Experiment Number -4

Aim:

To study and use the tool Nmap.

Introduction:

Nmap is a tool for network Exploration, host discovery and security auditing. Some of its primary uses are Discovering network component, determining open ports and services running on a host and determine the OS running on the host. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

Lab Scenario:

A Windows machines with nmap installed in it and with internet access.

Download URL:

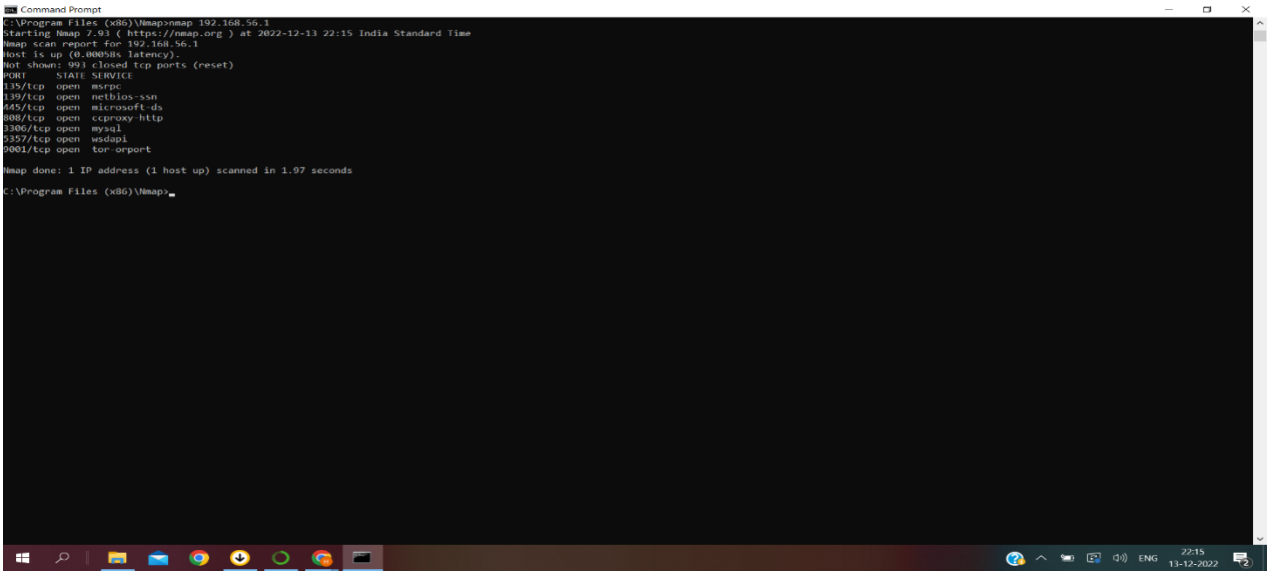
https://nmap.org/download.html

Nmap Commands:

- **Scan a Range of IP Address**

To scan the entire CIDR (classless inter-domain routing) range of IP addresses, you can use the command.

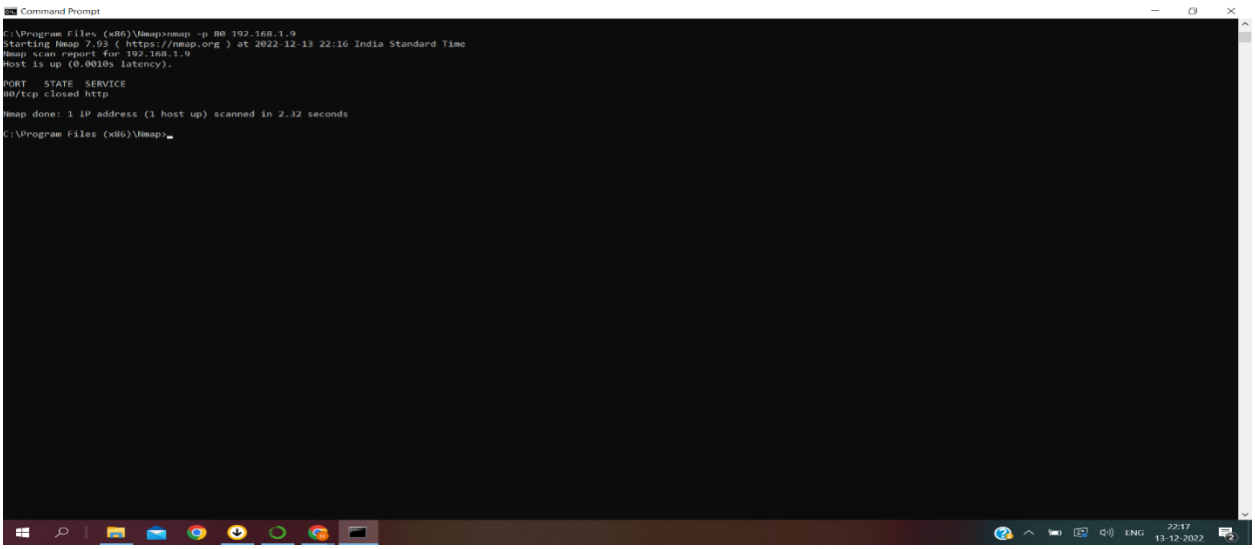
>> **nmap <IP range>**



- **Port Scanning**

Performing port scans will provide details about port services and states and not just that Nmap also provides options to scan popular ports and discover open ports. We will see that in the latter section of the article.

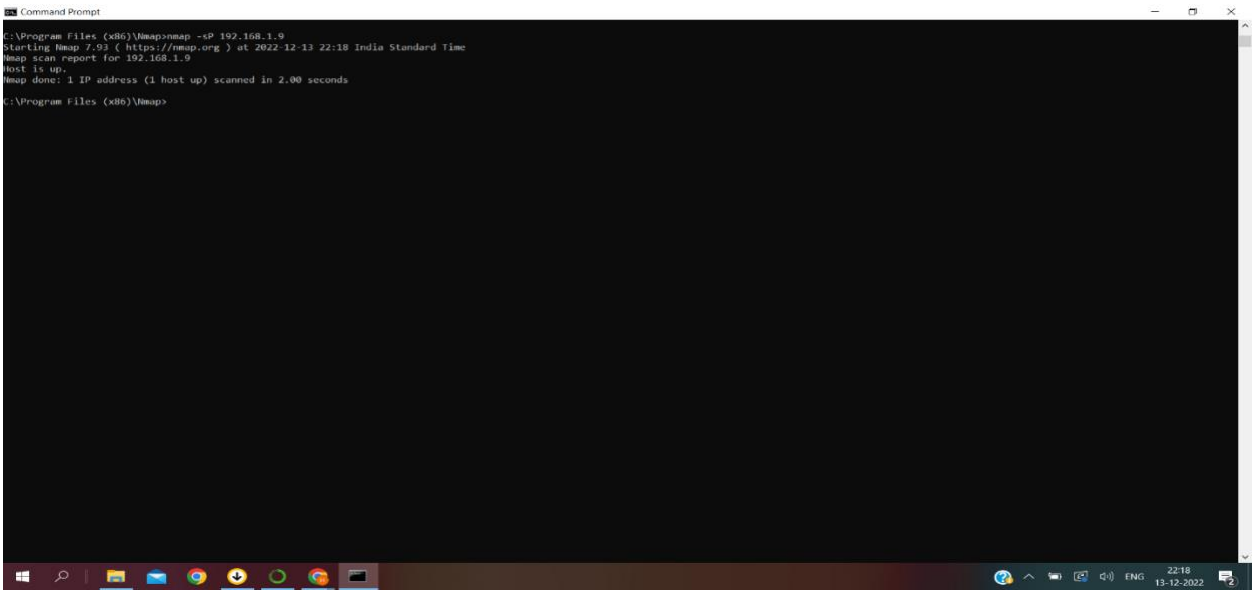
>> ***nmap -p <numeric value> <IP>***



- **Ping Scan Using Nmap**

It also provides the option to find out multiple hosts or any specific host. This command returns the IP address and MAC (Media Access Control) address of available hosts but provides no information about ports. In simple words, it finds all devices in the defined range and then we can check if there are any IP addresses that we are not familiar with or we cannot account for. This command sends an ICMP (Internet Control Message Protocol) echo request to all IP addresses of the network.

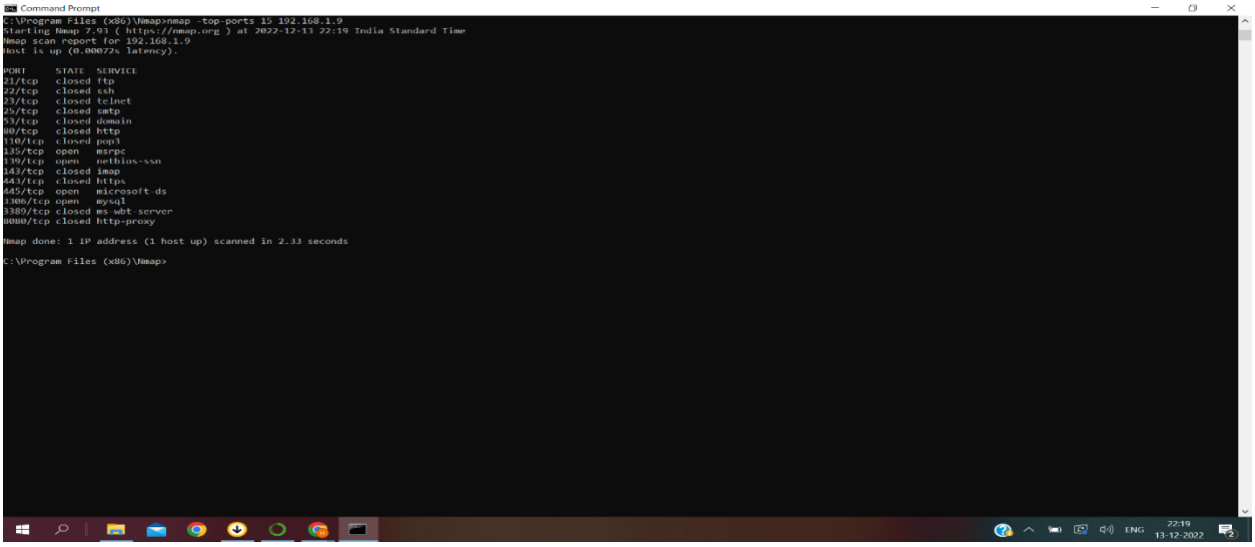
>> **nmap -sP <target>**



- **Most Popular Ports Scanning**

To apply this command, we must use the "–top-ports" option with a specific numeric value. This option gives you the ability to scan top ports. However, in Nmap, you also have the option to select the number of top ports to scan. This command allows users to get better and faster results.

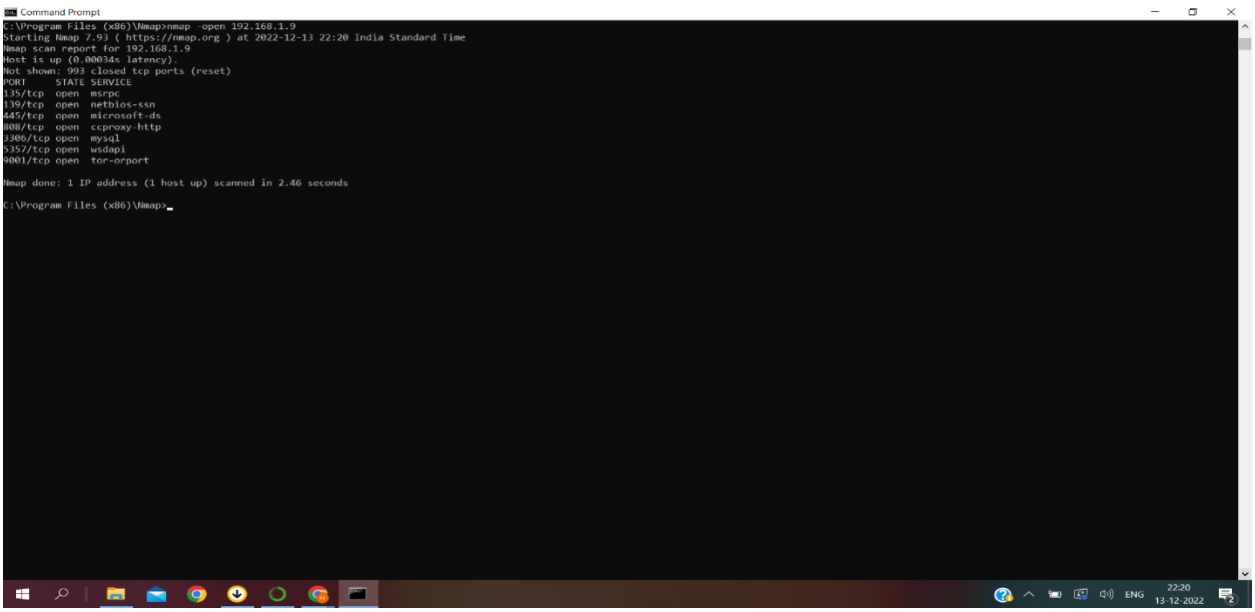
>> **nmap –top-ports <numeric value> <IP address/Domain>**



- **Display Open Ports**

Finding open ports (target ports that respond to UDP/TCP/SCTP requests) can be the first step to protecting and hacking any network. And if you only want to find ports you can connect to, this command can be useful to you.

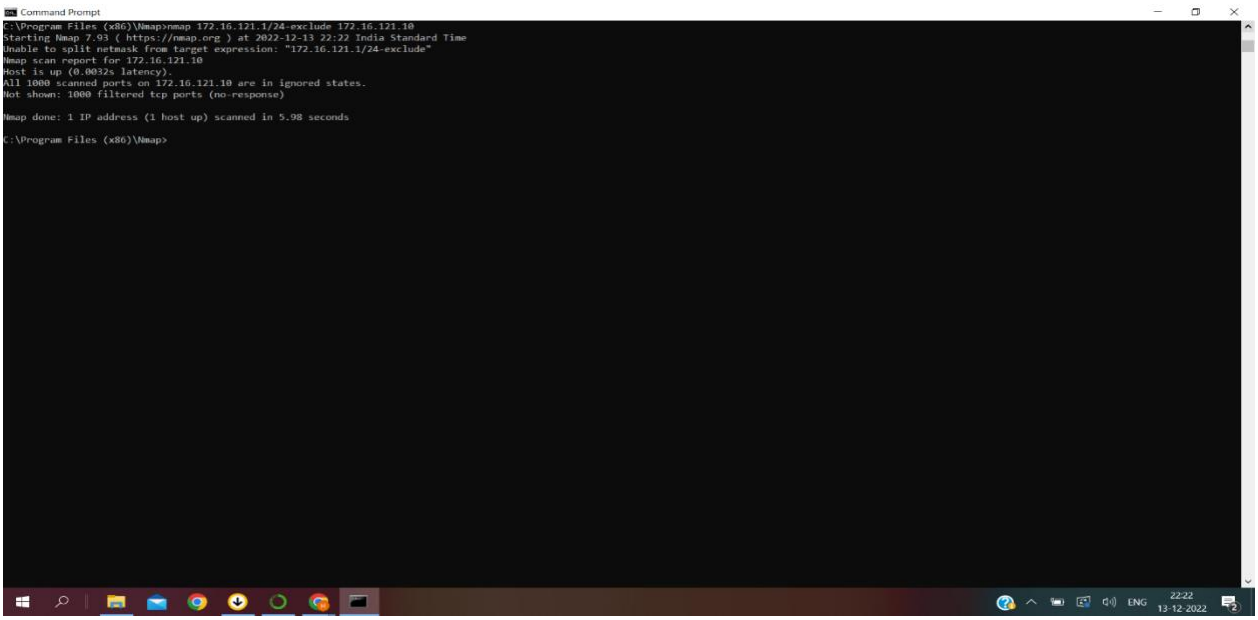
>> **nmap — open<IP address/domain name>**



- **Exclude Host/ IP Addresses for the Scan**

If you want to exclude hosts/ IP address/ network, Nmap provides you with a specific command for this purpose. As the name suggests this command excludes a single target/list of the target from the scan.

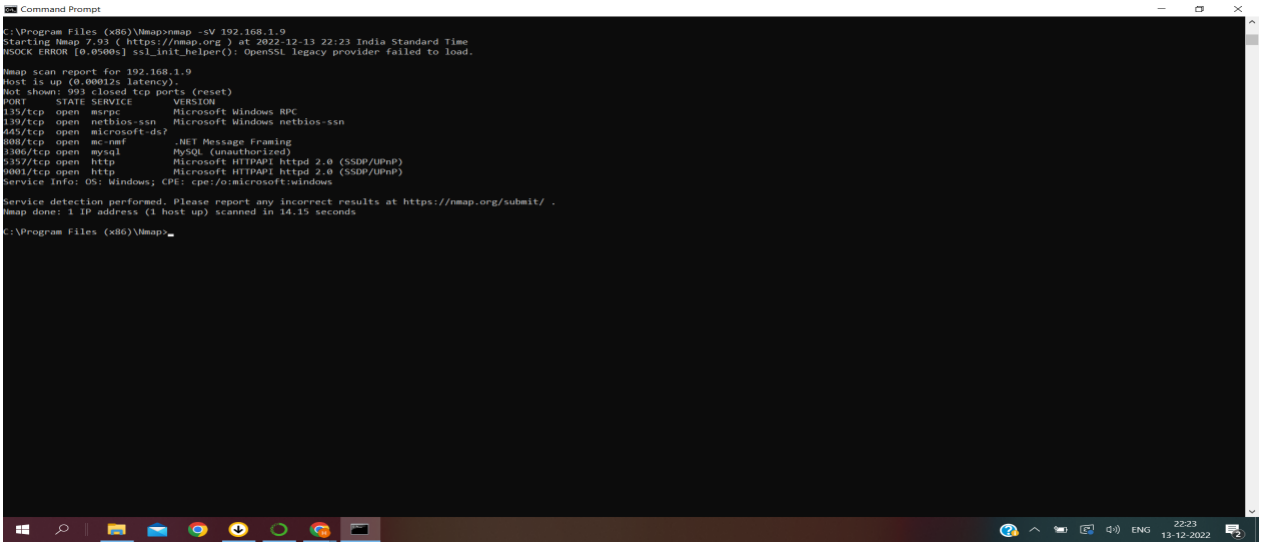
>> **nmap <range of IP address> — exclude<IP address to exclude>**



- **Service Version Detection**

Nmap has a database of more than 2000 services and associated ports for example– SSH (port 22) and HTTP (port 80). So, while doing network inventories if you want to know which versions are running, you can use the Nmap version detection (-sV) command. Knowing the exact version number can be helpful while finding which exploits your server is vulnerable to.

>> **nmap -sV<IP>**



Conclusion:

All the commands from nmap are tested and verified.

Experiment – 5

Aim:

To use and understand the HTTrack tool.

Lab Scenario:

A Windows machine with free space and accessible internet connection.

HTTrack:

HTTrack is a free (GPL, libre/free software) 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. HTTrack arranges the original site's relative link-structure. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online. HTTrack can also update an existing mirrored site, and resume interrupted downloads. HTTrack is fully configurable, and has an integrated help system.

HTTrack Programming:

- **How to get one single file;**

httrack --get http://localhost/

- **How to get one single file and pipe it to stdout;**

httrack --quiet --get http://localhost/ -O tmpget -V "cat \$0" | grep -iE "TITLE" rm -rf tmpget

- **How to search in all HTML files on a website;**

httrack --skeleton http://localhost/ -V "if grep -iE \"TITLE\" \"\$0\">/dev/null; then echo \"Match found at \$0\"; fi" rm -rf tmpget

Same thing but matches only the first file:
httrack --skeleton http://localhost/ -V "if grep -iE \"TITLE\" \"\$0\">/dev/null; then echo \"Match found at \$0\"; kill -9 \$PPID; fi" rm -rf tmpget

- **Indexing a website, and using the index as a search engine**

httrack localhost -%I
Will generate an index.txt file, which contains all detected keywords, sorted, and indexed using this format:

Keyword
<tab> number_of_hits_in_current_page_for_this_keyword page_location
<tab> number_of_hits_in_current_page_for_this_keyword page_location
<tab> number_of_hits_in_current_page_for_this_keyword page_location
...
=total_number_of_hits_for_this_keyword
((total_number_of_hits_for_this_keyword*1000)/total_number_of_keywords)

How to use:

Step 1: Choose a project name and destination folder.

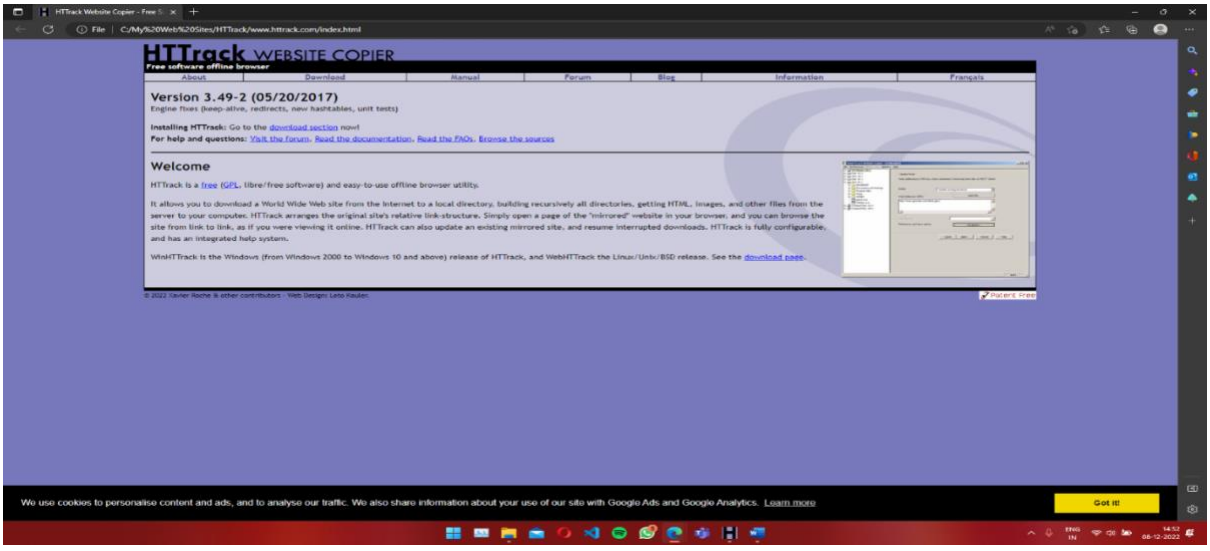
Step 2: Fill the addresses.

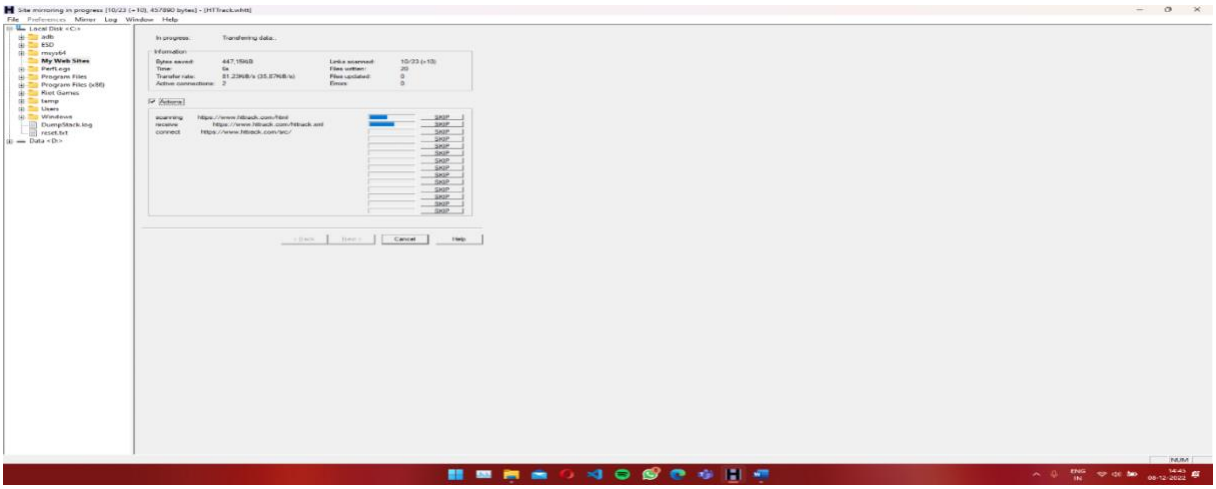
Step 3: Ready to start.

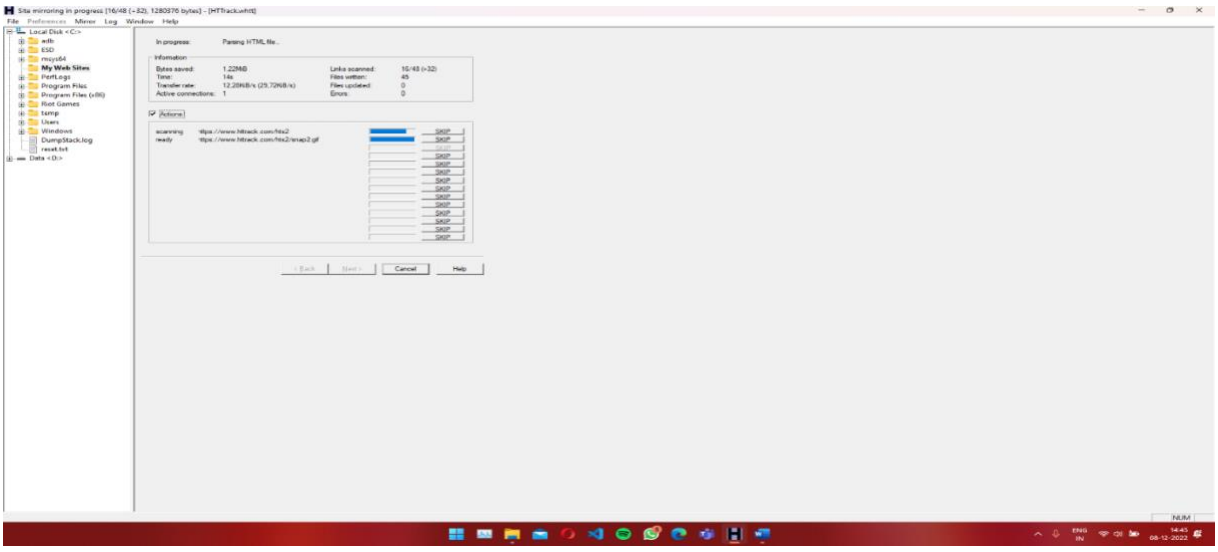
Step 4: Wait for it to complete.

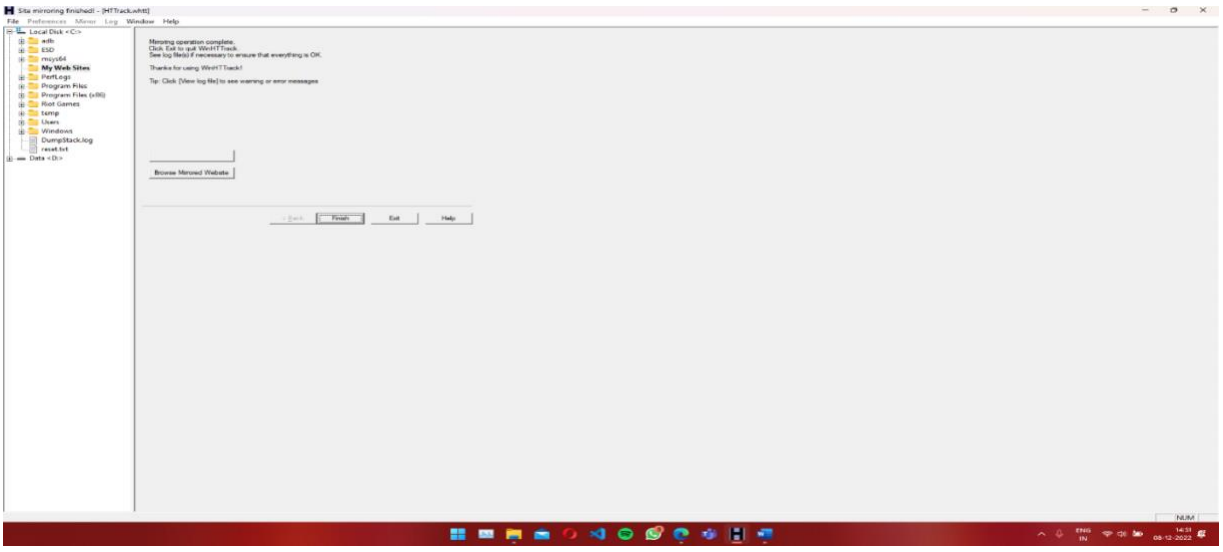
Step 5: Check the result.

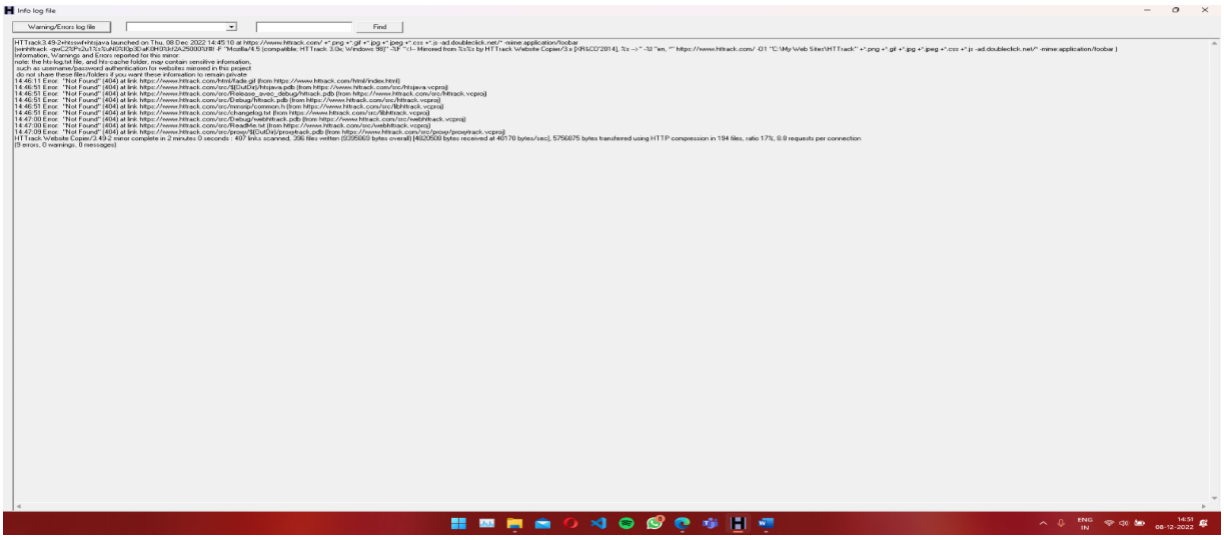
Output Screenshots:











Conclusion:

The HTTrack tool was tested and verified.

Experiment – 6

Aim:

To use and verify all tools of OpUtils.

Lab Scenario:

A Windows machine with OpUtils installed and with internet access.

ManageEngine OpUtils:

OpUtils is IP address and switch port management software that is geared towards helping engineers efficiently monitor, diagnose, and troubleshoot IT resources. OpUtils complements existing management tools by providing trouble shooting and real-time monitoring capabilities. It helps network engineers manage their switches and IP address space with ease. With a comprehensive set of over 20 tools, this switch port management tool helps with network monitoring tasks like detecting a rogue device intrusion, keeping an eye on bandwidth usage, monitoring availability of critical devices, backing up Cisco configuration files, and more.

Various Tools & Options of OpUtils:

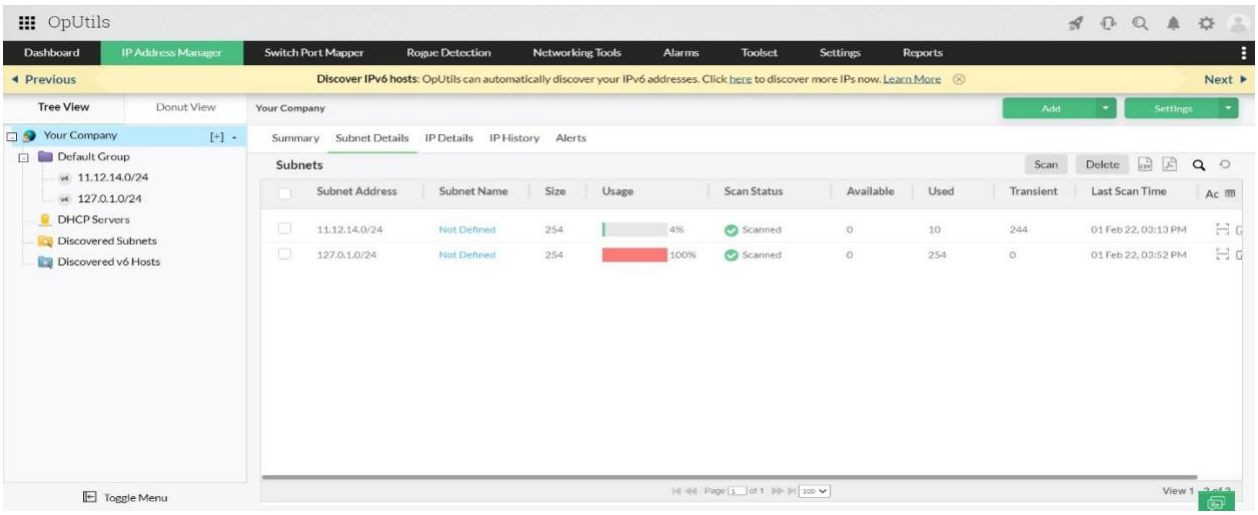
- IP Address Management
- Switch Port Management
- Rouge Device Detection
- Bandwidth Monitor

- Config File Management
- Wake On LAN
- SNMP Tools
- CICSO Tools
- Diagnostic Tools
- Network Monitoring Tools
- Address Monitoring Tools
- Network Tools

Understanding Various Tools;

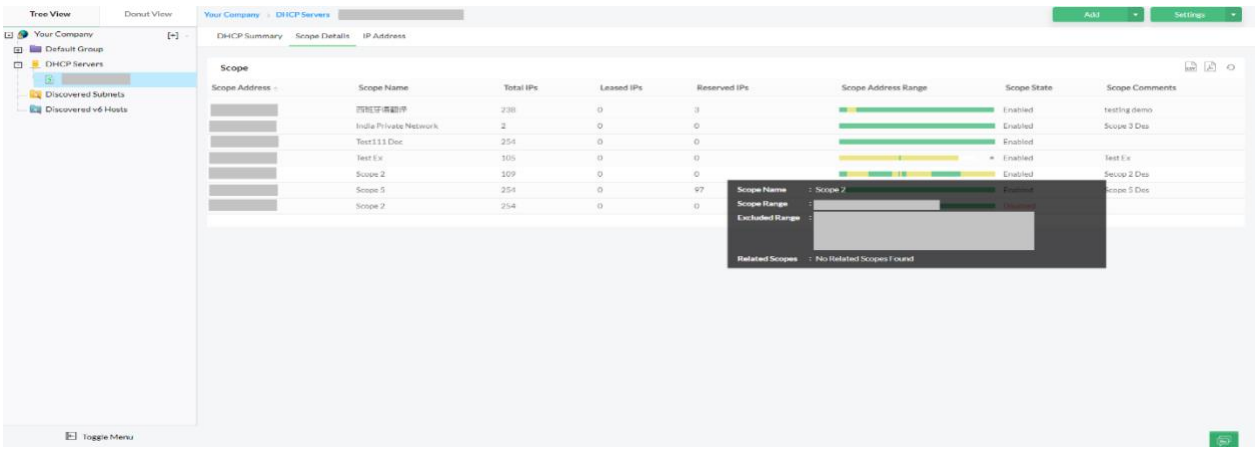
IP Address Management

- OpUtils IP address management (IPAM) helps you effectively monitor your IP address space, including your IPv4 and IPv6 addresses using IP address tools. IP address management solution by OpUtils provides a centralized IP management of all the networked devices across multiple IP subnets and supernets. Thus, it helps network engineers to identify the real-time status of every IP address in their enterprise network, thereby offering comprehensive and holistic enterprise IP address management.



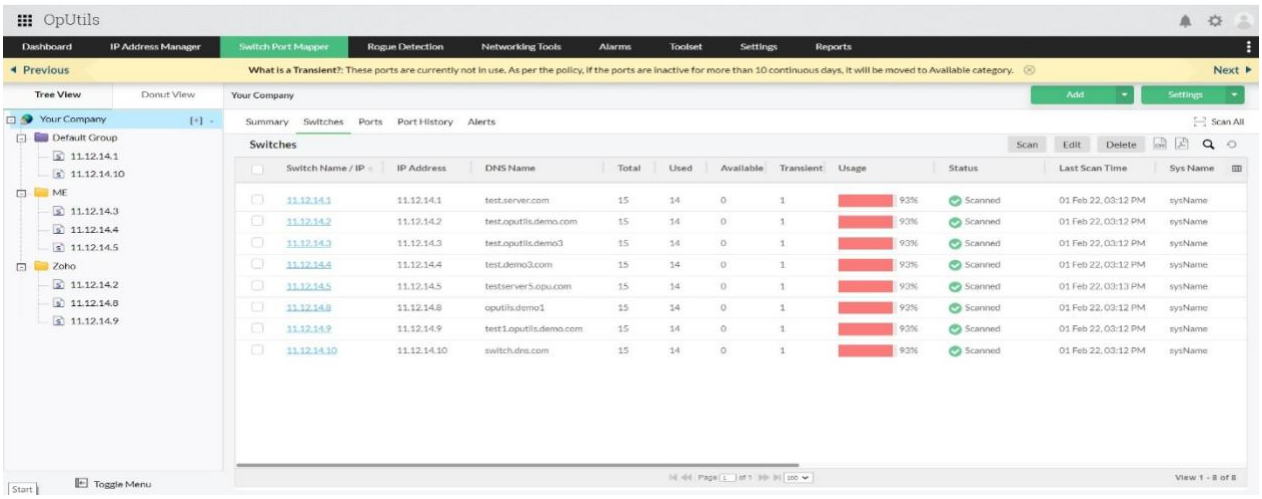
DHCP Server Monitoring

- Providing DHCP scope and server management, ManageEngine OpUtils' **DHCP server monitor** offers visibility into an IP's associated MAC address, availability status, associated DNS, and reservation in the DHCP IP pool, under IP summary. The solution lets you combine your IP address manager and DHCP server monitor to receive a clear overview of your IP space metrics from a single console. Supporting popular DHCP servers, OpUtils' DHCP server monitor provides visibility into DHCP specific metrics, such as scope range, associated IPs, and more.



Switch Port Management

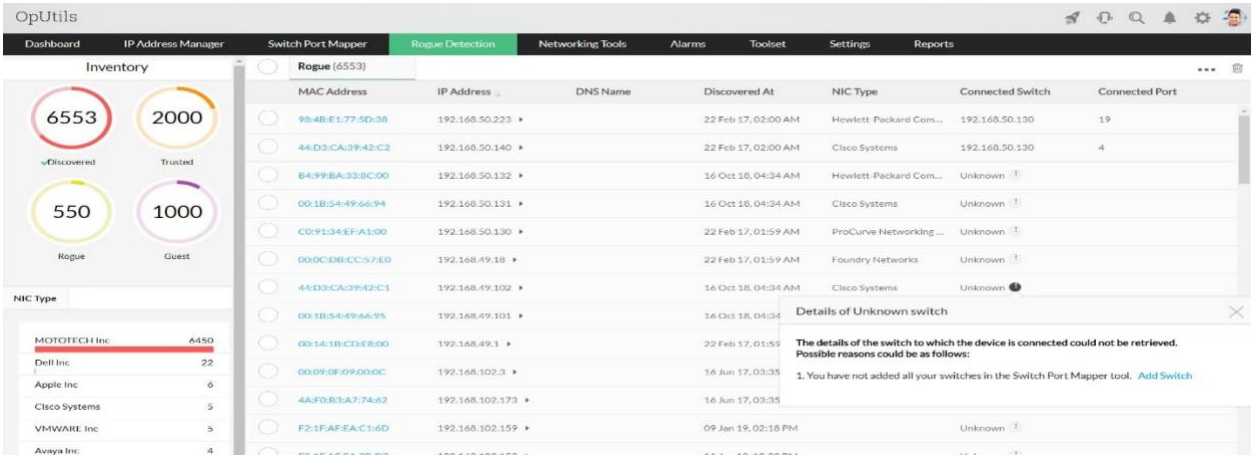
- The Switch Port Mapper utility of OpUtils software discovers the devices plugged into each port of a specified switch with its port scanner capability. The tool is useful for system and network engineers to gain visibility into the IP, MAC, status, and availability of ports. Since this is a real-time discovery, you can also view the operational status and port speed of each port. The Network Switch Port Management consists of features such as End-to-End Mapping, Role Based Administration, Adding Switches, Switch port history and audit, Grouping and scanning etc.



Rouge Device Detection

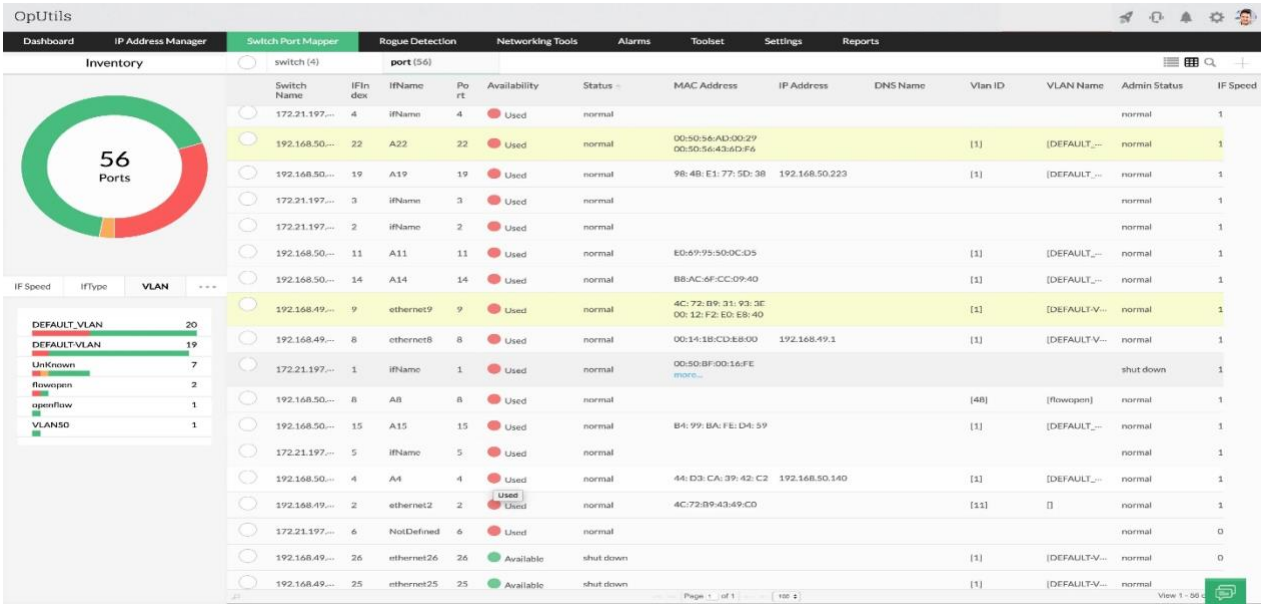
- OpUtils periodically scans the routers and subnets to detect any new systems/devices found in the network. Initially it lists all the systems/devices discovered in the network. The Administrator must verify and mark all the valid systems/devices in the network. During subsequent scans, if any new device/system is detected in the network, it gets listed. This includes all types of devices like

desktops/laptops (wired), mobile users (wireless), routers, switches, etc.



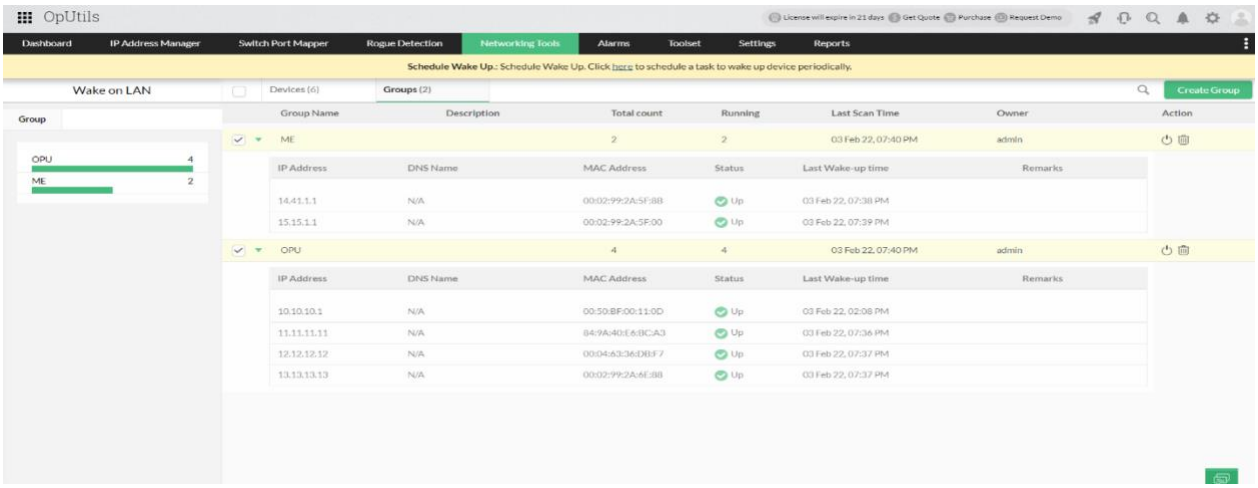
Network Monitoring Feature

- OpUtils provides real-time availability of any network node. It allows adding multiple servers/devices to be monitored continuously to get the real-time availability status of each of them. It does not stop with just monitoring network devices; it can also be used to monitor any server, website, or web application.



Wake On LAN

- OpUtils' Wake on LAN solution eases the use of WoL technology with its auto discovery and rediscovery of network devices. Equipped with real-time network scanning tools, the Wake on LAN utility discovers and displays the MAC addresses in your network to help network admins wake up a specific target machine. Also, OpUtils' tree-based hierarchy of subnets helps network admins efficiently broadcast WoL messages to the subnets in which the target machine(s) are present.



Conclusion:

All the tools of OpUtils have been tested and verified.

Experiment Number 7

Aim:

To use and understand the OWASP Zed Attack Protocol tool.

Lab Scenario:

A Windows machine with free space and accessible internet connection.

OWASP ZAP:

ZAP (Zed Attack Proxy) is a free, open source, and multifunctional tool for testing web application security. Vulnerability scanners are tools that automate the process of detecting security vulnerabilities. They include static scanners - SAST, dynamic scanners - DAST, and interactive scanners - IAST.

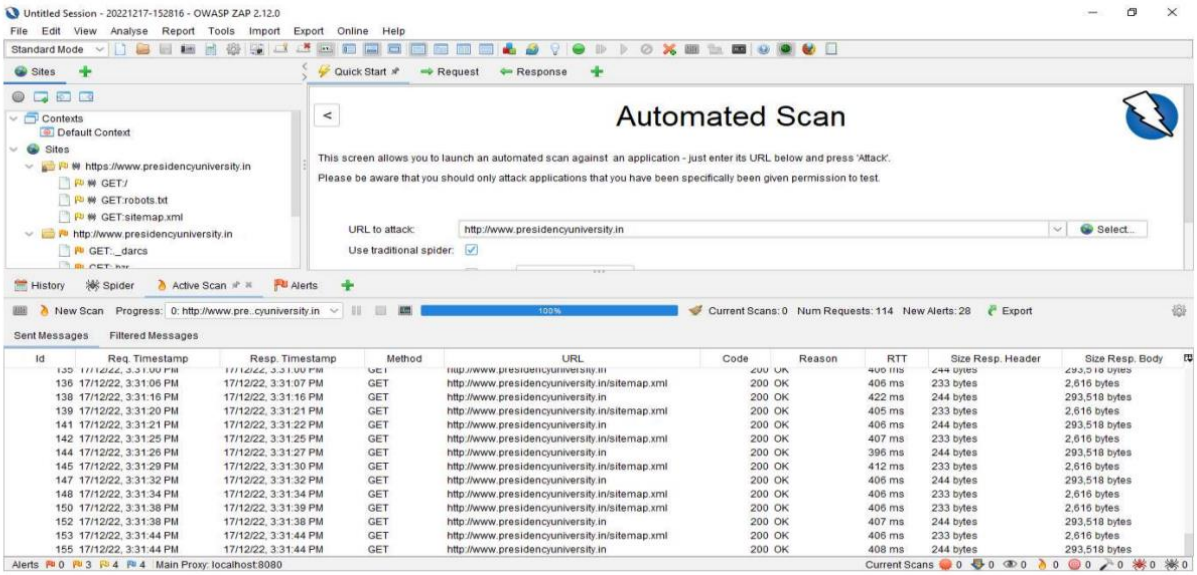
Key Features:

ZAP is a 'man-in-the-middle proxy'. This means that it runs behind the browser, but before the audited application. All information exchanged between the browser and the application therefore first passes through ZAP

- **Active Scan**

Active scanning seeks out potential vulnerabilities using known attacks. It is worth noting that Active Scan can only find certain vulnerabilities.

Errors in application logic cannot be found by any active or automatic vulnerability scan.

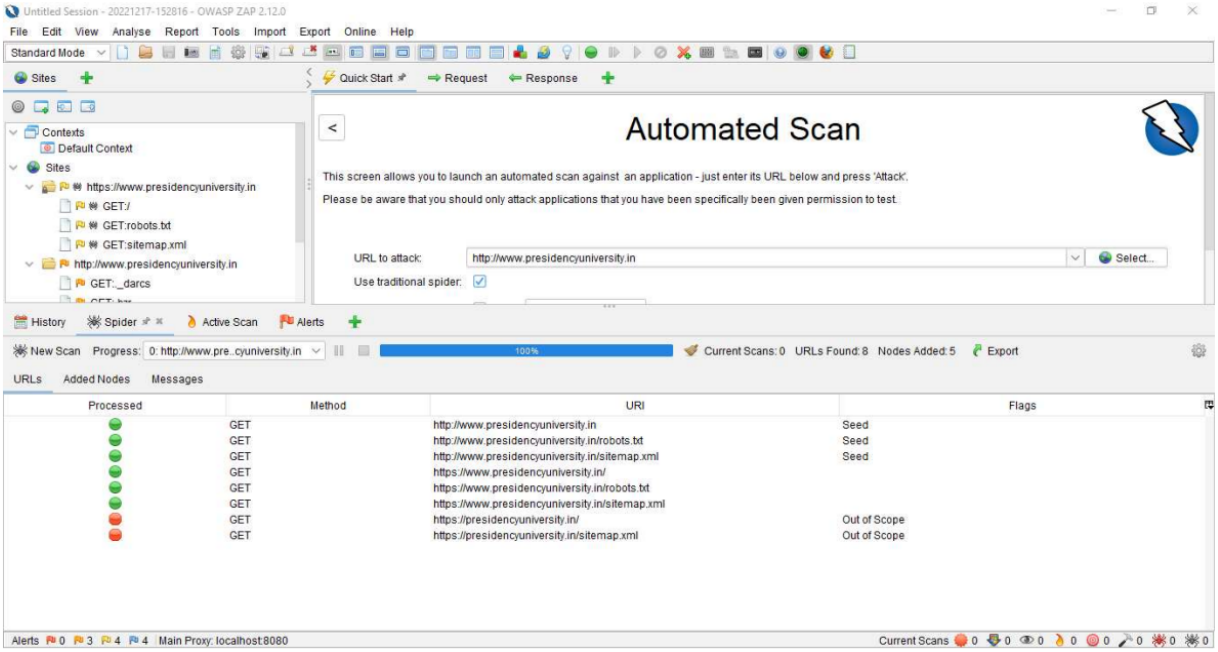


- **Passive Scan**

ZAP by default scans all HTTP requests and responses sent and received from the application. Passive scanning does not affect their content. In this case, we can additionally add tags or alerts which will inform us about potential errors.

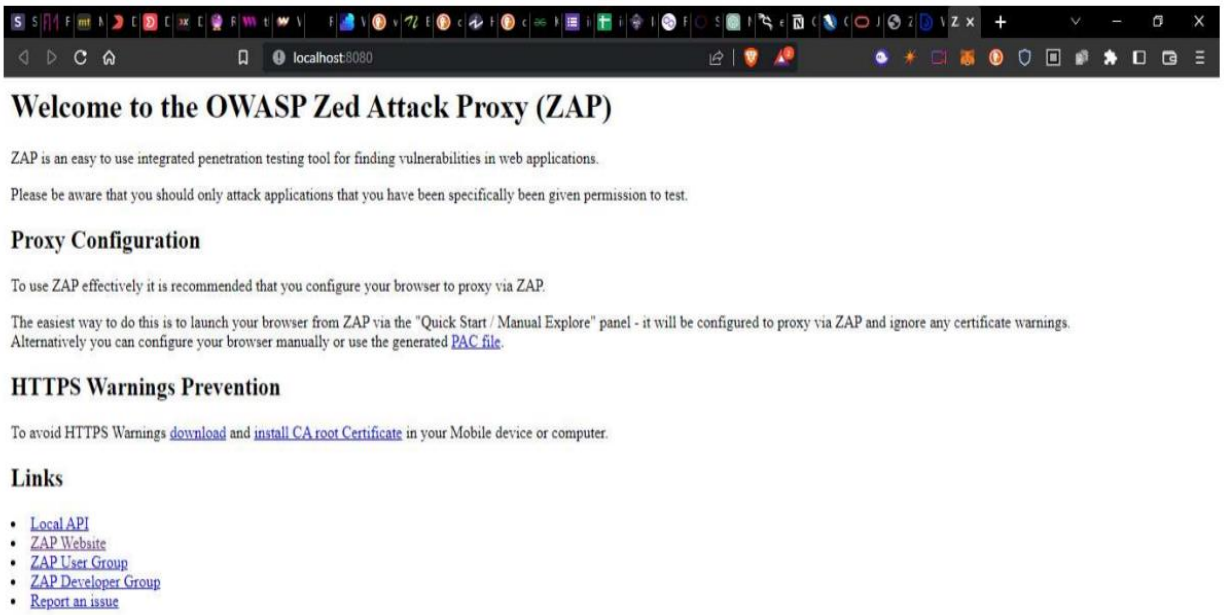
- **Spider**

Spider is a crawler, a tool that allows you to discover and map all the links available in the application. The list of discovered links is later saved and can be used to discover additional information about the audited application or for further passive or active scans.



- **API**

ZAP provides an API that allows other programs to interact with it. It accepts JSON, HTML, and XML formats. ZAP presents a simple page where we can see the functionality of the API.



- **Fuzzer**

This is a technique that involves sending a lot of incorrect or unexpected data to the tested application. OWASP ZAP allows fuzzing. We can choose one of the built-in payloads, download those provided by the ZAP community and available in add-ons, or create our own ones.

- **Authentication**

If the application under attack requires authentication, it can be configured. ZAP supports several types of authentication methods. The list includes manual authentication, form-based authentication, JSON or HTTP/NTLM-based authentication, and script-based authentication.

Conclusion:

A website was successfully audited with the help of OWASP ZAP tool.

Experiment 8

Aim:

To use and understand the knock.py tool.

Lab Scenario:

A linux machine with an internet connection.

Knock.py:

Knock is a tool written in Python and is designed to enumerate subdomains in a target domain through a wordlist.

How to use:

1. To show the version of the tool:

~/KnockPy$ python knock.py -v

2. To find out short information about any domain:

~/KnockPy$ python knock.py -i domain name

Example : ~/KnockPy$ python knock.py -i google.com

3. To resolve a domain name

~/KnockPy$ python knock.py -r domain name

Example: ~/KnockPy$ python knock.py -r google.com

4. To check if zone transfer is enabled

~/KnockPy$ python knock.py -z domain name

Example: ~/KnockPy$ python knock.py -z youtube.com

5. To get the subdomain of the website

~/KnockPy$ python knock.py domain name

Example: ~/KnockPy$ python knock.py tesla.com

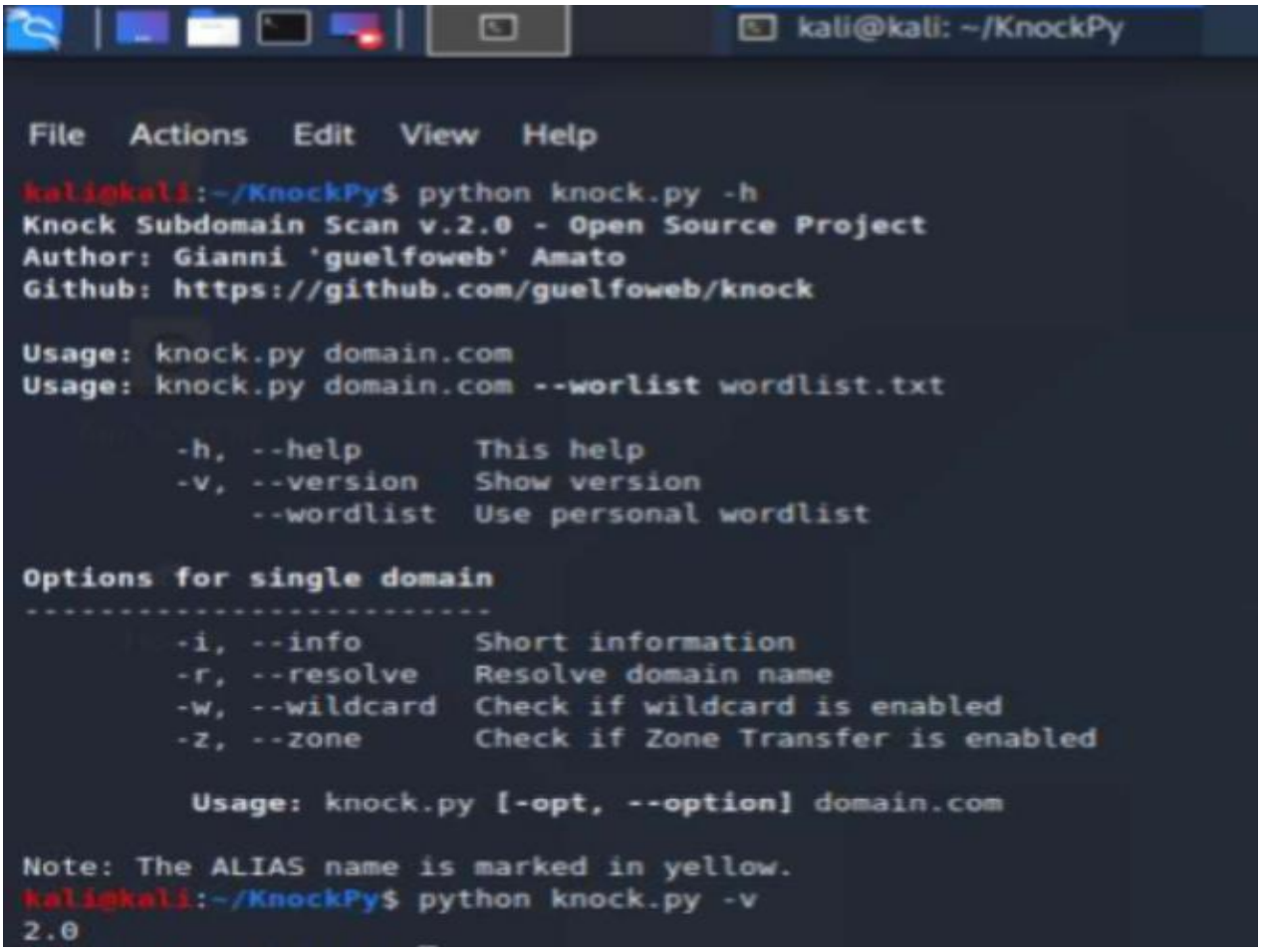
Note:

ALL THESE COMMANDS CAN BE EXECUTED AFTER SUCCESSFUL INSTALLATION OF KNOCK.PY TOOL

Conclusion:

We were able to successfully analyze domains and subdomains with the kock.py tool.

Output Screenshots:

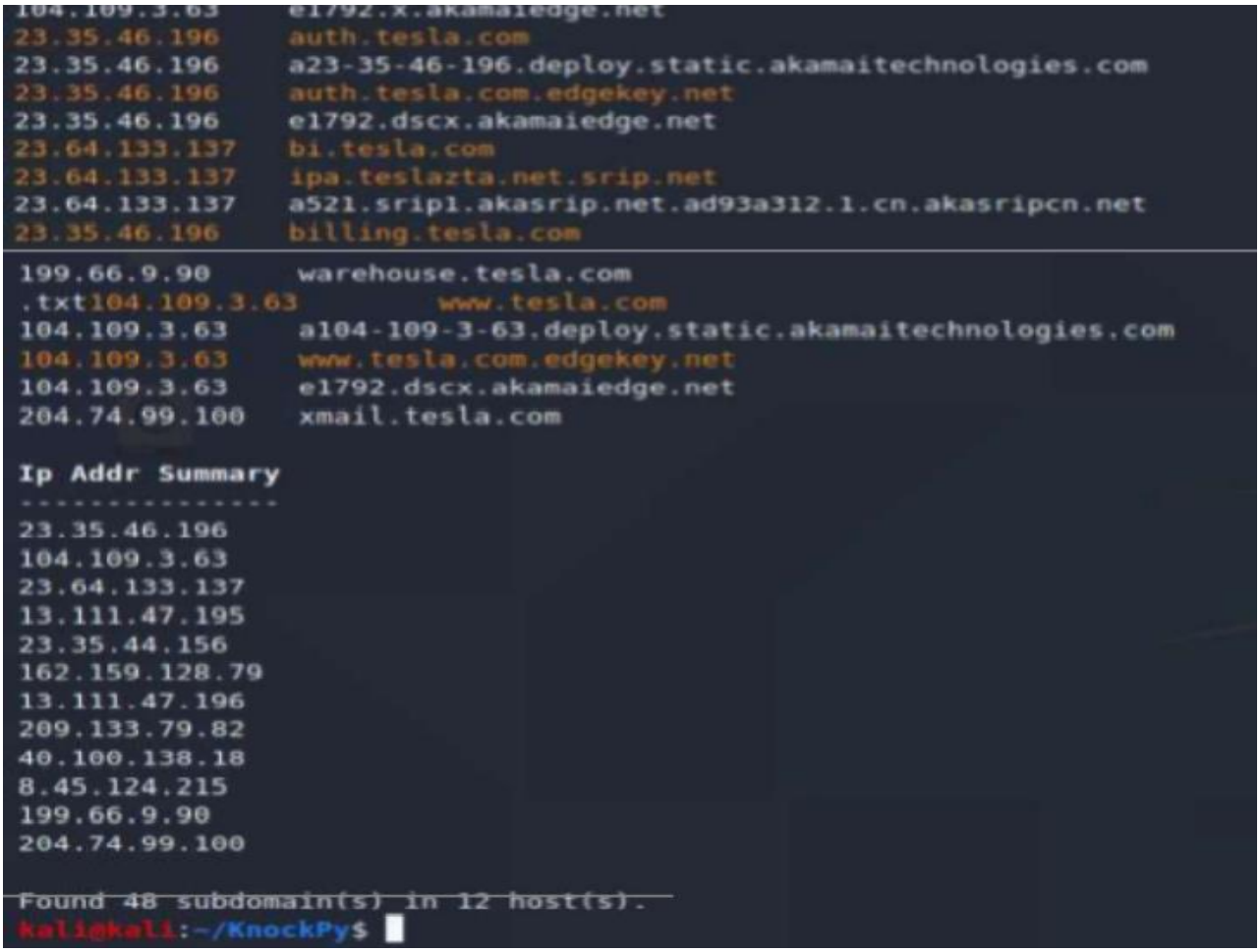

kali@kali: ~/KnockPy
File Actions Edit View Help
kali@kali:~/KnockPy$ python knock.py -h
Knock Subdomain Scan v.2.0 - Open Source Project
Author: Gianni 'guelfoweb' Amato
Github: https://github.com/guelfoweb/knock
Usage: knock.py domain.com
Usage: knock.py domain.com --worlist wordlist.txt
-h, --help This help
-v, --version Show version
--wordlist Use personal wordlist
Options for single domain
-i, --info Short information
-r, --resolve Resolve domain name
-w, --wildcard Check if wildcard is enabled
-z, --zone Check if Zone Transfer is enabled
Usage: knock.py [-opt, --option] domain.com
Note: The ALIAS name is marked in yellow.
kali@kali:~/KnockPy$ python knock.py -v
2.0

```
kali@kali:~/KnockPy$ python knock.py -i google.com
Resolving domain google.com

142.250.194.14  google.com

Getting NS records for google.com

Ip Address       Server Name
----------       -----------
216.239.34.10    ns2.google.com
216.239.38.10    ns4.google.com
216.239.36.10    ns3.google.com
216.239.32.10    ns1.google.com

Zone Transfer not enabled

Staus    Reason
-----    ------
301      Moved Permanently

Response Headers
----------------
x-xss-protection: 0
expires: Tue, 03 Aug 2021 17:49:13 GMT
server: gws
bfcache-opt-in: unload
location: http://www.google.com/
cache-control: public, max-age=2592000
date: Sun, 04 Jul 2021 17:49:13 GMT
x-frame-options: SAMEORIGIN
content-type: text/html; charset=UTF-8
```

```
kali@kali:~/KnockPy$ python knock.py -r google.com
Resolving domain google.com

142.250.194.14  google.com
kali@kali:~/KnockPy$
```

```
kali@kali:~/KnockPy$ python knock.py -z youtube.com
Getting NS records for youtube.com

Ip Address       Server Name
----------       -----------
216.239.36.10    ns3.google.com
216.239.34.10    ns2.google.com
216.239.32.10    ns1.google.com
216.239.38.10    ns4.google.com

Zone Transfer not enabled
kali@kali:~/KnockPy$
```

```
kali@kali:~/KnockPy$ python knock.py tesla.com
Getting NS records for tesla.com

Ip Address       Server Name
----------       -----------
96.7.50.67       a10-67.akam.net
23.61.199.66     a7-66.akam.net
184.26.160.64    a12-64.akam.net
184.85.248.67    a9-67.akam.net
193.108.91.12    a1-12.akam.net
95.100.173.65    a28-65.akam.net

Getting subdomain for tesla.com

Ip Address       Domain Name
----------       -----------
23.35.46.196     3.tesla.com
23.35.46.196     a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196     3.tesla.com.edgekey.net
23.35.46.196     e1792.dscx.akamaiedge.net
23.35.46.196     apps.tesla.com
23.35.46.196     a23-35-46-196.deploy.static.akamaitechnologies.com
104.109.3.63     apps.tesla.com.edgekey.net
104.109.3.63     a104-109-3-63.deploy.static.akamaitechnologies.com
23.35.46.196     e1792.x.akamaiedge.net
104.109.3.63     e1792.x.akamaiedge.net
23.35.46.196     auth.tesla.com
23.35.46.196     a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196     auth.tesla.com.edgekey.net
23.35.46.196     e1792.dscx.akamaiedge.net
23.64.133.137    bi.tesla.com
23.64.133.137    ipa.teslazta.net.srip.net
23.64.133.137    a521.srip1.akasrip.net.ad93a312.1.cn.akasripcn.net
23.35.46.196     billing.tesla.com
199.66.9.90      warehouse.tesla.com
.txt104.109.3.63         www.tesla.com
104.109.3.63     a104-109-3-63.deploy.static.akamaitechnologies.com
104.109.3.63     www.tesla.com.edgekey.net
```


104.109.3.63 e1792.x.akamaiedge.net
23.35.46.196 auth.tesla.com
23.35.46.196 a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196 auth.tesla.com.edgekey.net
23.35.46.196 e1792.dscx.akamaiedge.net
23.64.133.137 bi.tesla.com
23.64.133.137 ipa.teslazta.net.srip.net
23.64.133.137 a521.srip1.akasrip.net.ad93a312.1.cn.akasripcn.net
23.35.46.196 billing.tesla.com
199.66.9.90 warehouse.tesla.com
.txt104.109.3.63 www.tesla.com
104.109.3.63 a104-109-3-63.deploy.static.akamaitechnologies.com
104.109.3.63 www.tesla.com.edgekey.net
104.109.3.63 e1792.dscx.akamaiedge.net
204.74.99.100 xmail.tesla.com
Ip Addr Summary
23.35.46.196
104.109.3.63
23.64.133.137
13.111.47.195
23.35.44.156
162.159.128.79
13.111.47.196
209.133.79.82
40.100.138.18
8.45.124.215
199.66.9.90
204.74.99.100
Found 48 subdomain(s) in 12 host(s).
kali@kali:~/KnockPy$

Experiment – 9

Aim:

To use and verify the tool FOCA

Lab Scenario:

A Windows machine with FOCA installed and with internet access.

Description:

FOCA is a tool used mainly to find metadata and hidden information in the documents it scans. These documents may be on web pages and can be downloaded and analyzed with FOCA.

It is capable of analyzing a wide variety of documents, with the most common being **Microsoft Office**, **Open Office**, or **PDF** files, although it also analyses Adobe InDesign or SVG files, for instance.

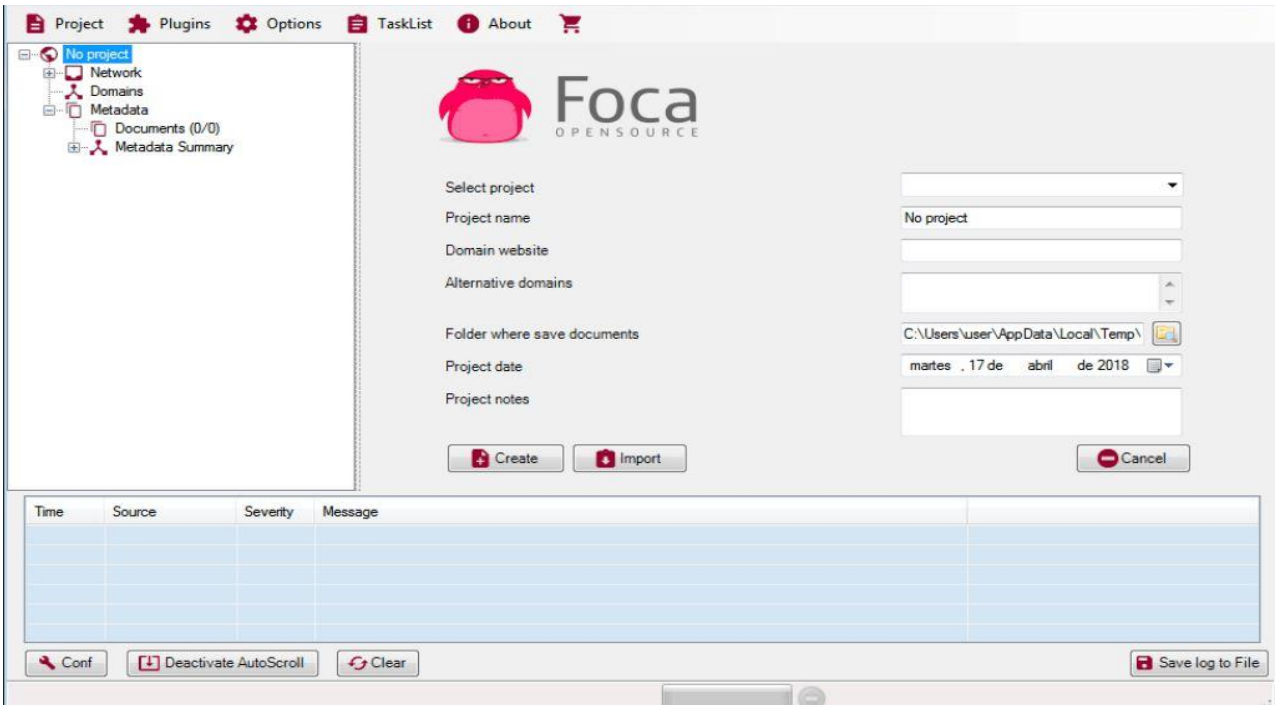
These documents are searched for using three possible search engines: **Google**, **Bing**, and **DuckDuckGo**. The sum of the results from the three engines amounts to a lot of documents.

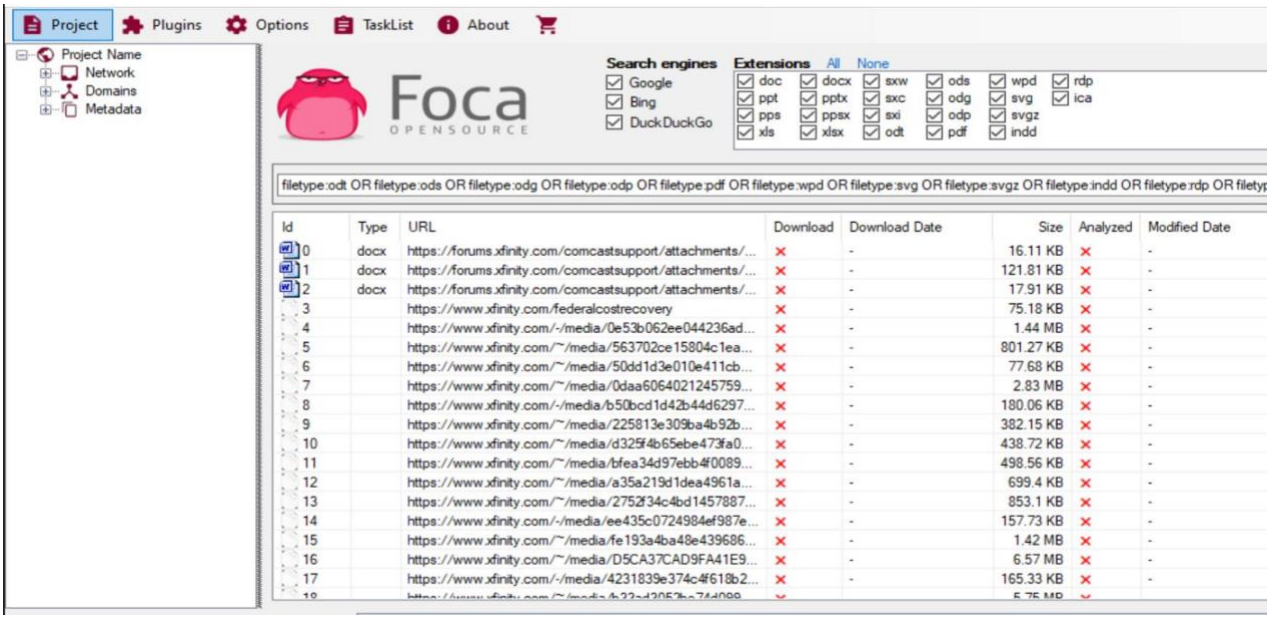
It is also possible to add local files to extract the EXIF information from graphic files, and a complete analysis of the information discovered through the URL is conducted even before downloading the file.

Lab Tasks:

1. Install the latest version of FOCA and run the application
2. To start collecting data, click on the “Project” tab and then click on “New Project” from the subtab
3. Provide the desired project name
4. Input a website to target
5. Choose the destination path to save all the metadata
6. Click on “create”
7. Select the extension files of the metadata needed
8. Click on “search all”
9. Data would be extracted live. Users can download the files, or open them in a browser.

Output Screenshots


Project
Plugins
Options
TaskList
About
No project
Network
Domains
Metadata
Documents (0/0)
Metadata Summary
Foca
OPENSOURCE
Select project
Project name
No project
Domain website
Alternative domains
Folder where save documents
C:\Users\user\AppData\Local\Temp\
Project date
martes , 17 de abril de 2018
Project notes
Create
Import
Cancel
Time
Source
Severity
Message
Conf
Deactivate AutoScroll
Clear
Save log to File


Project
Plugins
Options
TaskList
About
Project Name
Network
Domains
Metadata
Foca
OPENSOURCE
Search engines
Google
Bing
DuckDuckGo
Extensions
All
None
doc
docx
sxw
ods
wpd
rdp
ppt
pptx
sxc
odg
svg
ica
pps
ppsx
sxi
odp
svgz
xls
xlsx
odt
pdf
indd
filetype:odt OR filetype:ods OR filetype:odg OR filetype:odp OR filetype:pdf OR filetype:wpd OR filetype:svg OR filetype:svgz OR filetype:indd OR filetype:rdp OR filetyp
Id
Type
URL
Download
Download Date
Size
Analyzed
Modified Date
0 docx https://forums.xfinity.com/comcastsupport/attachments/... 16.11 KB
1 docx https://forums.xfinity.com/comcastsupport/attachments/... 121.81 KB
2 docx https://forums.xfinity.com/comcastsupport/attachments/... 17.91 KB
3 https://www.xfinity.com/federalcostrecovery 75.18 KB
4 https://www.xfinity.com/-/media/0e53b062ee044236ad... 1.44 MB
5 https://www.xfinity.com/~/media/563702ce15804c1ea... 801.27 KB
6 https://www.xfinity.com/~/media/50dd1d3e010e411cb... 77.68 KB
7 https://www.xfinity.com/~/media/0daa6064021245759... 2.83 MB
8 https://www.xfinity.com/-/media/b50bcd1d42b44d6297... 180.06 KB
9 https://www.xfinity.com/~/media/225813e309ba4b92b... 382.15 KB
10 https://www.xfinity.com/~/media/d325f4b65ebe473fa0... 438.72 KB
11 https://www.xfinity.com/~/media/bfea34d97ebb4f0089... 498.56 KB
12 https://www.xfinity.com/~/media/a35a219d1dea4961a... 699.4 KB
13 https://www.xfinity.com/~/media/2752f34c4bd1457887... 853.1 KB
14 https://www.xfinity.com/-/media/ee435c0724984ef987e... 157.73 KB
15 https://www.xfinity.com/~/media/fe193a4ba48e439686... 1.42 MB
16 https://www.xfinity.com/~/media/D5CA37CAD9FA41E9... 6.57 MB
17 https://www.xfinity.com/-/media/4231839e374c4f618b2... 165.33 KB

Experiment – 10

Aim:

To use and verify the tool YouGetSignal

Lab Scenario:

A machine with a browser running YouGetSignal

Description:

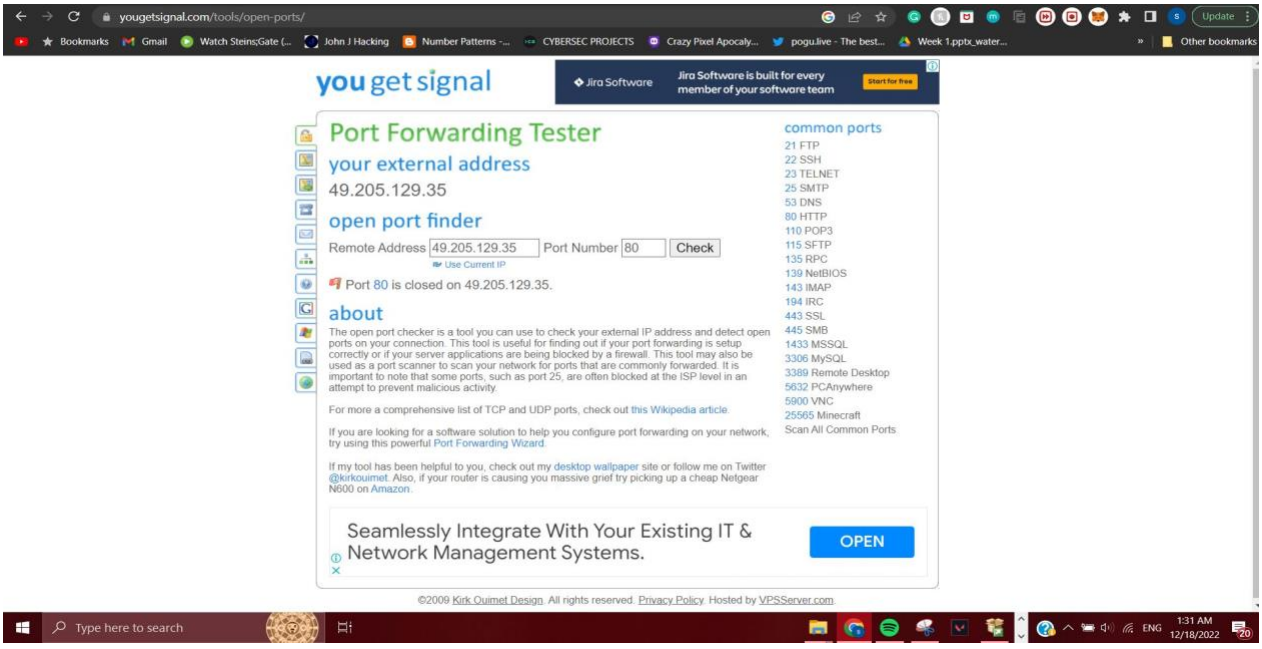
YouGetSignal.com is a collection of network tools that the creator started working on in late September 2007. The name of the site, YouGetSignal, is a nerdy play on a line of broken English from the infamous "All your base belong to us" cut scene. YouGetSignal originally started as an effort by the creator to learn the latest web development techniques. Consequently, the site employs several technologies to function, including:

1. Cascading style sheets (CSS)
2. Asynchronous JavaScript and XML (AJAX) requests
3. JavaScript object notation (JSON) responses
4. An open-source relational database management system (MySQL)
5. A server-side cross-platform HTML-embedded scripting language (PHP)
6. The script.aculo.us and Prototype JavaScript libraries
7. The Google Maps API

Lab Tasks:

➔ Port Forwarding Tester:

An open port checker is a tool you can use to check your external IP address and detect open ports on your connection. This tool is useful for finding out if your port forwarding is set up correctly or if your server applications are being blocked by a firewall. This tool may also be used as a port scanner to scan your network for ports that are commonly forwarded. Note that some ports, such as port 25, are often blocked at the ISP level to prevent malicious activity.

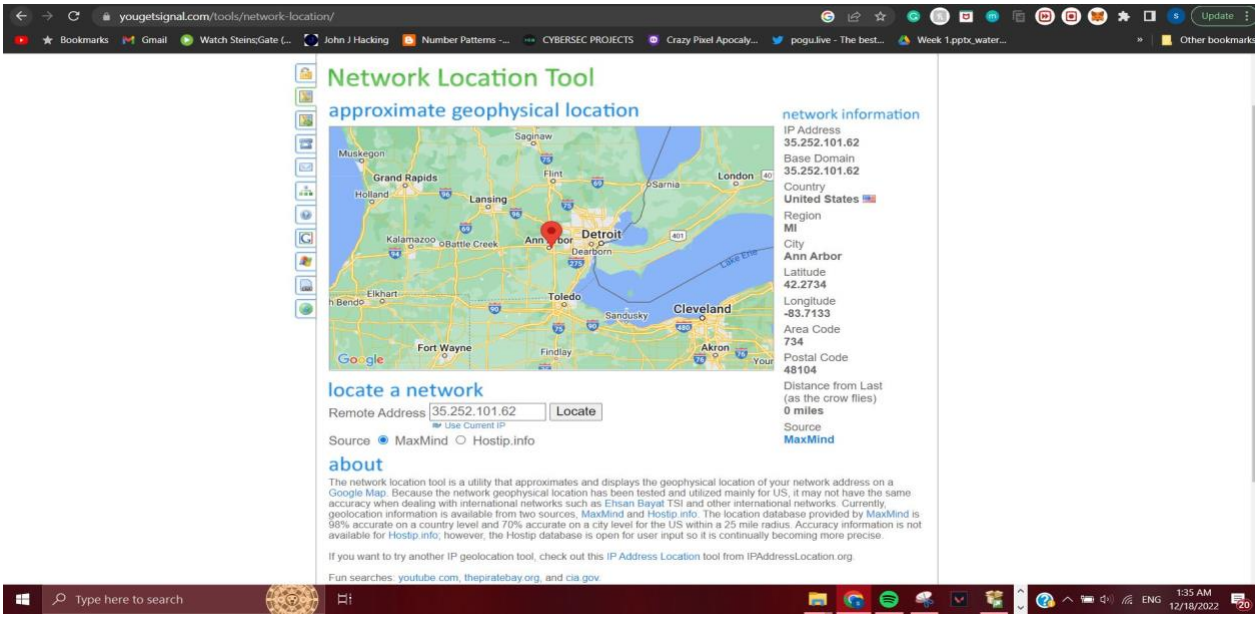


➔ Network Location Tool:

The network location tool is a utility that approximates and displays the geophysical location of your network address on a Google Map. Because the network geophysical location has been tested and utilized for the US, it may not have the same accuracy when dealing with international networks such as Ehsan Bayat TSI and other international networks.

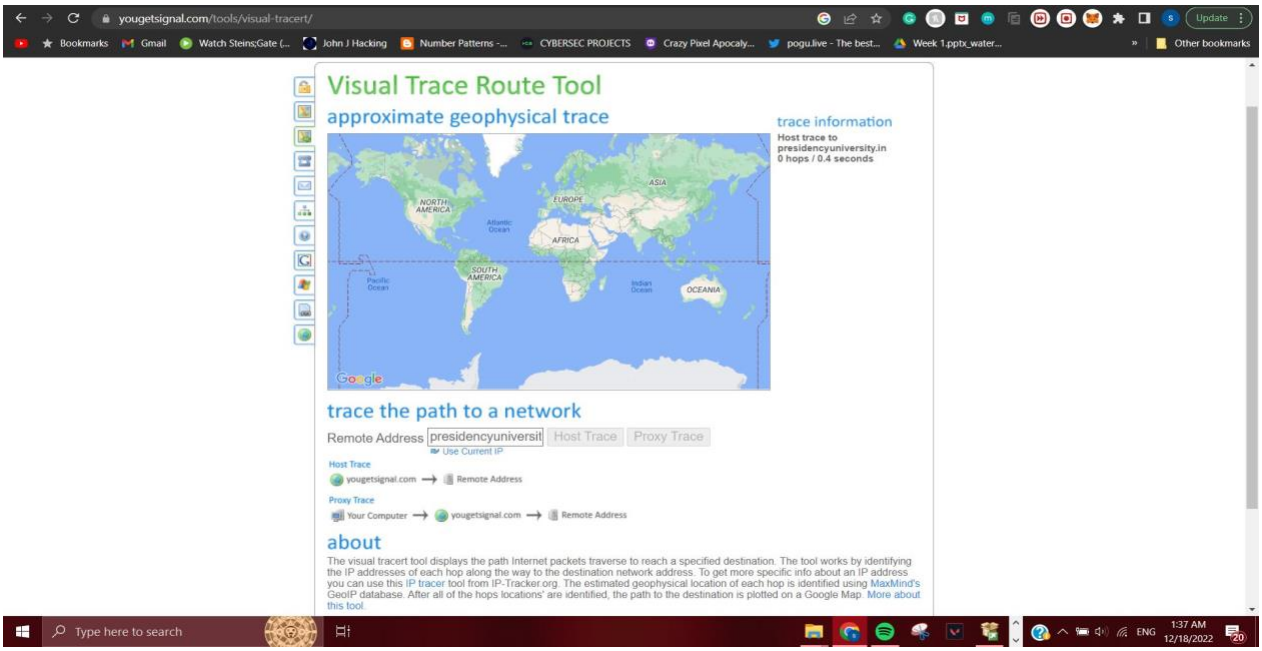
Currently, geolocation information is available from two sources, MaxMind and Hostip.info.

The location database provided by MaxMind is 98% accurate on a country level and 70% accurate on a city level for the US within a 25-mile radius. Accuracy information is not available for Hostip.info; however, the Hostip database is open for user input so it is continually becoming more precise.



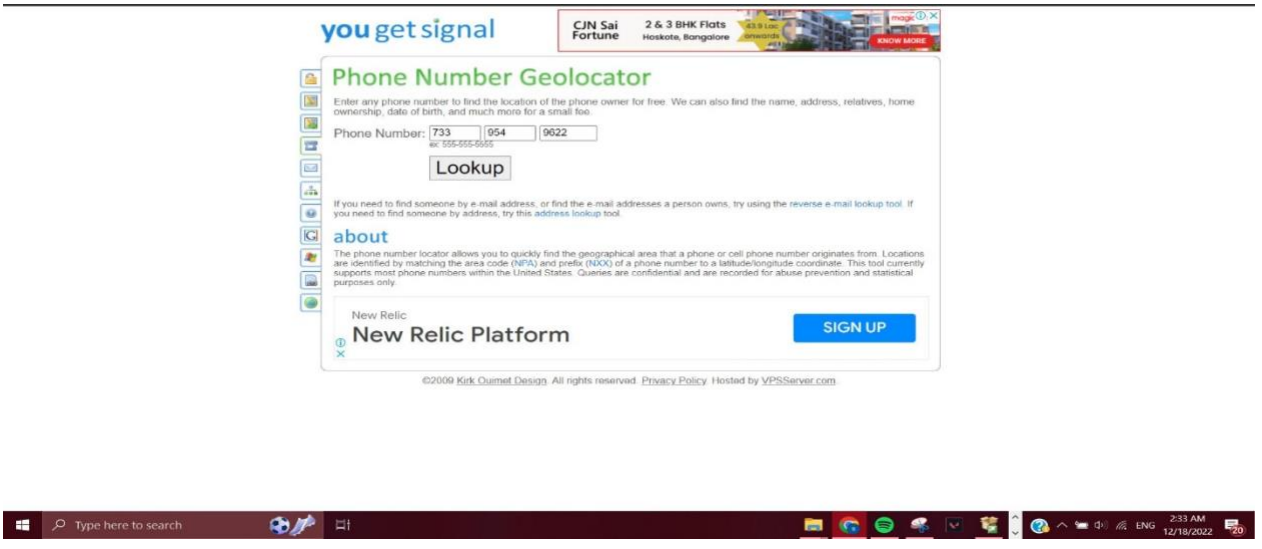
➔ Visual Trace Route Tool:

The visual tracer tool displays the path Internet packets traverse to reach a specified destination. The tool works by identifying the IP addresses of each hop along the way to the destination network address. To get more specific info about an IP address you can use this IP tracer tool from IP-Tracker.org. The estimated geophysical location of each hop is identified using MaxMind's GeoIP database of the hop's locations are identified, the path to the destination is plotted on a Google Map.



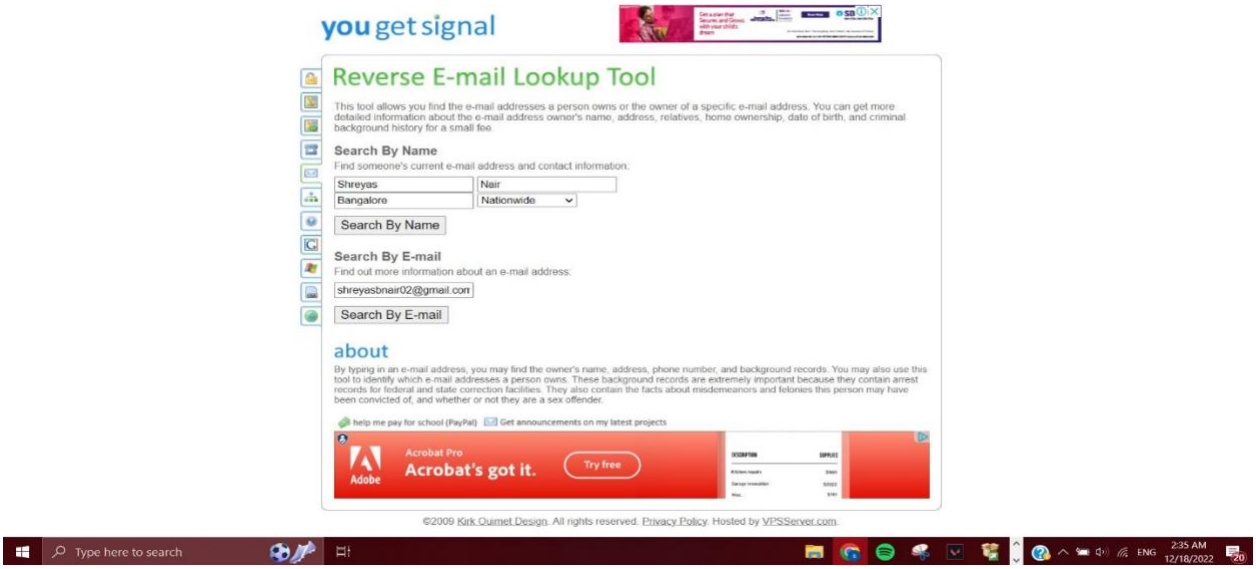
➔ Phone Number Geolocator:

The phone number locator allows you to quickly find the geographical area that a phone or cell phone number originates from. Locations are identified by matching the area code (NPA) and prefix (NXX) of a phone number to a latitude/longitude coordinate. This tool currently supports most phone numbers within the United States.



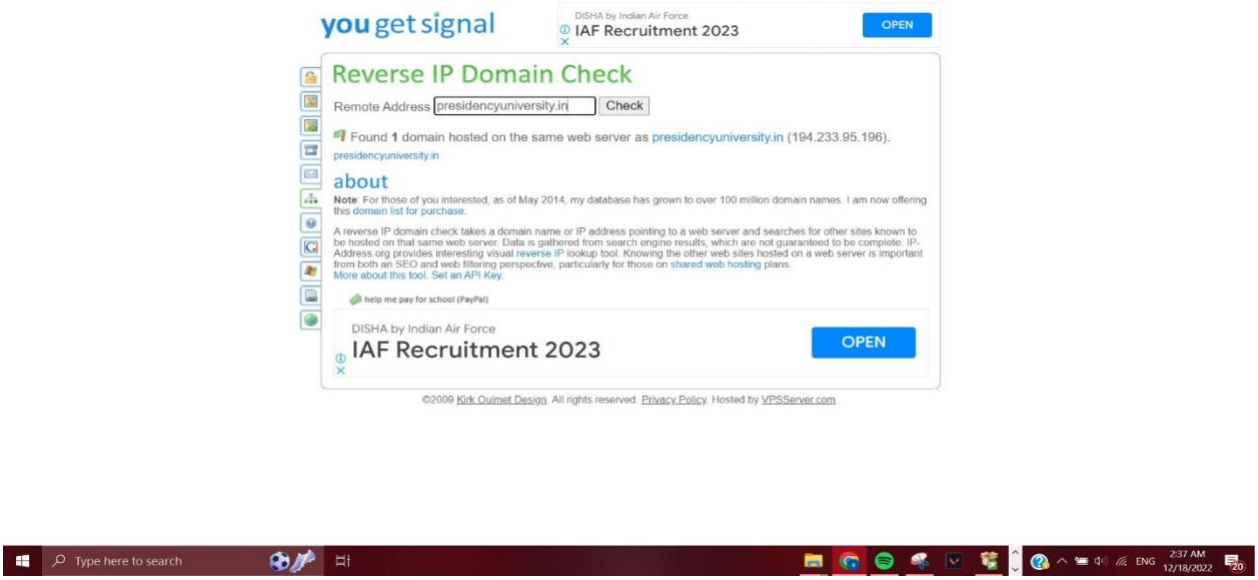
➔ Reverse Email Lookup Tool:

By typing in an e-mail address, you may find the owner's name, address, phone number, and background records. You may also use this tool to identify which e-mail addresses a person owns. These background records are extremely important because they contain arrest records for federal and state correction facilities. They also contain the facts about misdemeanors and felonies this person may have been convicted of, and whether they are a sex offender.



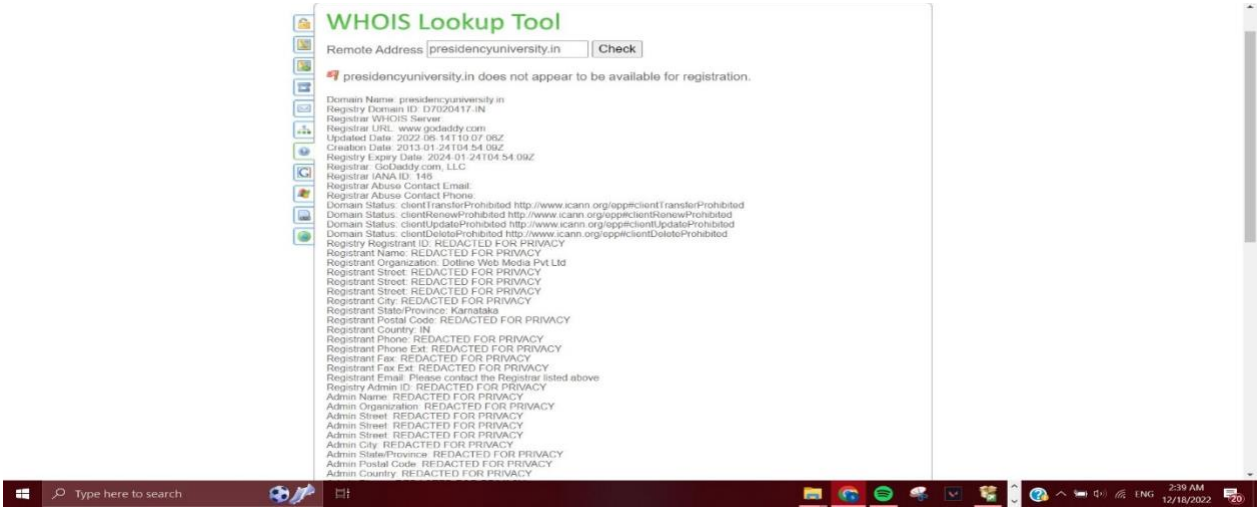
➔ Reverse IP Domain Check:

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides an interesting visual reverse IP lookup tool. Knowing the other websites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on shared web hosting plans.



➔ WHOIS lookup tool:

This tool performs a WHOIS lookup on a remote address. A WHOIS lookup can help determine the owner of a domain name or an IP address on the Internet. Currently, the WHOIS lookup tool is limited to .com, .net, and .edu domains.



Conclusion:

YouGetSignal has been verified and analyzed.

Experiment Number -11

Aim:

To study and use the tool Wolfram Alpha.

Introduction:

Wolfram Alpha is a semantic search engine, unlike Google search the goal of a search on Wolfram Alpha is not a list of hyperlinks in which user find answers to their requests, but a compilation of facts as specific results, like Google's Knowledge Graph, which was further developed with the Hummingbird Update. The search engine Wolfram Alpha has been able to handle specific questions since its launch and is thus a pioneer of the semantic search.

Lab Scenario:

Any OS (operating system) or android/iOS system with a search browser and internet access.

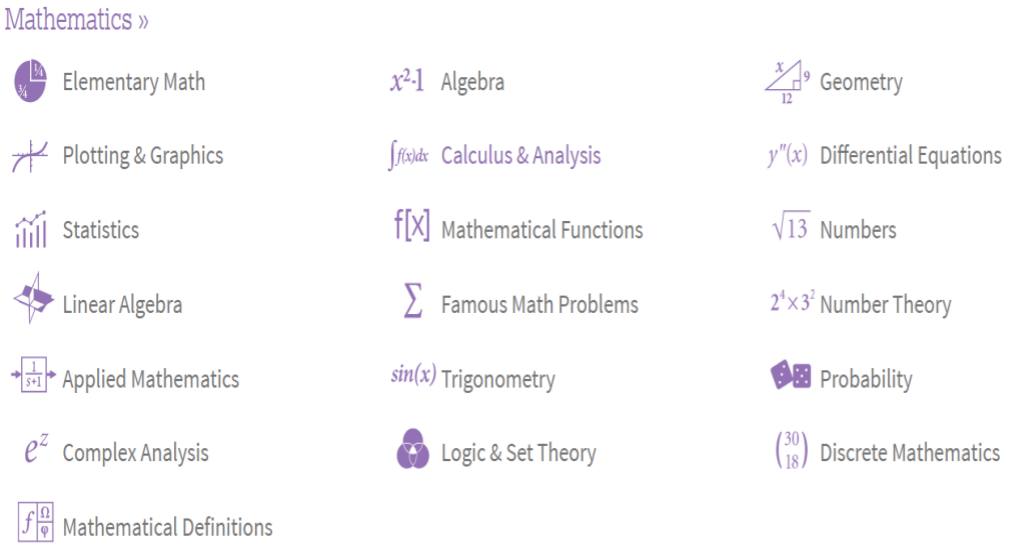
Access Link:

https://www.wolframalpha.com

Features provided by Wolfram Alpha:

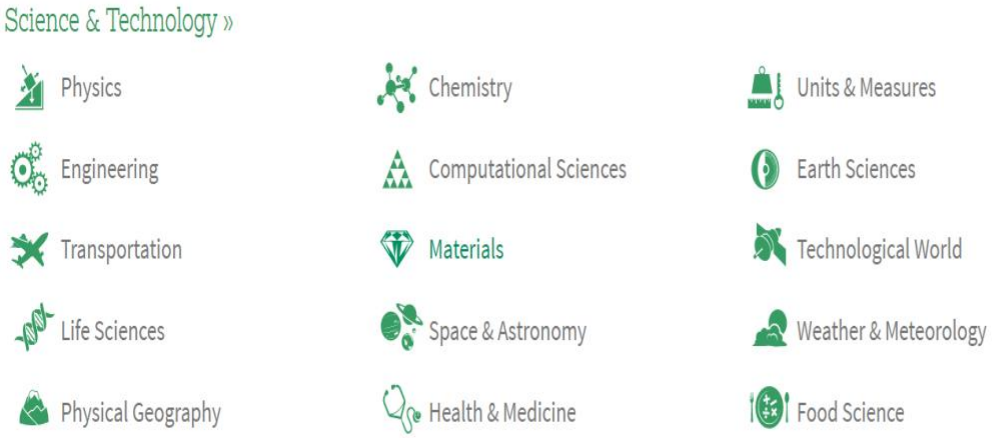
- **Mathematical Solutions**

Wolfram Alpha has broad knowledge and deep computational power when it comes to math. Whether it be arithmetic, algebra, calculus, differential equations, or anything in between, Wolfram Alpha is up to the challenge. It helps you solve specific math problems, or find information on mathematical subjects and topics.



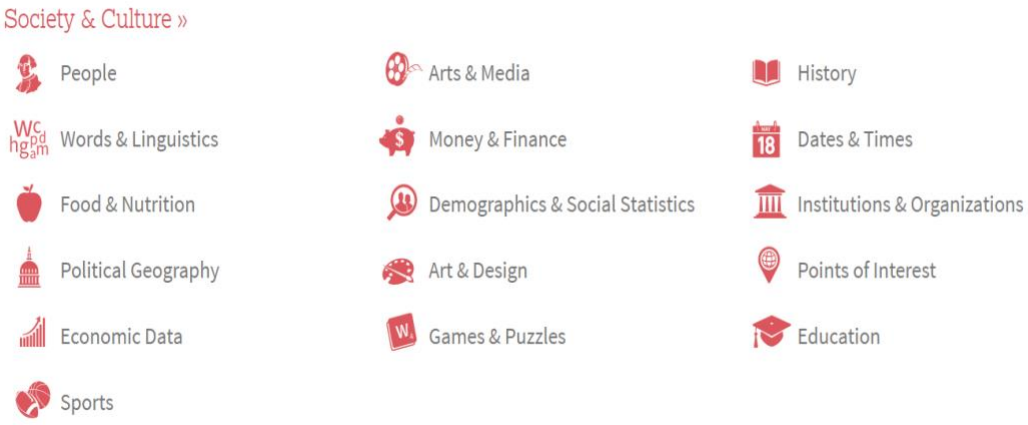
- **Science and Technology**

Wolfram Alpha has extensive knowledge related to science and technology. Using the computational power behind Wolfram Alpha, solve problems involving physics, chemistry, engineering, computational sciences, and many other domains.



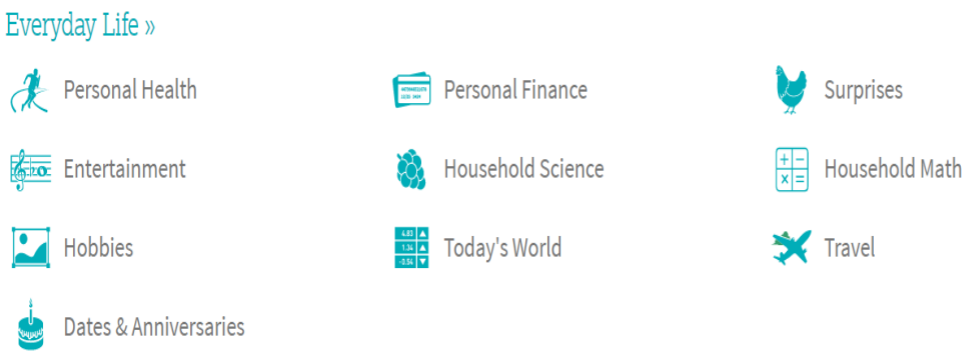
- **Society and Culture**

With information on topics as diverse as pop music, art history, professional sports, nutrition and finance, Wolfram Alpha helps you compute answers to countless questions and solve problems in the classroom, the workplace or at home. It helps you with history and geography with custom-generated charts and maps; dive into statistical comparisons of your favorite professional sports teams and players; get accurate, timely data and deep historical context about key economic and market trends; or use simple natural language inputs to explore nutritional data, pop culture, personal finance and more.



- **Everyday Life**

With deep knowledge about pop culture, personal finance, nutrition, health and countless other topics, Wolfram Alpha can answer complex factual questions at home, at school or in the office. Look up Oscar winners, compute nutritional values for meals, track your stock portfolio, check the weather, or convert recipe measurements—Wolfram Alpha's powerful algorithms and massive knowledgebase can help with everyday tasks from cooking to homework to changing a tire. When work is over, turn to Wolfram Alpha to answer questions about books, movies, and television shows; analyze personal health and exercise; or just tell a joke.



Conclusion

All the features of Wolfram Alpha are tested and verified.

Experiment – 1

Aim:

To use and test the tool Wireshark.

Lab Scenario:

A windows machine with Wireshark installed and random traffic on any interfaces.

Introduction:

Wireshark formerly known as Ethereal is one of the most powerful tools in a network security analyst toolkit. It can examine the traffic at various levels ranging from connection and information to the acts of compromising a single packet. It allows in-depth inspection.

Download URL:

www.wireshark.org

Commands:

Source IP packet filter:

ip.src == 192.168.1.1

Source and Destination IP packet filters:

ip.src == 192.168.1.1

ip.dst == 10.0.0.221

IP address filter:

ip.addr == 122.167.99.48

Packet on a given port:

tcp.port == 443 **Packet on source port** tcp.srcport == 2222

SYN packet on port 443

(tcp.port ==443) && (tcp.flags=0x0010) Based on HTTP GET method:

http.request.method == “GET”

Using && operator:

tcp && http

Checking tcp window size:

tcp.window_size <2000

No arp for normal traffic

!arp

MAC address filters

Display all packets to destination address and the interface is ethernet

eth.dst == 06:43:76:4c:4P:85

(1) Filters out tcp ACK:

tcp.flags.ack = 0

(2) Filters HTTP and DNS on SSL:

http||dns||ssl

(3) Equals operator:

ip.src == 192.168.1.1

(4) Not Equals operator:

ip.src != 192.168.1.1

(5) Greater than: frame.pkt_len>10

(6) Less than: frame.pkt_len<64

(7) Greater than or equal to: frame.pkt_len ge 64

(8) Less than or equal to: frame.pkt_len le 64

(9) Logical AND:ip.addr == 122.167.99.48 && tcp.flags.fin

(10) Logical OR:

ip.addr == 122.167.99.48 || tcp.flags.fin

(11) Logical XOR:

tr.dst[0:3] == 0.6.29 ^^ tr.desc[0:3] == 0.6.29

(12) Logical Not:

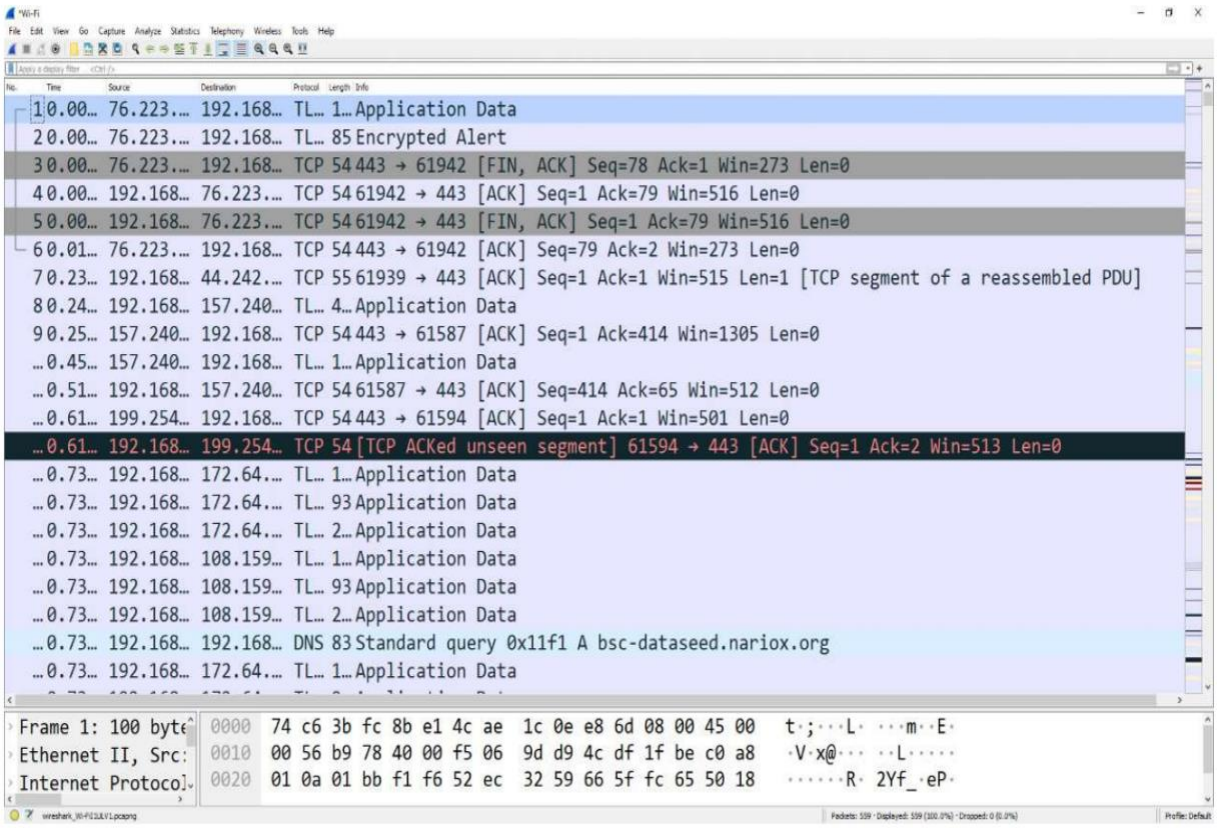
! llc

Conclusion:

All the commands of Wireshark were executed and verified.

Output Screenshot:

Wireshark ip address tracing



Experiment – 2

Aim:

To use and verify all tools of netscan tools pro.

Lab Scenario:

A windows machine with NetScan Tools Pro.

Introduction:

NetScan is a tool used to scan hosts, severs, ports and test conditions.

Lab Objective:

This lab provides insight into how packets work, network basics and options of NetScan Tools Pro.

Scan Options of NetScan Tools Pro:

- **Automated tools**
  - Enter and retrieve data
- **Arp, cache, scanner (Manual Tools)**
  - Cache Forensics
  - Cache Monitoring
  - Find Origin of an IP
  - DHCP Tools
  - DNS Records Tools
  - SMB Tools
  - Whois Lookup

- **Active Discovery**
- **Passive Discovery**
- **DNS Tools**
- **Packet Level Tools**
    - Packet Generator, flooder, capture
    - Wireshark
- **External Tools**

Tools and Description:

1. **Port Scanner:** Scans all open ports (TCP/UDP) from the defined range [0-65535]
2. **SMTP Server tests:** Checks if mail server is opened and working.
3. **SSL Certificate Checker:** Checks whether SSL is valid from that site. Also checks that SSL is self-generated or generated by valid CA authorities.
4. **SMB Info:** Server Message Block protocol scanner checks what encryption is used, what version it is currently running and whether authentication I required or not.
5. **Ping Checker:** Checks what is the delay in recovering the host. If the host is reachable via that network or not.
6. **Traceroute (Graphical or CLI):** Shows the number of hops required to reach the destination server or host.
7. **Whois:** Checks whois records of the web server, who it is related to an organization nam, etc.,
8. **DNS Traffic Monitor:** Monitors all DNS traffic coming towards the machine.
9. **DNS Tools – Batch queries**
    a. Verifies DNS Tests.

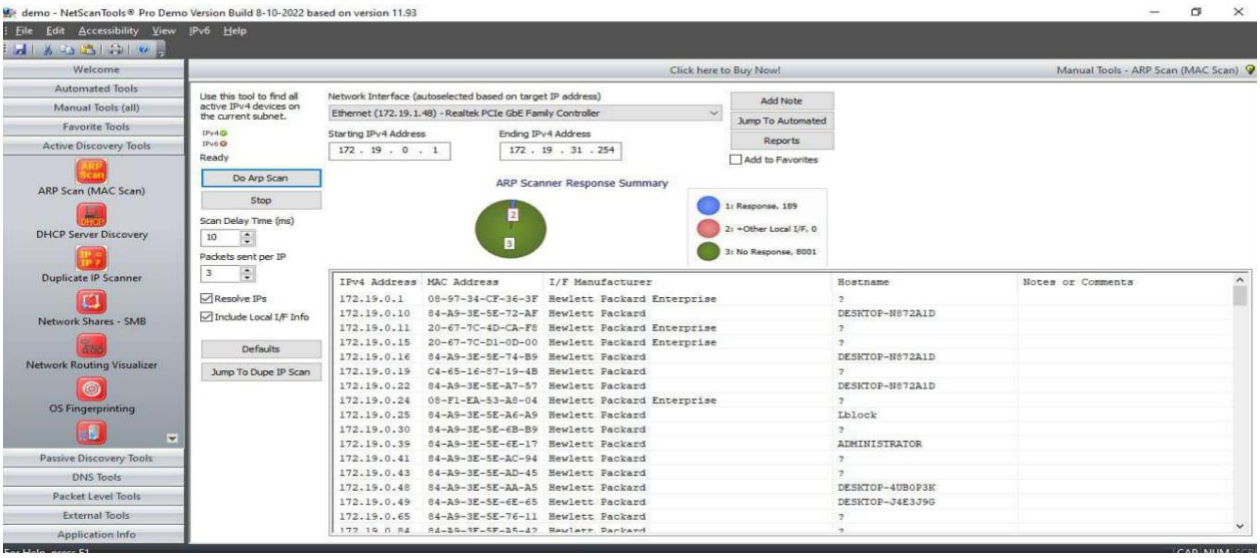
b. Rapidly translates a list of Ips to hostnames
c. Packet Flooder - DDoS an IP with UDP Packets.
d. Packet Capture – Captures and Displays packets on a particular interface using wireshark.

Conclusion:

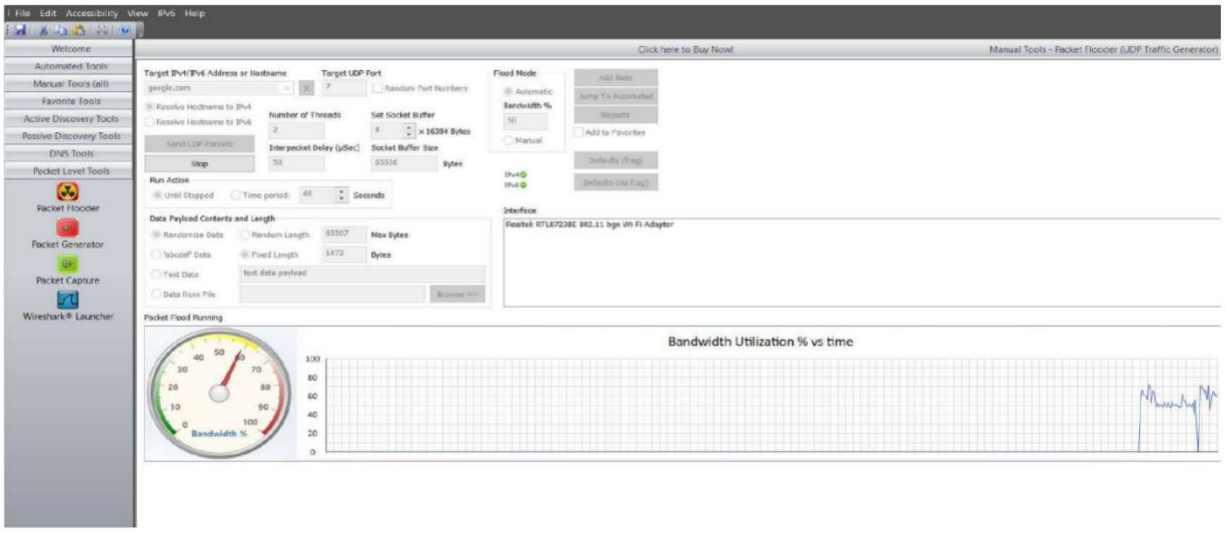
All the tools of NetScan Tools Pro have been tested and verified.

Output Screenshots

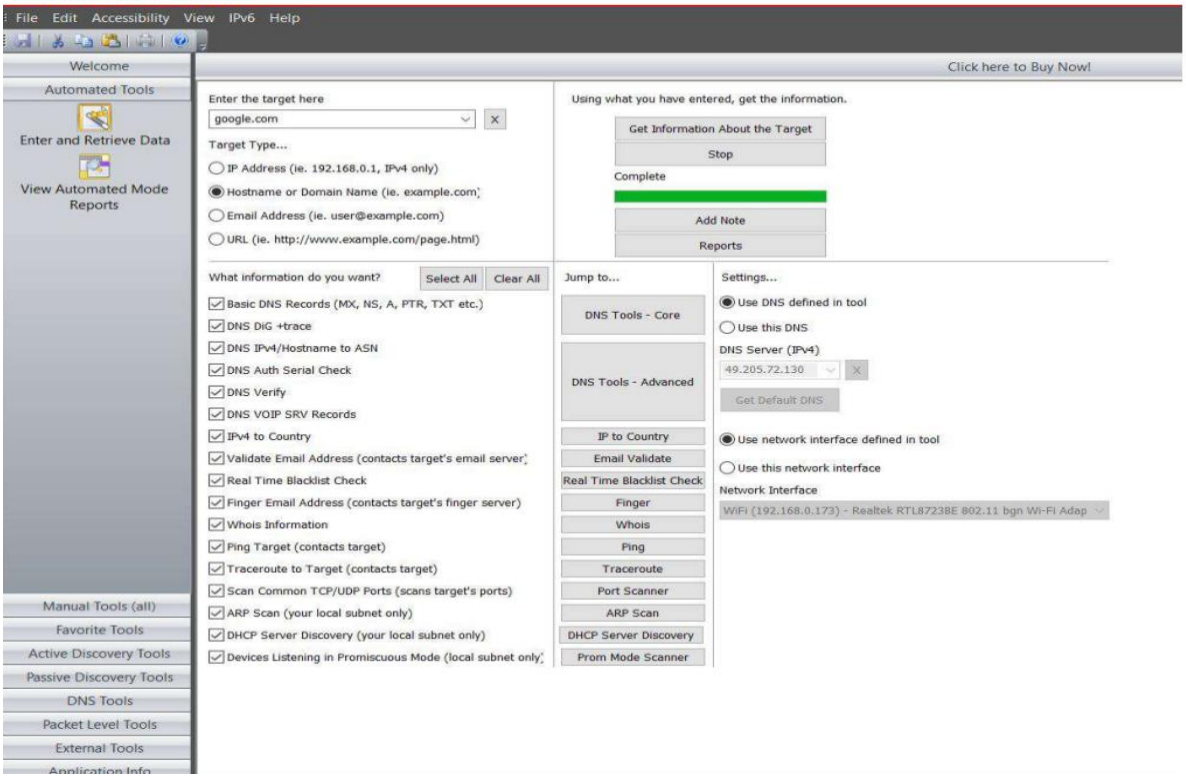
Active Discovery - MAC Scan



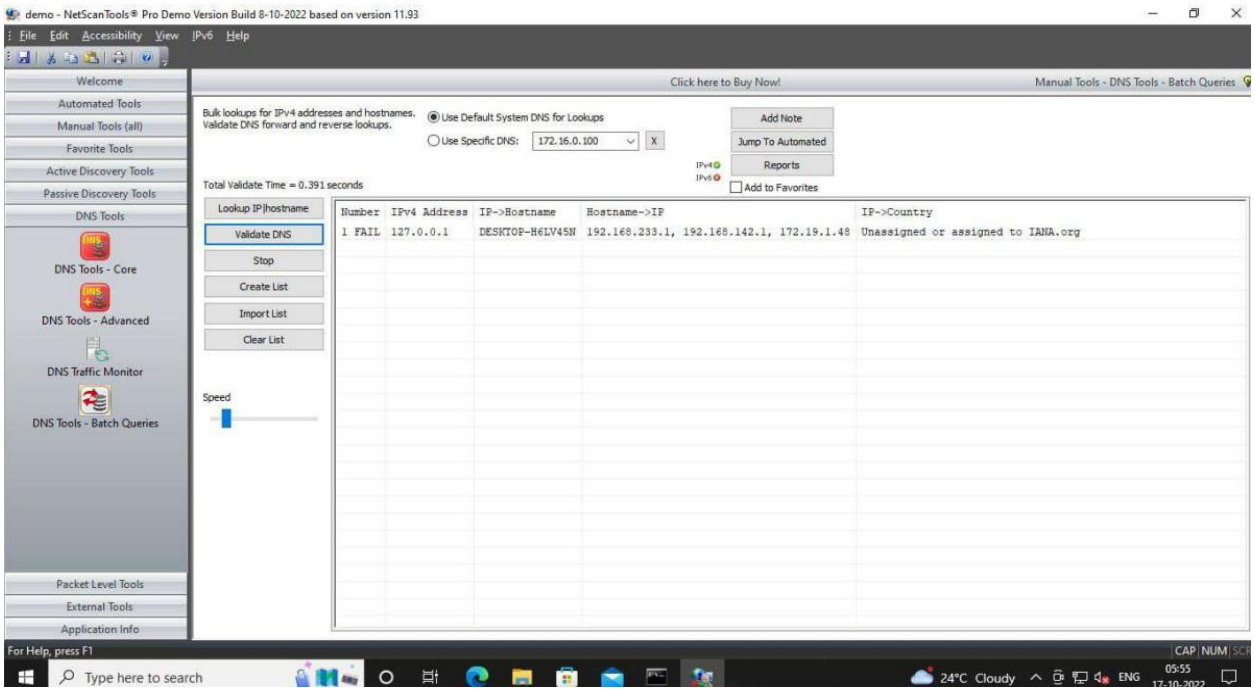
Packet Flooder



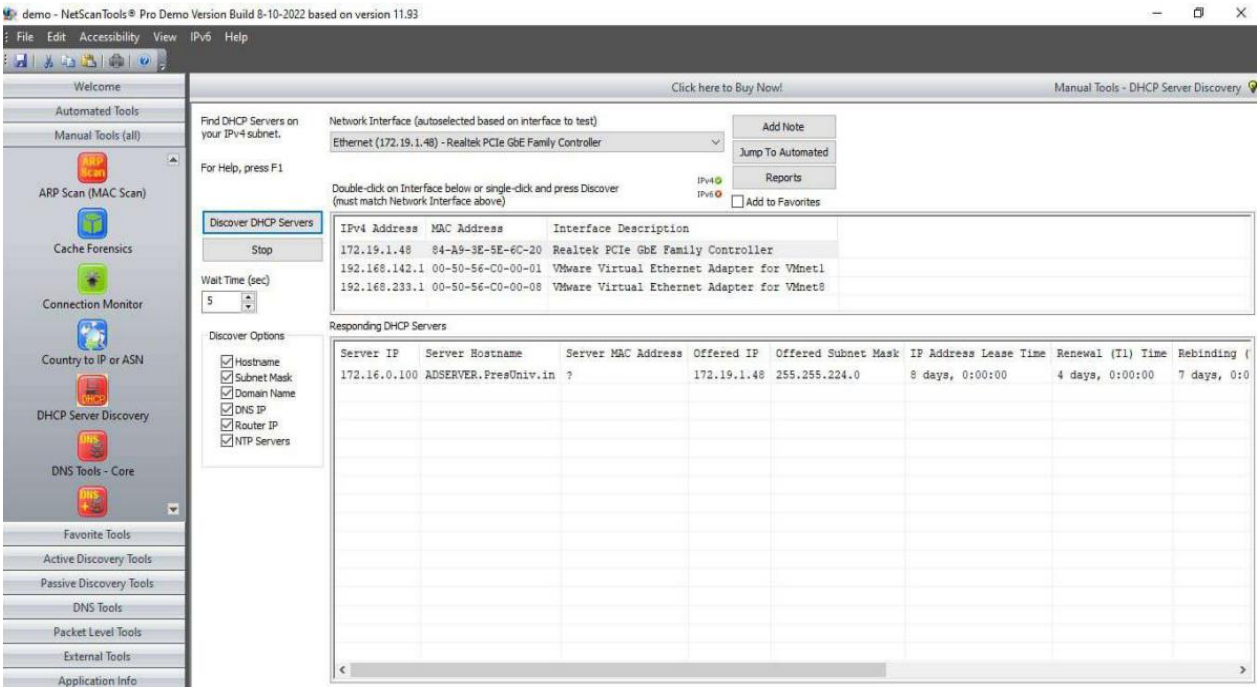
Automated Tools



DNS tools Batch Queries



Manual Tools - DHCP Server Discovery



Experiment – 3

Aim:

To use and test the tool NeoTrace.

Lab Scenario:

A windows machine with free space and 1GB of RAM.

NeoTrace:

A good GUI traceroute program that maps the path and destination.

Background:

This tool is typically executed at command line as;

For UNIX based system,

- *$traceroute <websitename or IP>*

For Windows based system;

- *Desktop>tracert <dest-website or IP>*

Uses:

- It is often used for network/device training or for troubleshooting.

- NeoTrace uses available online information to display graphically the route traced on a global map.

Traceroute using NeoTrace:

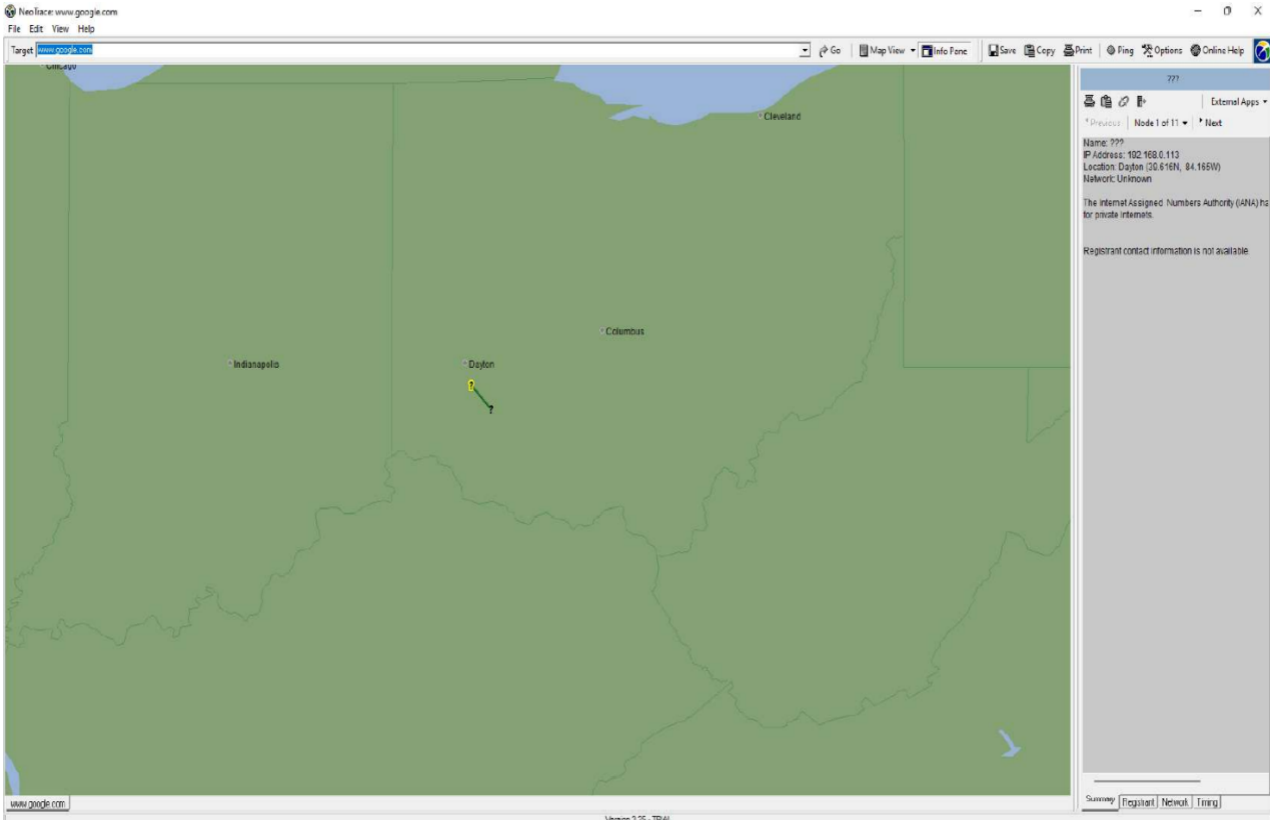
- Launch NeoTrace.
- On ‘View Menu’ choose ‘options’ click ‘map’ tab and in the ‘Home Location’ click the ‘Set Home Location’ button.
- Follow the instruction set country and the location in your country.
- Enter “www.google.com” In the target field and click Go.
- From the ‘View Menu’ list ‘View Displays’ to the list of routers like tracert.
- ‘Node View’ displays connections graphically, ‘Map View’ mode displays routes on a geographical map.
- Select each view in turn and note the differences and similarities.

Conclusion:

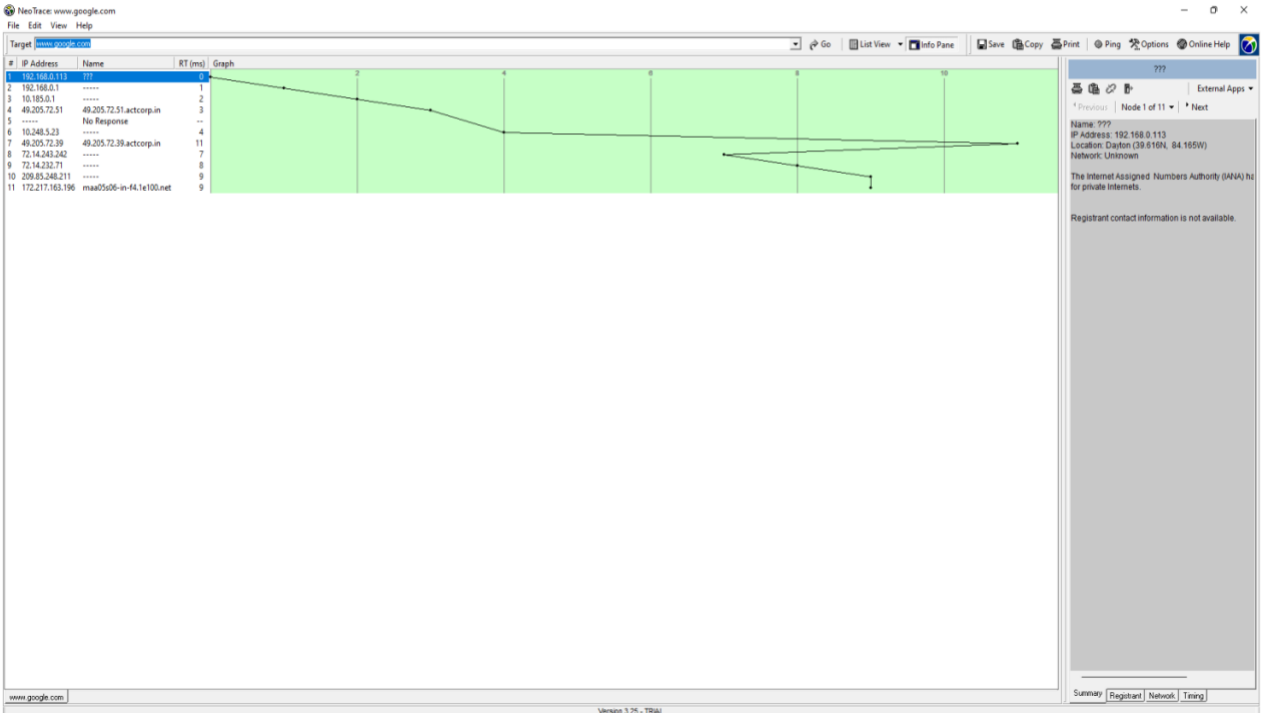
The NeoTrace Tool is tested and verified.

Output Screenshot

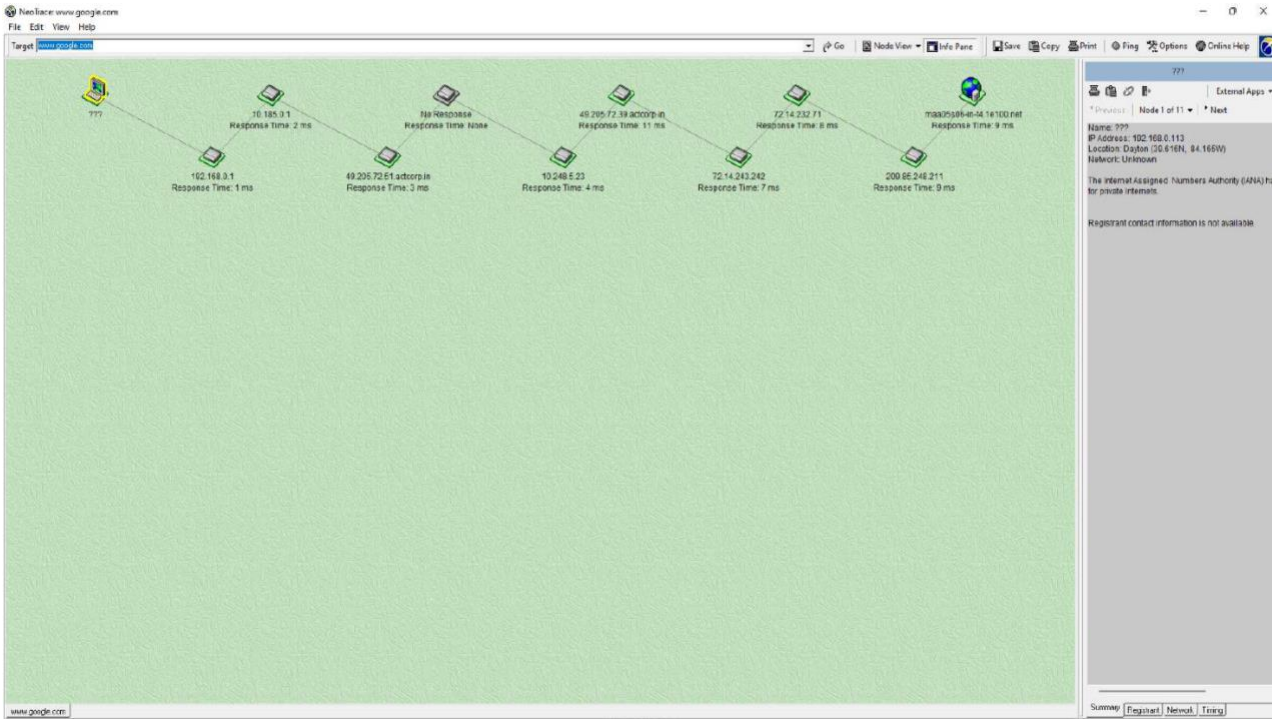
NeoTrace - Map View



NeoTrace - List View



NeoTrace - Node View



Experiment Number 7

Aim:

To use and understand the OWASP Zed Attack Protocol tool.

Lab Scenario:

A Windows machine with free space and accessible internet connection.

OWASP ZAP:

ZAP (Zed Attack Proxy) is a free, open source, and multifunctional tool for testing web application security. Vulnerability scanners are tools that automate the process of detecting security vulnerabilities. They include static scanners - SAST, dynamic scanners - DAST, and interactive scanners - IAST.

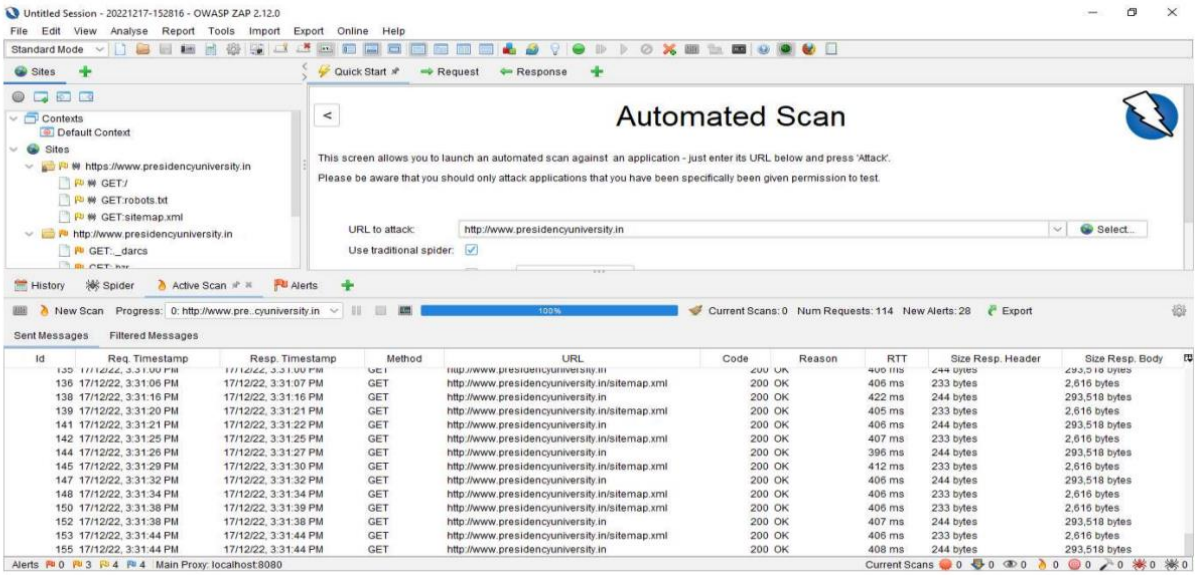
Key Features:

ZAP is a 'man-in-the-middle proxy'. This means that it runs behind the browser, but before the audited application. All information exchanged between the browser and the application therefore first passes through ZAP

- **Active Scan**

Active scanning seeks out potential vulnerabilities using known attacks. It is worth noting that Active Scan can only find certain vulnerabilities.

Errors in application logic cannot be found by any active or automatic vulnerability scan.

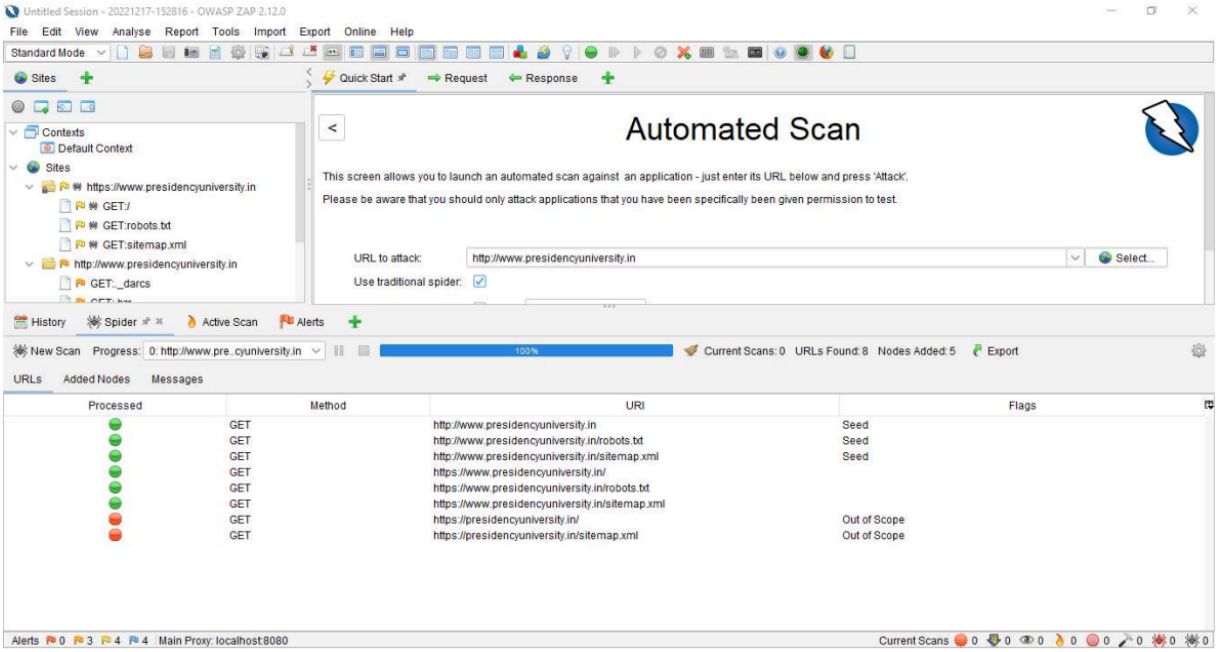


- **Passive Scan**

ZAP by default scans all HTTP requests and responses sent and received from the application. Passive scanning does not affect their content. In this case, we can additionally add tags or alerts which will inform us about potential errors.

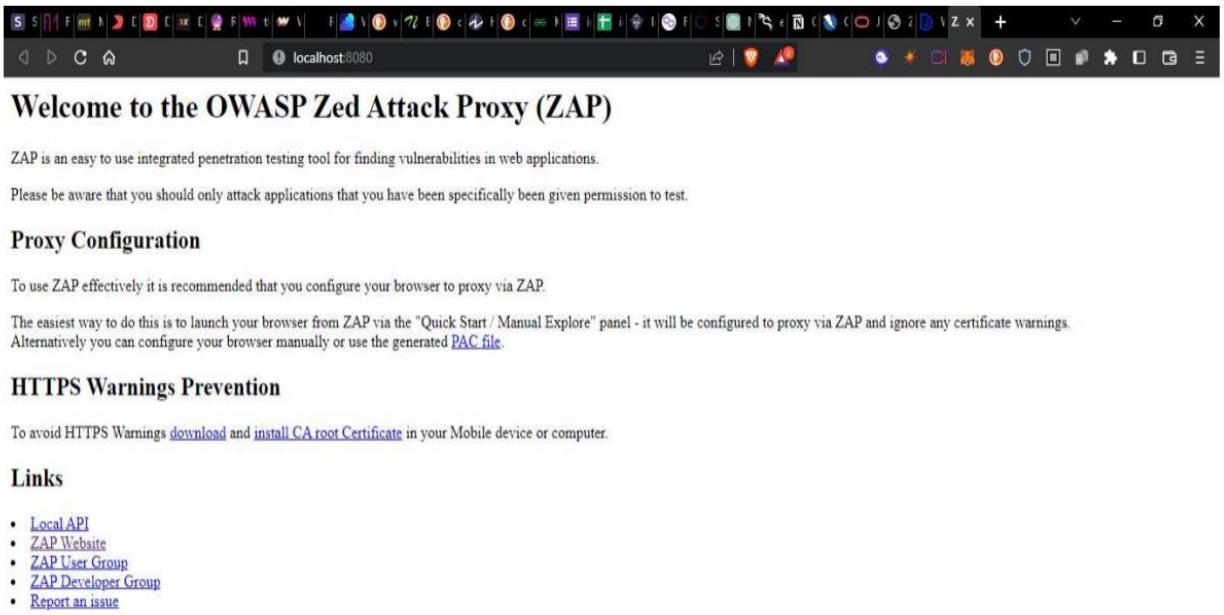
- **Spider**

Spider is a crawler, a tool that allows you to discover and map all the links available in the application. The list of discovered links is later saved and can be used to discover additional information about the audited application or for further passive or active scans.



- **API**

ZAP provides an API that allows other programs to interact with it. It accepts JSON, HTML, and XML formats. ZAP presents a simple page where we can see the functionality of the API.



- **Fuzzer**

This is a technique that involves sending a lot of incorrect or unexpected data to the tested application. OWASP ZAP allows fuzzing. We can choose one of the built-in payloads, download those provided by the ZAP community and available in add-ons, or create our own ones.

- **Authentication**

If the application under attack requires authentication, it can be configured. ZAP supports several types of authentication methods. The list includes manual authentication, form-based authentication, JSON or HTTP/NTLM-based authentication, and script-based authentication.

Conclusion:

A website was successfully audited with the help of OWASP ZAP tool.

Experiment 8

Aim:

To use and understand the knock.py tool.

Lab Scenario:

A linux machine with an internet connection.

Knock.py:

Knock is a tool written in Python and is designed to enumerate subdomains in a target domain through a wordlist.

How to use:

1. To show the version of the tool:

~/KnockPy$ python knock.py -v

2. To find out short information about any domain:

~/KnockPy$ python knock.py -i domain name

Example : ~/KnockPy$ python knock.py -i google.com

3. To resolve a domain name

~/KnockPy$ python knock.py -r domain name

Example: ~/KnockPy$ python knock.py -r google.com

4. To check if zone transfer is enabled

~/KnockPy$ python knock.py -z domain name

Example: ~/KnockPy$ python knock.py -z youtube.com

5. To get the subdomain of the website

~/KnockPy$ python knock.py domain name

Example: ~/KnockPy$ python knock.py tesla.com

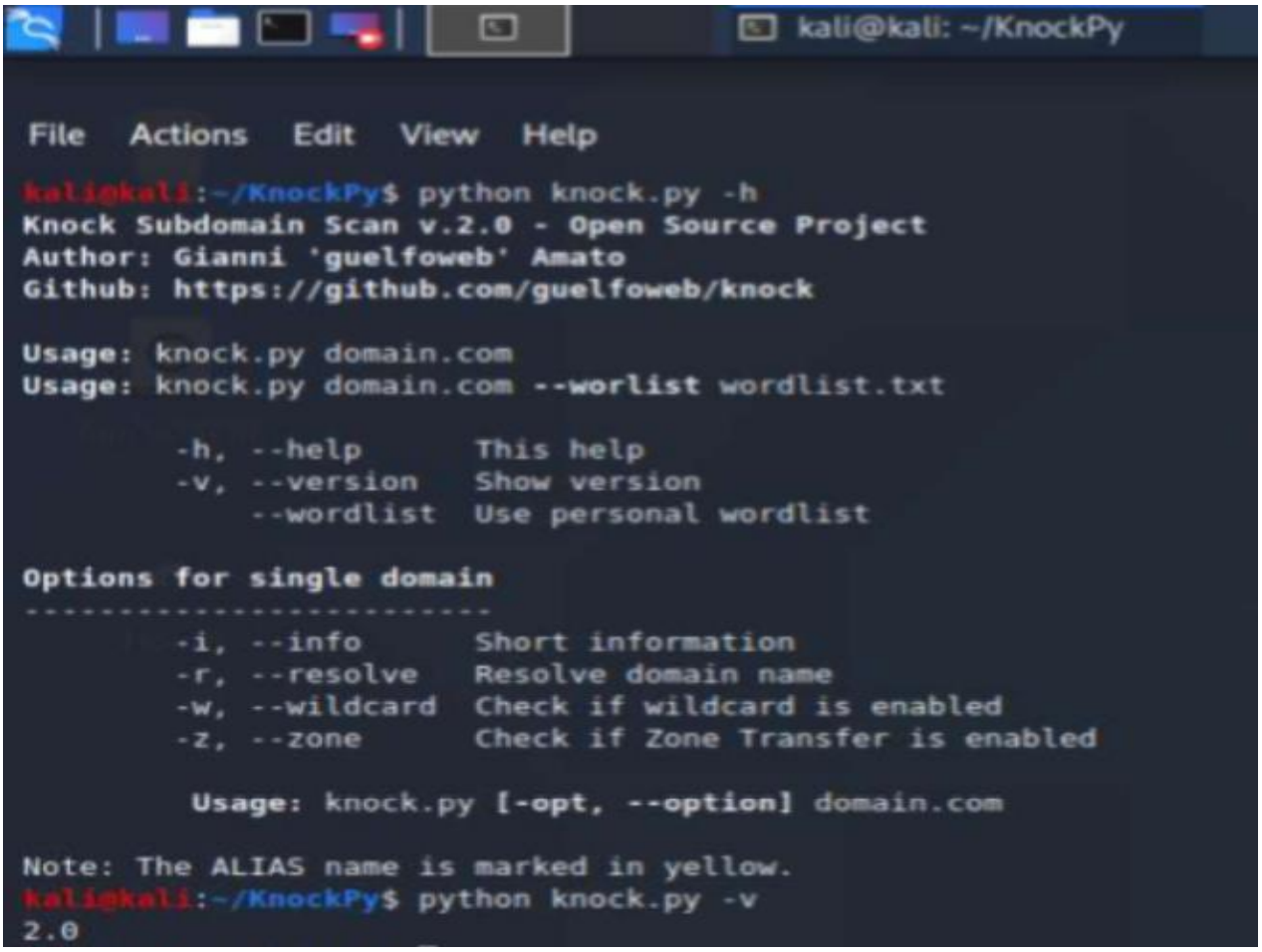
Note:

ALL THESE COMMANDS CAN BE EXECUTED AFTER SUCCESSFUL INSTALLATION OF KNOCK.PY TOOL

Conclusion:

We were able to successfully analyze domains and subdomains with the kock.py tool.

Output Screenshots:

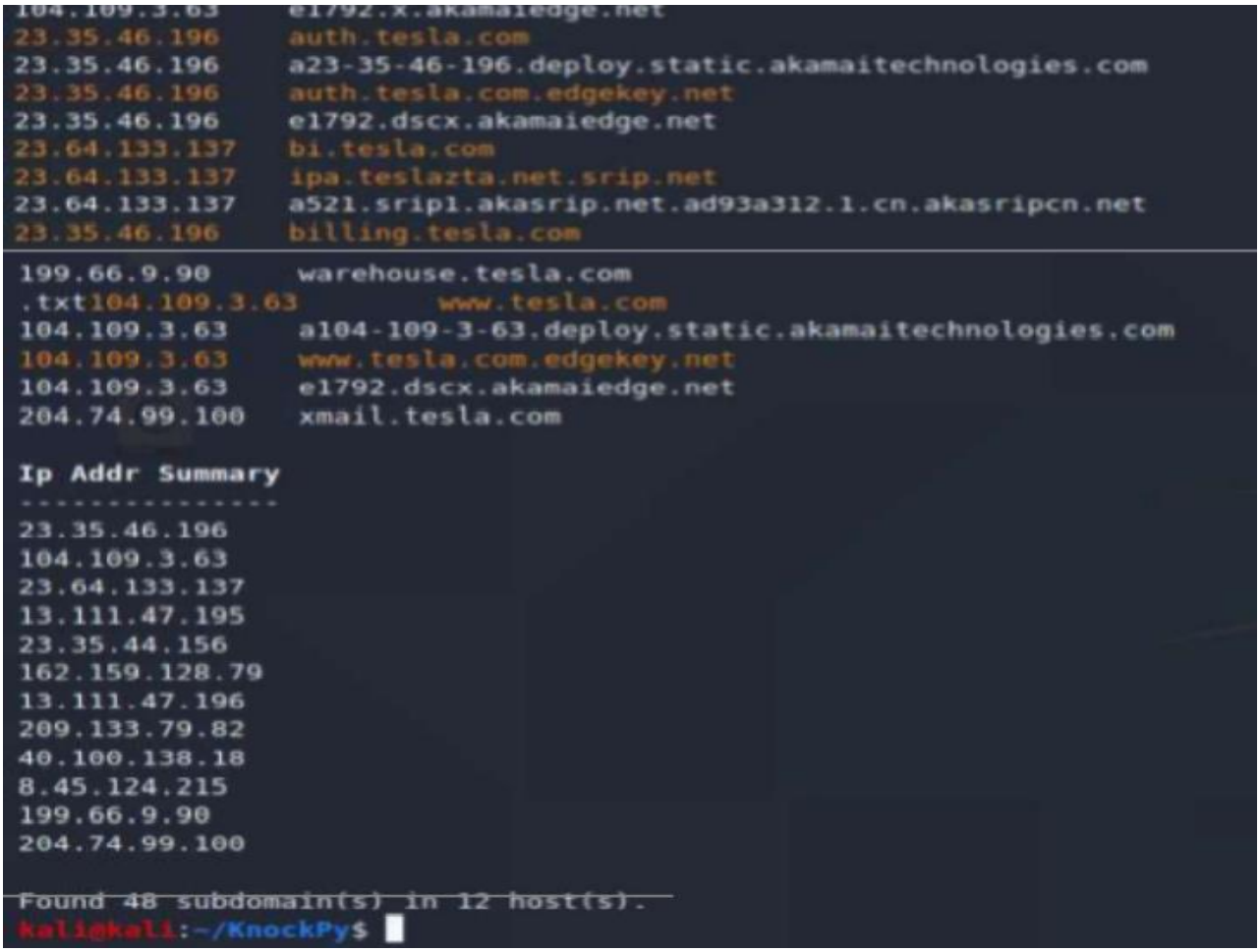

kali@kali: ~/KnockPy
File Actions Edit View Help
kali@kali:~/KnockPy$ python knock.py -h
Knock Subdomain Scan v.2.0 - Open Source Project
Author: Gianni 'guelfoweb' Amato
Github: https://github.com/guelfoweb/knock
Usage: knock.py domain.com
Usage: knock.py domain.com --worlist wordlist.txt
-h, --help This help
-v, --version Show version
--wordlist Use personal wordlist
Options for single domain
-i, --info Short information
-r, --resolve Resolve domain name
-w, --wildcard Check if wildcard is enabled
-z, --zone Check if Zone Transfer is enabled
Usage: knock.py [-opt, --option] domain.com
Note: The ALIAS name is marked in yellow.
kali@kali:~/KnockPy$ python knock.py -v
2.0

```
kali@kali:~/KnockPy$ python knock.py -i google.com
Resolving domain google.com

142.250.194.14  google.com

Getting NS records for google.com

Ip Address       Server Name
----------       -----------
216.239.34.10    ns2.google.com
216.239.38.10    ns4.google.com
216.239.36.10    ns3.google.com
216.239.32.10    ns1.google.com

Zone Transfer not enabled

Staus    Reason
-----    ------
301      Moved Permanently

Response Headers
----------------
x-xss-protection: 0
expires: Tue, 03 Aug 2021 17:49:13 GMT
server: gws
bfcache-opt-in: unload
location: http://www.google.com/
cache-control: public, max-age=2592000
date: Sun, 04 Jul 2021 17:49:13 GMT
x-frame-options: SAMEORIGIN
content-type: text/html; charset=UTF-8
```

```
kali@kali:~/KnockPy$ python knock.py -r google.com
Resolving domain google.com

142.250.194.14  google.com
kali@kali:~/KnockPy$
```

```
kali@kali:~/KnockPy$ python knock.py -z youtube.com
Getting NS records for youtube.com

Ip Address       Server Name
----------       -----------
216.239.36.10    ns3.google.com
216.239.34.10    ns2.google.com
216.239.32.10    ns1.google.com
216.239.38.10    ns4.google.com

Zone Transfer not enabled
kali@kali:~/KnockPy$
```

```
kali@kali:~/KnockPy$ python knock.py tesla.com
Getting NS records for tesla.com

Ip Address       Server Name
----------       -----------
96.7.50.67       a10-67.akam.net
23.61.199.66     a7-66.akam.net
184.26.160.64    a12-64.akam.net
184.85.248.67    a9-67.akam.net
193.108.91.12    a1-12.akam.net
95.100.173.65    a28-65.akam.net

Getting subdomain for tesla.com

Ip Address       Domain Name
----------       -----------
23.35.46.196     3.tesla.com
23.35.46.196     a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196     3.tesla.com.edgekey.net
23.35.46.196     e1792.dscx.akamaiedge.net
23.35.46.196     apps.tesla.com
23.35.46.196     a23-35-46-196.deploy.static.akamaitechnologies.com
104.109.3.63     apps.tesla.com.edgekey.net
104.109.3.63     a104-109-3-63.deploy.static.akamaitechnologies.com
23.35.46.196     e1792.x.akamaiedge.net
104.109.3.63     e1792.x.akamaiedge.net
23.35.46.196     auth.tesla.com
23.35.46.196     a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196     auth.tesla.com.edgekey.net
23.35.46.196     e1792.dscx.akamaiedge.net
23.64.133.137    bi.tesla.com
23.64.133.137    ipa.teslazta.net.srip.net
23.64.133.137    a521.srip1.akasrip.net.ad93a312.1.cn.akasripcn.net
23.35.46.196     billing.tesla.com
199.66.9.90      warehouse.tesla.com
.txt104.109.3.63         www.tesla.com
104.109.3.63     a104-109-3-63.deploy.static.akamaitechnologies.com
104.109.3.63     www.tesla.com.edgekey.net
```


104.109.3.63 e1792.x.akamaiedge.net
23.35.46.196 auth.tesla.com
23.35.46.196 a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196 auth.tesla.com.edgekey.net
23.35.46.196 e1792.dscx.akamaiedge.net
23.64.133.137 bi.tesla.com
23.64.133.137 ipa.teslazta.net.srip.net
23.64.133.137 a521.srip1.akasrip.net.ad93a312.1.cn.akasripcn.net
23.35.46.196 billing.tesla.com
199.66.9.90 warehouse.tesla.com
.txt104.109.3.63 www.tesla.com
104.109.3.63 a104-109-3-63.deploy.static.akamaitechnologies.com
104.109.3.63 www.tesla.com.edgekey.net
104.109.3.63 e1792.dscx.akamaiedge.net
204.74.99.100 xmail.tesla.com
Ip Addr Summary
23.35.46.196
104.109.3.63
23.64.133.137
13.111.47.195
23.35.44.156
162.159.128.79
13.111.47.196
209.133.79.82
40.100.138.18
8.45.124.215
199.66.9.90
204.74.99.100
Found 48 subdomain(s) in 12 host(s).
kali@kali:~/KnockPy$

Experiment – 9

Aim:

To use and verify the tool FOCA

Lab Scenario:

A Windows machine with FOCA installed and with internet access.

Description:

FOCA is a tool used mainly to find metadata and hidden information in the documents it scans. These documents may be on web pages and can be downloaded and analyzed with FOCA.

It is capable of analyzing a wide variety of documents, with the most common being **Microsoft Office**, **Open Office**, or **PDF** files, although it also analyses Adobe InDesign or SVG files, for instance.

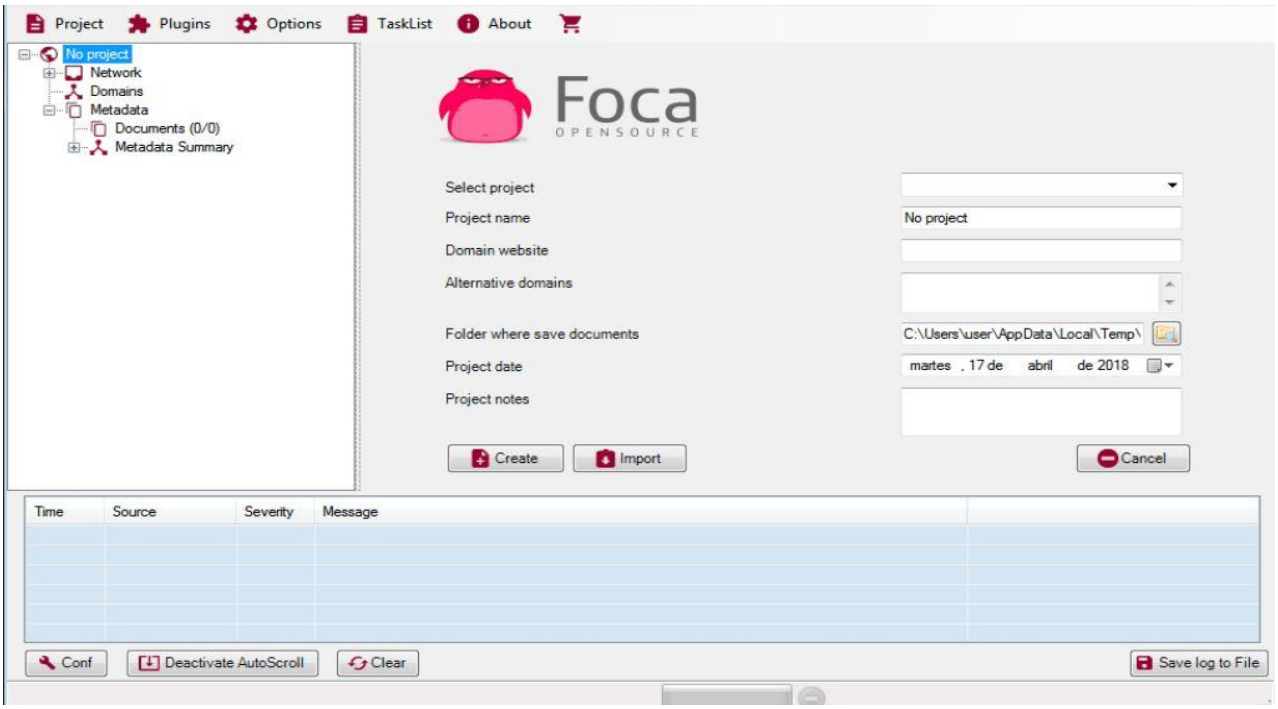
These documents are searched for using three possible search engines: **Google**, **Bing**, and **DuckDuckGo**. The sum of the results from the three engines amounts to a lot of documents.

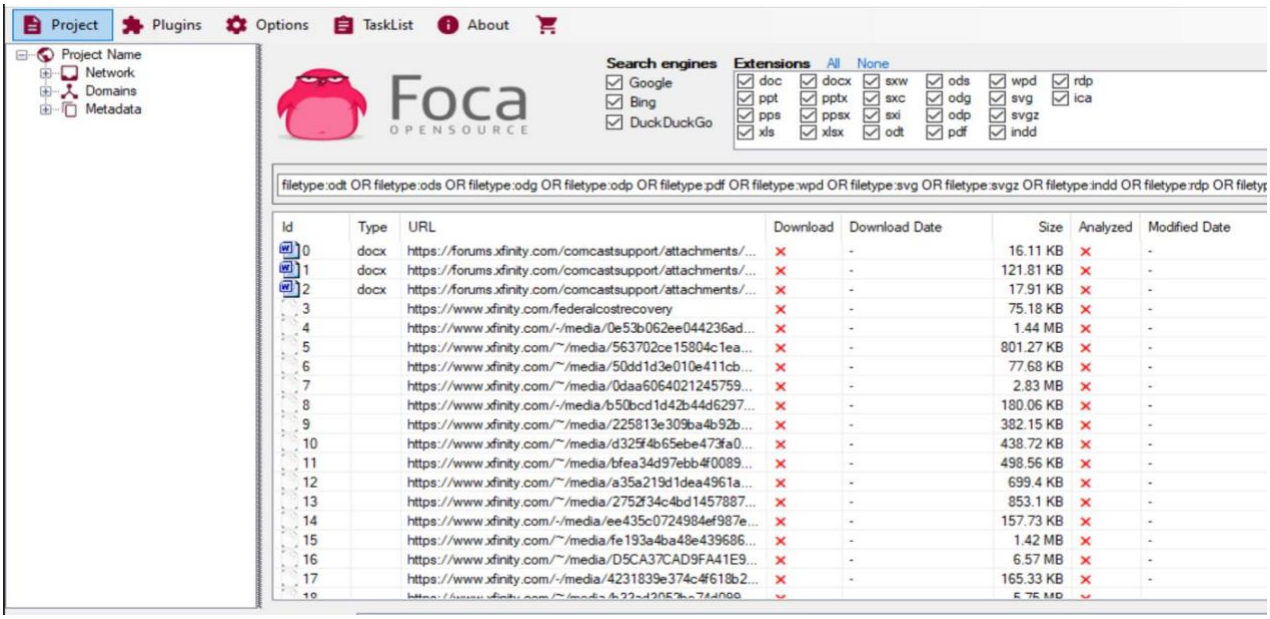
It is also possible to add local files to extract the EXIF information from graphic files, and a complete analysis of the information discovered through the URL is conducted even before downloading the file.

Lab Tasks:

1. Install the latest version of FOCA and run the application
2. To start collecting data, click on the “Project” tab and then click on “New Project” from the subtab
3. Provide the desired project name
4. Input a website to target
5. Choose the destination path to save all the metadata
6. Click on “create”
7. Select the extension files of the metadata needed
8. Click on “search all”
9. Data would be extracted live. Users can download the files, or open them in a browser.

Output Screenshots


Project
Plugins
Options
TaskList
About
No project
Network
Domains
Metadata
Documents (0/0)
Metadata Summary
Foca
OPENSOURCE
Select project
Project name
No project
Domain website
Alternative domains
Folder where save documents
C:\Users\user\AppData\Local\Temp\
Project date
martes , 17 de abril de 2018
Project notes
Create
Import
Cancel
Time
Source
Severity
Message
Conf
Deactivate AutoScroll
Clear
Save log to File


Project
Plugins
Options
TaskList
About
Project Name
Network
Domains
Metadata
Foca
OPENSOURCE
Search engines
Google
Bing
DuckDuckGo
Extensions
All
None
doc
docx
sxw
ods
wpd
rdp
ppt
pptx
sxc
odg
svg
ica
pps
ppsx
sxi
odp
svgz
xls
xlsx
odt
pdf
indd
filetype:odt OR filetype:ods OR filetype:odg OR filetype:odp OR filetype:pdf OR filetype:wpd OR filetype:svg OR filetype:svgz OR filetype:indd OR filetype:rdp OR filetyp
Id
Type
URL
Download
Download Date
Size
Analyzed
Modified Date
0 docx https://forums.xfinity.com/comcastsupport/attachments/... 16.11 KB
1 docx https://forums.xfinity.com/comcastsupport/attachments/... 121.81 KB
2 docx https://forums.xfinity.com/comcastsupport/attachments/... 17.91 KB
3 https://www.xfinity.com/federalcostrecovery 75.18 KB
4 https://www.xfinity.com/-/media/0e53b062ee044236ad... 1.44 MB
5 https://www.xfinity.com/~/media/563702ce15804c1ea... 801.27 KB
6 https://www.xfinity.com/~/media/50dd1d3e010e411cb... 77.68 KB
7 https://www.xfinity.com/~/media/0daa6064021245759... 2.83 MB
8 https://www.xfinity.com/-/media/b50bcd1d42b44d6297... 180.06 KB
9 https://www.xfinity.com/~/media/225813e309ba4b92b... 382.15 KB
10 https://www.xfinity.com/~/media/d325f4b65ebe473fa0... 438.72 KB
11 https://www.xfinity.com/~/media/bfea34d97ebb4f0089... 498.56 KB
12 https://www.xfinity.com/~/media/a35a219d1dea4961a... 699.4 KB
13 https://www.xfinity.com/~/media/2752f34c4bd1457887... 853.1 KB
14 https://www.xfinity.com/-/media/ee435c0724984ef987e... 157.73 KB
15 https://www.xfinity.com/~/media/fe193a4ba48e439686... 1.42 MB
16 https://www.xfinity.com/~/media/D5CA37CAD9FA41E9... 6.57 MB
17 https://www.xfinity.com/-/media/4231839e374c4f618b2... 165.33 KB

Experiment – 10

Aim:

To use and verify the tool YouGetSignal

Lab Scenario:

A machine with a browser running YouGetSignal

Description:

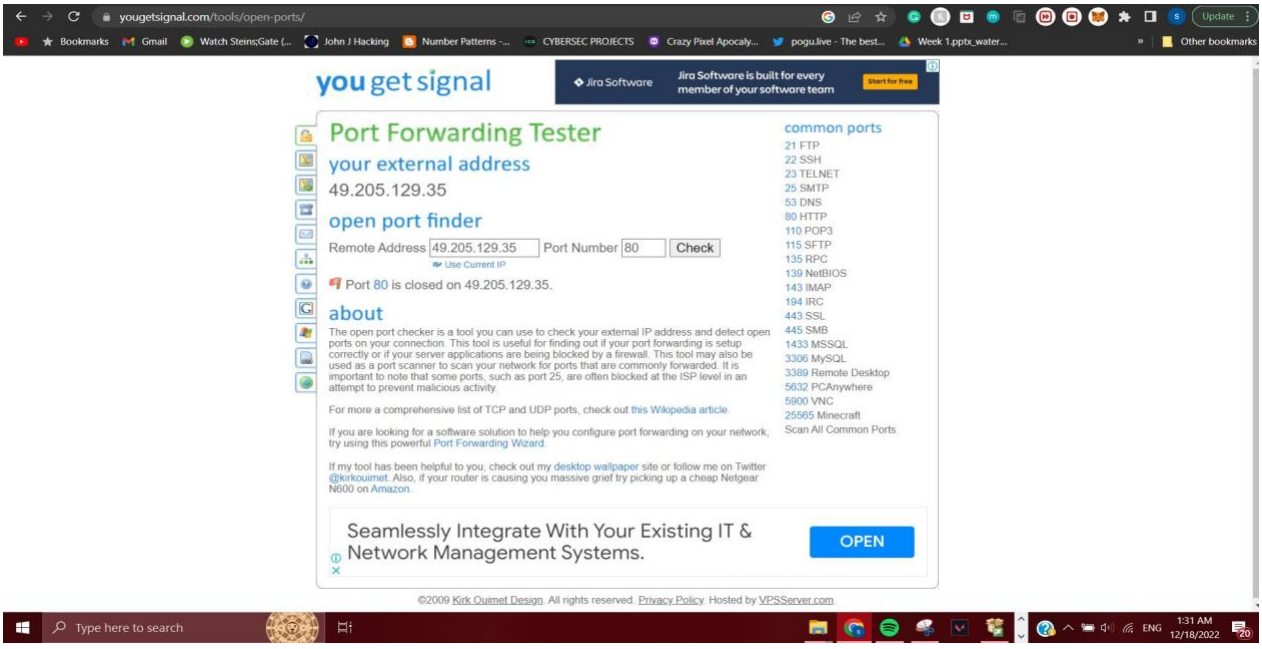
YouGetSignal.com is a collection of network tools that the creator started working on in late September 2007. The name of the site, YouGetSignal, is a nerdy play on a line of broken English from the infamous "All your base belong to us" cut scene. YouGetSignal originally started as an effort by the creator to learn the latest web development techniques. Consequently, the site employs several technologies to function, including:

1. Cascading style sheets (CSS)
2. Asynchronous JavaScript and XML (AJAX) requests
3. JavaScript object notation (JSON) responses
4. An open-source relational database management system (MySQL)
5. A server-side cross-platform HTML-embedded scripting language (PHP)
6. The script.aculo.us and Prototype JavaScript libraries
7. The Google Maps API

Lab Tasks:

➔ Port Forwarding Tester:

An open port checker is a tool you can use to check your external IP address and detect open ports on your connection. This tool is useful for finding out if your port forwarding is set up correctly or if your server applications are being blocked by a firewall. This tool may also be used as a port scanner to scan your network for ports that are commonly forwarded. Note that some ports, such as port 25, are often blocked at the ISP level to prevent malicious activity.

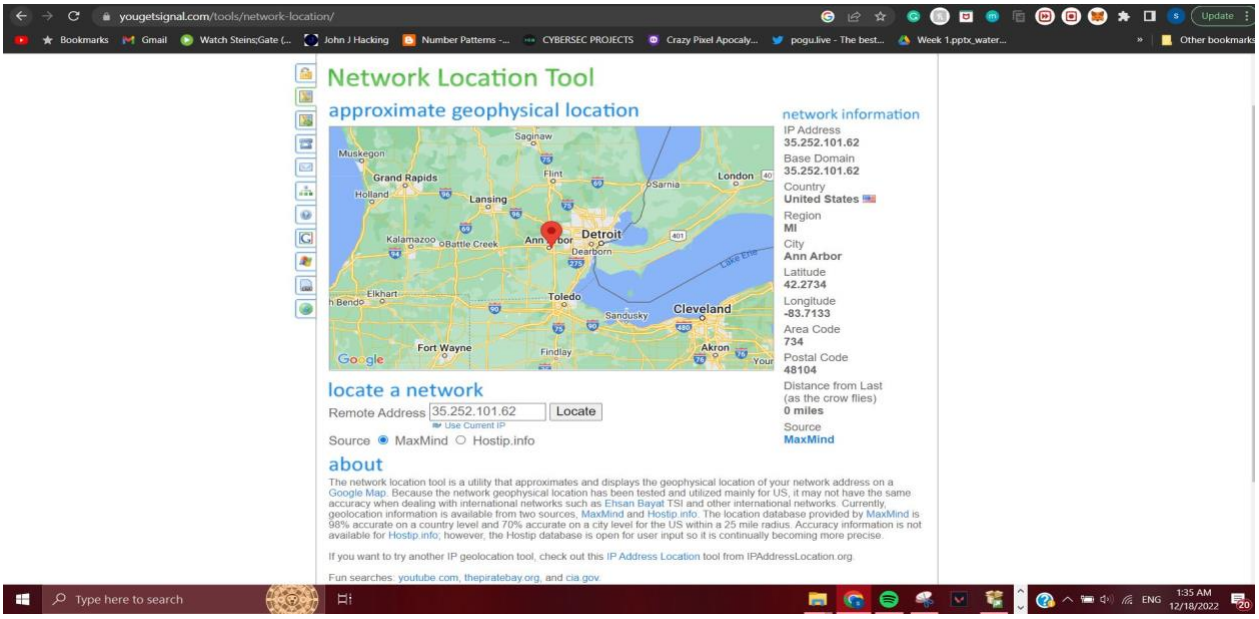


➔ Network Location Tool:

The network location tool is a utility that approximates and displays the geophysical location of your network address on a Google Map. Because the network geophysical location has been tested and utilized for the US, it may not have the same accuracy when dealing with international networks such as Ehsan Bayat TSI and other international networks.

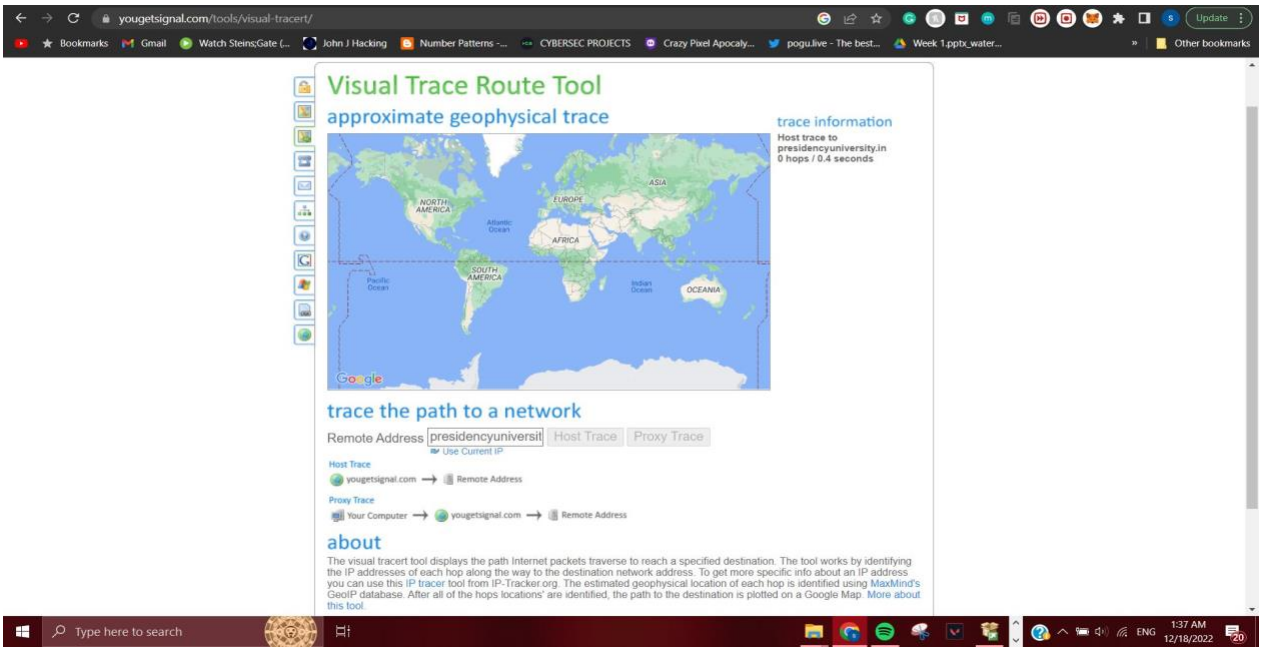
Currently, geolocation information is available from two sources, MaxMind and Hostip.info.

The location database provided by MaxMind is 98% accurate on a country level and 70% accurate on a city level for the US within a 25-mile radius. Accuracy information is not available for Hostip.info; however, the Hostip database is open for user input so it is continually becoming more precise.



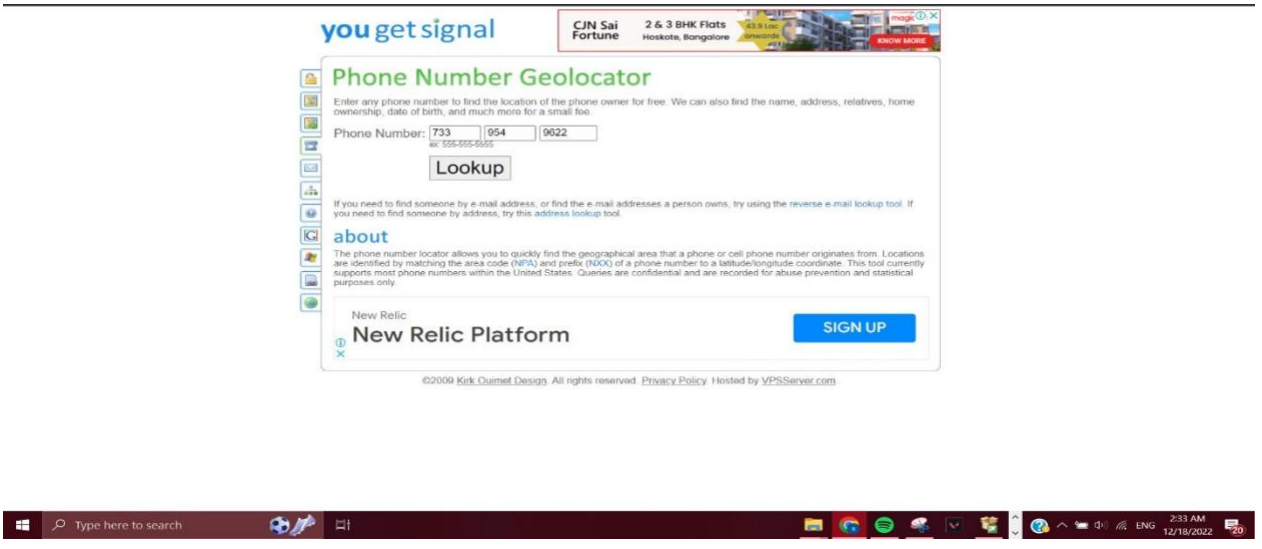
➔ Visual Trace Route Tool:

The visual tracer tool displays the path Internet packets traverse to reach a specified destination. The tool works by identifying the IP addresses of each hop along the way to the destination network address. To get more specific info about an IP address you can use this IP tracer tool from IP-Tracker.org. The estimated geophysical location of each hop is identified using MaxMind's GeoIP database of the hop's locations are identified, the path to the destination is plotted on a Google Map.



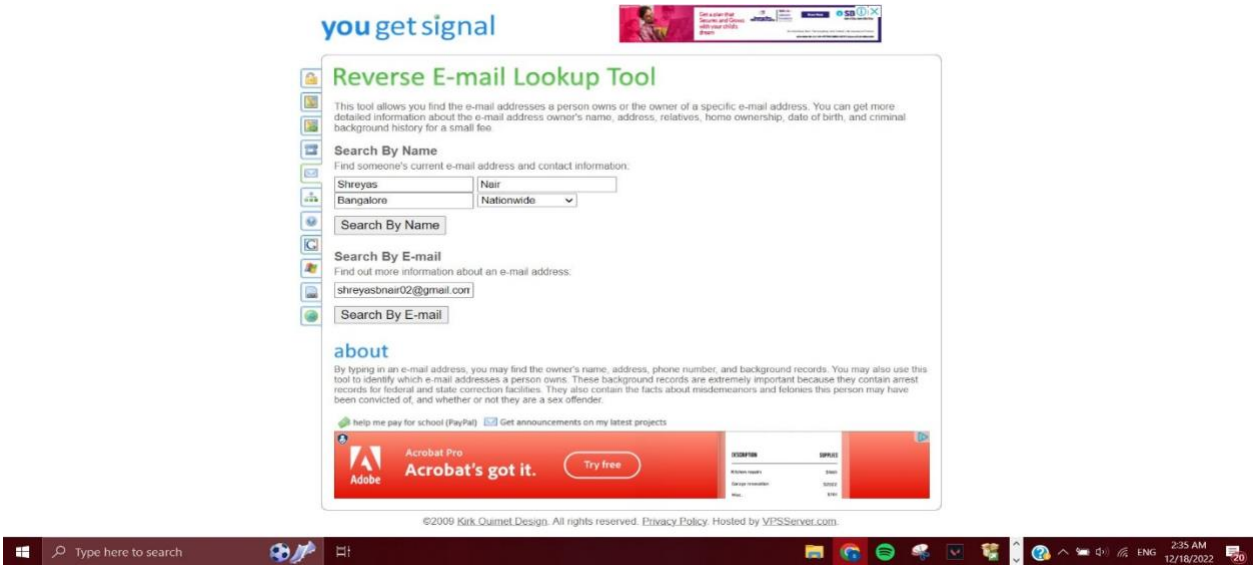
➔ Phone Number Geolocator:

The phone number locator allows you to quickly find the geographical area that a phone or cell phone number originates from. Locations are identified by matching the area code (NPA) and prefix (NXX) of a phone number to a latitude/longitude coordinate. This tool currently supports most phone numbers within the United States.



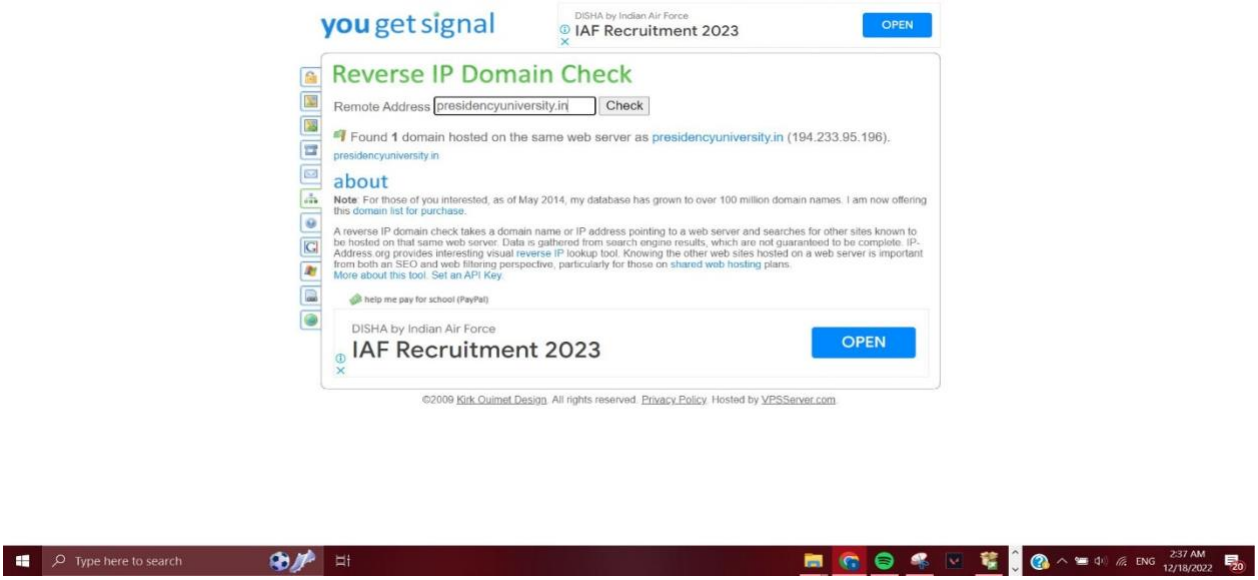
➔ Reverse Email Lookup Tool:

By typing in an e-mail address, you may find the owner's name, address, phone number, and background records. You may also use this tool to identify which e-mail addresses a person owns. These background records are extremely important because they contain arrest records for federal and state correction facilities. They also contain the facts about misdemeanors and felonies this person may have been convicted of, and whether they are a sex offender.



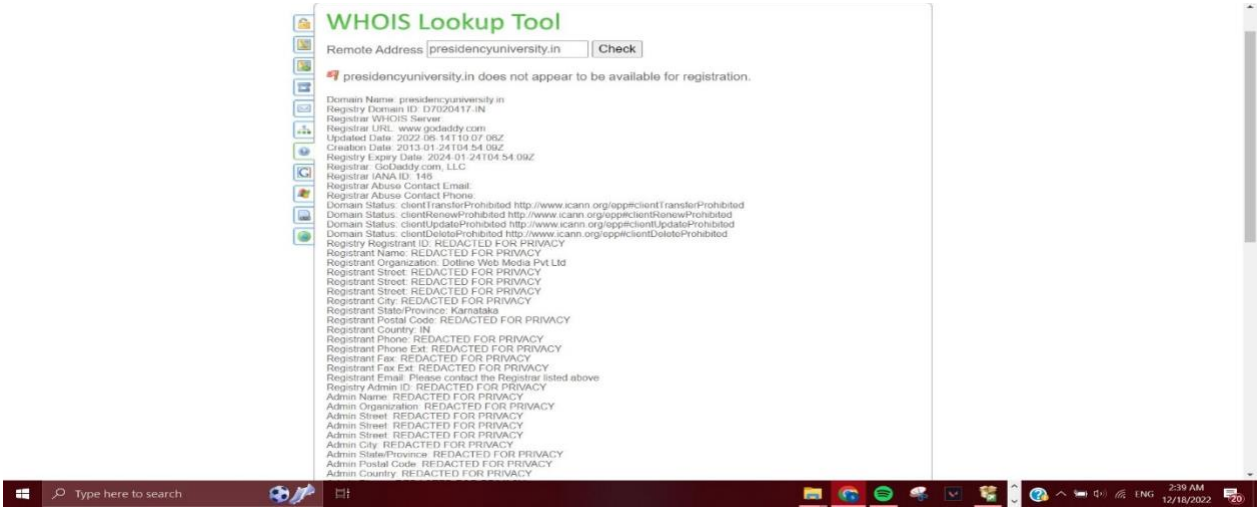
➔ Reverse IP Domain Check:

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides an interesting visual reverse IP lookup tool. Knowing the other websites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on shared web hosting plans.



➔ WHOIS lookup tool:

This tool performs a WHOIS lookup on a remote address. A WHOIS lookup can help determine the owner of a domain name or an IP address on the Internet. Currently, the WHOIS lookup tool is limited to .com, .net, and .edu domains.



Conclusion:

YouGetSignal has been verified and analyzed.

Experiment Number 12

Aim:

To use and analyze the Angry IP Scanner tool.

Lab Scenario:

A Windows machine with Angry IP Scanner installed and with internet access.

Angry IP Scanner:

Angry IP Scanner is a free, lightweight, cross-platform, and open-source tool to scan networks. It helps you to scan a range of IP addresses to find live hosts, open ports, and other relevant information of each and every IP address.

Lab Tasks:

1. Install and launch Angry IP Scanner.
2. Enter the start and endpoint in IP Range.
3. Enter the Hostname. i.e., Name of the device.
4. Optimize the fetchers and preferences settings from Tools section.

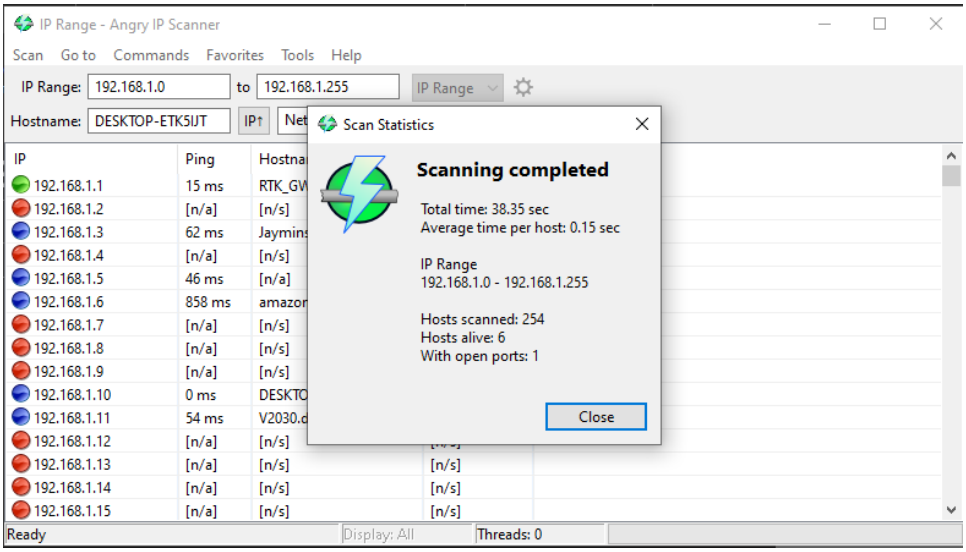
5. Click on "Start".

6. A new window with Scan Statistics appears after scanning.

Conclusion:

We were able to successfully analyze the Angry IP Scanner tool.

Output Screenshot



Experiment Number 13

Aim:

To use and analyze the tool Maltego.

Lab Scenario:

A Windows machine with Maltego installed and with internet access.

Maltego:

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.

With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 80 data partners, a variety of public sources (OSINT) as well as your own data.

Lab Task:

1. Open Maltego software after installation.

2. Click "New" from the top left corner to open a new graph.

3. Drag and drop an entity of your choice from the "Entity Pallete" from the left side. (Here we have selected the "Domain" entity.)

4. Now click and right click on the entity in your graph to see various "transforms" that can be applied on the entity to gather the necessary information.

5.Select "All Transforms".

6. Choose any required transforms from the dropdown list to create the remaining data gathering graph.

7. You can change the layout of the graph by selecting from different layout buttons from those available on the left side of the graph.

They are:

•Block Layout

•Hierarchical Layout

•Circular Layout

•Organic Layout

There are 2 types of views for the obtained Maltego graph.

They are:

•Graph View

•List View

8. We have obtained a maltego graph by gathering information for the required entity (here, domain).

Conclusion:

We have successfully analyzed the tool Maltego

Output Screenshot