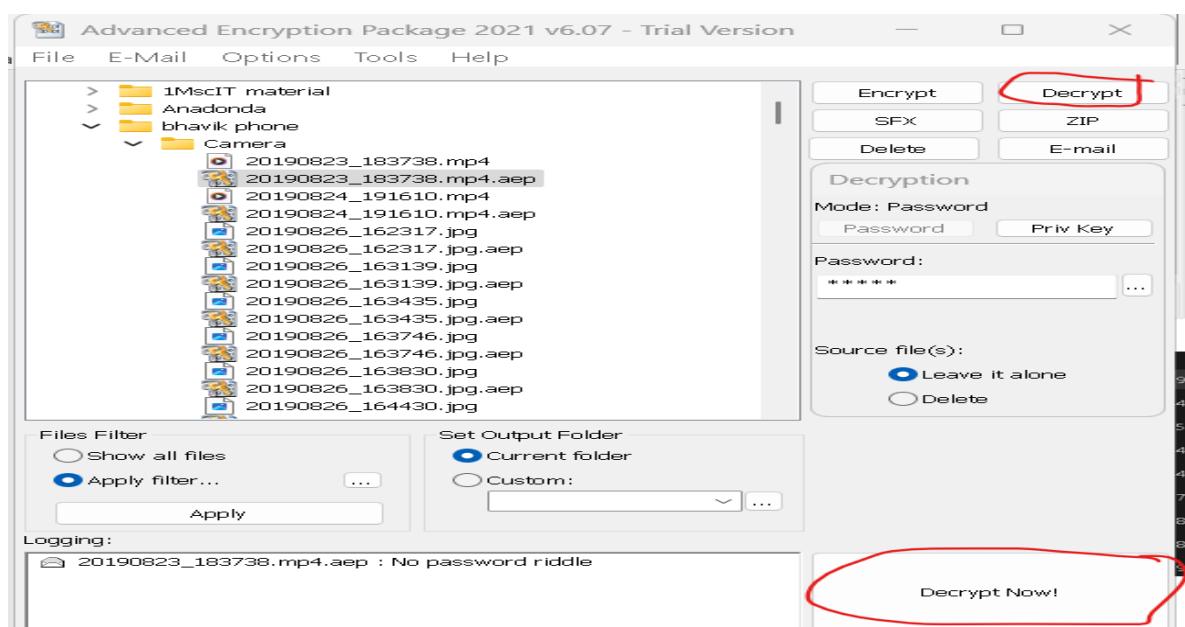
Step 2: As we can below see an encrypted file has been created



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



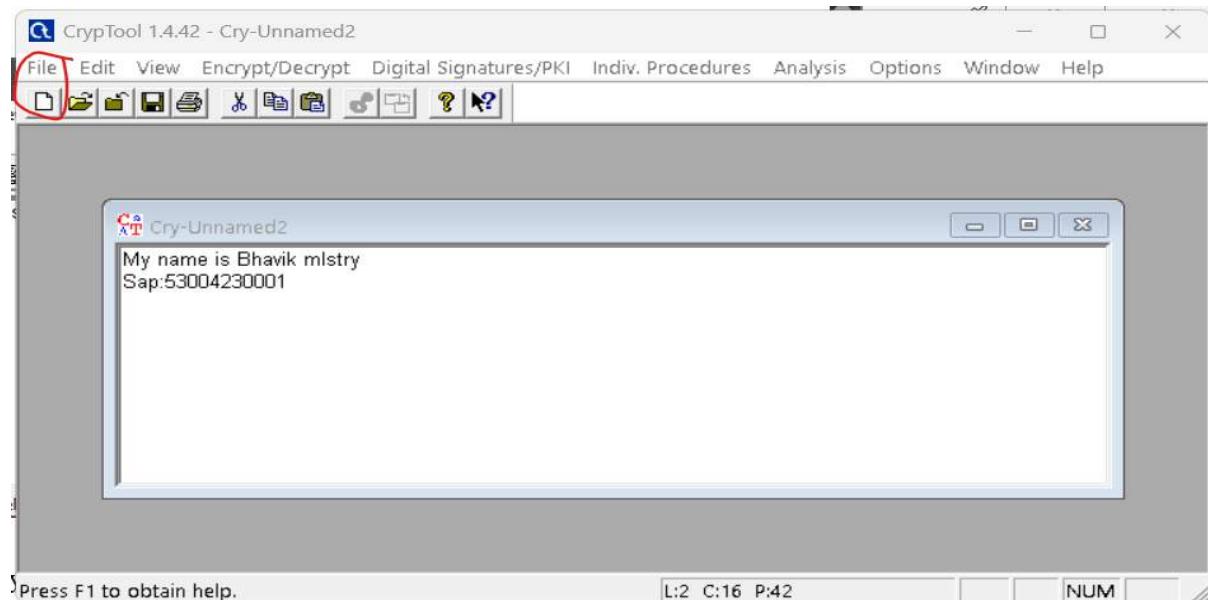
Step 4 : Follow the same steps for Decryption.



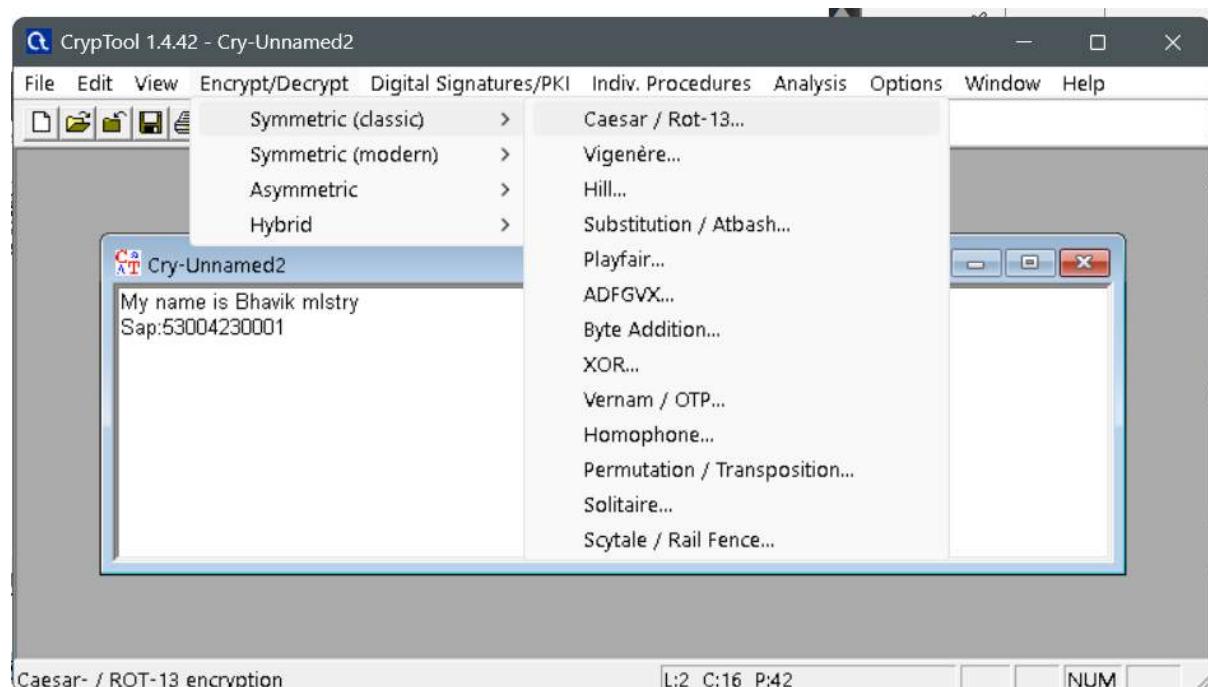
2) CrypTool

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.

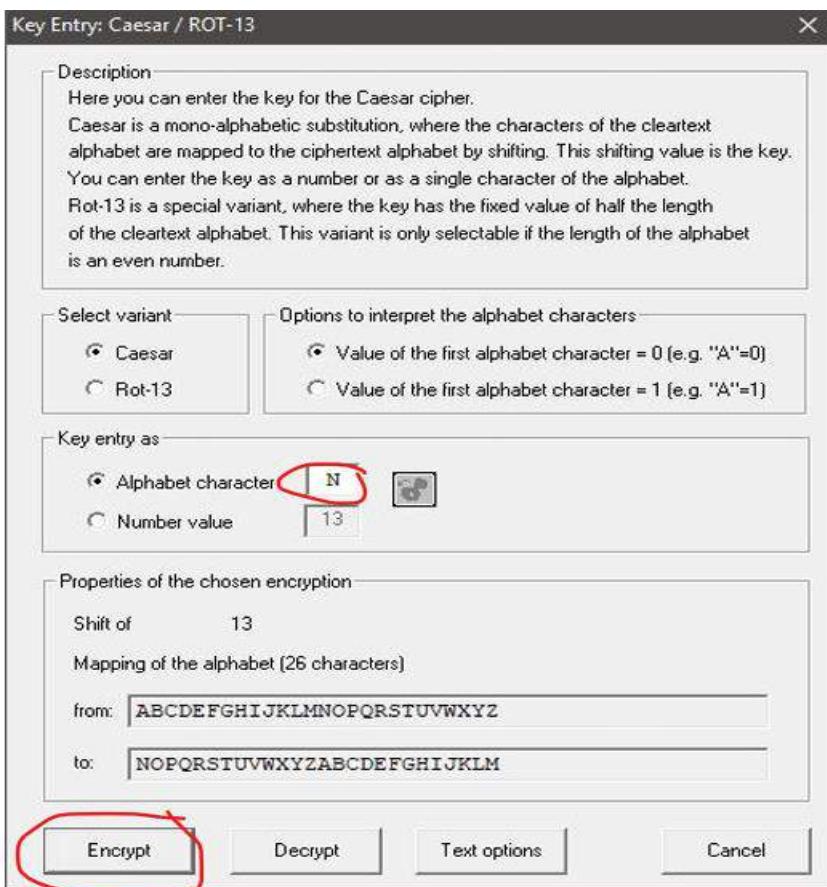
Step 1: Start CrypTool and go to File-> New to create a new empty file. Enter some Text in this file.->save it.



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

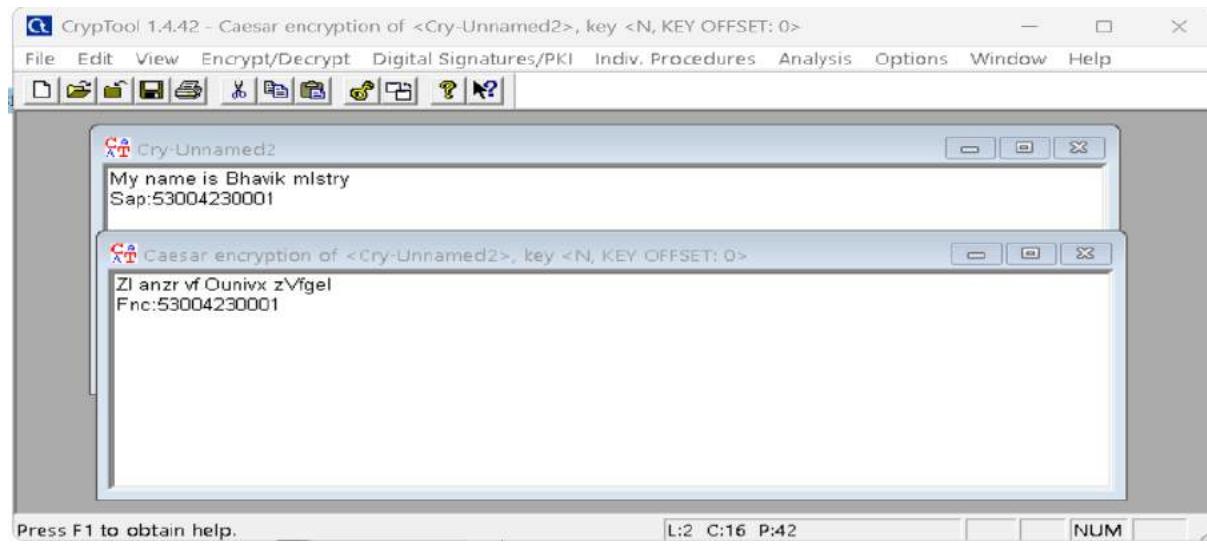


Step 3: Enter the alphabet character to be replaced. Entering N here will replace A by N, B by O and so on. Meaning a shift of 13 character along the alphabet. Click on Encrypt.



Step 4 : Given below is the Encrypted Text.

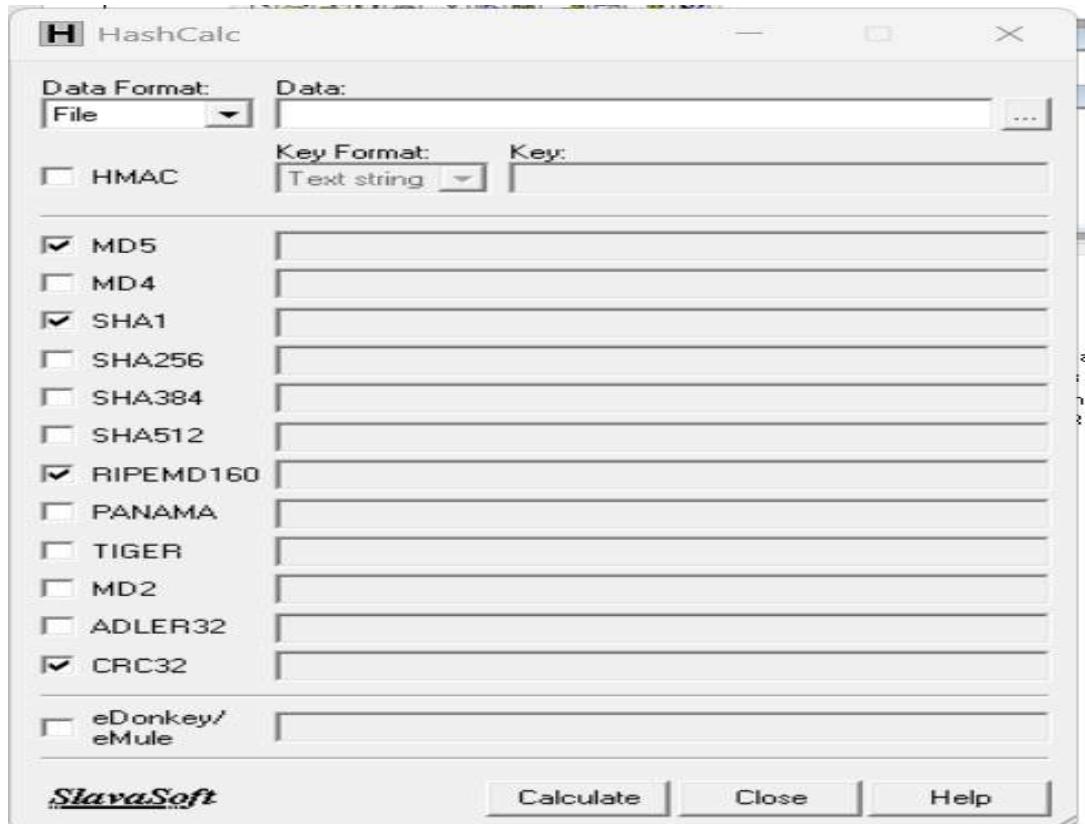
Step 5 : Performing the same steps and clicking on Decrypt, allows us to Decrypt the Encrypted Text.



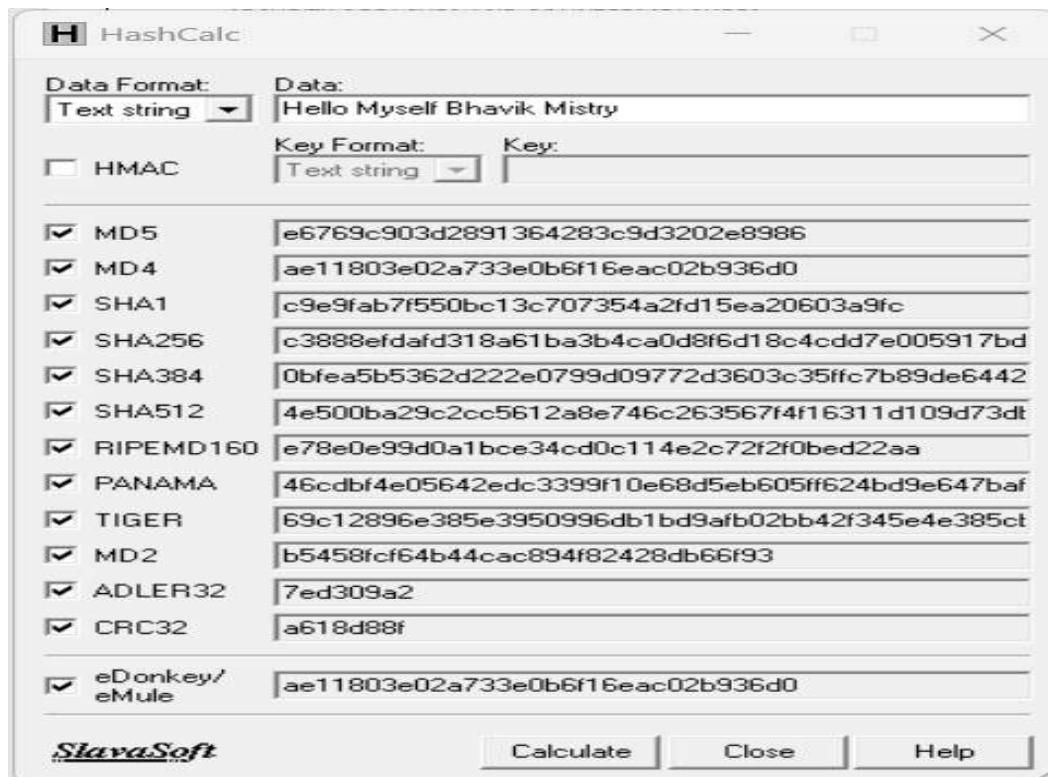
3) HashCalc

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

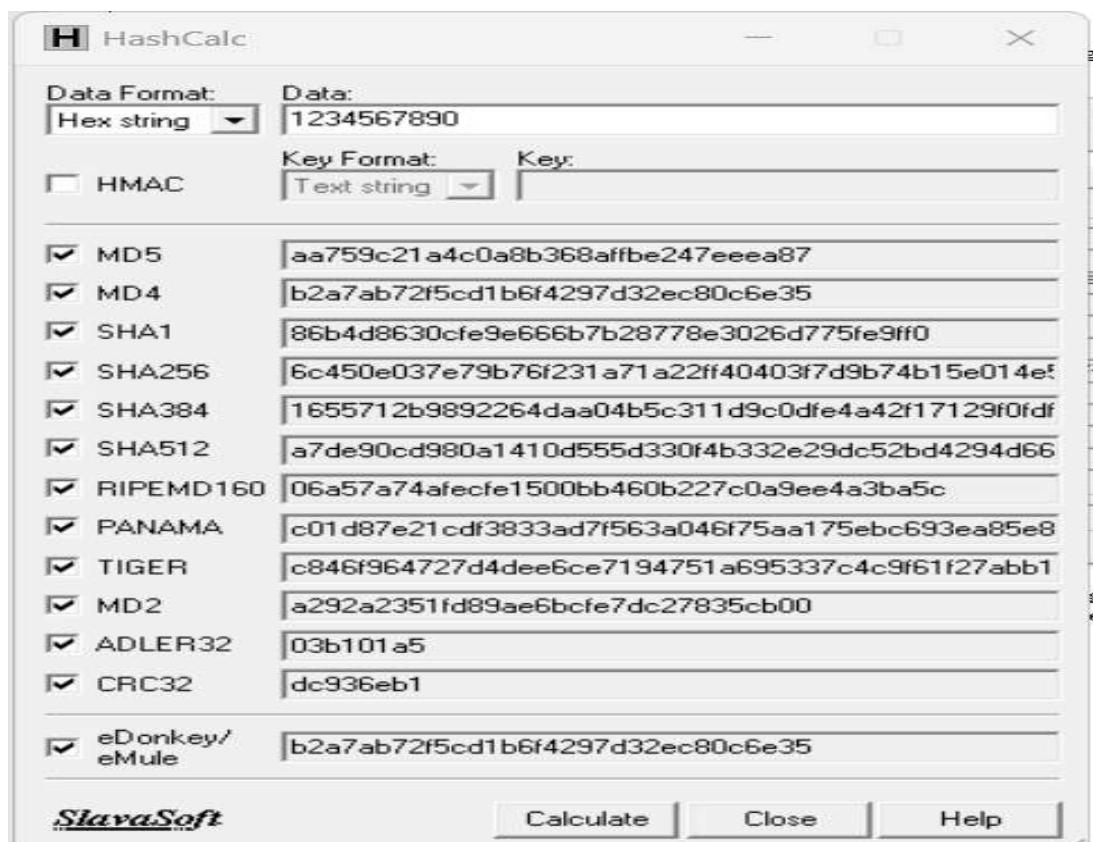
Step 1: Install and Open HashCalc.



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 htPrint . 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 click on Analyze.

Name	Hits	Match %
Microsoft IIS 6.0	46	100
Apache 2.2.4	41	89.13...
Apache 2.2.2	40	86.95...
Apache 2.2.3	40	86.95...
Apache 1.3.33	39	84.78...
Apache 2.0.46	39	84.78...
Apache 2.0.52	39	84.78...
Apache 2.0.54	39	84.78...
Sun ONE Web Server 6.1	39	84.78...
AOLserver 4.0.10	37	80.43...
Apache 2.0.45	37	80.43...
Apache 2.0.55	37	80.43...

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

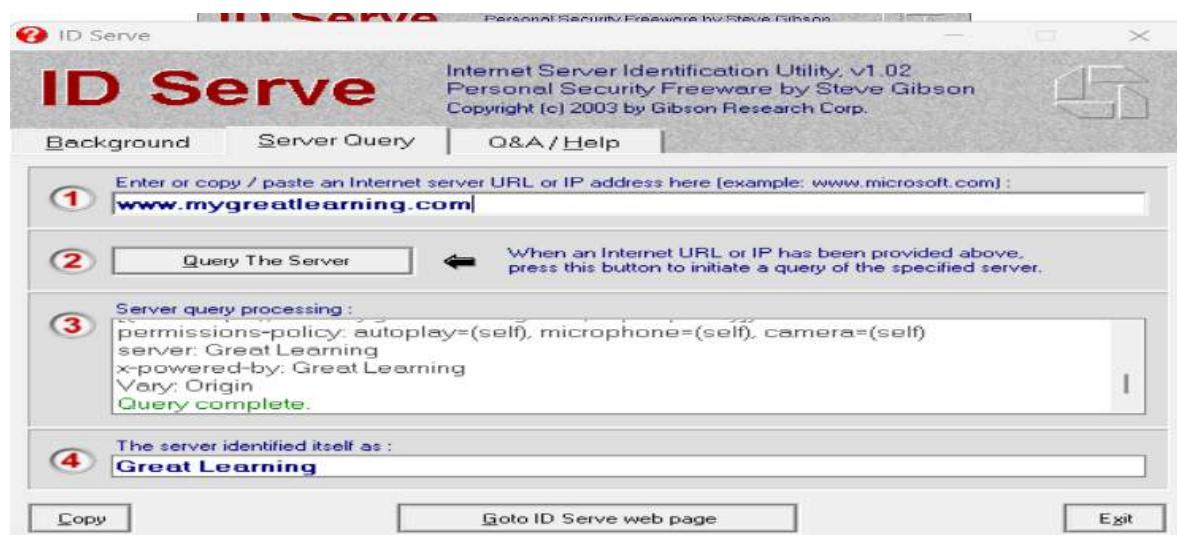
Protocol Name	HTTP
Protocol Version	1.1
Statuscode	403
Statusustext	
Banner	Apache
X-Powered-By	
Header Spaces	1
Capital after Dash	1

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.





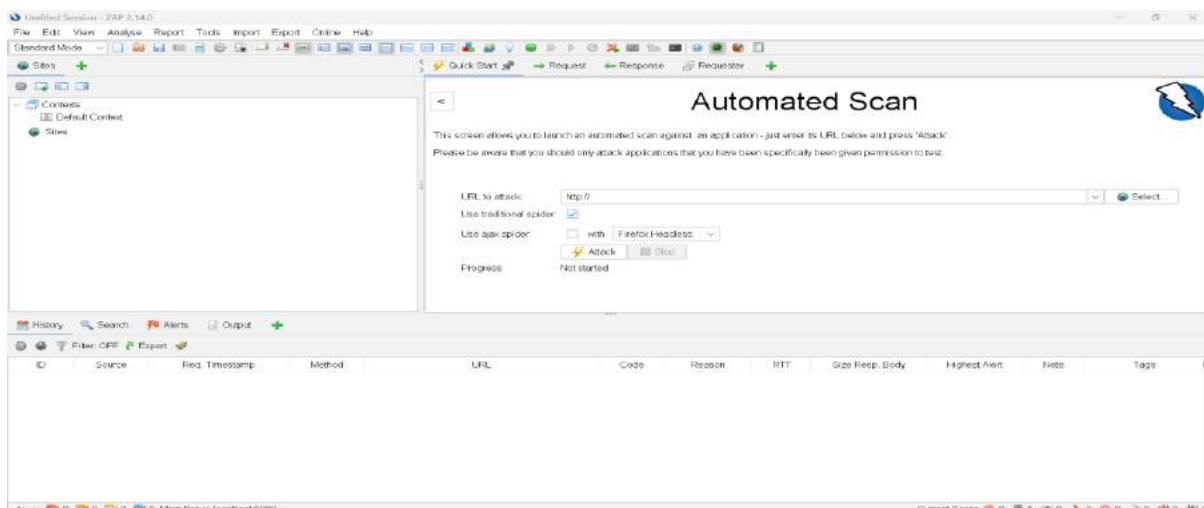
Practical

Session Hijacking

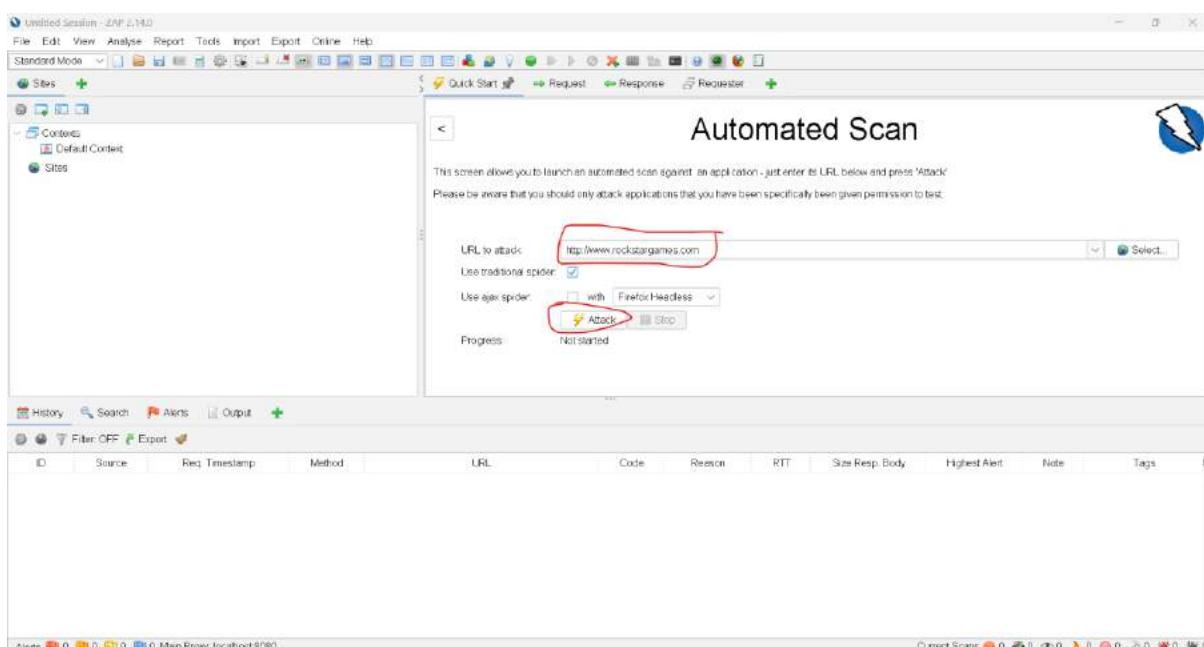
ZAP:

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.



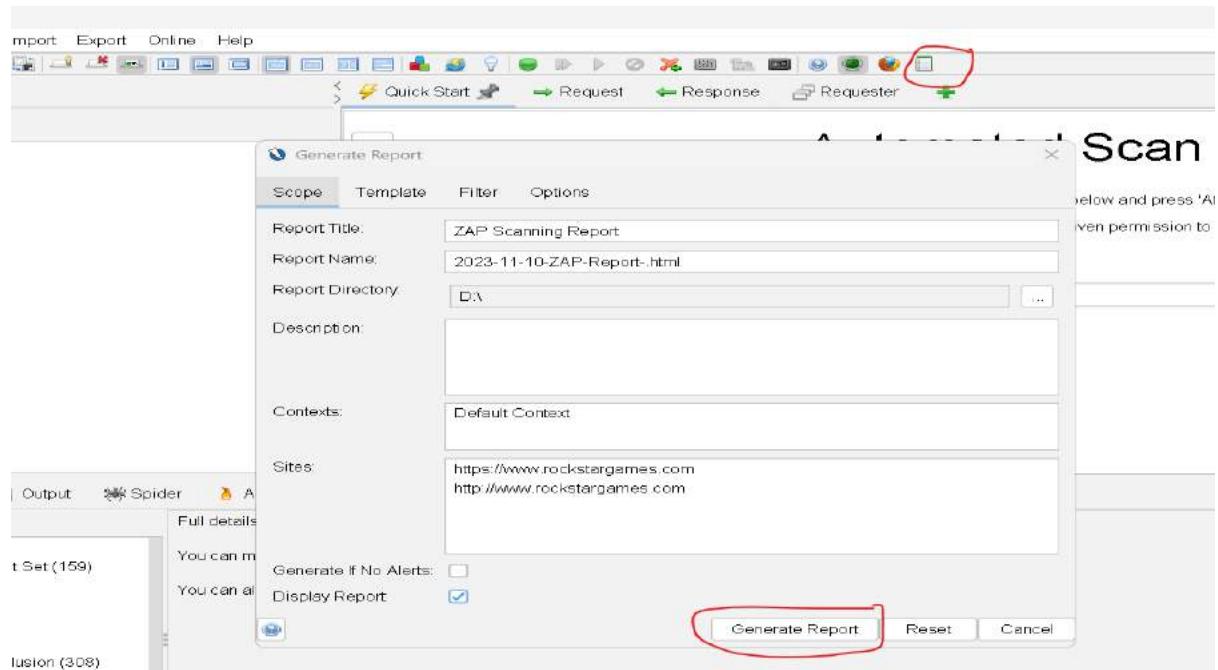
Step 2: In the URL to attack text box-> enter the full URL of the web application you want to attack-> Click the Attack.



The screenshot shows the ZAP 2.14.0 interface with the title bar "Untitled Session - ZAP 2.14.0". The menu bar includes File, Edit, View, Analyse, Report, Tools, Input, Export, Online, Help. The toolbar has icons for Standard Mode, Site Scan, Contexts, Requests, Responses, and Requester. The left sidebar shows "Sites" with a plus sign, "Contexts" (Default Context), and "Sites". The main window title is "Automated Scan". A message says, "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'." It also cautions, "Please be aware that you should only attack applications that you have been specifically been given permission to test." Below this, there's a form with "URL to attack" set to "http://www.rockstargames.com", a checked checkbox for "Use traditional spider", and another for "Use ajax spider" which is unchecked. A "Select..." button is next to the spider type checkboxes. A "Progress" section shows "Attack complete - see the Alerts tab for details of any issues found." At the bottom, the navigation bar includes History, Search, Alerts, Output, Spider, Active Scan, and a New Scan button. The status bar shows "Current Scans 0", "Num Requests 127", "New Alerts 35", and "Export". The bottom right corner has a "ZAP" logo.

The screenshot shows the OWASP ZAP application interface. At the top, there's a menu bar with File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help. Below the menu is a toolbar with various icons for file operations like Open, Save, Print, and a search bar. On the left, there's a sidebar titled 'Sites' with sections for 'Contents' (Default Context) and 'Sites'. The main window has a title 'Automated Scan' with a sub-instruction: 'This screen allows you to launch an automated scan against an application - just enter its URL below and press "Attack"'. It also includes a note: 'Please be aware that you should only attack applications that you have been specifically been given permission to test.' Below this, there are fields for 'URL to attack' (set to http://www.rockstergames.com), 'Use traditional spider' (checkbox checked), 'Use quick spider' (checkbox unchecked), and an 'Attack' button. At the bottom, a progress message says 'Attack complete - see the Alerts tab for details of any issues found'. The bottom navigation bar includes tabs for History, Search, Alerts (which is selected), Output, Spider, Active Scan, and a green plus sign icon.

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](#)

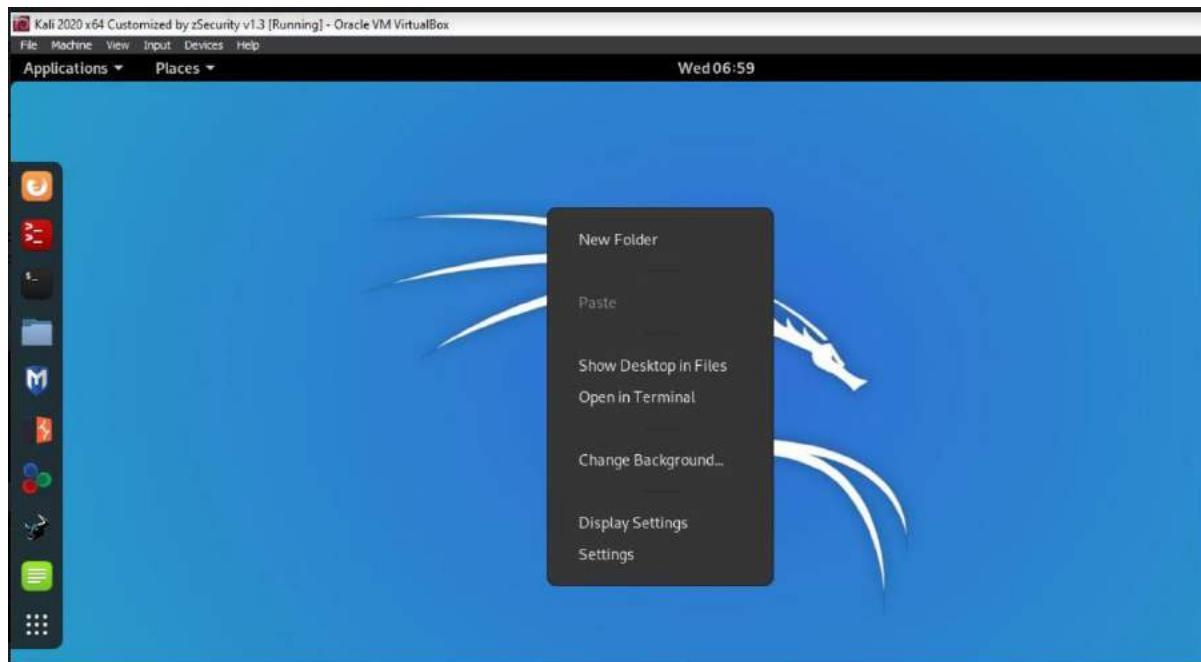
Practical

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



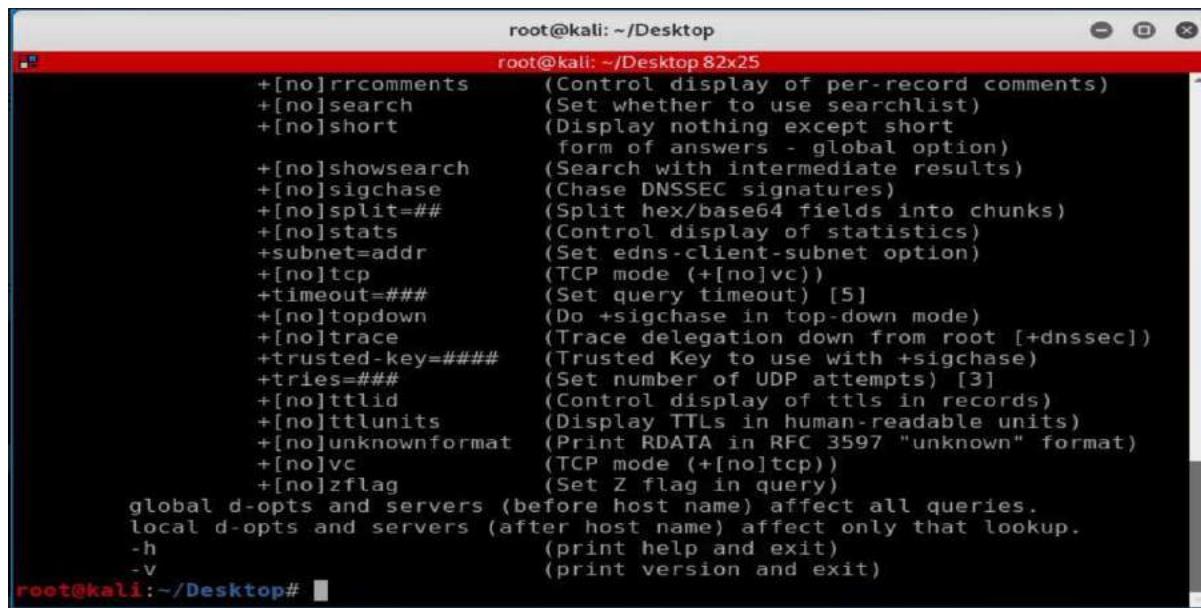
Step 2:- Now in the terminal window enter the command dig -h and press enter. You will get the following output.

A screenshot of a terminal window on Kali Linux. The command 'dig -h' is being entered at the root prompt 'root@kali: ~/Desktop#'. The terminal window has a red header bar with the text 'root@kali: ~/Desktop' and 'root@kali: ~/Desktop 8x25'. The terminal window is black with white text.

```
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# dig -h
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# dig -h
+[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)
```

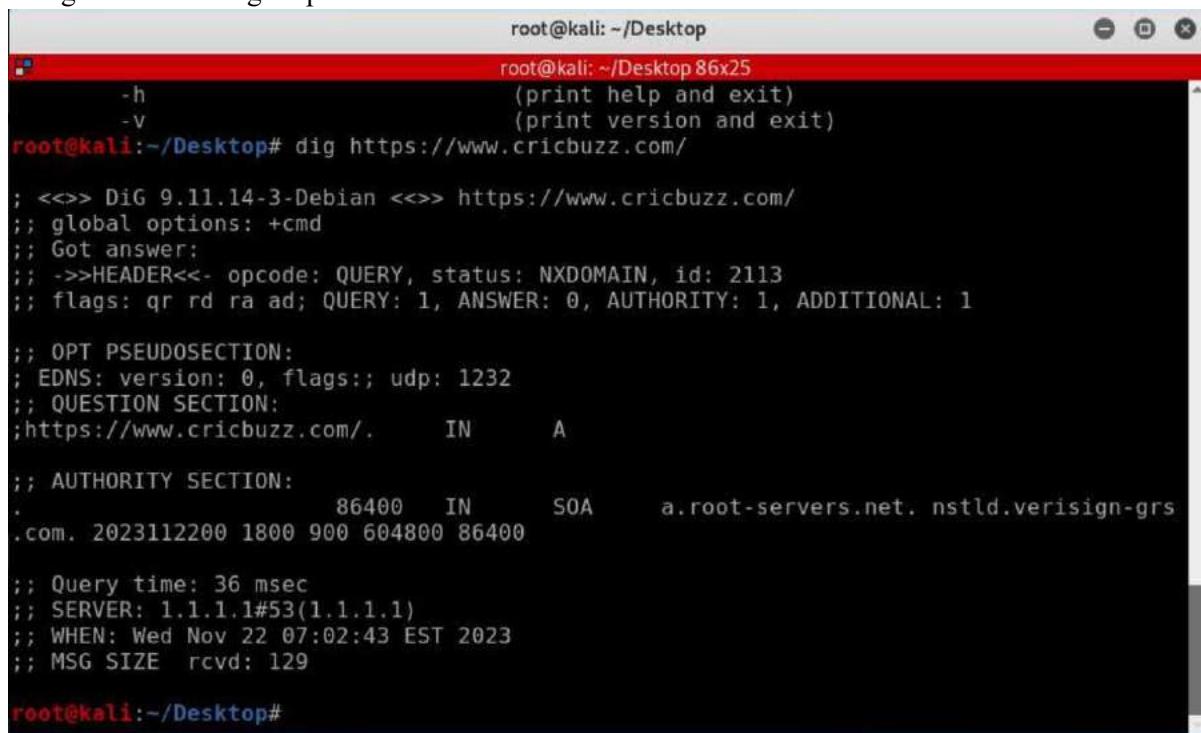


```

root@kali: ~/Desktop
root@kali: ~/Desktop 82x25
+[no]rrcomments      (Control display of per-record comments)
+[no]search          (Set whether to use searchlist)
+[no]short           (Display nothing except short
                      form of answers - global option)
+[no]showsearch      (Search with intermediate results)
+[no]sigchase         (Chase DNSSEC signatures)
+[no]split=##         (Split hex/base64 fields into chunks)
+[no]stats            (Control display of statistics)
+subnet=addr         (Set edns-client-subnet option)
+[no]tcp              (TCP mode (+[no]vc))
+timeout=###         (Set query timeout) [5]
+[no]topdown          (Do +sigchase in top-down mode)
+[no]trace             (Trace delegation down from root [+dnssec])
+trusted-key=#####   (Trusted Key to use with +sigchase)
+tries=###            (Set number of UDP attempts) [3]
+[no]ttlqid           (Control display of ttls in records)
+[no]ttlunits          (Display TTLs in human-readable units)
+[no]unknownformat    (Print RDATA in RFC 3597 "unknown" format)
+[no]vc                (TCP mode (+[no]tcp))
+[no]zflag             (Set Z flag in query)
global d-opts and servers (before host name) affect all queries.
local d-opts and servers (after host name) affect only that lookup.
-h                  (print help and exit)
-v                  (print version and exit)
root@kali: ~/Desktop#

```

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



```

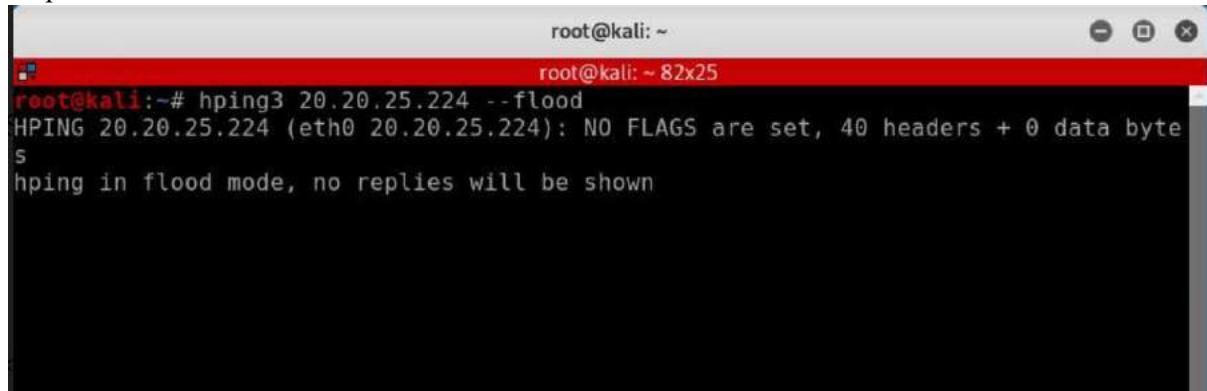
root@kali: ~/Desktop
root@kali: ~/Desktop 86x25
-h                  (print help and exit)
-v                  (print version and exit)
root@kali: ~/Desktop# dig https://www.cricbuzz.com/
; <>> DiG 9.11.14-3-Debian <>> https://www.cricbuzz.com/
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 2113
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;https://www.cricbuzz.com/. IN A
;; AUTHORITY SECTION:
.          86400 IN SOA a.root-servers.net. nstld.verisign-grs
.com. 2023112200 1800 900 604800 86400
;; Query time: 36 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Wed Nov 22 07:02:43 EST 2023
;; MSG SIZE rcvd: 129
root@kali: ~/Desktop#

```

3) Hping3

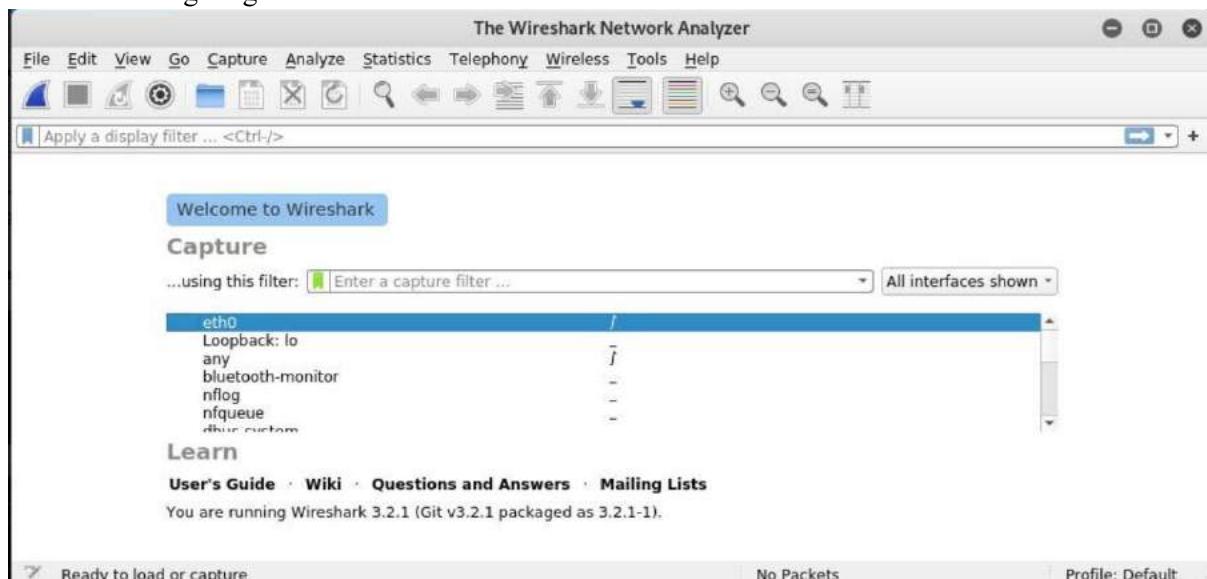
Hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols.

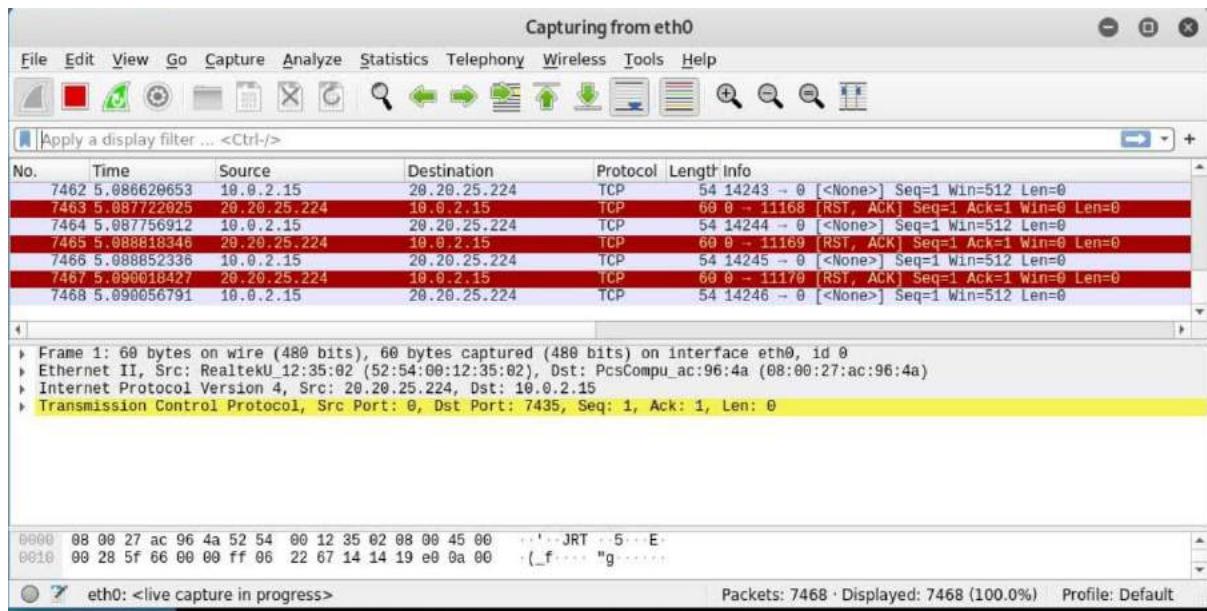
Step 1:- In Kali Linux, open the terminal and enter the command ‘hping3 20.20.24.224--flood’ and press enter, you will get the following output.



```
root@kali: ~
root@kali: ~ 82x25
root@kali:~# hping3 20.20.25.224 --flood
HPING 20.20.25.224 (eth0 20.20.25.224): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Step 2:- Now go to Applications and run Wireshark, select eth0 as interface as shown in the figure given below.





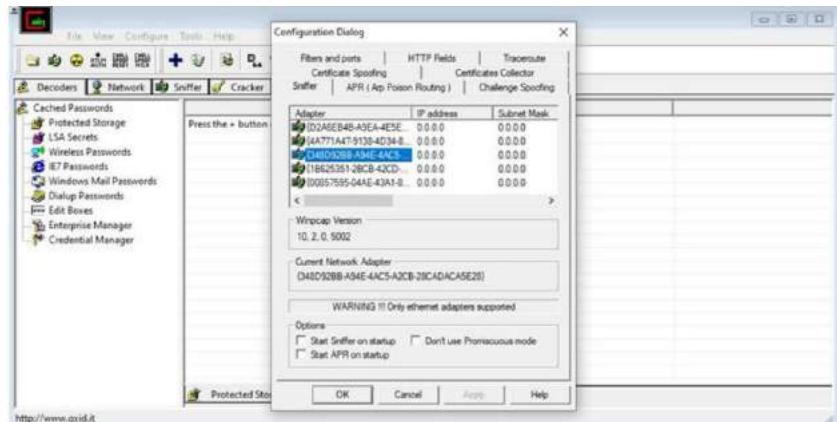
Practical

Network Sniffing.

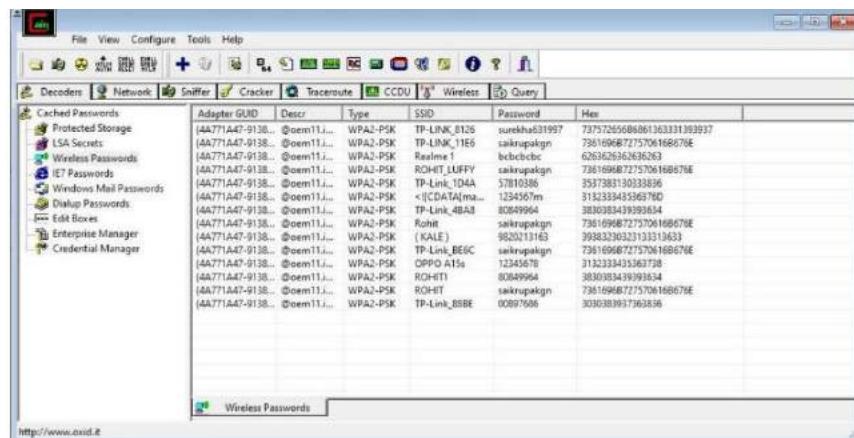
1) Cain & Cabel

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

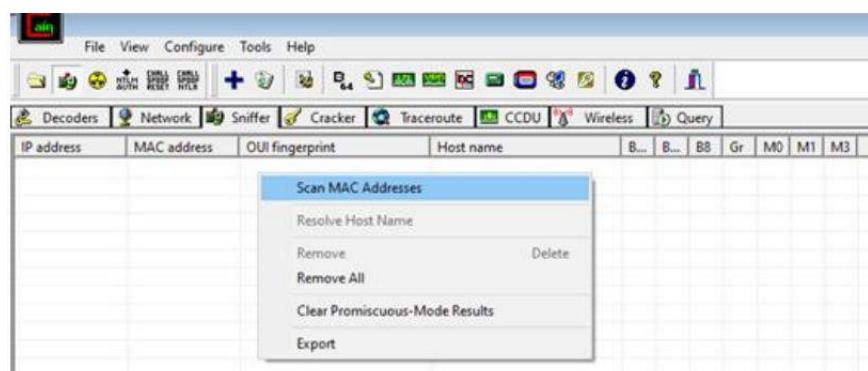
Step1: Open Cain n Abel. Click on configure. Select Adapter

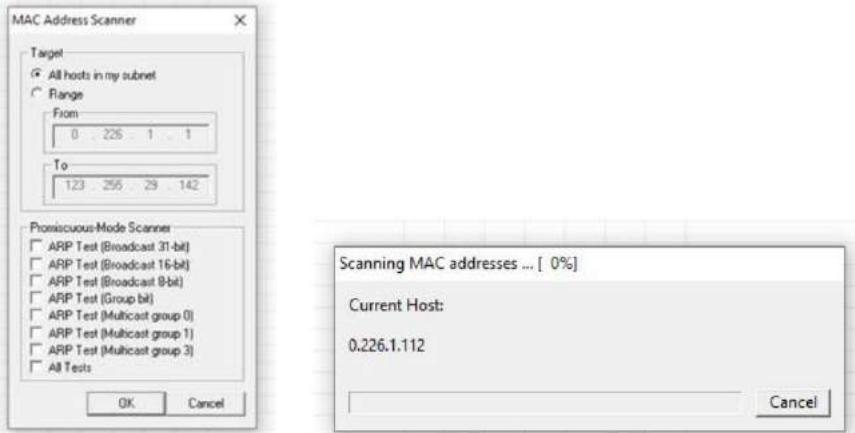


Step2: Go to Wireless password option to get wireless passwords

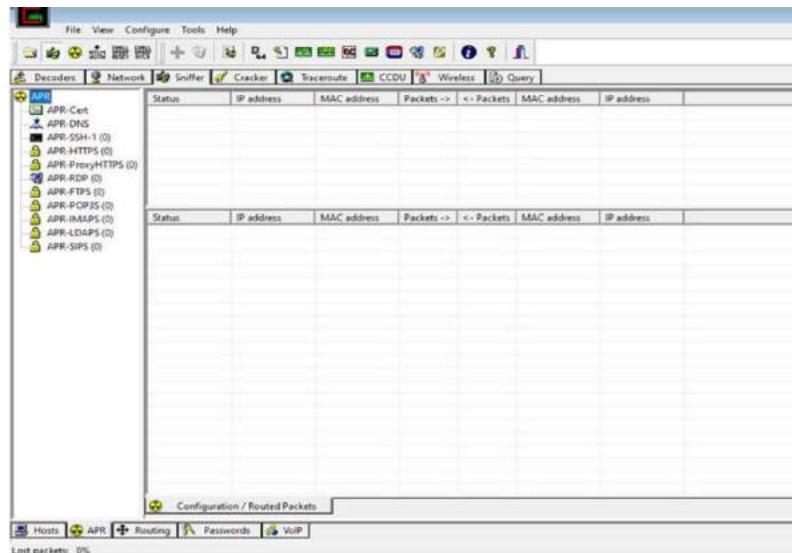


Step3: Activate Sniffer by clicking LAN Card Icon. Right click on sniffer list and choose scan MAC address. Select all tests

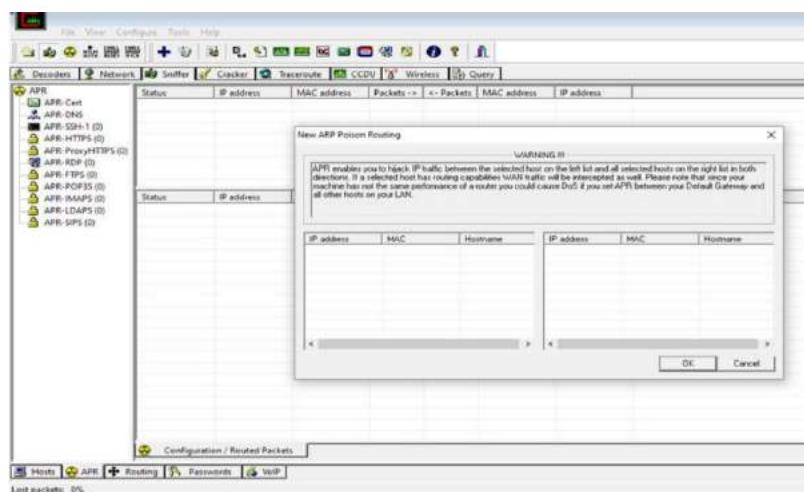




Step4: Activate apr. Click apr tab and click add to list.



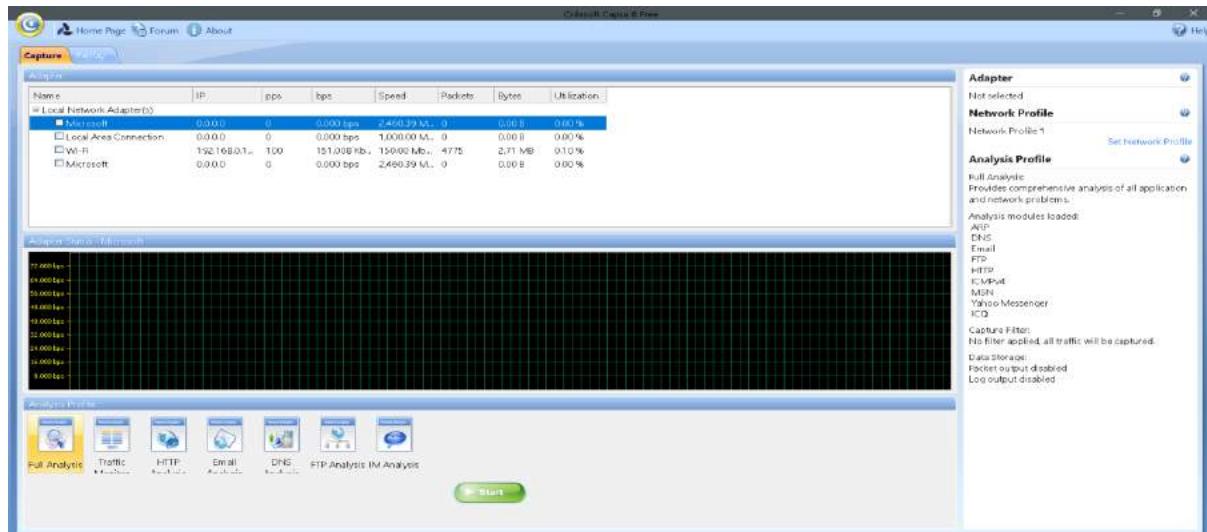
Step5: Choose machines between which you want to poison.



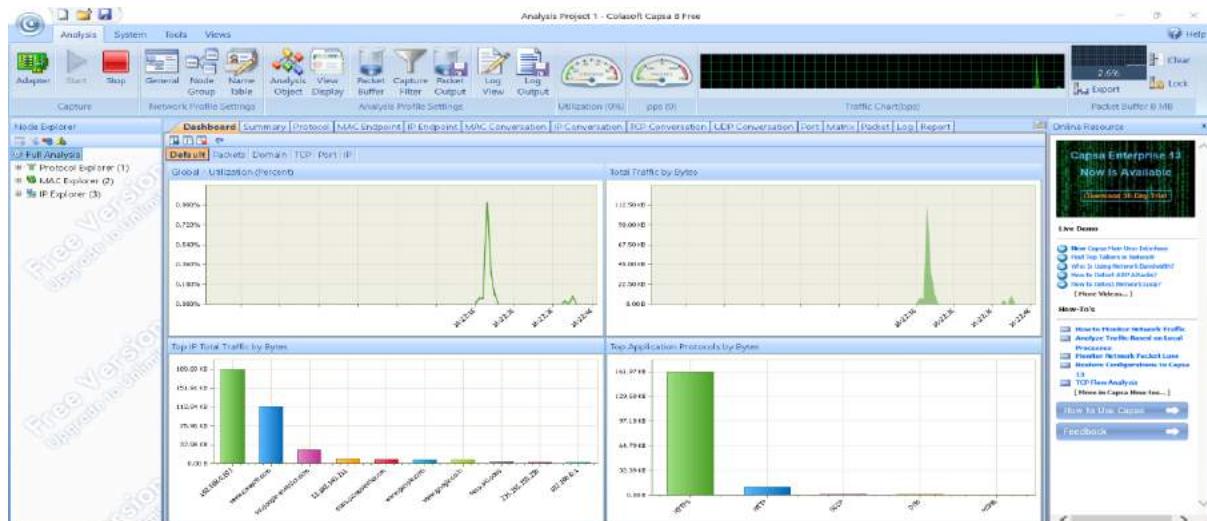
2) Caspa free Network Analyser

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

The screenshot shows the NetworkMiner interface. At the top, there's a navigation bar with tabs: Dashboard, Summary (which is selected), Protocol, MAC Endpoint, IP Endpoint, MAC Conversation, IP Conversation, and TCP Co. Below the navigation bar is a toolbar with icons for file operations.

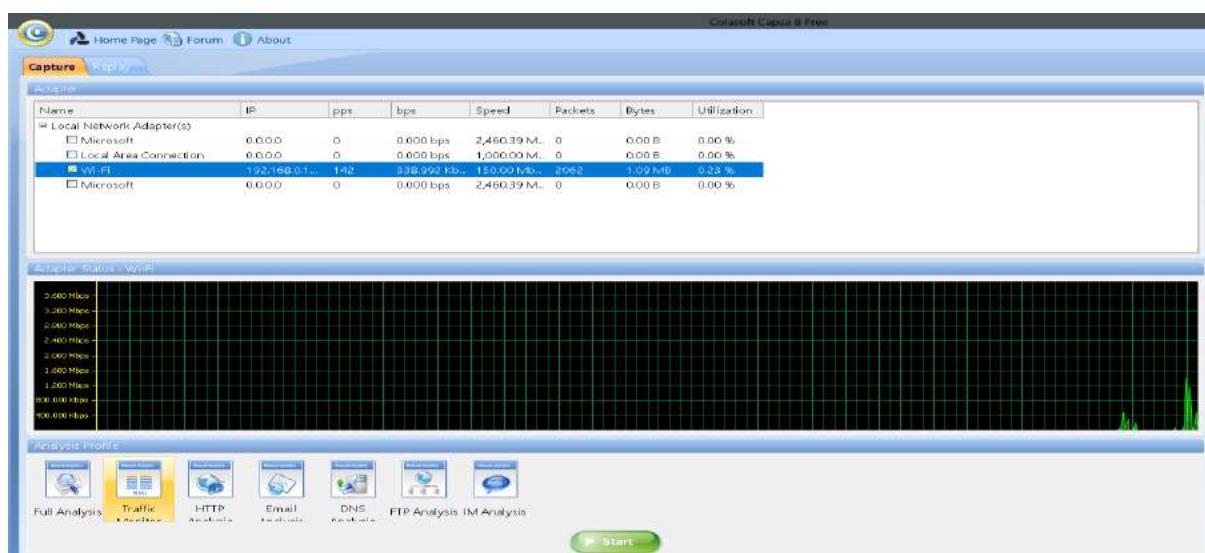
The main area displays a table of network statistics. The columns are: Statistics Item, Bytes, Packets, Utilization, bps, and pps. The table includes sections for Traffic, Pkt Size Distribution, Address, Protocol, and Conversation. The 'Traffic' section shows:

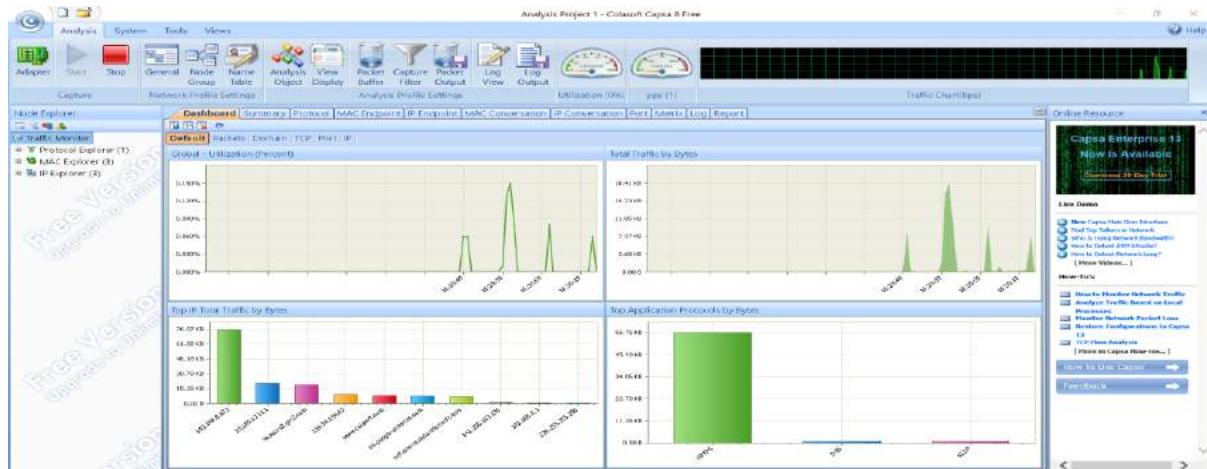
	Bytes	Packets	Utilization	bps	pps
Total	271.88 KB	731	0.003%	3.160 Kbps	4
Broadcast	92.00 B	2	0.000%	0.000 bps	0
Multicast	3.83 KB	20	0.002%	1.768 Kbps	1
Average Packet Size				380.000 Bytes	

The 'Pkt Size Distribution' section shows the count of packets for different sizes (e.g., <=64, 65-127, 128-255, etc.). The 'Address' section lists MAC and IP addresses with their counts. The 'Protocol' section lists various layers with their counts. The 'Conversation' section shows MAC conversations with their counts.

At the bottom of the interface, there are status indicators: -Fi, Network Profile 1 - Bandwidth - 100Mbps, Inactive 00:02:10, 731, 0, and Ready.

Step 3 : Now for Traffice Monitor-> Dashboard.





Summary

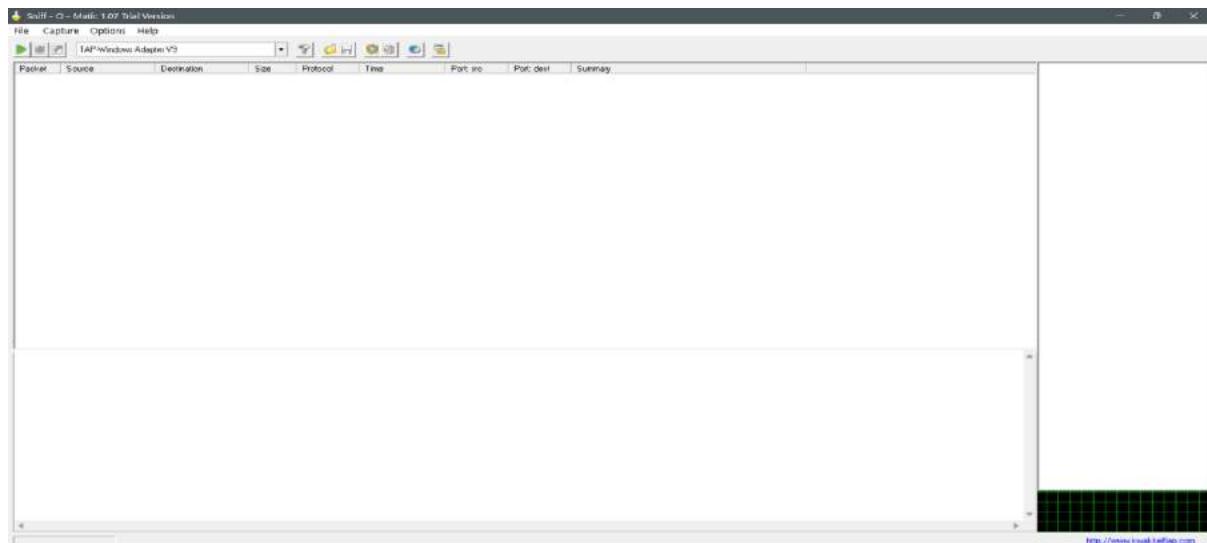
This screenshot shows the 'Summary' tab of the Colasoft Capsa 8 Free interface. It displays a detailed table of network statistics across various categories. The table includes columns for 'Statistics Item', 'Current Value', and specific metrics like 'Bytes', 'Packets', 'Utilization', 'bps', and 'pps'. The categories include Traffic, Pkt Size Distribution, Address, and Protocol.

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	5.59 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.

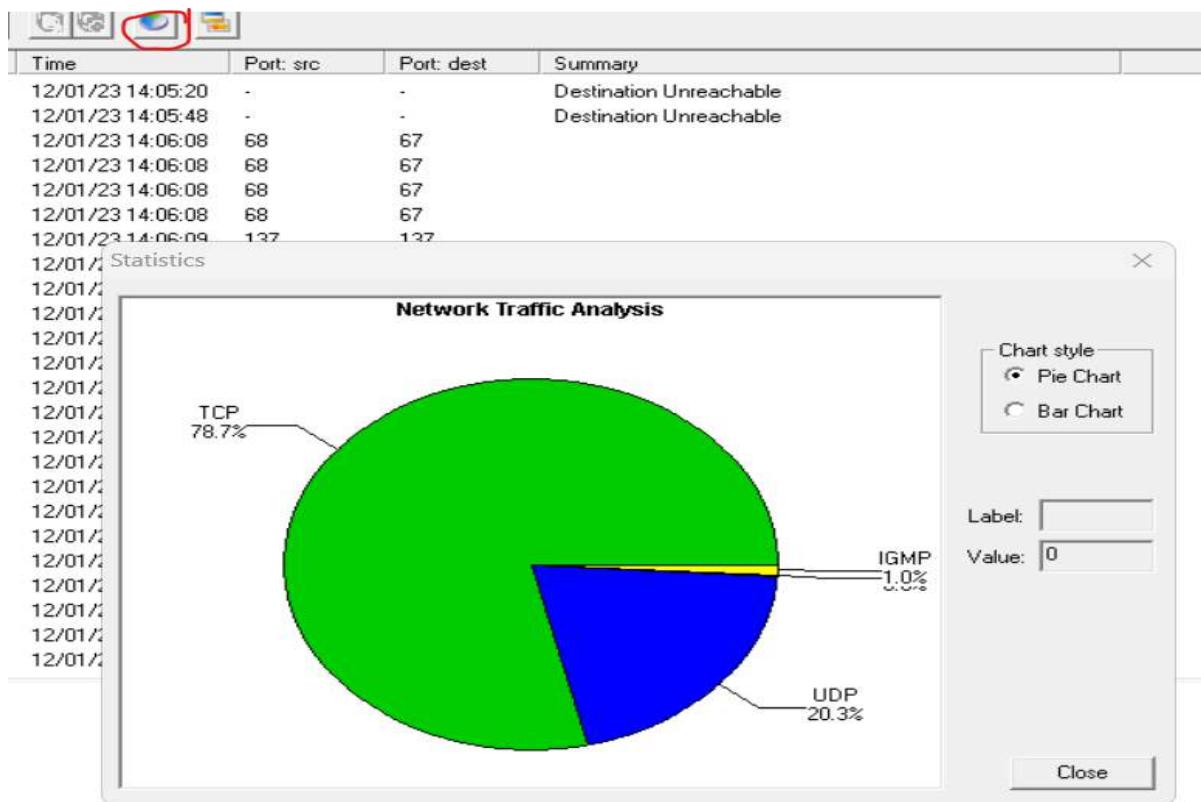
Step1: Download and run the Tool



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

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	

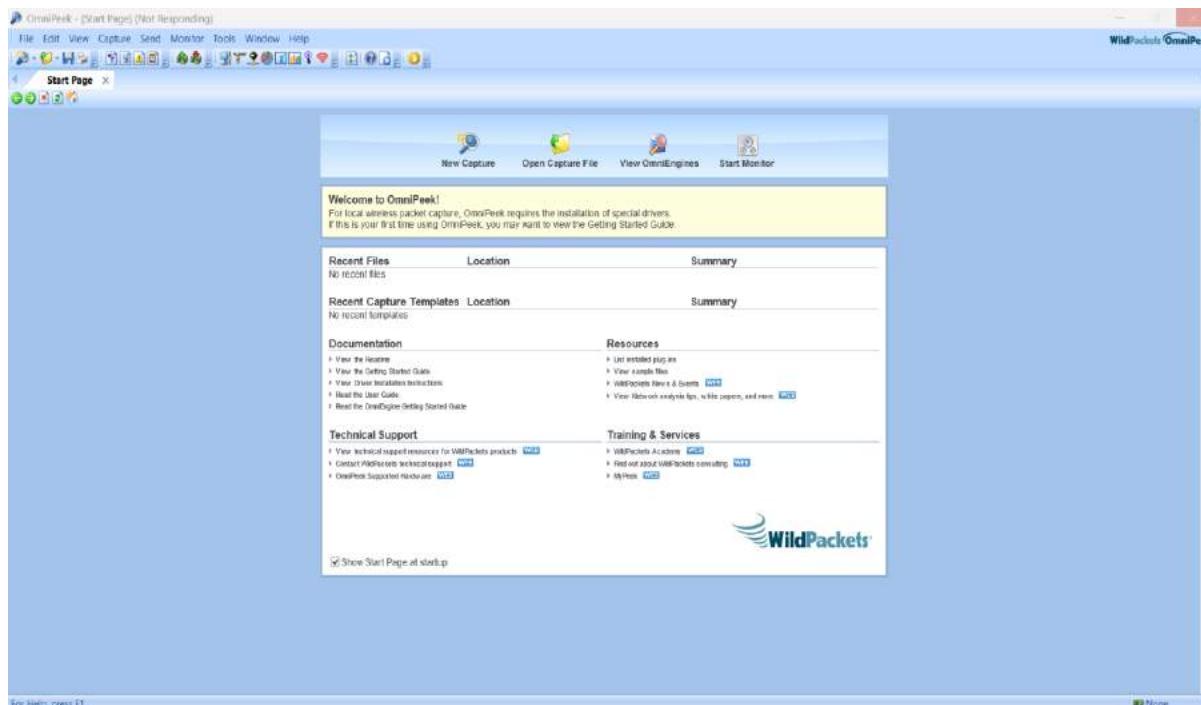
Step3: click on the statistics option.



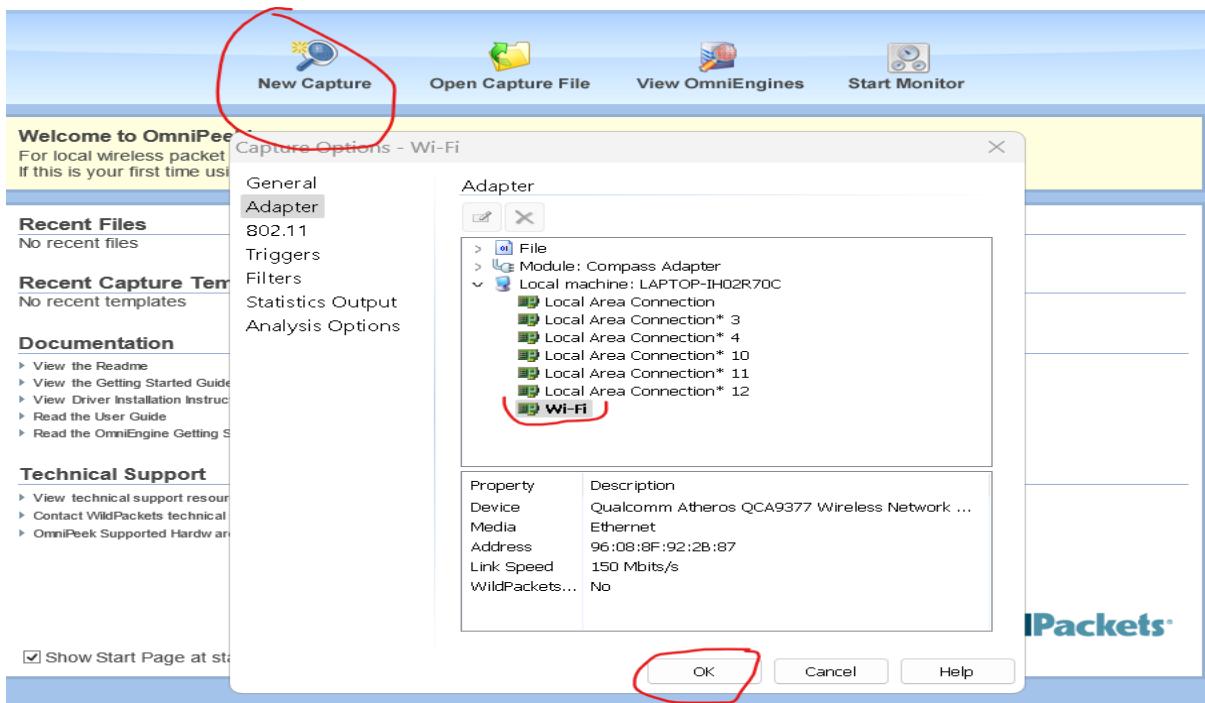
4) OmniPeek

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

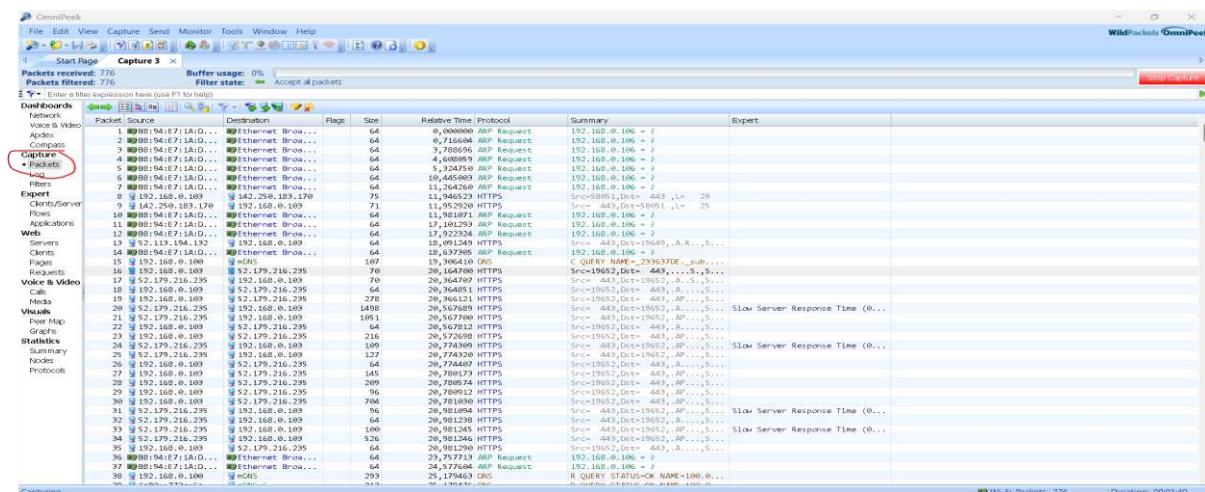
Step 1 : OpenOmniPeek Network Analyzer Software.



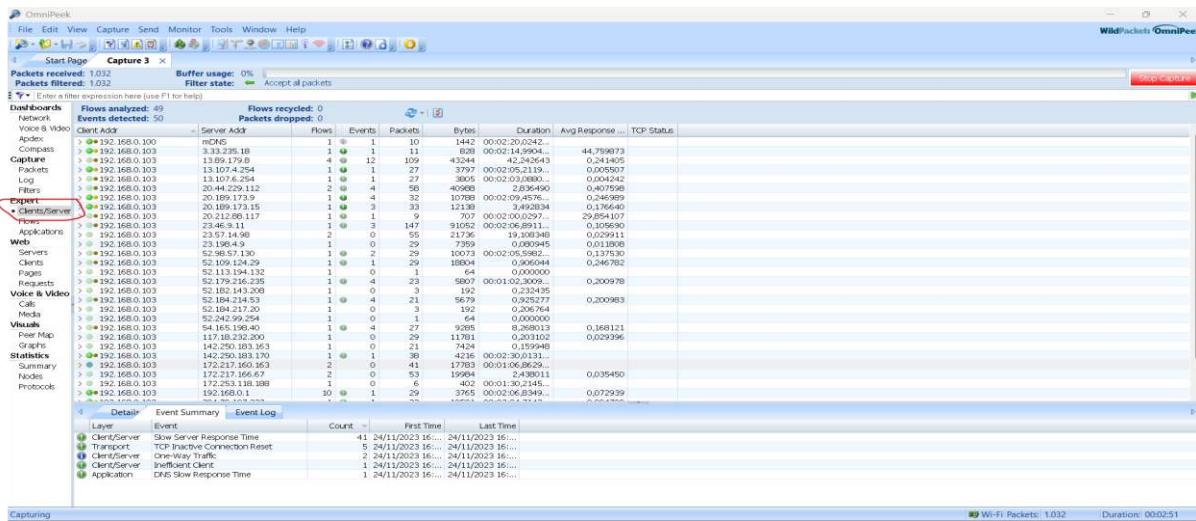
Step 2 : Select Wi-Fi and click on start.



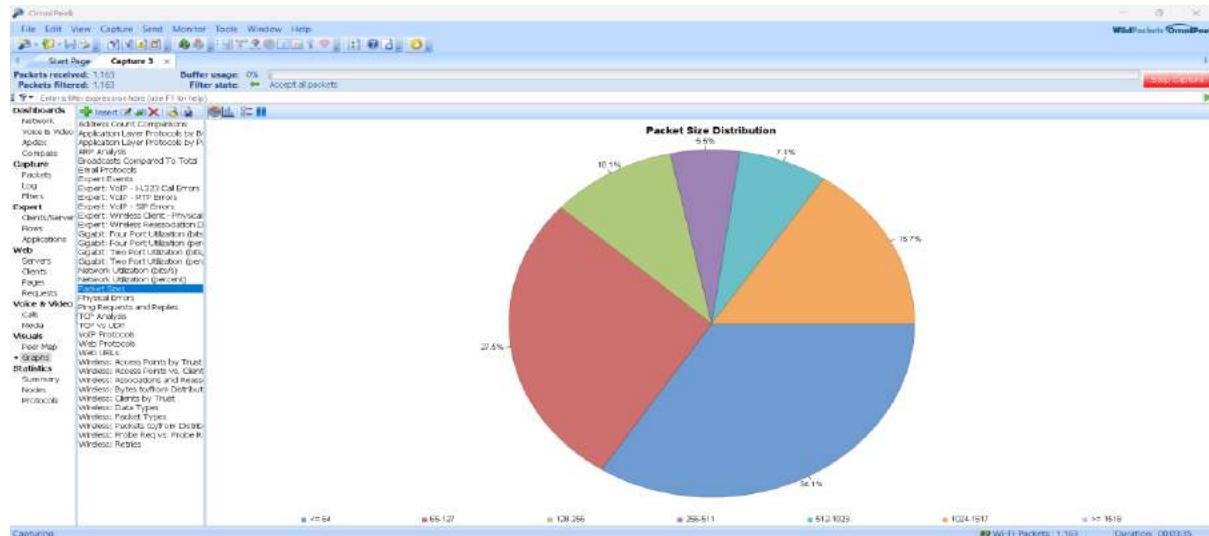
Step 3 : Go to Capture-> Packets to see the source and destination of a traffic.



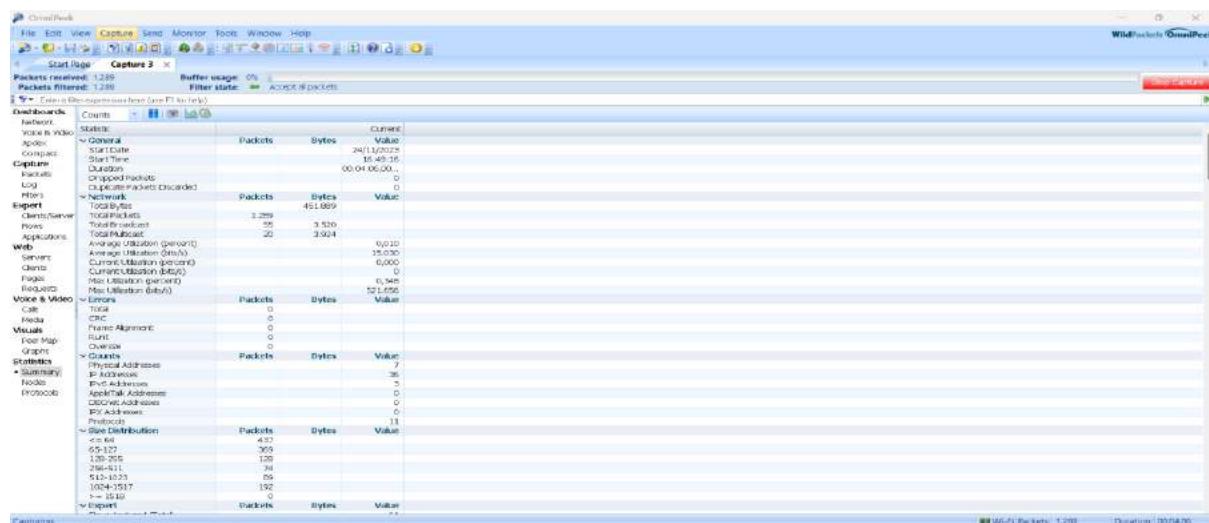
Step 4 : Go to Expert-> Client address and Server address.



Step 5 : Go to Visuals-> Graph.

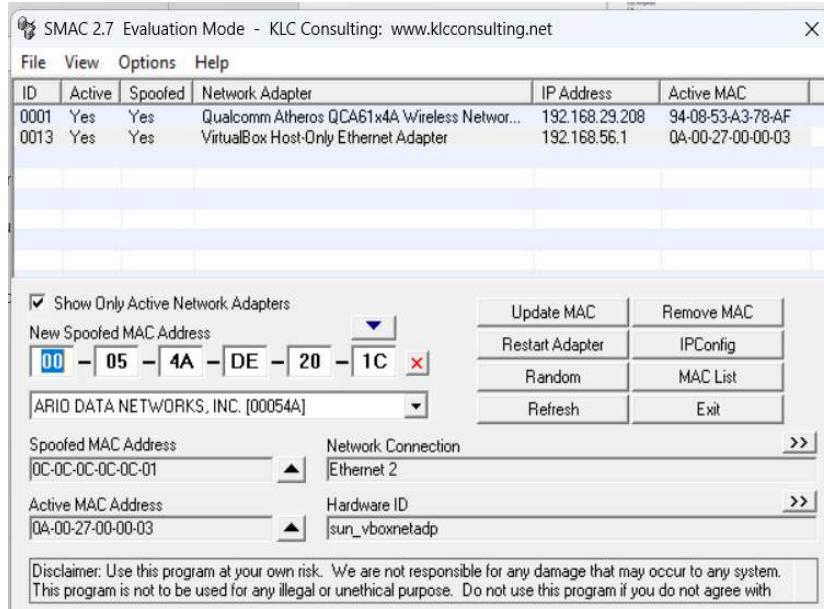


Step 6 : Go to Statistics-> Summary.

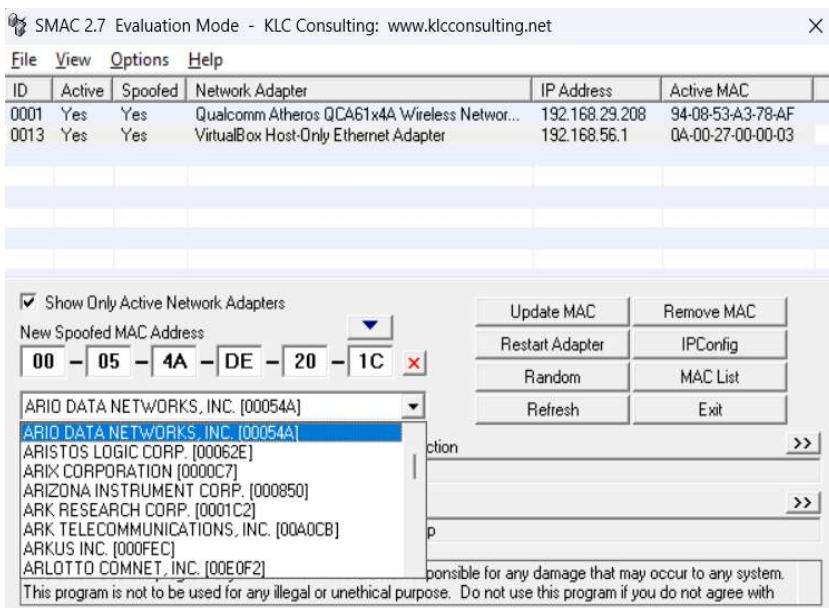


5) SMAC

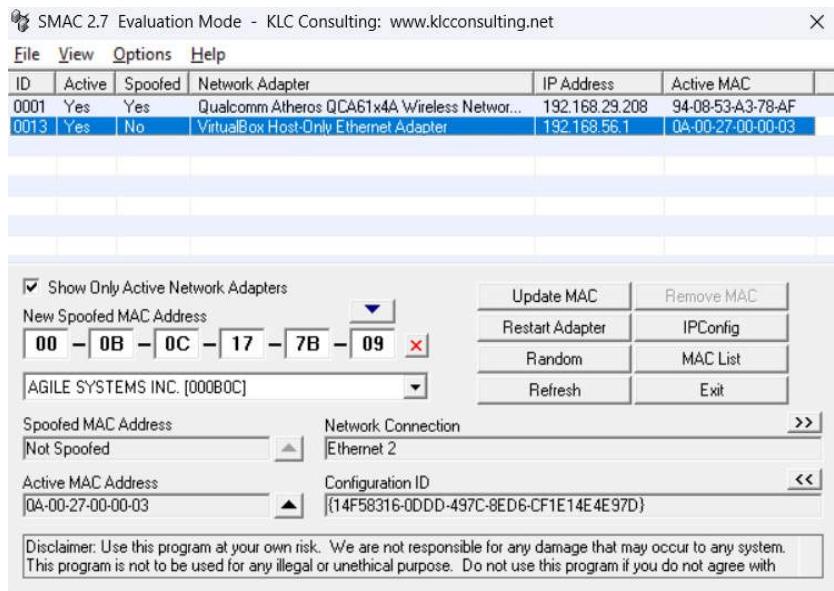
Step 1: Open SMAC, go to options and click on automatically restart adapter. Now select one network adapter. Now either you can manually type in the mac address or click on the arrow to get mac address or click on random to get mac address.



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] > <u>marketplace search</u>						
	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

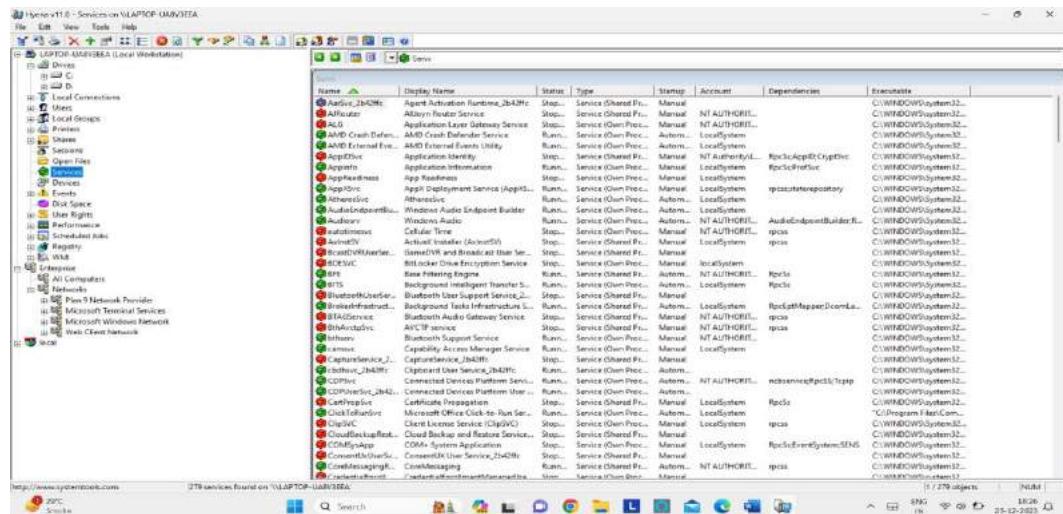
-----
GOOGLE.COM
-----
[*] URL: http://whois.arin.net/rest/pocs;domain=Google.com
[*] URL: http://whois.arin.net/rest/poc/CREEK14-ARIN
[*] [contact] Alex Creek (alexcreek@google.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/ABA104-ARIN
[*] [contact] Ari Barkan (ari@google.com) - Whois 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.

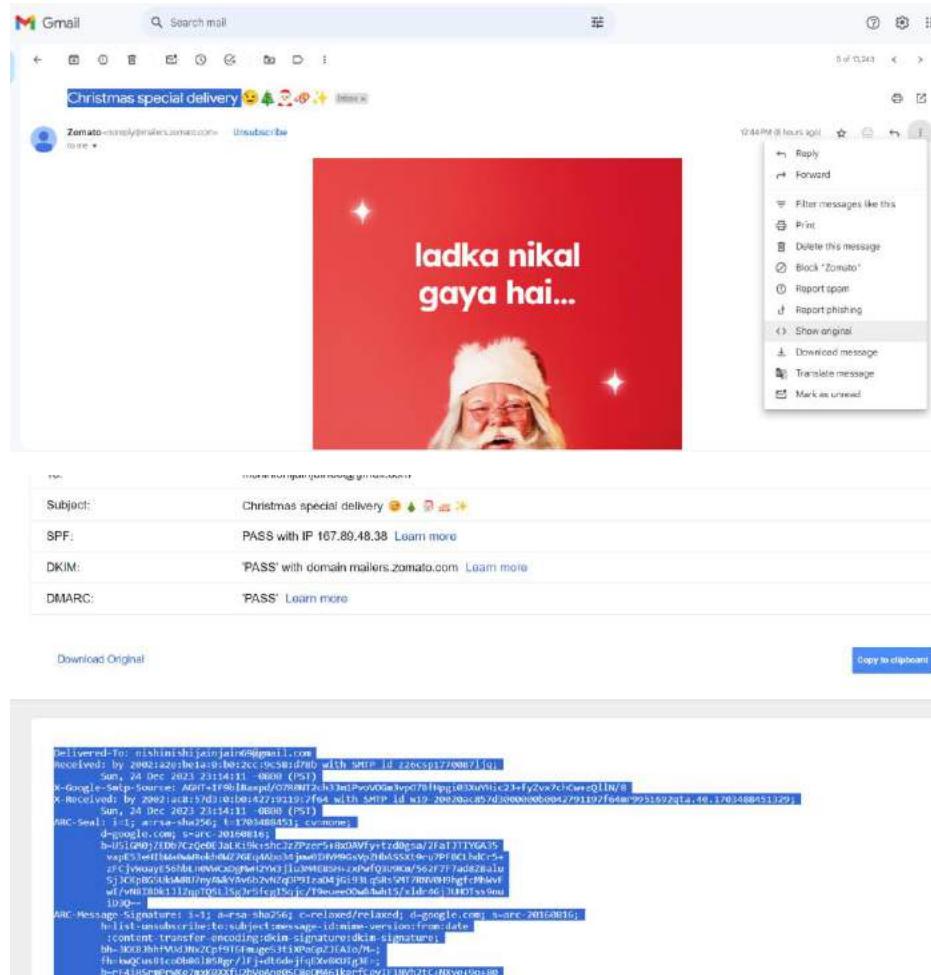


3) EmailTrackerPro

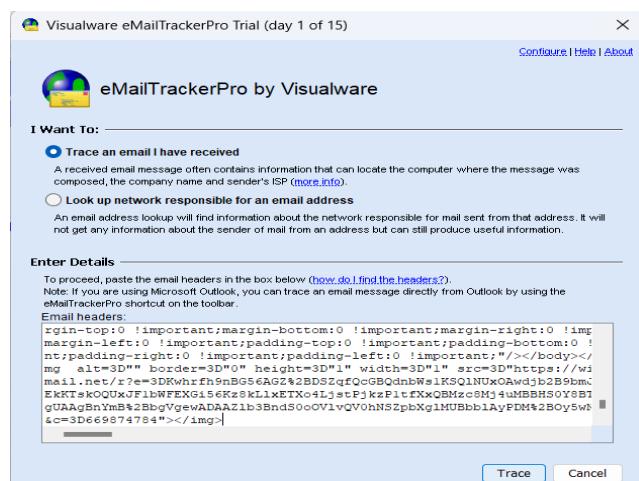
Step1: Open the application and click on I want to trace an email



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



Step3: Now copy the entire dataset it into the email headers section and click on trace



The trace has started

The trace is running, data will update as it becomes available.

Email Summary

From: noreply@mailers.zomato.com
To: nishnishijainjain69@gmail.com
Date: Mon, 25 Dec 2023 07:14:09 +0000 (UTC)
Subject: Christmas special delivery 🎄🎁
Location: ???

Misdirected: No
Abuse Address: Tracing...
Abuse Reporting: To automatically generate an email abuse report [click here](#)
From IP: 167.89.48.38

Network Whois
Domain Whois
Email Header

You are on day 1 of a 15 day trial. To apply a licence [click here](#) or for purchase information [click here](#).

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

The trace is complete, the information found is displayed on the right

Email Summary

From: noreply@mailers.zomato.com
To: nishnishijainjain69@gmail.com
Date: Mon, 25 Dec 2023 07:14:09 +0000 (UTC)
Subject: Christmas special delivery 🎄🎁
Location: [America]

Misdirected: No
Abuse Address: abuse@sendgrid.com
Abuse Reporting: To automatically generate an email abuse report [click here](#)
From IP: 167.89.48.38

System Information:

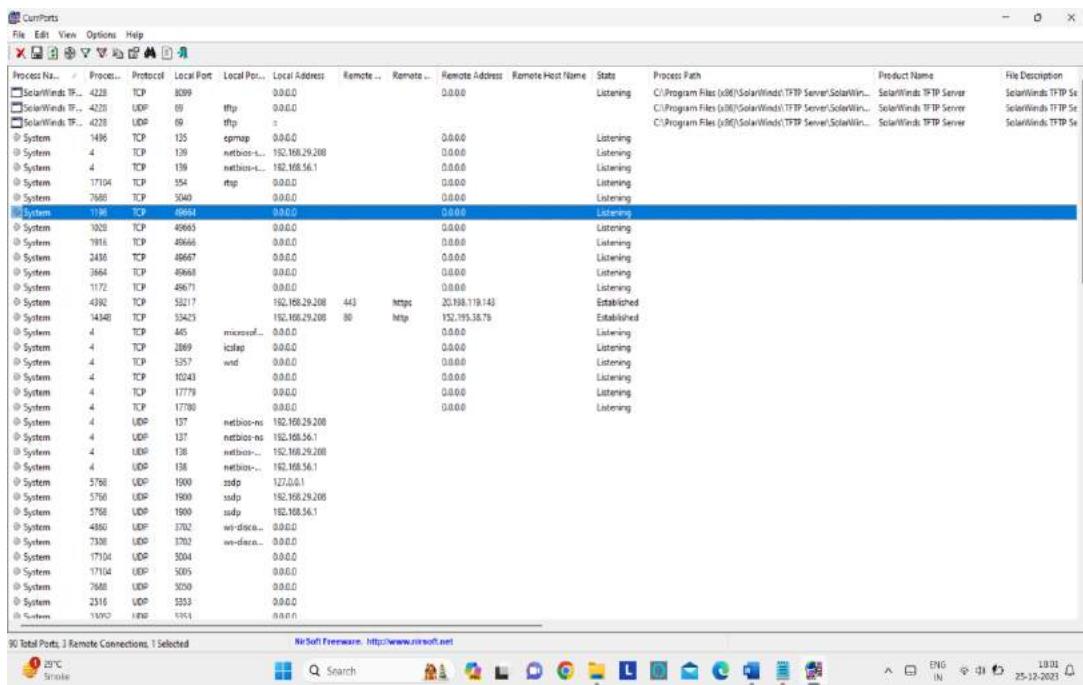
- There is no SMTP server running on this system (the port is closed).
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

Network Whois
Domain Whois
Email Header

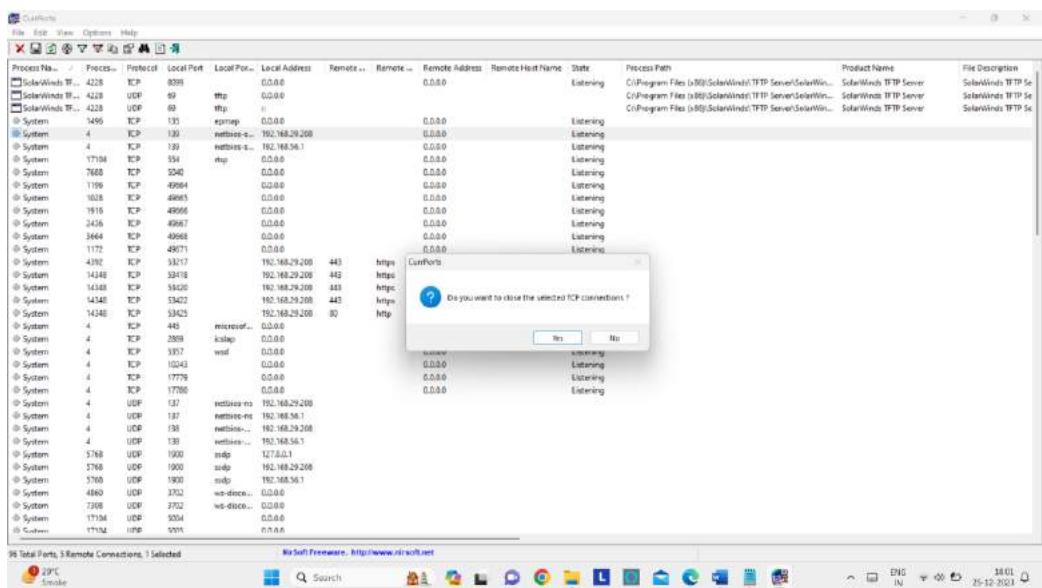
You are on day 1 of a 15 day trial. To apply a licence [click here](#) or for purchase information [click here](#).

4) Currports

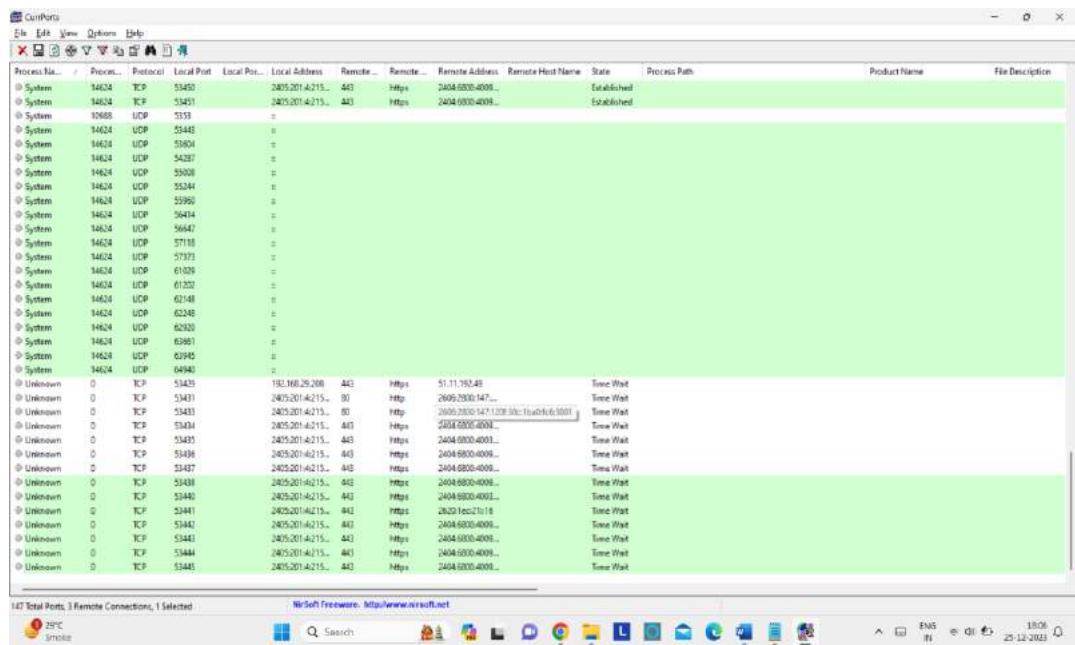
CurrPorts displays the list of all currently opened TCP/IP and UDP ports on your local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file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



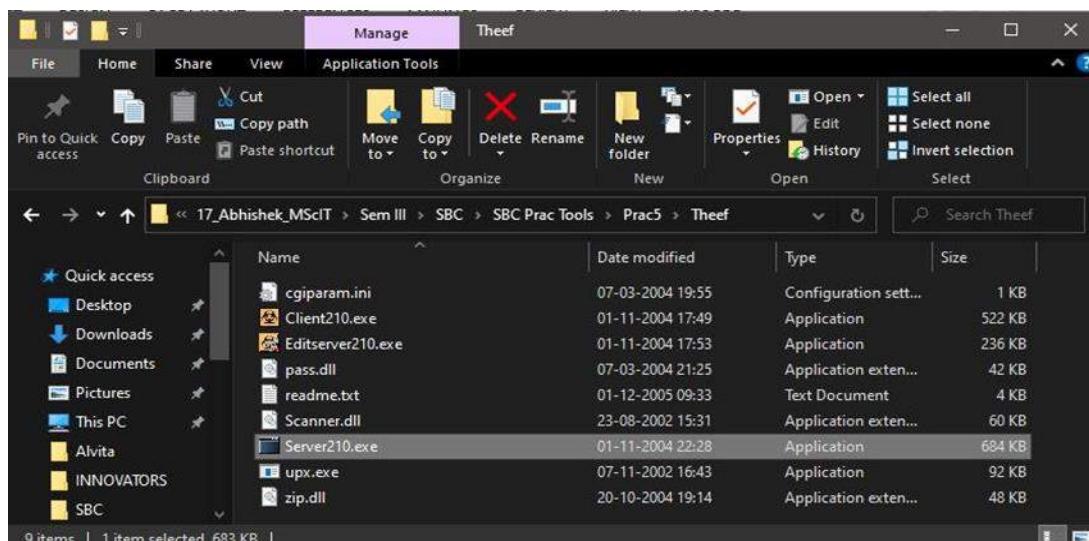
CurrPorts also automatically mark with green color for active TCP/UDP ports owned by applications



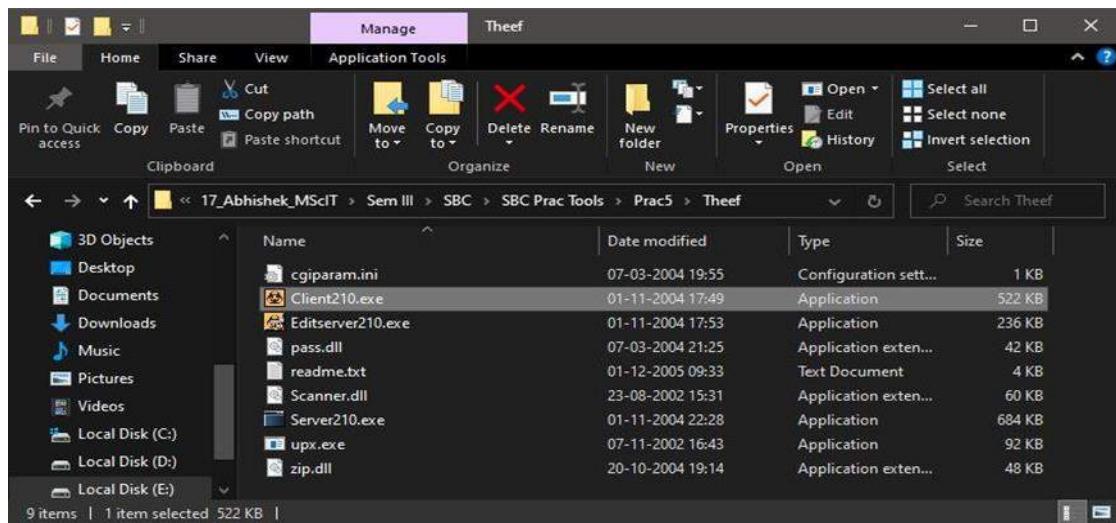
5)Theef

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.

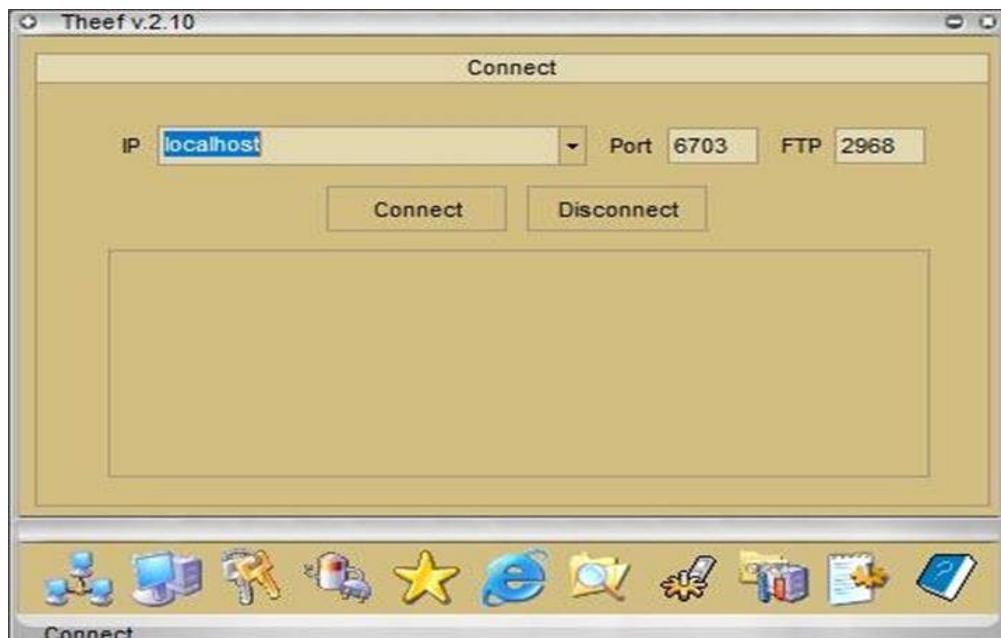
Step 1 : Double-click Server210.exe to run the Trojan.



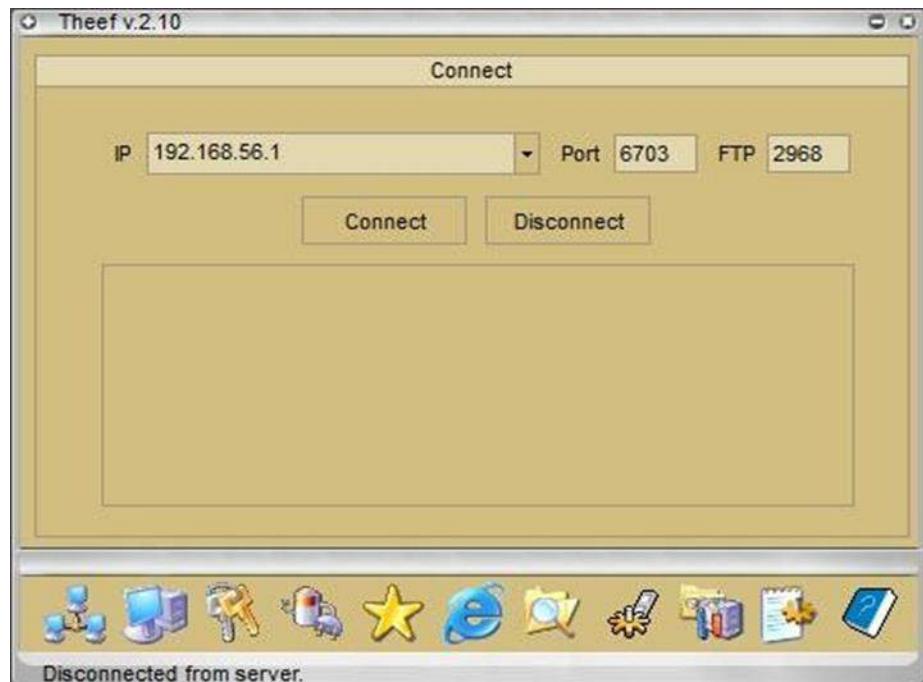
Step2: Double click on Client210.exe to access the victim machine remotely



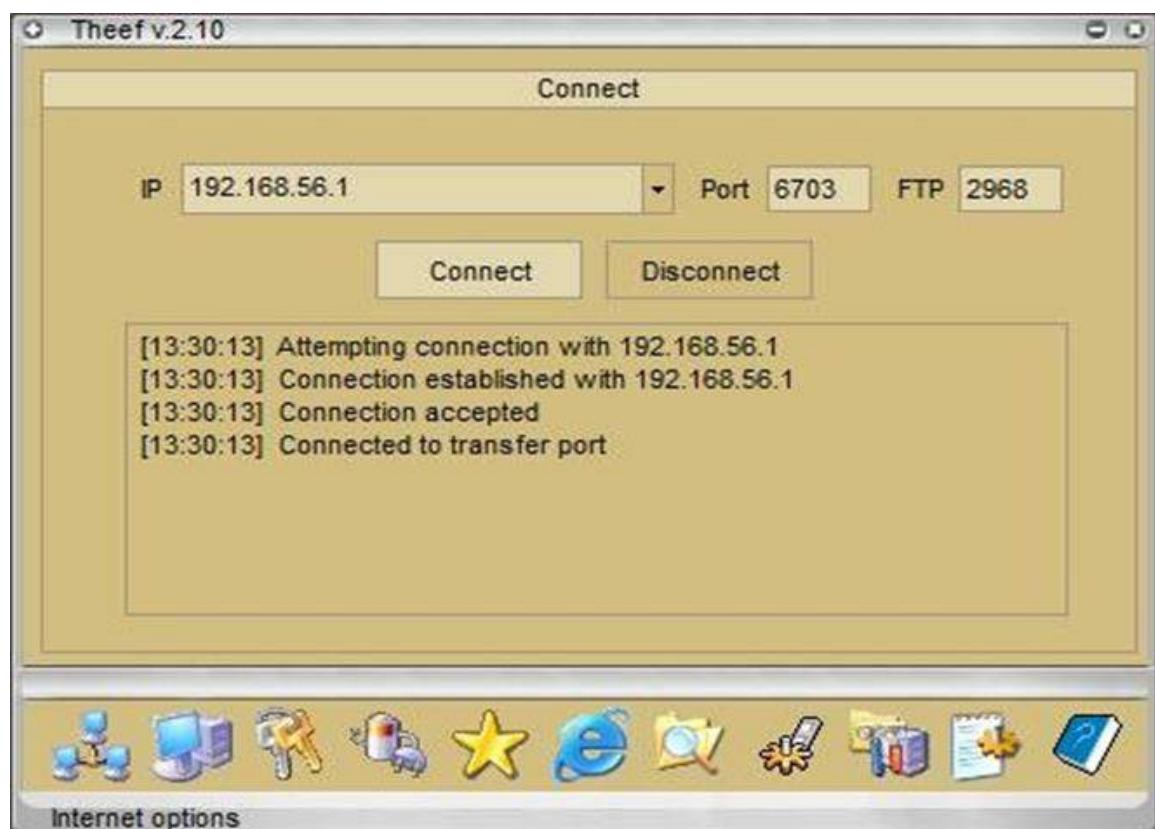
Step3: The main window of theef appears



Step 4 : Enter an IP address in the IP field, and leave the port and FTP fields as their default. 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 the window. In Computer



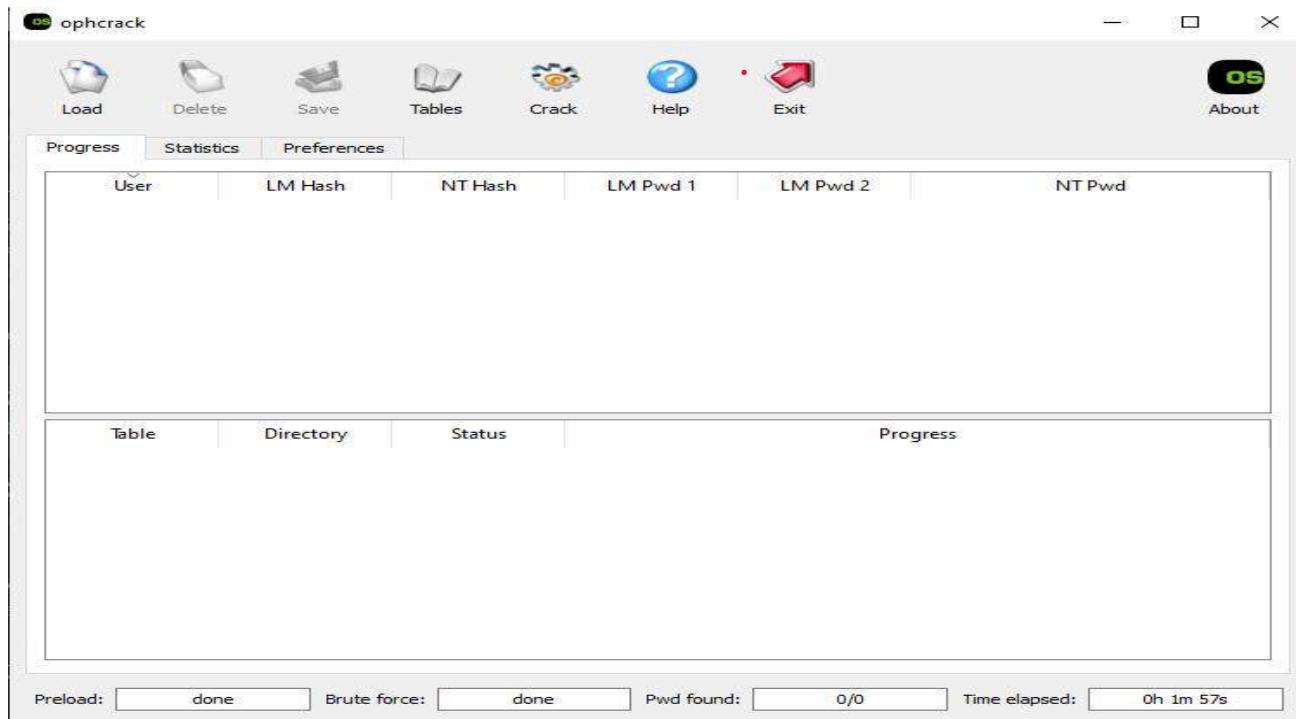
Information, you are able to view PC Details, OS Info, Home, and Network by clicking on their respective buttons.



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

Character Set:
Bahikk@3333

Length:	Passwords:	Generate Passwords	Calculate Hashes
7	32		

Passwords:

```
3Bka@33
k3hkk3h
kB31333
3ik33k8
ka3kB3a
kkB1h33
aBkaih@
33Bk3a3
hk3@333
@k3333
B333kh
33@B3hi
k33k33k
3kB333@
k33333@
hBkB@3@
```

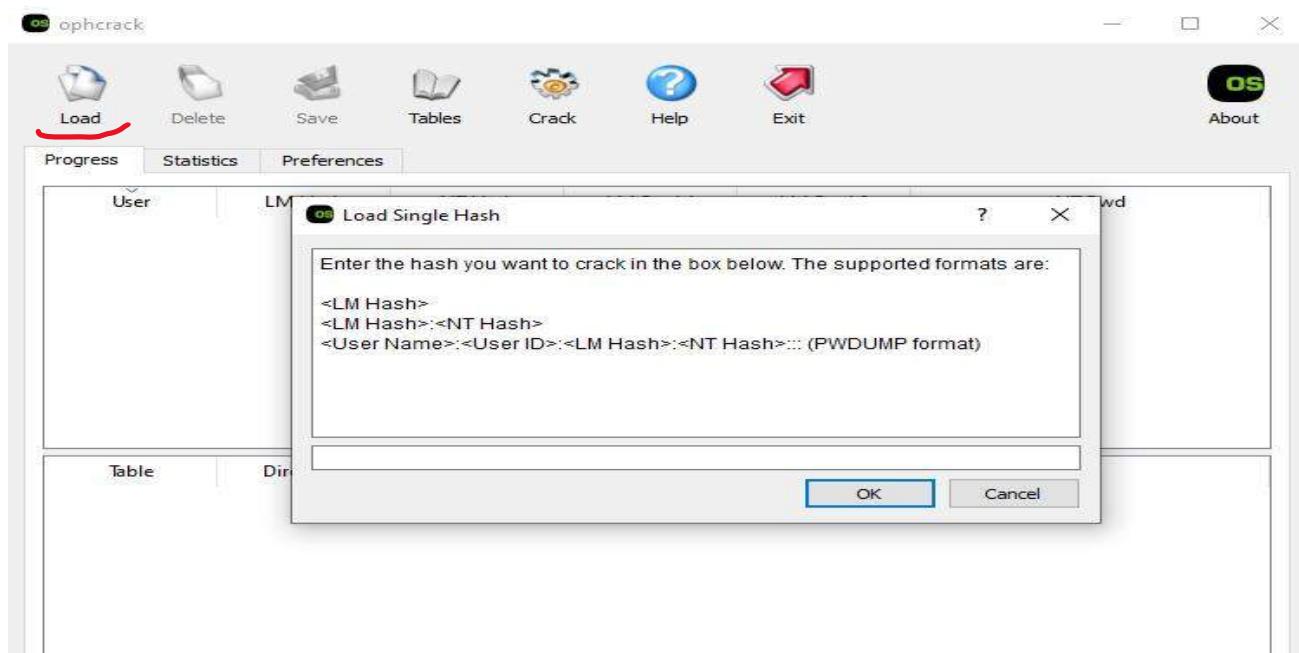
NTLM Hashes:

```
3ED744E0217B1C91FDB7827718572621
3C38C4134D2DEE64D269103B3215C30B
392AC42172BF7E1DC339B75FD8BAB255
EE3F4941301E3B31F8B77540F5C9EBAA
0BEA2352D1844839C5E9703E386CEBD1
80595A3E45681655C5F146E7A108F382
8FF59AEBD8D5AE7521E05AAF7D8C0A92
49F4AEAD04F5D089658CBBAECB5C4996F
27F32790F211224E934C7BC8B14CFBSA
AA5385E0AF8F8D84E92DE2240F34BAAB
6D2062CD2BEB7E0FE621613749B273DC
6305F4A5171C6559AA99C63325A1C802
0561BD282FD381C168F2FDAB70FB19F
FA94985D87E257E527B28495523C1656
B53A6DD2CE9A647DDC721A4F0A0249D4
0C377BB9875DD307E5B08C0DC7DBB23D
```

LM Hashes:

```
5CC8689BB664CD67AAD3B435B51404EE
75BB74892CB24D75AAD3B435B51404EE
023123BF99843D6EAAD3B435B51404EE
7368A64E38906684AAD3B435B51404EE
8025E85BA423A3F2AAD3B435B51404EE
2F7EE7E08F557784AAD3B435B51404EE
E58A02FE263E77DAAAD3B435B51404EE
2C11FA73F58D1EF8AAD3B435B51404EE
78979D5A6351ECA9AAD3B435B51404EE
4BA5FC3898226C76AAD3B435B51404EE
41652149D405F829AAD3B435B51404EE
38CA075233B25AC6AAD3B435B51404EE
DF30FFE9B5981FAAD3B435B51404EE
12CBC54DB8FB3963AAD3B435B51404EE
850FB37D1B541868AAD3B435B51404EE
1D496ED552058D16AAD3B435B51404EE
```

Step 3: Now click on 'Load' to enter



Step4: Now click on crack to crack the password

