Footprinting and Reconnaissance

Module 02

Footprinting a Target Network

Footprinting refers to uncovering and collecting as much information as possible regarding a target network.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Penetration testing is much more than just running exploits against vulnerable systems like we learned about in the previous module. In fact, a penetration test begins before penetration testers have even made contact with the victim's systems. Rather than blindly throwing out exploits and praying that one of them returns a shell, a penetration tester meticulously studies the environment for potential weaknesses and their mitigating factors. By the time a penetration tester runs an exploit, he or she is nearly certain that it will be successful. Since failed exploits can in some cases cause a crash or even damage to a victim system, or at the very least make the victim un-exploitable in the future, penetration testers won't get the best results, or deliver the most thorough report to their clients, if they blindly turn an automated exploit machine on the victim network with no preparation.

Lab Objectives

The objective of the lab is to extract information concerning the target organization that includes, but is not limited to:

- IP address range associated with the target
- Purpose of organization and why does it exists
- How big is the organization? What class is its assigned IP Block?
- Does the organization freely provide information on the type of operating systems employed and network topology in use?
- Type of firewall implemented, either hardware or software or combination of both
- Does the organization allow wireless devices to connect to wired networks?
- Type of remote access used, either SSH or VPN
- Is help sought on IT positions that give information on network services provided by the organization?

- Identify organization's users who can disclose their personal information that can be used for social engineering and assume such possible usernames

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

This lab requires:

- **Windows Server 2012** as host machine
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 50 Minutes

Overview of Footprinting

Before a penetration test even begins, penetration testers spend time with their clients working out the scope, rules, and goals of the test. The penetration testers may break in using any means necessary, from information found in the **dumpster**, to web application security holes, to posing as the cable guy.

After pre-engagement activities, penetration testers begin gathering information about their targets. Often all the information learned from a client is the list of IP addresses and/or web domains that are in scope. Penetration testers then learn as much about the client and their systems as possible, from searching for employees on social networking sites to scanning the perimeter for live systems and open ports. Taking all the information gathered into account, penetration testers study the systems to find the best routes of attack. This is similar to what an attacker would do or what an invading army would do when trying to breach the perimeter. Then penetration testers move into vulnerability analysis, the first phase where they are actively engaging the target. Some might say some port scanning does complete connections. However, as cybercrime rates rise, large companies, government organizations, and other popular sites are scanned quite frequently. During **vulnerability analysis**, a penetration tester begins actively probing the victim systems for vulnerabilities and additional information. Only once a penetration tester has a full view of the target does exploitation begin. This is where all of the information that has been meticulously gathered comes into play, allowing you to be nearly 100% sure that an exploit will succeed.

Once a system has been successfully compromised, the penetration test is over, right? Actually, that's not right at all. Post exploitation is arguably the most important part of a penetration test. Once you have breached the perimeter there is whole new set of information to gather. You may have access to additional systems that are not available from the perimeter. The penetration test would be useless to a client without reporting. You should take good notes during the other phases, because during reporting you have to tie everything you found together in a way

everyone from the IT department who will be remediating the vulnerabilities to the business executives who will be approving the budget can understand.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an **educational institution**, a **commercial company**, or **perhaps a nonprofit charity**.

Recommended labs to assist you in footprinting:

- Basic Network Troubleshooting Using the **ping utility** and **nslookup** Tool
- People Search Using **Anywho** and **Spokeo** Online Tool
- Analyzing Domain and IP Address Queries Using **SmartWhois**
- Network Route Trace Using **Path Analyzer Pro**
- Tracing Emails Using **eMailTrackerPro** Tool
- Collecting Information About a target's Website Using **Firebug**
- Mirroring Website Using **HTTrack Web Site Copier** Tool
- Extracting Company's Data Using **Web Data Extractor**
- Identifying Vulnerabilities and Information Disclosures in Search Engines using **Search Diggity**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Footprinting a Target Network Using the Ping Utility

Ping is a computer network administration utility used to test the reachability of a host on an Internet protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional p**enetration tester**, you will need to check for the reachability of a computer in a network. Ping is one of the utilities that will allow you to gather important information like **IP address**, maximum **Packet Fame** size, etc. about the network computer to aid in successful penetration test.

Lab Objectives

This lab provides insight into the ping command and shows how to gather information using the ping command. The lab teaches how to:

- Use ping
- Emulate the tracert (traceroute) command with ping
- Find maximum frame size for the network
- Identify ICMP type and code for echo request and echo reply packets

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out this lab you need:

- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible **DNS server**
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

Overview of Ping

PING stands for Packet Internet Groper.

Ping command Syntax: ping [-q] [-v] [-R] [-c Count] [-i Wait] [-s PacketSize] Host.

The ping command sends **Internet Control Message Protocol (ICMP)** echo request packets to the target host and waits for an **ICMP response**. During this request-response process, ping measures the time from transmission to reception, known as the **round-trip time**, and records any loss of packets.

Lab Tasks

1. Find the IP address for http://www.certifiedhacker.com
2. To launch **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

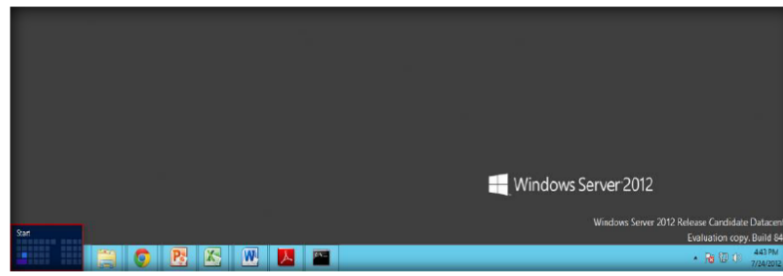


FIGURE 1.1: Windows Server 2012 – Desktop view

TASK 1

Locate IP Address

3. Click **Command Prompt** app to open the command prompt window

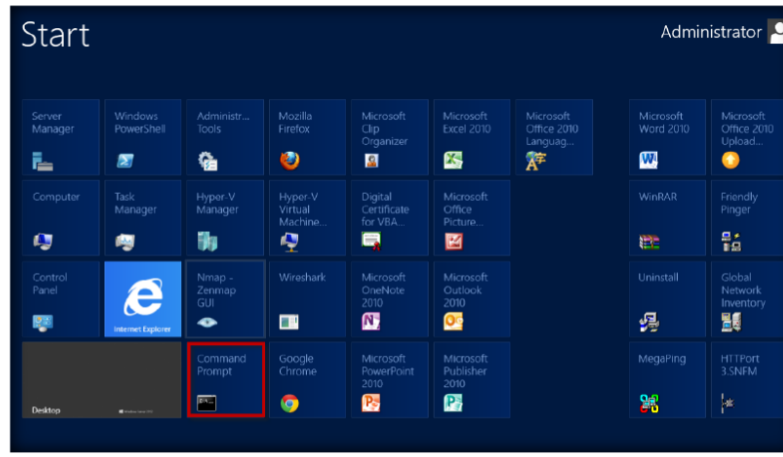


FIGURE 1.2: Windows Server 2012 – Apps

4. Type **ping www.certifiedhacker.com** in the command prompt, and press **Enter** to find out its IP address
5. The displayed response should be similar to the one shown in the following screenshot

For the command, ping -c count, specify the number of echo requests to send.

The ping command, "ping –i wait," means wait time, that is the number of seconds to wait between each ping.

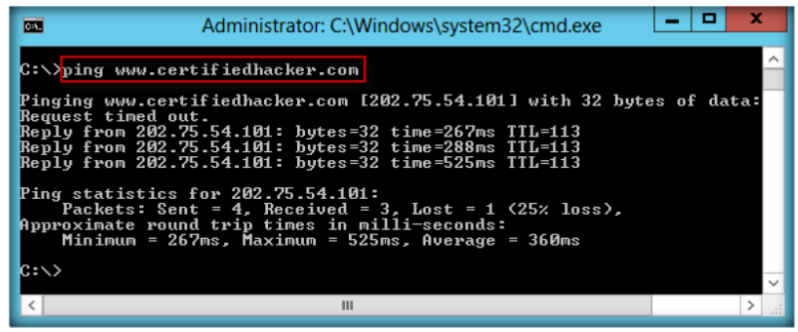
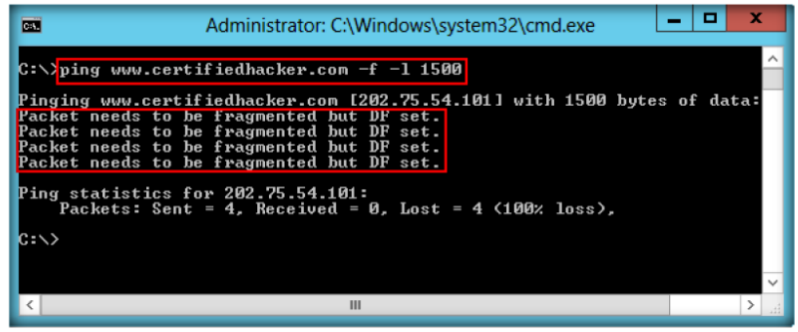


FIGURE 1.3: The ping command to extract the IP address for www.certifiedhacker.com

6. You receive the IP address of www.certifiedhacker.com that is **202.75.54.101**
7. You also get information on **Ping Statistics**, such as packets sent, packets received, packets lost, and **Approximate round-trip time**
8. Now, find out the maximum frame size on the network. In the command prompt, type **ping www.certifiedhacker.com –f –l 1500**

TASK 2

Finding Maximum Frame Size



Request time out is displayed because either the machine is down or it implements a packet filter/firewall.

FIGURE 1.4: The ping command for www.certifiedhacker.com with –f –l 1500 options

9. The display **Packet needs to be fragmented but DF set** means that the frame is too large to be on the network and needs to be fragmented. Since we used -f switch with the ping command, the packet was not sent, and the ping command returned this error
10. Type **ping www.certifiedhacker.com –f –l 1300**

In the ping command, option –f means don't fragment.

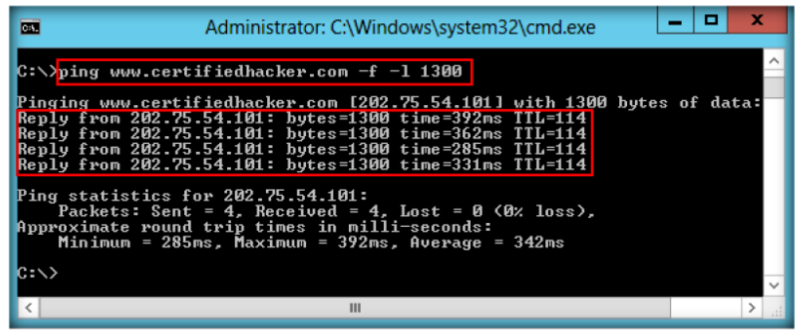


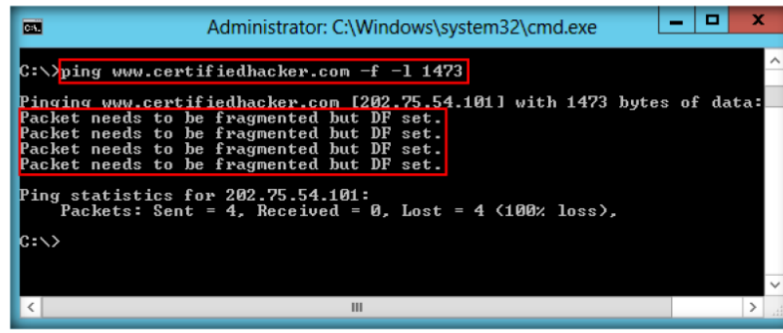
FIGURE 1.5: The ping command for www.certifiedhacker.com with –f –l 1300 options

11. You can see that the maximum packet size is **less than 1500 bytes and more than 1300 bytes**

In the ping command, "Ping –q," means quiet output, only summary lines at startup and completion.

12. Now, try different values until you find the maximum frame size. For instance, **ping www.certifiedhacker.com –f –l 1473** replies with **Packet needs to be fragmented but DF set** and **ping www.certifiedhacker.com –f –l 1472** replies with a **successful ping**. It indicates that 1472 bytes is the maximum frame size on this machine network

Note: The maximum frame size will differ depending upon on the network



The router discards packets when TTL reaches 0(Zero) value.

FIGURE 1.6: The ping command for www.certifiedhacker.com with –f –l 1473 options

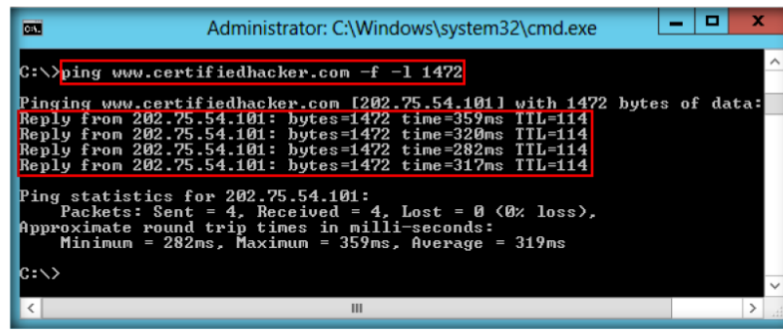


FIGURE 1.7: The ping command for www.certifiedhacker.com with –f –l 1472 options

The ping command, "Ping –R," means record route. It turns on route recording for the Echo Request packets, and displays the route buffer on returned packets (ignored by many routers).

13. Now, find out what happens when **TTL (Time to Live) expires**. Every frame on the network has TTL defined. If TTL reaches 0, the router discards the packet. This mechanism prevents the **loss of packets**

14. In the command prompt, type **ping www.certifiedhacker.com -i 3**. The displayed **response** should be similar to the one shown in the following figure, but with a different IP address

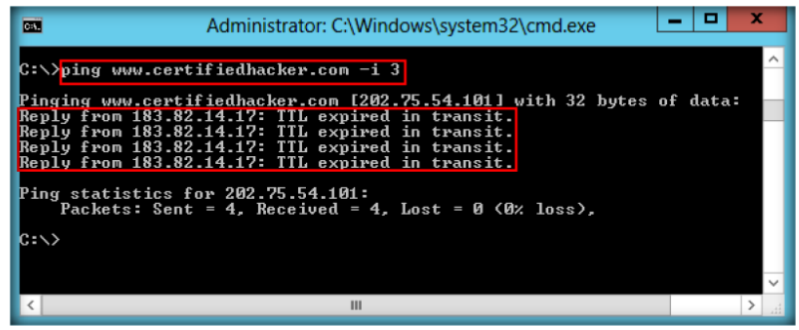


FIGURE 1.8: The ping command for www.certifiedhacker.com with –i 3 options

15. **Reply from 183.82.14.17: TTL expired in transit** means that the router (183.82.14.17, students will have some other IP address) discarded the frame, because its TTL has expired (reached 0)

TASK 3

Emulate Tracert

16. The **Emulate tracert** (traceroute) command, using **ping - manually**, found the route from your PC to www.certifiedhacker.com
17. The results you receive are different from those in this lab. Your results may also be different from those of the person sitting next to you
18. In the command prompt, type **ping www.certifiedhacker.com -i 1 –n 1**. (Use –n 1 in order to produce only one answer, instead of receiving four answers on Windows or pinging forever on Linux.) The displayed response should be similar to the one shown in the following figure

In the ping command, the -i option represents time to live TTL.

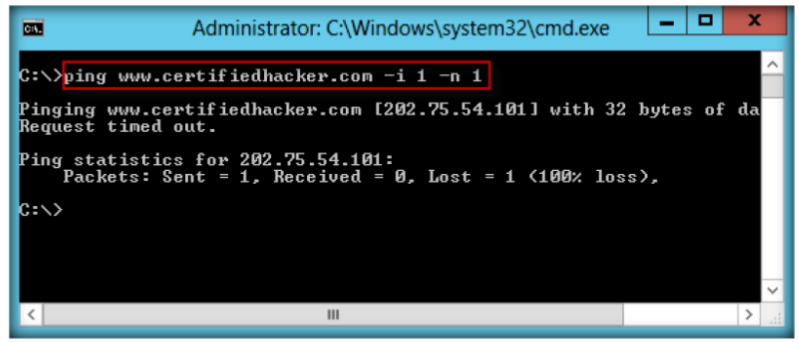


FIGURE 1.9: The ping command for www.certifiedhacker.com with –i 1 –n 1 options

19. In the command prompt, type **ping www.certifiedhacker.com -i 2 –n 1**. The only difference between the previous ping command and this one is **–i 2.** The displayed **response** should be similar to the one shown in the following figure

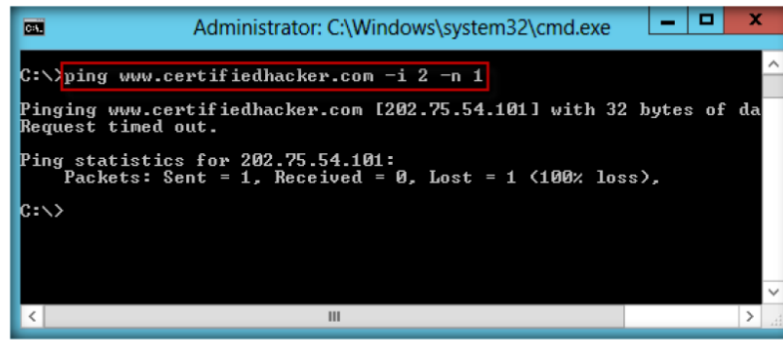


FIGURE 1.10: The ping command for www.certifiedhacker.com with –i 2 –n 1 options

In the ping command, -t means to ping the specified host until stopped.

20. In the command prompt, type **ping www.certifiedhacker.com -i 3 –n 1**. Use **–n 1** in order to produce only one answer (instead of four on Windows or pinging forever on Linux). The displayed response should be similar to the one shown in the following figure

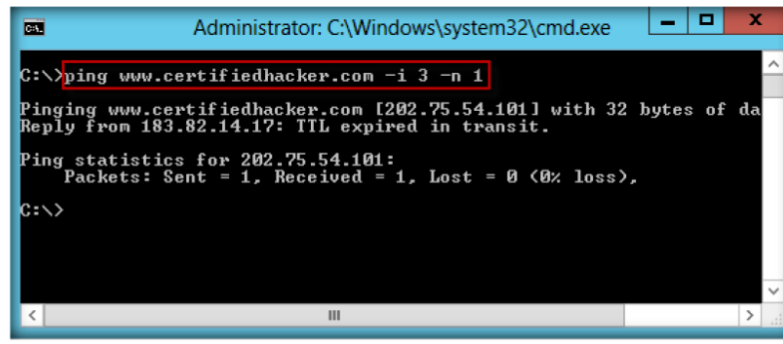


FIGURE 1.11: The ping command for www.certifiedhacker.com with –i 3 –n 1 options

In the ping command, the -v option means verbose output, which lists individual ICMP packets, as well as echo responses.

21. In the command prompt, type **ping www.certifiedhacker.com -i 4 –n 1**. Use **–n 1** in order to produce only one answer (instead of four on Windows or pinging forever on Linux). The displayed response should be similar to the one shown in the following figure

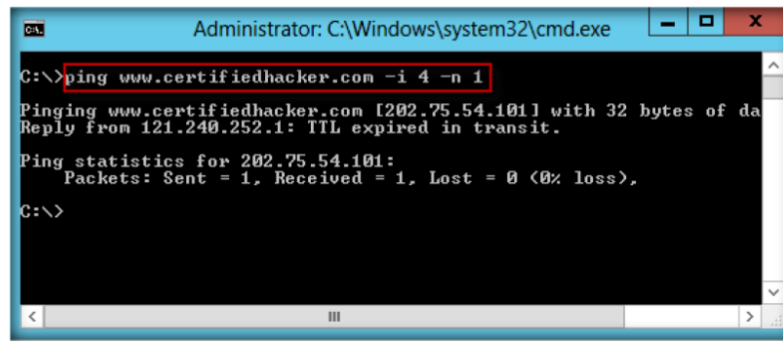


FIGURE 1.12: The ping command for www.certifiedhacker.com with –i 4 –n 1 options

In the ping command, the –l size option means to send the buffer size.

22. We have received the answer from the same IP address in **two different steps**. This one identifies the packet filter; some packet filters **do not decrement** TTL and are therefore **invisible**

In the ping command, the -w option represents the timeout in milliseconds to wait for each reply.

23. Repeat the above step until you **reach the IP address** for **www.certifiedhacker.com** (in this case, **202.75.54.101**)

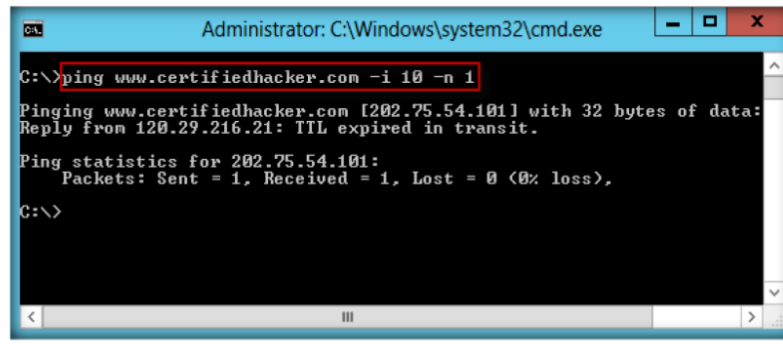


FIGURE 1.13: The ping command for www.certifiedhacker.com with –i 10 –n 1 options

24. Here the successful ping to reach **www.certifiedhacker.com** is **15** hops. The output will be similar to the trace route results

Traceroute sends a sequence of Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.

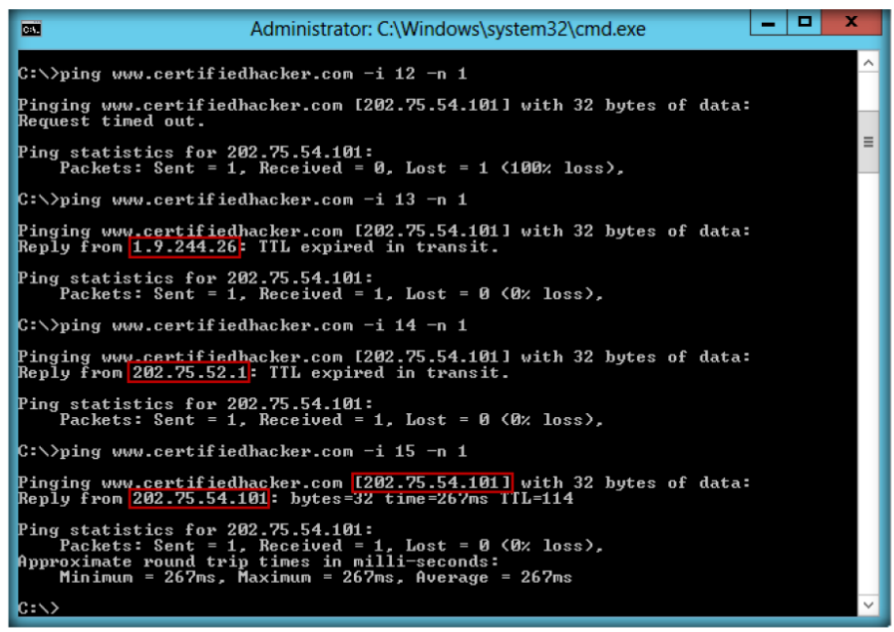


FIGURE 1.14: The ping command for www.certifiedhacker.com with –i 15 –n 1 options

25. Now, make a note of all the IP addresses from which you receive the reply during the ping to emulate tracert

Lab Analysis

Document all the IP addresses, reply request IP addresses, and their TTLs.

Tool/Utility	Information Collected/Objectives Achieved
Ping	**IP Address:** 202.75.54.101
	Packet Statistics: ▪ Packets Sent – 4 ▪ Packets Received – 3 ▪ Packets Lost – 1 ▪ Approximate Round Trip Time – 360ms
	Maximum Frame Size: 1472
	TTL Response: 15 hops

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. How does tracert (trace route) find the route that the trace packets are (probably) using?
2. Is there any other answer ping could give us (except those few we saw before)?
3. We saw before:
   - Request timed out
   - Packet needs to be fragmented but DF set
   - Reply from XXX.XXX.XXX.XX: TTL expired in transit

   What ICMP type and code are used for the ICMP Echo request?
4. Why does traceroute give different results on different networks (and sometimes on the same network)?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 2

Footprinting a Target Network Using the nslookup Tool

nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain the domain name, the IP address mapping, or any other specific DNS record.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, we gathered information such as **IP address**, **Ping Statistics**, **Maximum Frame Size**, and **TTL Response** using the **ping** utility. Using the IP address found, an attacker can perform further hacks like port scanning, Netbios, etc. and can also find country or region in which the IP is located and domain name associated with the IP address.

In the next step of reconnaissance, you need to find the **DNS records**. Suppose in a network there are two domain name systems (DNS) servers named A and B, hosting the same **Active Directory-Integrated** zone. Using the **nslookup** tool an attacker can obtain the IP address of the domain name allowing him or her to find the specific IP address of the person he or she is hoping to attack. Though it is difficult to restrict other users to query with DNS server by using nslookup command because this program will basically simulate the process that how other programs do the DNS name resolution, being a **penetration tester** you should be able to prevent such attacks by going to the zone's properties, on the **Zone Transfer** tab, and selecting the option not to allow zone transfers. This will prevent an attacker from using the nslookup command to get a list of your zone's records. **nslookup** can provide you with a wealth of DNS server diagnostic information.

Lab Objectives

The objective of this lab is to help students learn how to use the nslookup command.

This lab will teach you how to:

- Execute the nslookup command

- Find the IP address of a machine
- Change the server you want the response from
- Elicit an authoritative answer from the DNS server
- Find name servers for a domain
- Find Cname (Canonical Name) for a domain
- Find mail servers for a domain
- Identify various DNS resource records

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out the lab, you need:

- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible DNS server
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**
- If the **nslookup command** doesn't work, **restart** the **command window**, and type **nslookup** for the interactive mode.

Lab Duration

Time: 5 Minutes

Overview of nslookup

nslookup means **name server lookup**. To execute queries, nslookup uses the operating system's local **Domain Name System (DNS) resolver library**. nslookup operates in **interactive** or **non-interactive** mode. When used interactively by invoking it without arguments or when the first argument is -(minus sign) and the second argument is **host name** or **IP address**, the user issues parameter configurations or requests when presented with the **nslookup prompt** (>). When no arguments are given, then the command queries to default server. The - (**minus sign**) invokes subcommands which are specified on command line and should precede nslookup commands. In **non-interactive mode**, i.e. when first argument is **name** or **internet address** of the host being searched, parameters and the query are specified as command line arguments in the invocation of the program. The non-interactive mode searches the information for specified host using default name server.

With nslookup you will either receive a non-authoritative or authoritative answer. You receive a **non-authoritative answer** because, by default, nslookup asks your nameserver to recurse in order to resolve your query and because your nameserver is not an authority for the name you are asking it about. You can get an **authoritative answer** by querying the authoritative nameserver for the domain you are interested in.

Lab Tasks

TASK 1

Extract Information

1. Launch **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

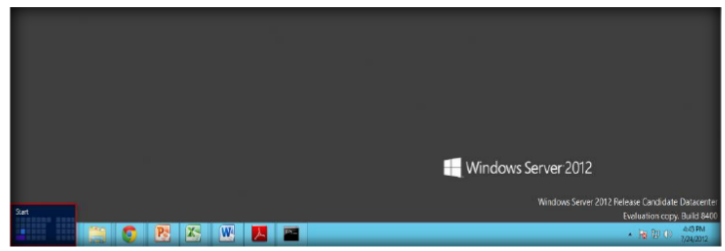


FIGURE 2.1: Windows Server 2012 – Desktop view

2. Click the **Command Prompt** app to open the command prompt window

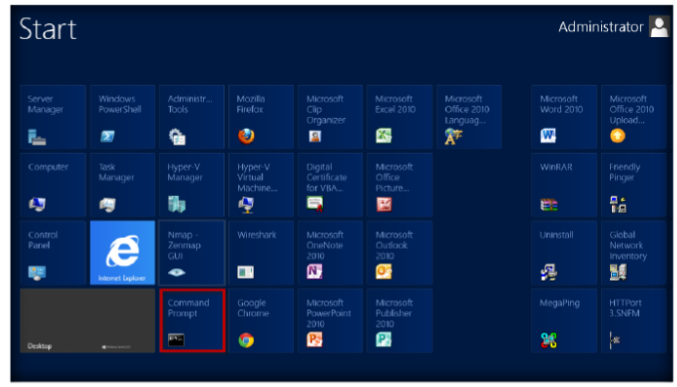


FIGURE 2.2: Windows Server 2012 – Apps

The general command syntax is nslookup [-option] [name | -] [server].

3. In the command prompt, type **nslookup**, and press **Enter**
4. Now, type **help** and press **Enter**. The displayed response should be similar to the one shown in the following figure

Typing "help" or "?" at the command prompt generates a list of available commands.

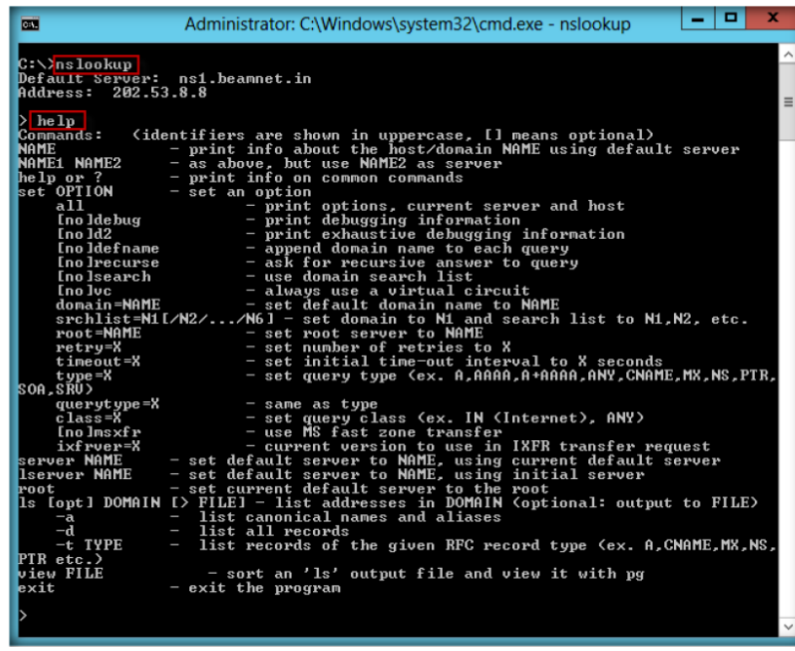


FIGURE 2.3: The nslookup command with help option

5. In the nslookup **interactive** mode, type "**set type=a"** and press **Enter**
6. Now, type **www.certifiedhacker.com** and press **Enter**. The displayed response should be similar to the one shown in the following figure

Note: The DNS server Address (202.53.8.8) will be different from the one shown in the screenshot

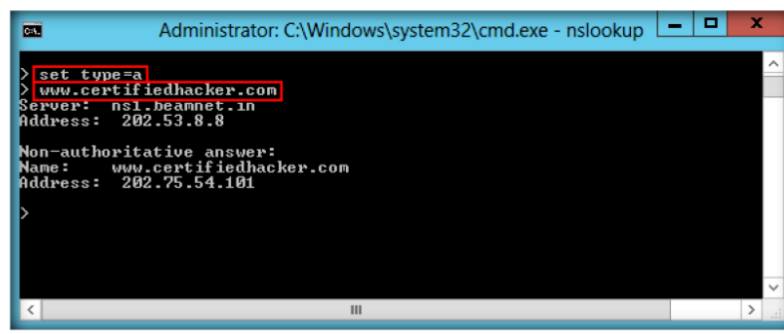


FIGURE 2.4: In nslookup command, set type=a option

TASK 2

Use Elicit Authoritative

7. You get **Authoritative** or **Non-authoritative answer**. The answer varies, but in this lab, it is **Non-authoritative answer**
8. In nslookup interactive mode, type **set type=cname** and press **Enter**
9. Now, type **certifiedhacker.com** and press **Enter**

Note: The DNS server address (**8.8.8.8**) will be different than the one in screenshot

10. The displayed response should be similar to the one shown as follows:

```
> set type=cname
```

```
> certifiedhacker.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

TASK 3

Find Cname

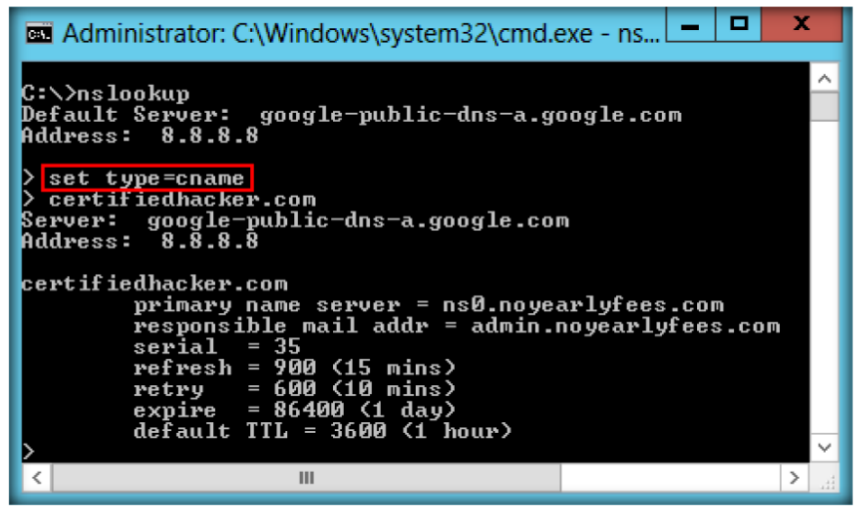


FIGURE 2.5: In nslookup command, set type=cname option

11. In nslookup interactive mode, type **server 64.147.99.90** (or any other IP address you receive in the previous step) and press **Enter**.
12. Now, type **set type=a** and press **Enter**.
13. Type **www.certifiedhacker.com** and press **Enter.** The displayed response should be similar to the one shown in the following figure.

In nslookup command, root option means to set the current default server to the root.

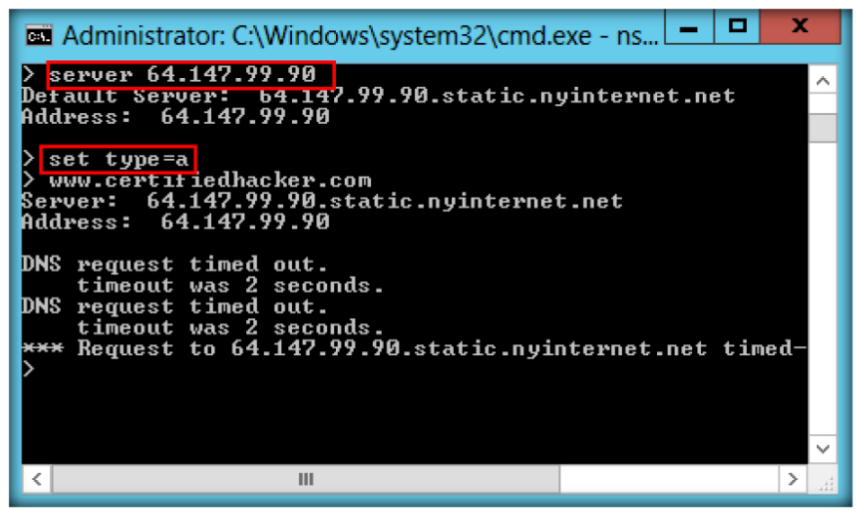


FIGURE 2.6: In nslookup command, set type=a option

14. If you receive a **request timed out** message, as shown in the previous figure, then your firewall is preventing you from sending DNS queries outside your LAN.

15. In nslookup interactive mode, type **set type=mx** and press **Enter**.
16. Now, type **certifiedhacker.com** and press **Enter.** The displayed response should be similar to the one shown in the following figure.

To make querytype of NS a default option for your nslookup commands, place one of the following statements in the user_id.NSLOOKUP.ENV data set: set querytype=ns or querytype=ns.

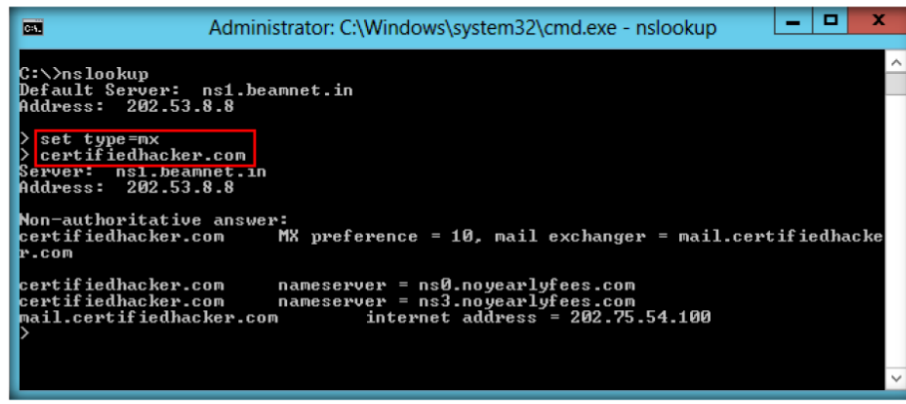


FIGURE 2.7: In nslookup command, set type=mx option

Lab Analysis

Document all the IP addresses, DNS server names, and other DNS information.

Tool/Utility	Information Collected/Objectives Achieved
nslookup	**DNS Server Name:** 202.53.8.8
	Non-Authoritative Answer: 202.75.54.101
	CNAME (Canonical Name of an alias) ▪ **Alias:** certifiedhacker.com ▪ **Canonical name:** google-public-dns-a.google.com
	MX (Mail Exchanger): mail.certifiedhacker.com

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze and determine each of the following DNS resource records:
   - SOA

- NS
- A
- PTR
- CNAME
- MX
- SRV

2. Evaluate the difference between an authoritative and non-authoritative answer.
3. Determine when you will receive request time out in nslookup.

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 3

People Search Using the AnyWho Online Tool

AnyWho is an online white pages people search directory for quickly looking up individual phone numbers.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have already learned that the first stage in penetration testing is to gather as much information as possible. In the previous lab, you were able to find information related to **DNS records** using the nslookup tool. If an attacker discovers a flaw in a DNS server, he or she will exploit the flaw to perform a cache poisoning attack, making the server cache the incorrect entries locally and serve them to other users that make the same request. As a penetration tester, you must always be cautious and take preventive measures against attacks targeted at a name server by **securely configuring name servers** to reduce the attacker's ability to corrupt a zone file with the amplification record.

To begin a penetration test it is also important to gather information about a **user location** to intrude into the user's organization successfully. In this particular lab, we will learn how to locate a client or user location using the **AnyWho** online tool.

Lab Objectives

The objective of this lab is to demonstrate the footprinting technique to collect **confidential information** on an organization, such as their **key personnel** and their **contact details**, using people search services. Students need to perform people search and phone number lookup using http://www.anywho.com.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

In the lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 5 Minutes

Overview of AnyWho

AnyWho is a part of the **ATTi family** of brands, which mostly focuses on local searches for products and services. The site lists information from the **White Pages** (Find a Person/Reverse Lookup) and the **Yellow Pages** (Find a Business).

Lab Tasks

1. Launch **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop

AnyWho allow you to search for local businesses by name to quickly find their Yellow Pages listings with basic details and maps, plus any additional time and money-saving features, such as coupons, video profiles or online reservations.

FIGURE 3.1: Windows Server 2012 – Desktop view

2. Click the **Google Chrome** app to launch the Chrome browser or launch any other browser

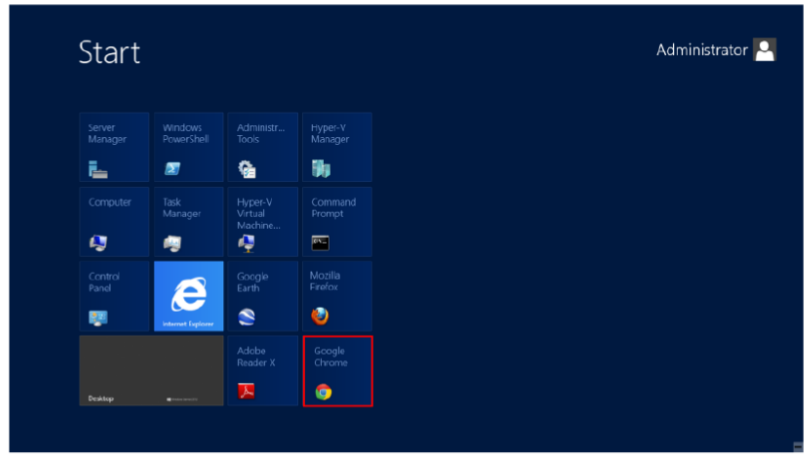


FIGURE 3.2: Windows Server 2012 – Apps

TASK 1

People Search with AnyWho

3. In the browser, type **http://www.anywho.com**, and press **Enter** on the keyboard

AnyWho is part of the ATTi family of brands, which focuses on local search products and services.

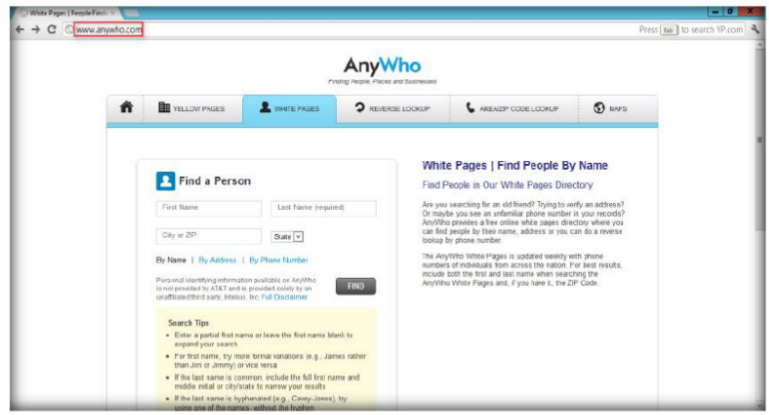


FIGURE 3.3: AnyWho - Home Page http://www.anywho.com

4. Input the name of the person you want to search for in the **Find a Person** section and click **Find**

Include both the first and last name when searching the AnyWho White Pages.

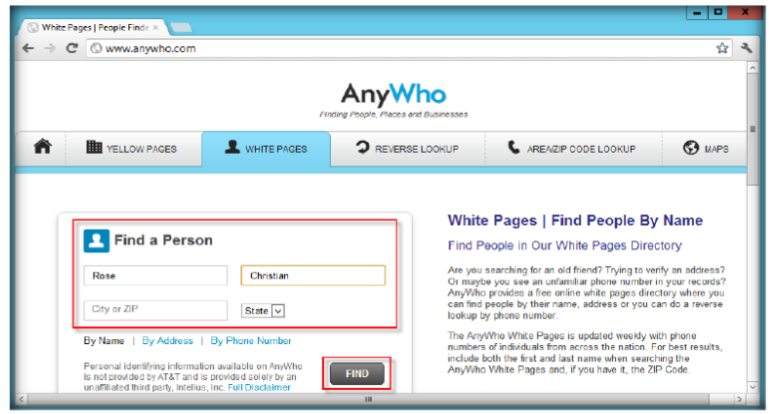


FIGURE 3.4: AnyWho – Name Search

5. AnyWho redirects you to **search results** with the name you have entered. The number of results might vary

Yellow Pages listings (searches by category or name) are obtained from YP.COM and are updated on a regular basis.

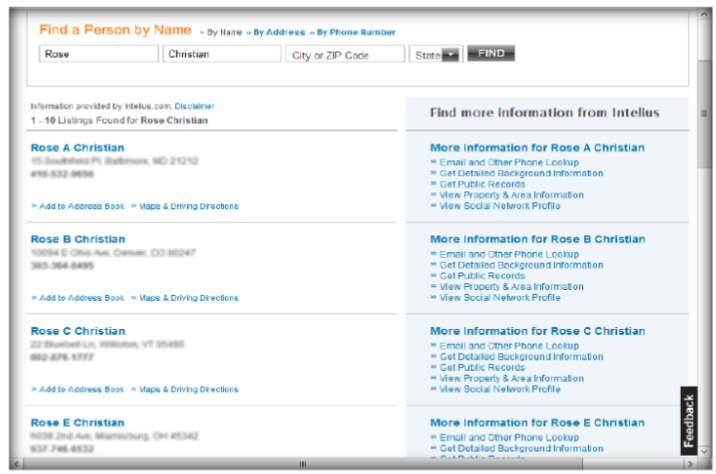


FIGURE 3.5: AnyWho People Search Results

TASK 2

Viewing Person Information

6. Click the **search results** to see the address details and phone number of that person

The search results display address, phone number and directions for the location.

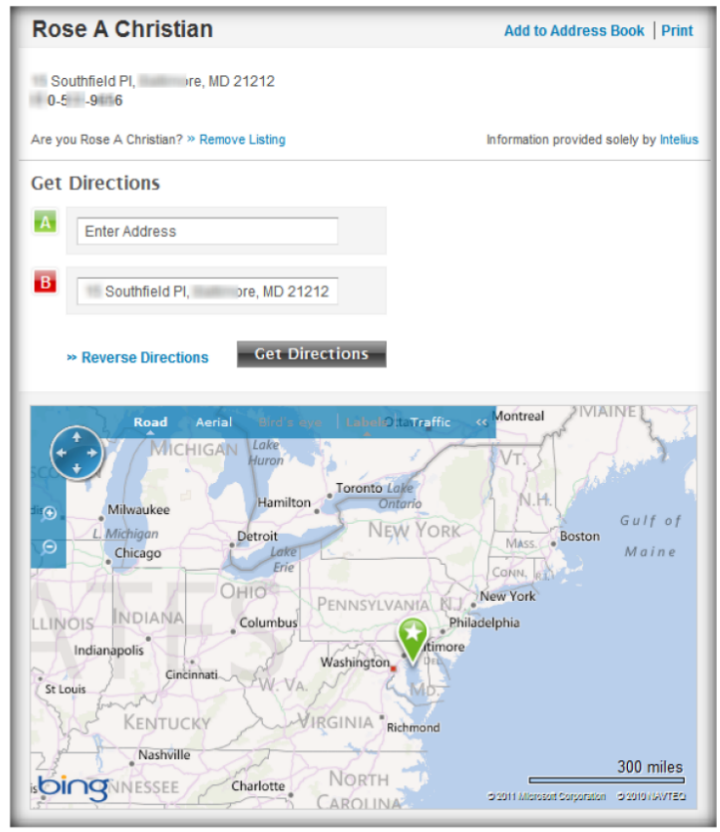


FIGURE 3.6: AnyWho - Detail Search Result of Rose A Christian

7. Similarly, perform a reverse search by giving phone number or address in the **Reverse Lookup** field

The Reverse Phone Lookup service allows visitors to enter in a phone number and immediately lookup who it is registered to.

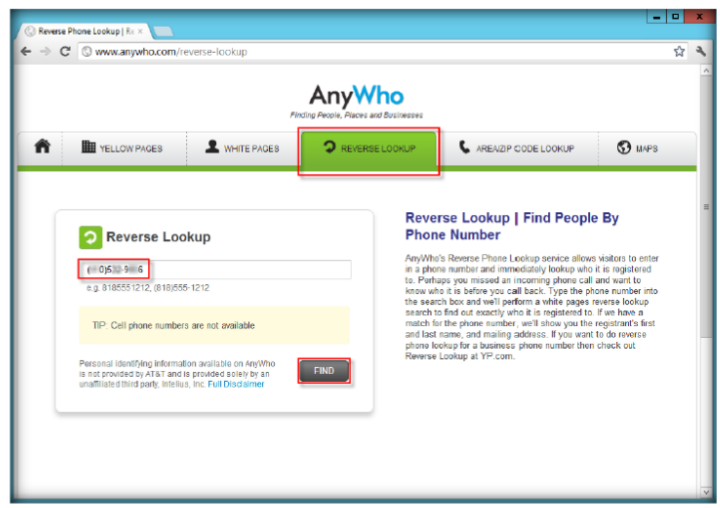


FIGURE 3.7: AnyWho Reverse Lookup Page

8. Reverse lookup will redirect you to the search result page with the detailed information of the person for particular phone number or email address

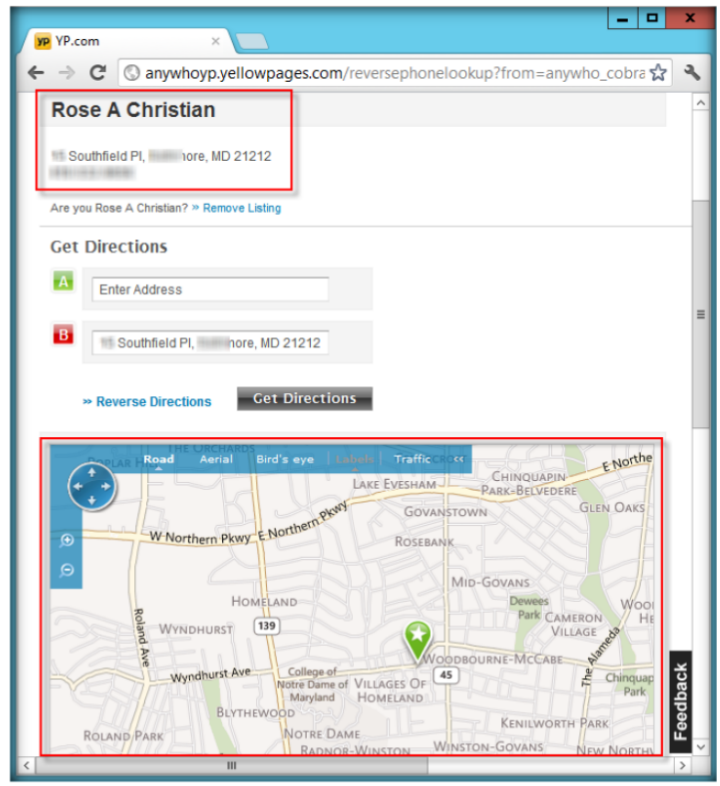


FIGURE 3.8: AnyWho - Reverse Lookup Search Result

Unpublished directory records are not displayed. If you want your residential listing removed, you have a couple of options:

To have your listing unpublished, contact your local telephone company.

To have your listing removed from AnyWho without obtaining an unpublished telephone number, follow the instructions provided in AnyWho Listing Removal to submit your listing for removal.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
AnyWho	**WhitePages (Find people by name):** Exact location of a person with address and phone number
	Get Directions: Precise route to the address found for a person
	Reverse Lookup (Find people by phone number): Exact location of a person with complete address

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Can you collect all the contact details of the key people of any organization?
2. Can you remove your residential listing? If yes, how?
3. If you have an unpublished listing, why does your information show up in AnyWho?
4. Can you find a person in AnyWho that you know has been at the same location for a year or less? If yes, how?
5. How can a listing be removed from AnyWho?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 4

People Search Using the Spokeo Online Tool

Spokeo is an online people search tool providing real-time information about people. This tool helps with online footprinting and allows you to discover details about people.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

For a penetration tester, it is always advisable to collect all possible information about a client before beginning the test. In the previous lab, we learned about collecting people information using the **AnyWho** online tool; similarly, there are many tools available that can be used to gather information on people, employees, and organizations to conduct a penetration test. In this lab, you will learn to use the **Spokeo** online tool to collect **confidential information** of key persons in an organization.

Lab Objectives

The objective of this lab is to demonstrate the footprinting techniques to collect **people information** using people search services. Students need to perform a people search using http://www.spokeo.com.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

In the lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 5 Minutes

Overview of Spokeo

Spokeo aggregates vast quantities of public data and organizes the information into easy-to-follow profiles. Information such as name, email address, phone number, address, and user name can be easily found using this tool.

Lab Tasks

TASK 1

People Search with Spokeo

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

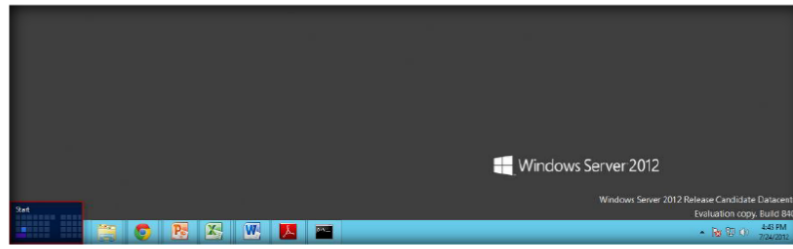


FIGURE 4.1: Windows Server 2012 – Desktop view

2. Click the **Google Chrome** app to launch the Chrome browser

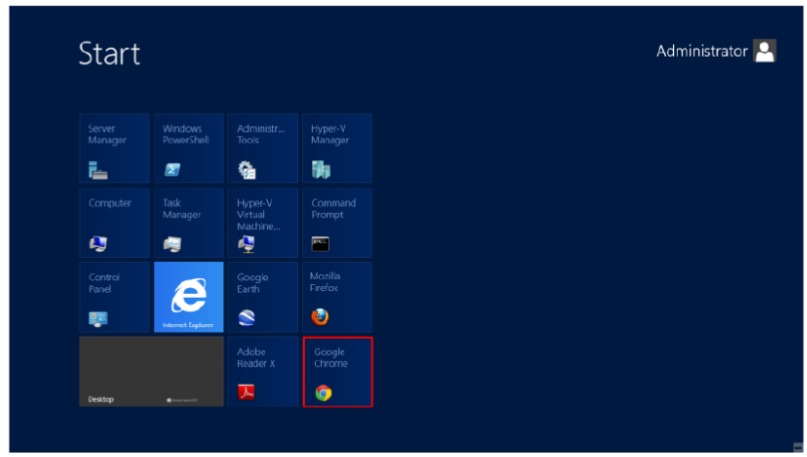


FIGURE 4.2: Windows Server 2012 – Apps

3. Open a web browser, type **http://www.spokeo.com**, and press **Enter** on the keyboard

Spokeo's people search allows you to find old friends, reunite with classmates, teammates and military buddies, or find lost and distant family.

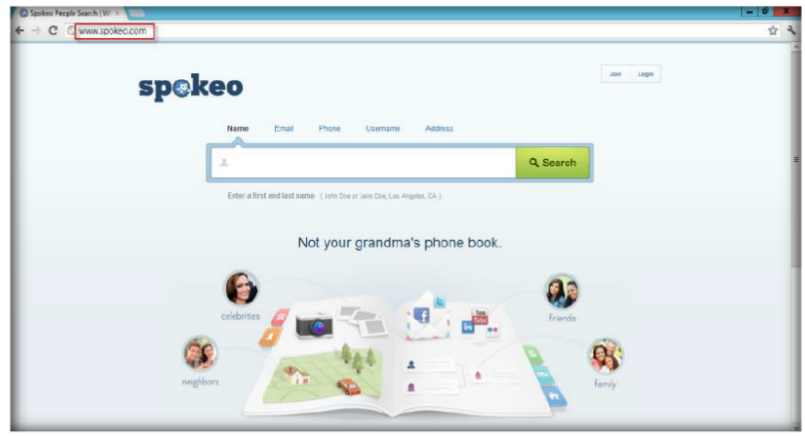


FIGURE 4.3: Spokeo home page http://www.spokeo.com

Apart from Name search, Spokeo supports four types of searches:

- Email Address
- Phone Number
- Username
- Residential Address

4. To begin the search, input the name of the person you want to search for in the **Name** field and click **Search**

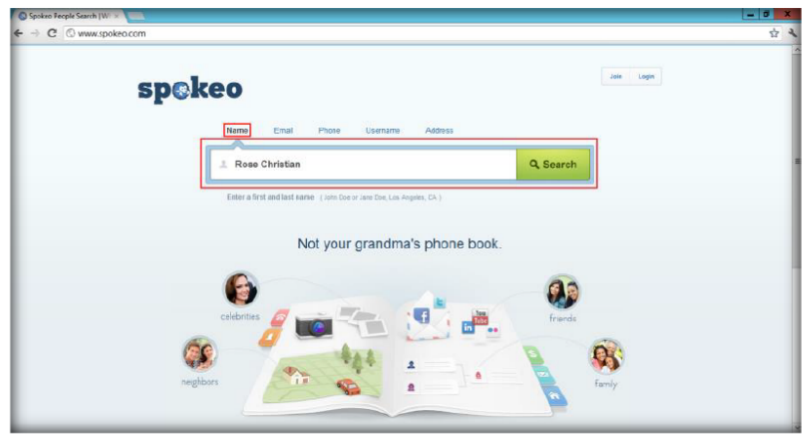


FIGURE 4.4: Spokeo – Name Search

5. Spokeo redirects you to **search results** with the name you have entered

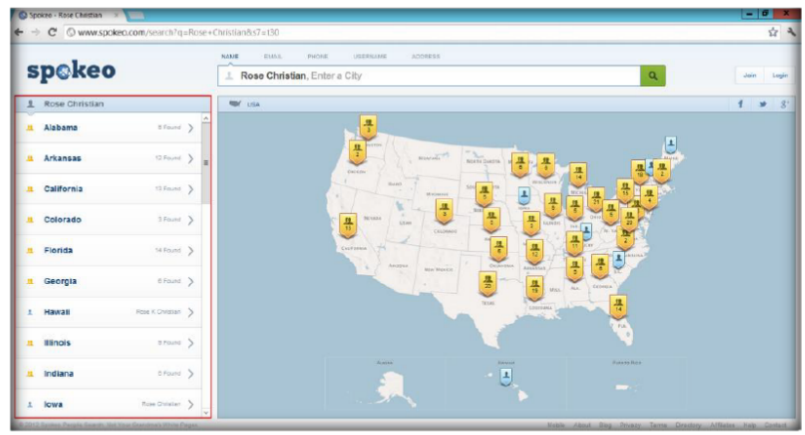


FIGURE 4.5: Spokeo People Search Results

Spokeo's email search scans through 90+ social networks and public sources to find the owner's name, photos, and public profiles.

6. Click the **State** name in which the person you are searching lives

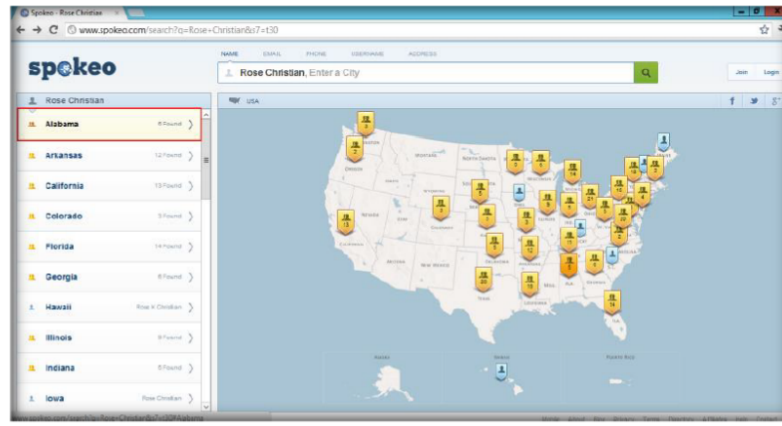


FIGURE 4.6: Spokeo People Search Results

Public profiles from social networks are aggregated in Spokeo and many places, including search engines.

7. Now, click the appropriate **City** name for your search

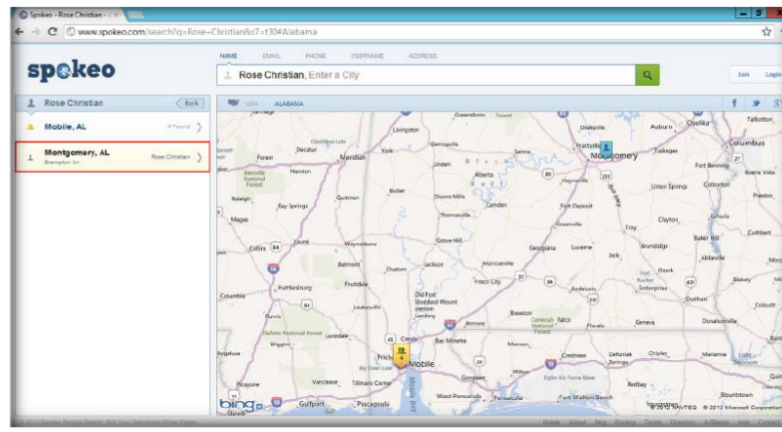


FIGURE 4.7: Spokeo People Search Results

8. Search results displaying the **Address**, **Phone Number**, **Email Address**, **City** and **State**, etc.

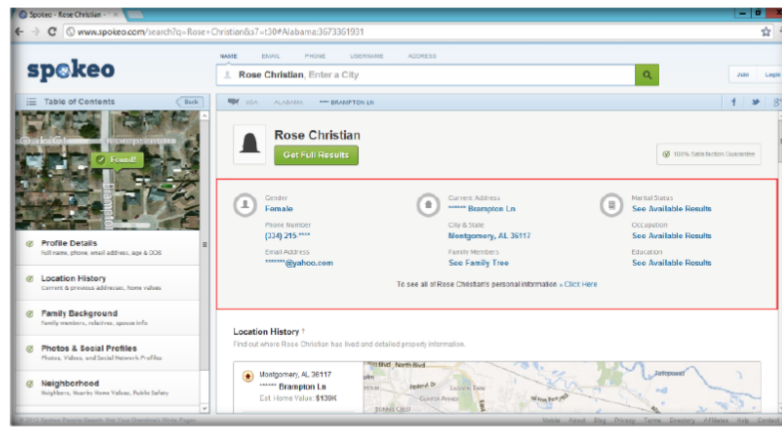


FIGURE 4.8: Spokeo People Search Results

All results will be displayed once the search is completed

9. Search results displaying the **Location History**

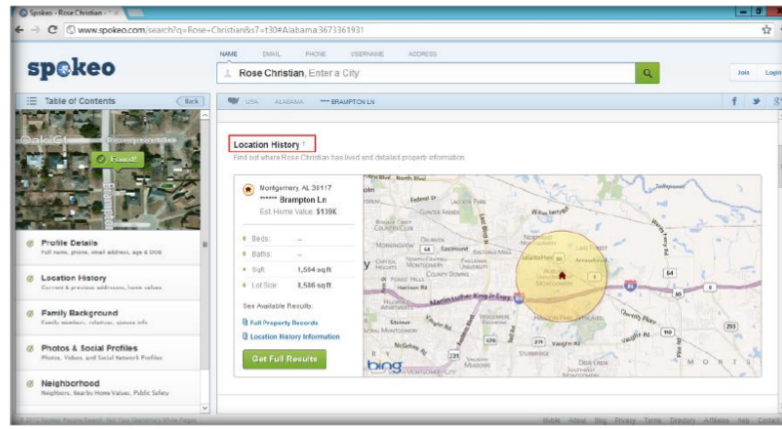


FIGURE 4.9: Spokeo People Search Results

10. Spokeo search results display the **Family Background**, **Family Economic Health** and **Family Lifestyle**

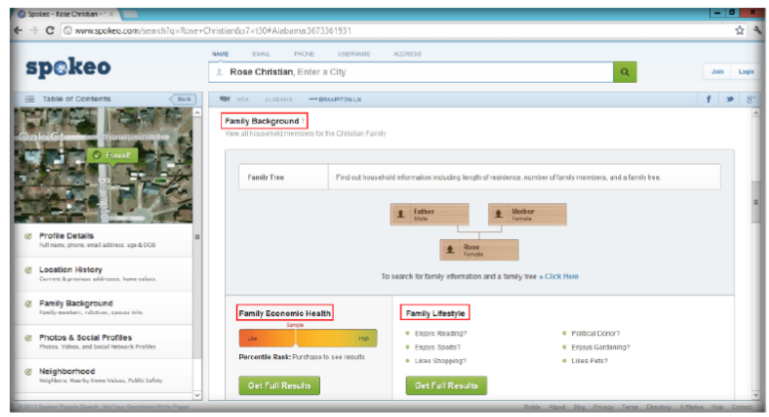


FIGURE 4.10: Spokeo People Search Results

Online maps and street view are used by over 300,000 websites, including most online phone books and real estate websites.

11. Spokeo search results display the **Neighborhood** for the search done

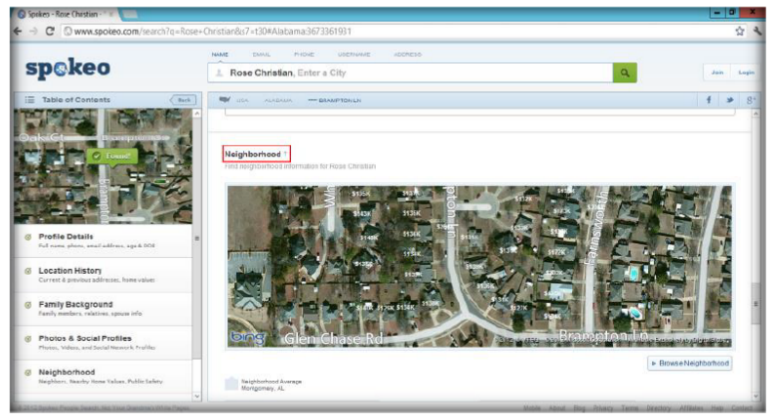


FIGURE 4.11: Spokeo People Search Results

Spokeo's reverse phone lookup functions like a personal caller-ID system. Spokeo's reverse phone number search aggregates hundreds of millions of phone book records to help locate the owner's name, location, time zone, email and other public information.

12. Similarly, perform a **Reverse** search by giving phone number, address, email address, etc. in the **Search** field to find details of a key person or an organization

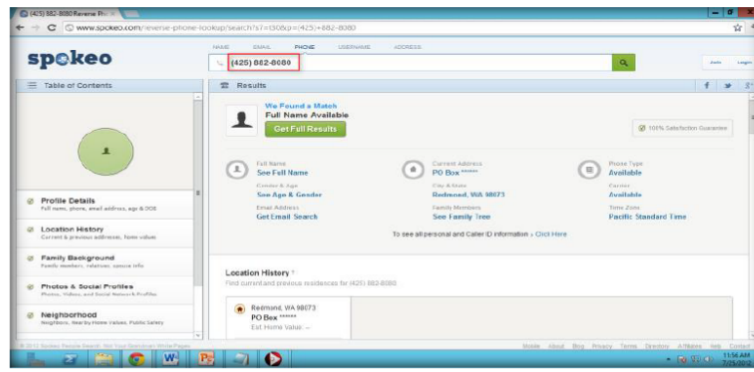


FIGURE 4.12: Spokeo Reverse Search Result of Microsoft Redmond Office

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Spokeo	**Profile Details:** ▪ Current Address ▪ Phone Number ▪ Email Address ▪ Marital Status ▪ Education ▪ Occupation
	Location History: Information about where the person has lived and detailed property information
	Family Background: Information about household members for the person you searched
	Photos & Social Profiles: Photos, videos, and social network profiles
	Neighborhood: Information about the neighborhood
	Reverse Lookup: Detailed information for the search done using phone numbers

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. How do you collect all the contact details of key people using Spokeo?
2. Is it possible to remove your residential listing? If yes, how?
3. How can you perform a reverse search using Spokeo?
4. List the kind of information that a reverse phone search and email search will yield.

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 5

Analyzing Domain and IP Address Queries Using SmartWhois

SmartWhois is a network information utility that allows you to look up most available information on a hostname, IP address, or domain.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, you learned to determine a person or an organization's location using the **Spokeo** online tool. Once a penetration tester has obtained the user's location, he or she can gather personal details and confidential information from the user by posing as a neighbor, the cable guy, or through any means of social engineering. In this lab, you will learn to use the **SmartWhois** tool to look up all of the available information about any IP address, hostname, or domain and using these information, penetration testers gain access to the network of the particular organization for which they wish to perform a penetration test.

Lab Objectives

The objective of this lab is to help students analyze **domain** and **IP address** queries. This lab helps you to get most available information on a **hostname**, **IP address**, and **domain**.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

In the lab you need:

- A computer running any version of **Windows** with **Internet** access
- Administrator privileges to run **SmartWhois**
- The **SmartWhois** tool, available in **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\WHOIS Lookup Tools\SmartWhois** or downloadable from http://www.tamos.com
- If you decide to download the latest version, then **screenshots** shown in the lab might differ

Lab Duration

http://www.tamos.com

Time: 5 Minutes

Overview of SmartWhois

SmartWhois is network information utility that allows you to look up most available information on a **hostname**, **IP address**, or **domain**, including country, state or province, city, name of the **network provider**, technical support contact information, and administrator.

SmartWhois can be configured to work from behind a firewall by using HTTP/HTTPS proxy servers. Different SOCKS versions are also supported.

SmartWhois helps you to search for information such as:

- The owner of the domain
- The domain registration date and the owner's contact information
- The owner of the IP address block

Lab Tasks

Note: If you are working in the iLabs environment, directly jump to **step number 13**

1. Follow the wizard-driven **installation** steps and install SmartWhois.
2. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

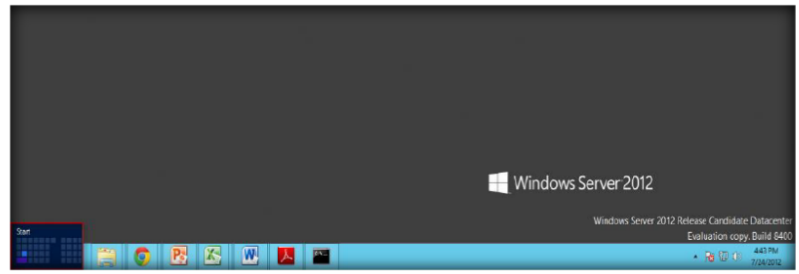


FIGURE 5.1: Windows Server 2012 – Desktop view

SmartWhois can save obtained information to an archive file. Users can load this archive the next time the program is launched and add more information to it. This feature allows you to build and maintain your own database of IP addresses and host names.

3. To launch **SmartWhois**, click **SmartWhois** in apps

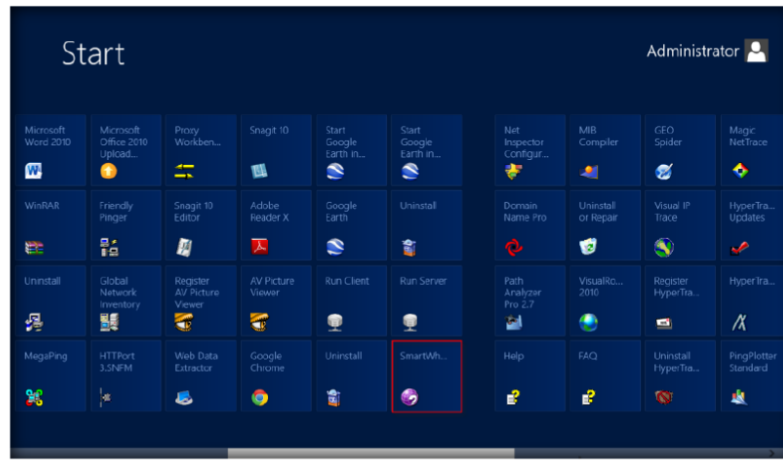


FIGURE 5.2: Windows Server 2012 – Apps

TASK 1

Lookup IP

4. The **SmartWhois** main window appears

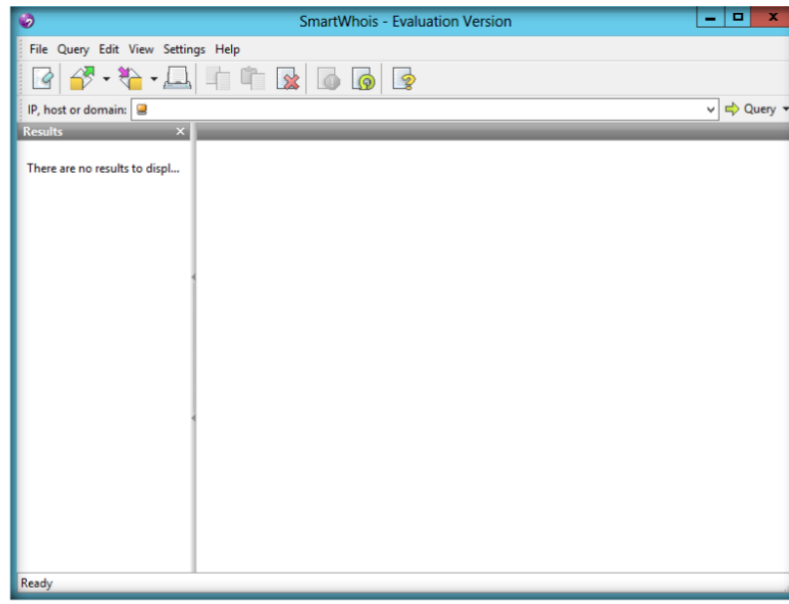


FIGURE 5.3: The SmartWhois main window

If you need to query a non-default whois server or make a special query click View → Whois Console from the menu or click the Query button and select Custom Query.

5. Type an **IP address, hostname**, or **domain name** in the field tab. An example of a domain name query is shown as follows, www.google.com.

FIGURE 5.4: A SmartWhois domain search

6. Now, click the **Query** tab to find a drop-down list, and then click **As Domain** to enter domain name in the field.

SmartWhois is capable of caching query results, which reduces the time needed to query an address; if the information is in the cache file it is immediately displayed and no connections to the whois servers are required..

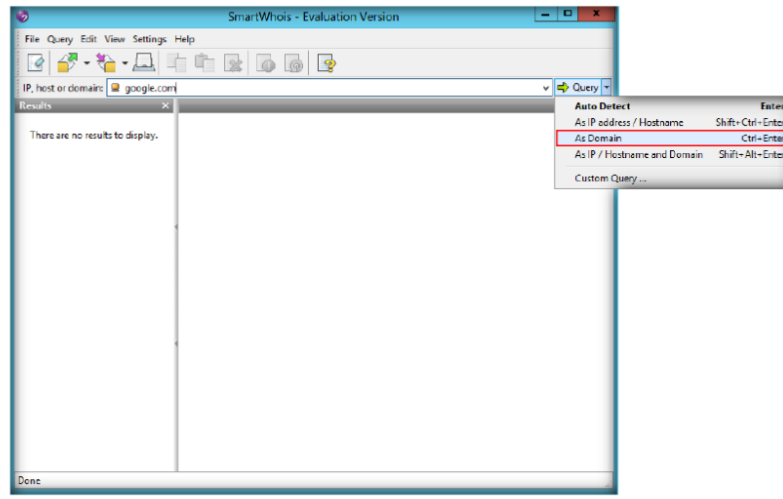


FIGURE 5.5: The SmartWhois – Selecting Query type

7. In the left pane of the window, the **result** displays, and the right pane displays the results of your **query**.

SmartWhois can process lists of IP addresses, hostnames, or domain names saved as plain text (ASCII) or Unicode files. The valid format for such batch files is simple: Each line must begin with an IP address, hostname, or domain. If you want to process domain names, they must be located in a separate file from IP addresses and hostnames.

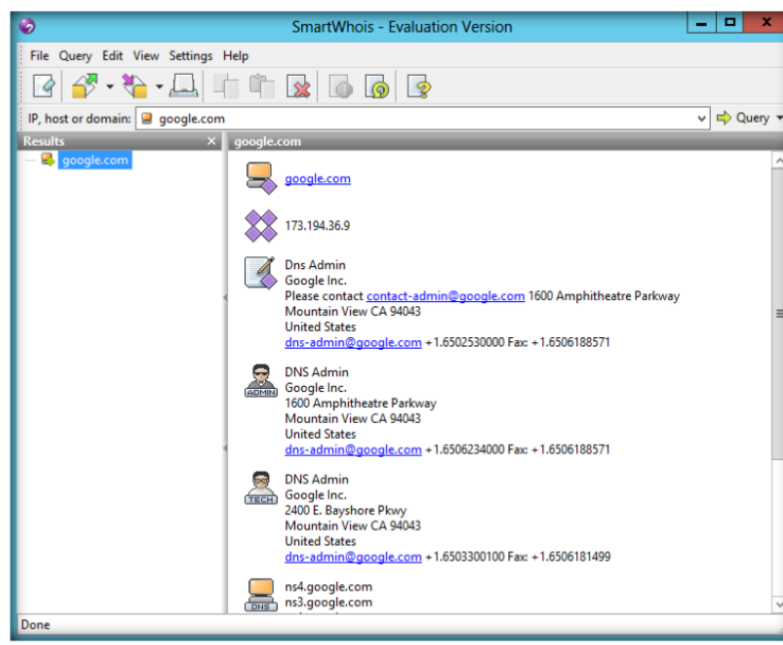


FIGURE 5.6: The SmartWhois – Domain query result

8. Click the **Clear** icon in the toolbar to clear the history.

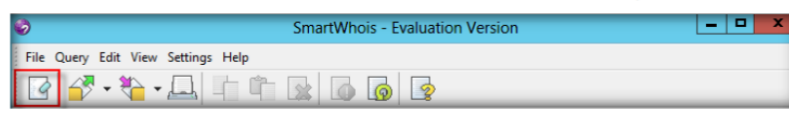


FIGURE 5.7: A SmartWhois toolbar

TASK 2

Host Name Query

9. To perform a sample **host name query**, type www.facebook.com.

10. Click the **Query** tab, and then select **As IP/Hostname** and enter a hostname in the field.

FIGURE 5.8: A SmartWhois host name query

11. In the left pane of the window, the **result** displays, and in the right pane, the text area displays the results of your **query**.

If you want to query a domain registration database, enter a domain name and hit the Enter key while holding the Ctrl key, or just select As Domain from the Query dropdown menu.

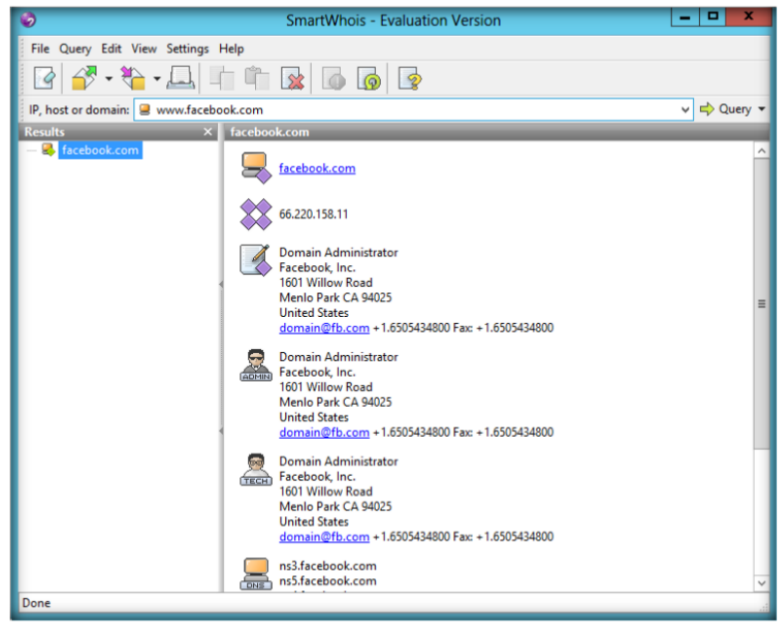


FIGURE 5.9: A SmartWhois host name query result

If you're saving results as a text file, you can specify the data fields to be saved. For example, you can exclude name servers or billing contacts from the output file. Click Settings→Options→Text & XML to configure the options.

12. Click the **Clear** icon in the toolbar to clear the history.
13. To perform a sample **IP Address** query, type the IP address 10.0.0.3 (Windows 8 IP address) in the **IP, host or domain** field.

FIGURE 5.10: A SmartWhois IP address query

14. In the left pane of the window, the **result** displays, and in the right pane, the text area displays the results of your **query**.

SmartWhois supports command line parameters specifying IP address/hostname/domain, as well as files to be opened/saved.

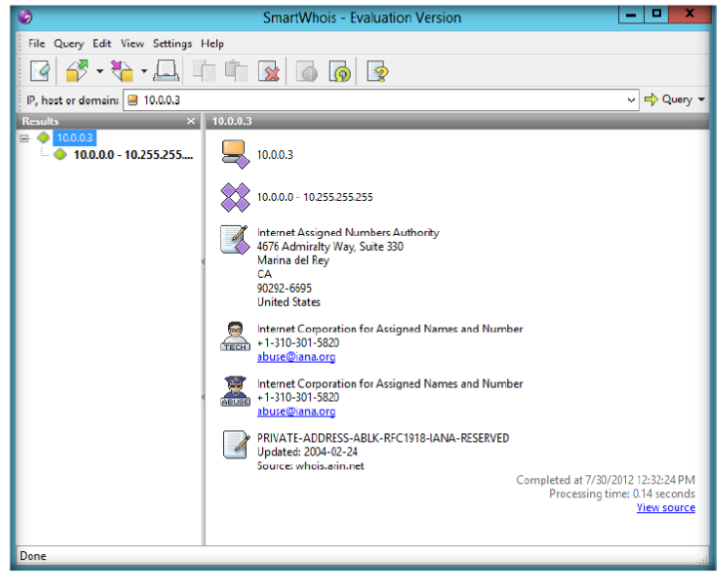


FIGURE 5.11: The SmartWhois IP query result

Lab Analysis

Document all the IP addresses/hostnames for the lab for further information.

Tool/Utility	Information Collected/Objectives Achieved
SmartWhois	**Domain name query results:** Owner of the website
	Host name query results: Geographical location of the hosted website
	IP address query results: Owner of the IP address block

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine whether you can use SmartWhois if you are behind a firewall or a proxy server.
2. Why do you get Connection timed out or Connection failed errors?
3. Is it possible to call SmartWhois directly from my application? If yes, how?

4. What are LOC records, and are they supported by SmartWhois?
5. When running a batch query, you get only a certain percentage of the domains/IP addresses processed. Why are some of the records unavailable?

Internet Connection Required	
☐ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 6

Network Route Trace Using Path Analyzer Pro

Path Analyzer Pro delivers advanced network route tracing with performance tests, DNS, whois, and network resolution to investigate network issues.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Using the information **IP address**, **hostname**, **domain**, etc. found in the previous lab, access can be gained to an organization's network, which allows a penetration tester to thoroughly learn about the organization's network environment for possible vulnerabilities. Taking all the information gathered into account, penetration testers study the systems to find the best **routes of attack**. The same tasks can be performed by an attacker and the results possibly will prove to be very fatal for an organization. In such cases, as a penetration tester you should be competent to trace **network route**, determine **network path**, and troubleshoot **network issues**. Here you will be guided to trace the network route using the tool **Path Analyzer Pro**.

Lab Objectives

The objective of this lab is to help students **research email addresses**, network paths, and IP addresses. This lab helps to determine what ISP, router, or servers are responsible for a **network problem**.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

In the lab you need:

- Path Analyzer pro: Path Analyzer pro is located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro**
- You can also download the latest version of **Path Analyzer Pro** from the link http://www.pathanalyzer.com/download.opp
- If you decide to download the latest version, then **screenshots** shown in the lab might differ

- Install this tool on **Windows Server 2012**
- Double-click **PAPro27.msi**
- Follow the wizard driven installation to install it
- Administrator privileges to run **Path Analyzer Pro**

Lab Duration

Time: 10 Minutes

Overview of Network Route Trace

Traceroute is a computer network tool for measuring the **route path** and **transit** times of packets across an Internet protocol (IP) network. The traceroute tool is available on almost all Unix-like operating systems. Variants, such as **tracepath** on modern Linux installations and **tracert** on Microsoft Windows operating systems with similar functionality, are also available.

Traceroute is a system administrators' utility to trace the route IP packets take from a source system to some destination system.

Lab Tasks

1. Follow the wizard-driven installation steps to install Path Analyzer Pro
2. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

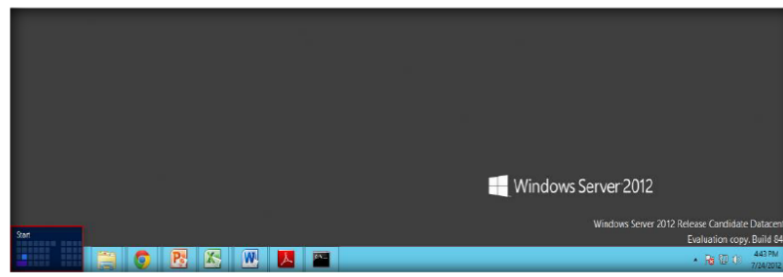
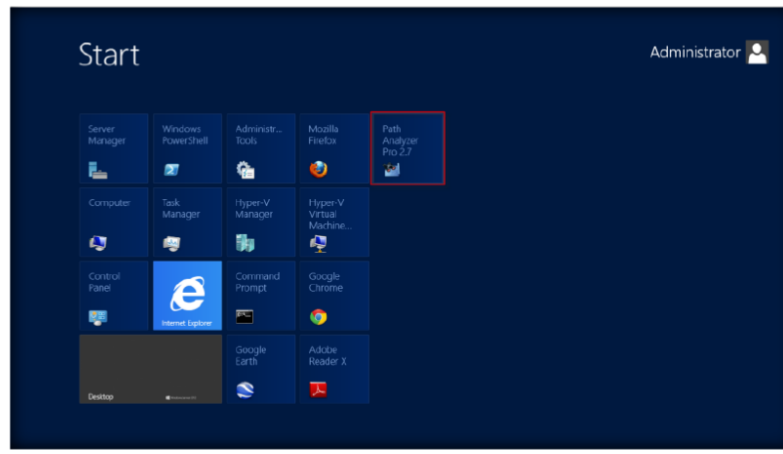


FIGURE 6.1: Windows Server 2012 – Desktop view

3. To launch **Path Analyzer Pro**, click **Path Analyzer Pro** in apps



Path Analyzer Pro summarizes a given trace within seconds by generating a simple report with all the important information on the target--we call this the Synopsis.

FIGURE 6.2: Windows Server 2012 – Apps

4. Click the **Evaluate** button on Registration Form
5. The main window of Path Analyzer Pro appears as shown in the following screenshot

TASK 1

Trace Network

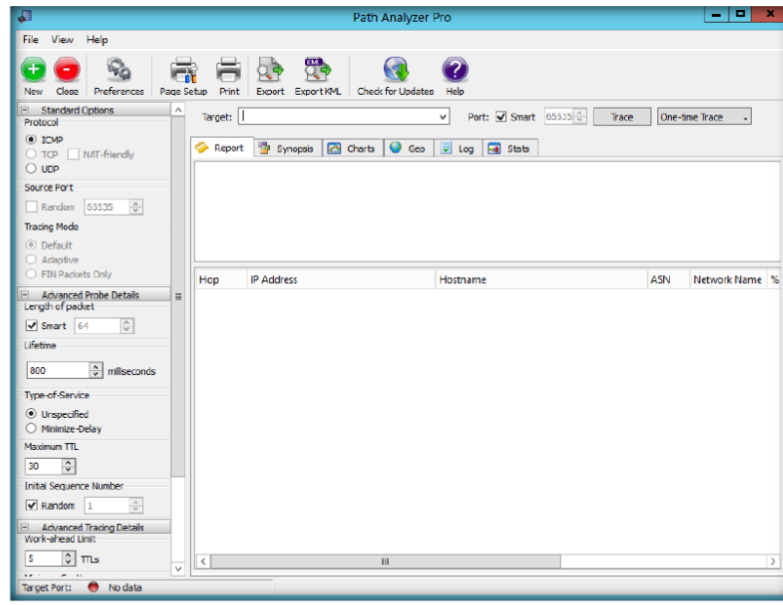


FIGURE 6.3: The Path Analyzer Pro Main window

FIN Packets Only- generates only TCP packets with the FIN flag set in order to solicit an RST or TCP reset packet as a response from the target. This option may get beyond a firewall at the target, thus giving the user more trace data, but it could be misconstrued as a malicious attack.

6. Select the **ICMP** protocol in the **Standard Options** section.

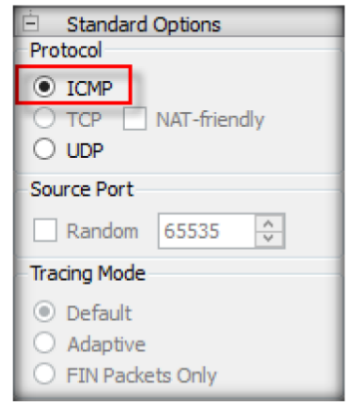


FIGURE 6.4: The Path Analyzer Pro Standard Options

Path Analyzer Pro summarize all the relevant background information on its target, be it an IP address, a hostname, or an email address.

7. Under **Advanced Probe Details**, check the **Smart** option in the **Length of packet** section and leave the rest of the options in this section at their default settings.

Note: Firewall is required to be disabled for appropriate output

Path Analyzer Pro benefits:

- Research IP addresses, email addresses, and network paths
- Pinpoint and troubleshoot network availability and performance issues
- Determine what ISP, router, or server is responsible for a network problem
- Locate firewalls and other filters that may be impacting connections
- Visually analyze a network's path characteristics
- Graph protocol latency, jitter, and other factors
- Trace actual applications and ports, not just IP hops
- Generate, print, and export a variety of impressive reports
- Perform continuous and timed tests with real-time reporting and history

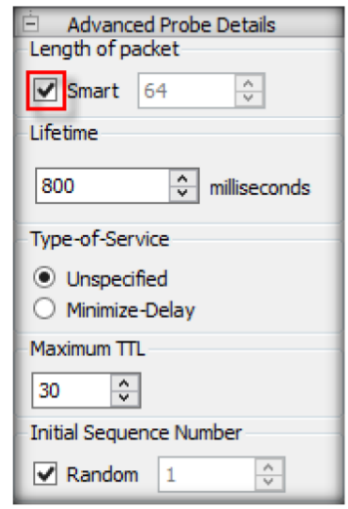


FIGURE 6.5: The Path Analyzer Pro Advanced Probe Details window

8. In the **Advanced Tracing Details** section, the options remain at their default settings.
9. Check **Stop on control messages (ICMP)** in the **Advance Tracing Details** section

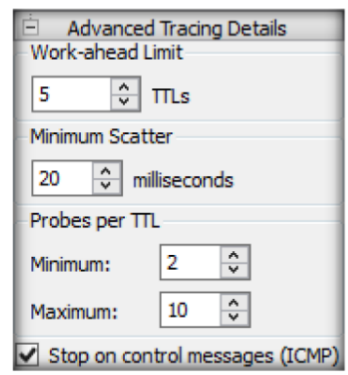


FIGURE 6.6: The Path Analyzer Pro Advanced Tracing Details window

10. To perform the trace after checking these options, select the target host, for instance www.google.com, and check the Port: **Smart as default (65535)**.

FIGURE 6.7: A Path Analyzer Pro Advance Tracing Details option

Note: Path Analyzer Pro is not designed to be used as an attack tool.

11. In the drop-down menu, select the duration of time as **Timed Trace**

FIGURE 6.8: A Path Analyzer Pro Advance Tracing Details option

12. Enter the **Type time of trace** in the previously mentioned format as HH: MM: SS.

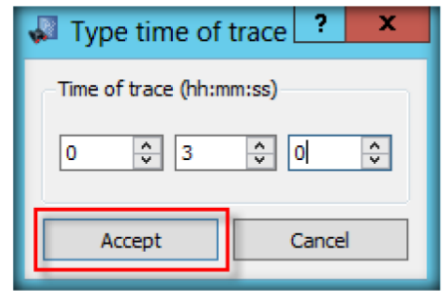


FIGURE 6.9: The Path Analyzer Pro Type time of trace option

TASK 2

Trace Reports

13. While Path Analyzer Pro performs this trace, the **Trace** tab changes automatically to **Stop**.

FIGURE 6.10: A Path Analyzer Pro Target Option

14. To see the trace results, click the **Report** tab to display a linear **chart depicting** the number of hops between you and the target.

The Advanced Probe Details settings determine how probes are generated to perform the trace. These include the Length of packet, Lifetime, Type of Service, Maximum TTL, and Initial Sequence Number.

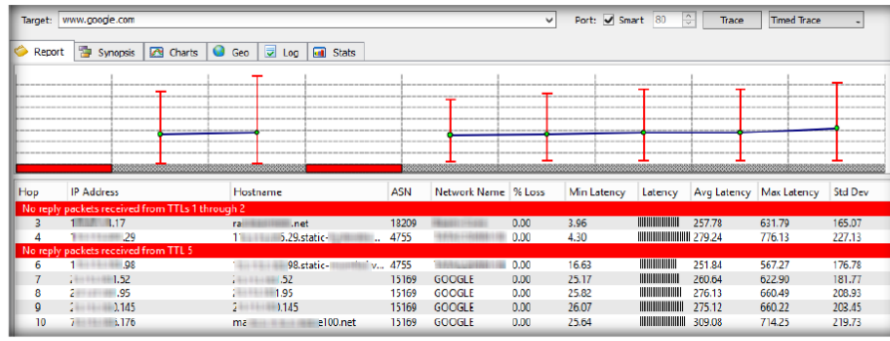


FIGURE 6.11: A Path Analyzer Pro Target option

15. Click the **Synopsis** tab, which displays a one-page summary of your trace results.

Length of packet: This option allows you to set the length of the packet for a trace. The minimum size of a packet, as a general rule, is approximately 64 bytes, depending on the protocol used. The maximum size of a packet depends on the physical network but is generally 1500 bytes for a regular Ethernet network or 9000 bytes using Gigabit Ethernet networking with jumbo frames.

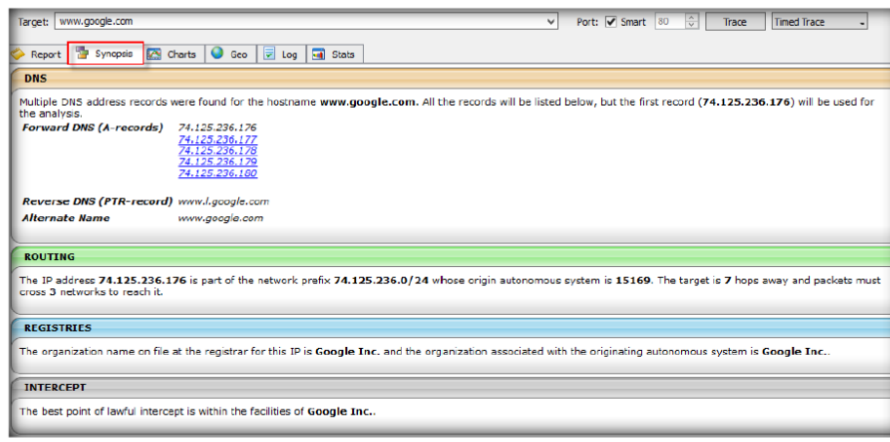


FIGURE 6.12: A Path Analyzer Pro Target option

TASK 3

View Charts

16. Click the **Charts** tab to view the results of your trace.

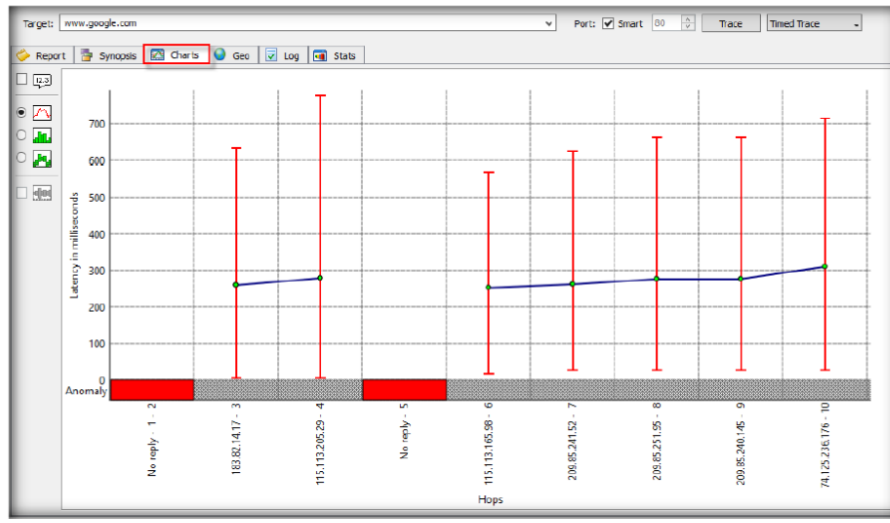


FIGURE 6.13: The Path Analyzer Pro Chart Window

Path Analyzer Pro uses Smart as the default Length of packet. When the Smart option is checked, the software automatically selects the minimum size of packets based on the protocol selected under Standard Options.

17. Click **Geo**, which displays an **imaginary** world map format of your trace.

TASK 4

View Imaginary Map

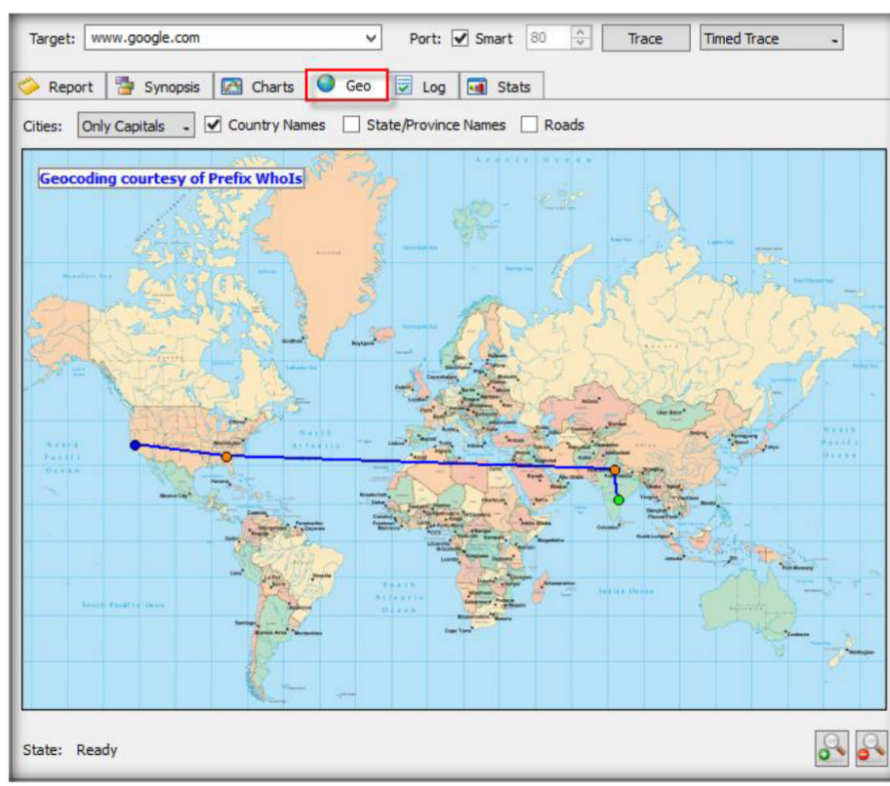


FIGURE 6.14: The Path Analyzer Pro chart window

TASK 5

Vital Statistics

18. Now, click the **Stats** tab, which features the **Vital Statistics** of your current trace.

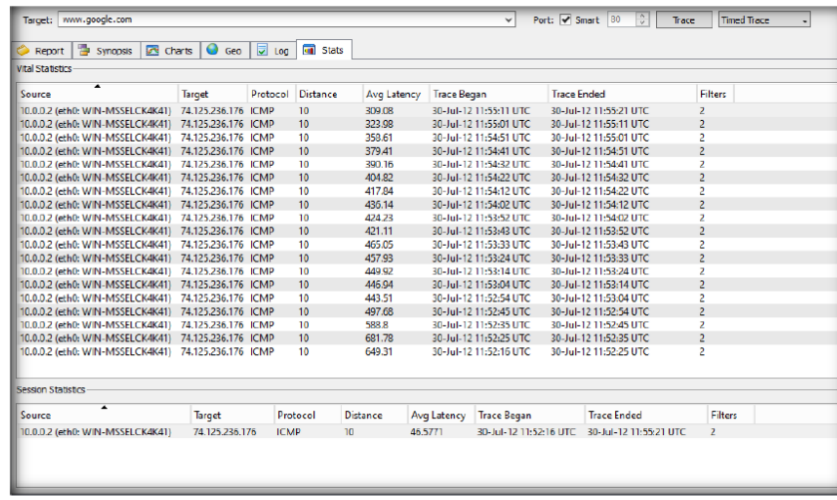


FIGURE 6.15: The Path Analyzer Pro Statistics window

Maximum TTL: The maximum Time to Live (TTL) is the maximum number of hops to probe in an attempt to reach the target. The default number of hops is set to 30. The Maximum TTL that can be used is 255.

19. Now **Export** the report by clicking **Export** on the toolbar.

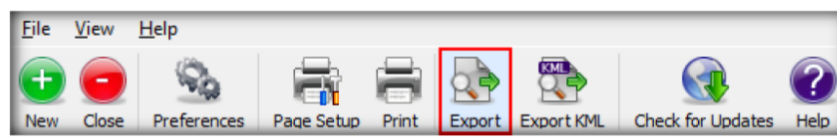


FIGURE 6.16: The Path Analyzer Pro Save Report As window

TASK 6

Save File

20. By default, the report will be saved at **D:\Program Files (x86)\Path Analyzer Pro 2.7**. However, you may change it to your preferred location.

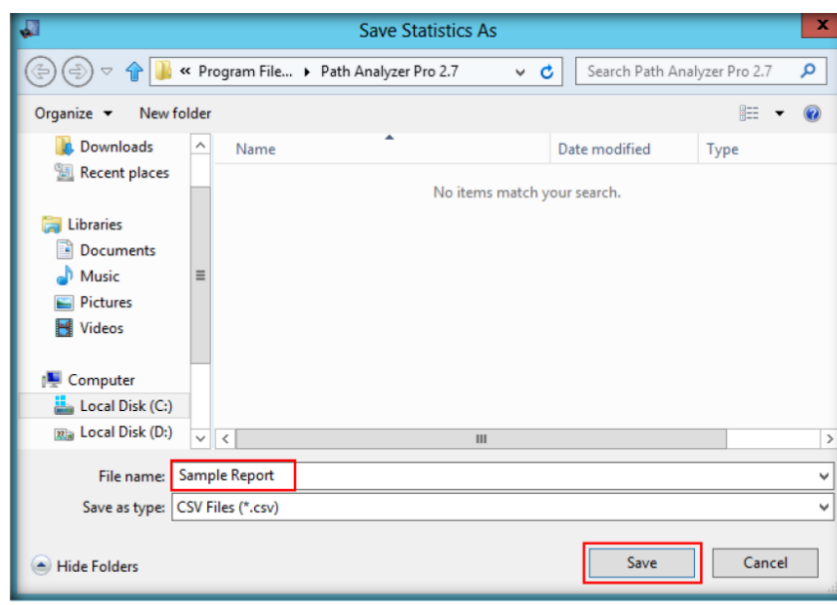


FIGURE 6.17: The Path Analyzer Pro Save Report As window

The Initial Sequence Number is set as a counting mechanism within the packet between the source and the target. It is set to Random as the default, but you can choose another starting number by unchecking the Random button and filling in another number. Please Note: The Initial Sequence Number applies only to TCP connections.

Lab Analysis

Document the IP addresses that are traced for the lab for further information.

Tool/Utility	Information Collected/Objectives Achieved
Path Analyzer Pro	**Report:** ▪ Number of hops ▪ IP address ▪ Hostname ▪ ASN ▪ Network name ▪ Latency
	Synopsis: Displays summary of valuable information on DNS, Routing, Registries, Intercept
	Charts: Trace results in the form of chart
	Geo: Geographical view of the path traced
	Stats: Statistics of the trace

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. What is the standard deviation measurement, and why is it important?
2. If your trace fails on the first or second hop, what could be the problem?
3. Depending on your TCP tracing options, why can't you get beyond my local network?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 7

Tracing an Email Using the eMailTrackerPro Tool

eMailTrackerPro is a tool that analyzes email headers to disclose the original sender's location.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, you gathered information such as number of **hops** between a host and client, **IP address**, etc. As you know, data packets often have to go through routers or firewalls, and a hop occurs each time packets are passed to the next router. The number of hops determines the distance between the source and destination host. An attacker will analyze the hops for the firewall and determine the protection layers to hack into an organization or a client. Attackers will definitely try to hide their true **identity** and **location** while intruding into an organization or a client by gaining illegal access to other users' computers to accomplish their tasks. If an attacker uses emails as a means of attack, it is very essential for a penetration tester to be familiar with **email headers** and their related details to be able to **track** and **prevent** such attacks with an organization. In this lab, you will learn to trace email using the **eMailTrackerPRo** tool.

Lab Objectives

The objective of this lab is to demonstrate email tracing **using eMailTrackerPro**. Students will learn how to:

- Trace an email to its true **geographical** source
- **Collect Network** (ISP) and **domain Whois** information for any email traced

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

In the lab, you need the eMailTrackerPro tool.

- eMailTrackerPro is located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro**

- You can also download the latest version of **eMailTrackerPro** from the link http://www.emailtrackerpro.com/download.html
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- Follow the **wizard-driven** installation steps and install the tool
- This tool installs **Java runtime** as a part of the installation
- Run this tool in **Windows Server 2012**
- Administrative privileges are required to run this tool
- This lab requires a valid email account (**Hotmail, Gmail, Yahoo, etc.**). We suggest you sign up with any of these services to obtain a new email account for this lab
- Please do not use your **real email accounts** and **passwords** in these exercise

Lab Duration

Time: 10 Minutes

eMailTrackerPro helps identify the true source of emails to help track suspects, verify the sender of a message, trace and report email abusers.

Overview of eMailTrackerPro

Email tracking is a method to **monitor or spy** on email delivered to the intended recipient:

- When an email message was received and read
- If destructive email is sent
- The GPS location and map of the recipient
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages are set to expire after a specified time

Lab Tasks

TASK 1

Trace an Email

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

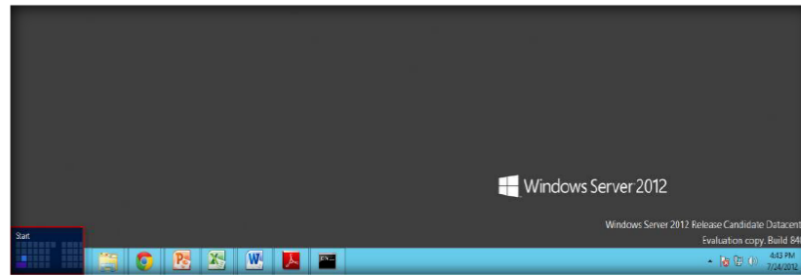


FIGURE 7.1: Windows Server 2012 – Desktop view

2. On the **Start** menu, click **eMailTrackerPro** to launch the application eMailTrackerPro

eMailTrackerPro Advanced Edition includes an online mail checker which allows you to view all your emails on the server before delivery to your computer.

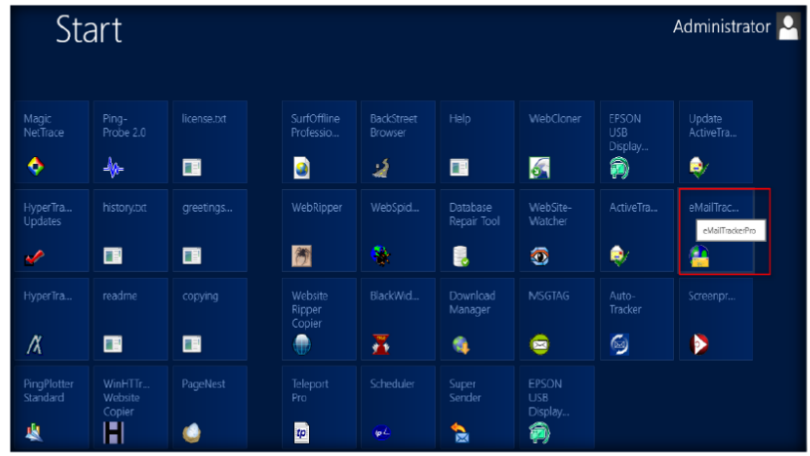
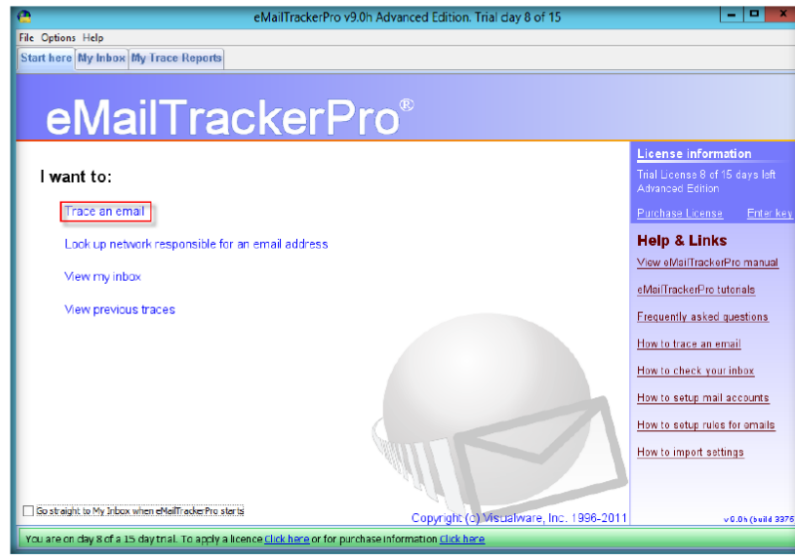


FIGURE 7.2: Windows Server 2012 – Apps

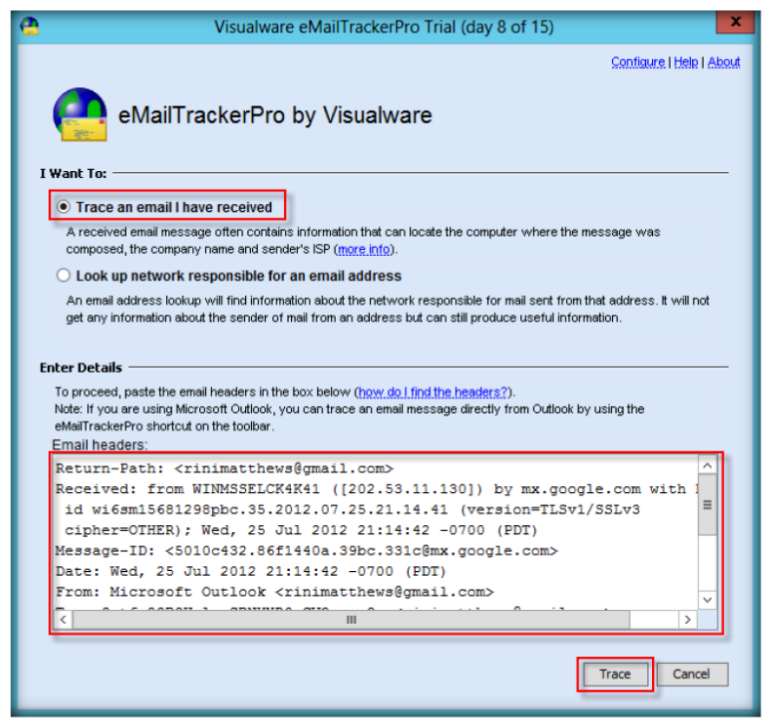
3. Click **OK** if the **Edition Selection** pop-up window appears
4. Now you are ready to start **tracing** email headers with **eMailTrackerPro**
5. Click the **Trace an email** option to start the trace



This tool also uncovers common SPAM tactics.

FIGURE 7.3: The eMailTrackerPro Main window

6. Clicking **Trace an email** will direct you to the **eMailTrackerPro by Visualware** window
7. Select **Trace an email I have received**. Now, copy the email header from the email you wish to trace and paste it in **Email headers** field under **Enter Details** and click **Trace**



The filter system in eMailTrackerPro allows you to create custom filters to match your incoming mail.

FIGURE 7.4: The eMailTrackerPro by Visualware Window

TASK 2

Finding Email Header

Note: In Outlook, find the email header by following these steps:

- Double-click the email to open it in a new window
- Click the small arrow in the lower-right corner of the **Tags** toolbar box to open **Message Options** information box
- Under **Internet headers**, you will find the **Email header**, as displayed in the screenshot

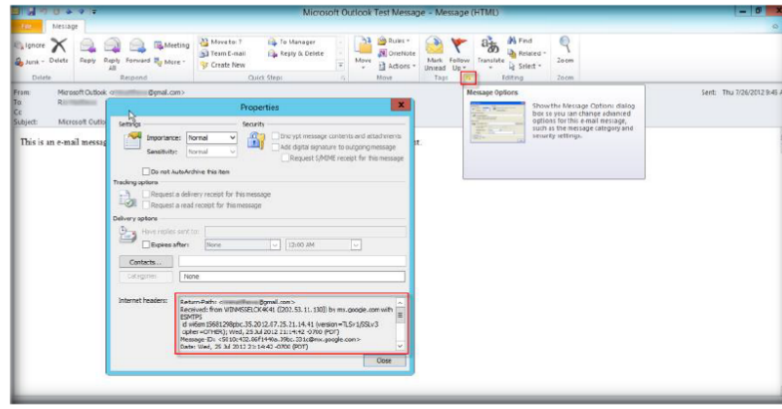


FIGURE 7.5: Finding Email Header in Outlook 2010

The abuse report option from the **My Trace Reports** window automatically launches a browser window with the abuse report included.

8. Clicking the **Trace** button will direct you to the **Trace report** window
9. The email location is traced in a GUI world map. The location and IP addresses may vary. You can also view the summary by selecting **Email Summary section** on the right side of the window
10. The **Table** section right below the Map shows the entire Hop in the route with the **IP** and suspected locations for each hop
11. **IP address** might be different than the one shown in the screenshot

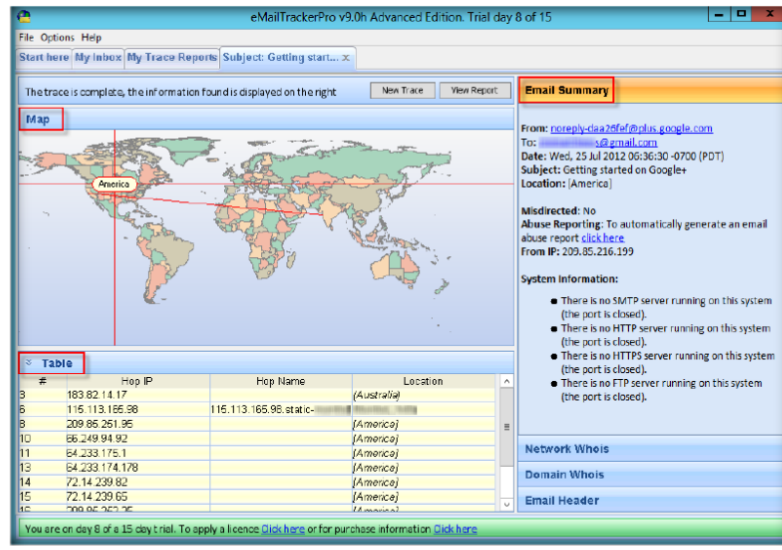


FIGURE 7.6: eMailTrackerPro – Email Trace Report

Each email message includes an Internet header with valuable information, eMailTrackerPro analyzes the message header and reports the IP address of the computer where the message originated, its estimated location, the individual or organization the IP address is registered to, the network provider, and additional information as available

TASK 3

Trace Reports

12. You can view the complete trace report on **My Trace Reports** tab

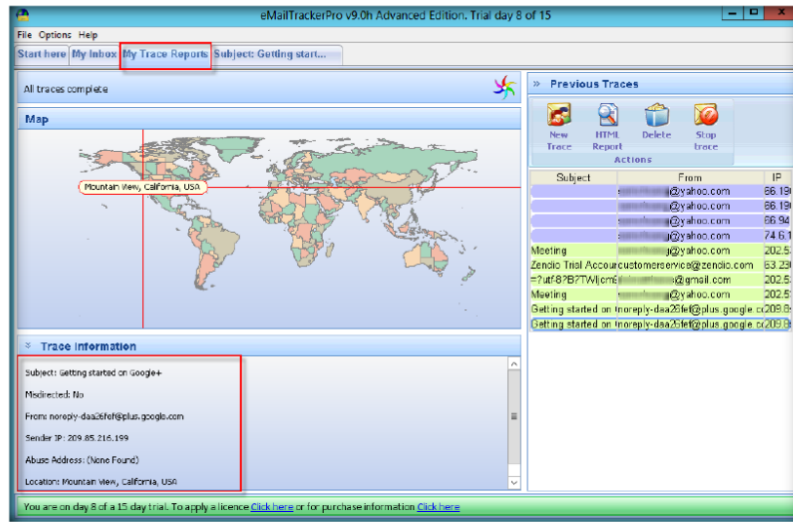


FIGURE 7.7: The eMailTrackerPro - My Trace Reports tab

Tracking an email is useful for identifying the company and network providing service for the address.

Lab Analysis

Document all the live emails discovered during the lab with all additional information.

emailTrackerPro can detect abnormalities in the email header and warn you that the email may be spam

Tool/Utility	Information Collected/Objectives Achieved
eMailTrackerPro	**Map:** Location of traced email in GUI map
	Table: Hop in the route with IP
	Email Summary: Summary of the traced email ▪ From & To email address ▪ Date ▪ Subject ▪ Location
	Trace Information: ▪ Subject ▪ Sender IP ▪ Location

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. What is the difference between tracing an email address and tracing an email message?
2. What are email Internet headers?
3. What does "unknown" mean in the route table of the identification report?
4. Does eMailTrackerPro work with email messages that have been forwarded?
5. Evaluate whether an email message can be traced regardless of when it was sent.

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 8

Collecting Information about a Target Website Using Firebug

Firebug integrates with Firefox, providing a lot of development tools allowing you to edit, debug, and monitor CSS, HTML, and JavaScript live in any web page.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As you all know, email is one of the important tools that has been created. Unfortunately, attackers have misused emails to send spam to communicate in secret and hide themselves behind the spam emails, while attempting to undermine business dealings. In such instances, it becomes necessary for penetration testers to trace an email to find the **source of email** especially where a crime has been committed using email. You have already learned in the previous lab how to find the location by tracing an email using eMailTrackerPro to provide such information as **city**, **state**, **country**, etc. from where the email was actually sent.

The majority of penetration testers use the Mozilla Firefox as a web browser for their pen test activities. In this lab, you will learn to use **Firebug** for a web application penetration test and gather complete information. Firebug can prove to be a useful **debugging** tool that can help you track rogue **JavaScript** code on servers.

Lab Objectives

The objective of this lab is to help students learn editing, debugging, and monitoring CSS, HTML, and JavaScript in any websites.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

In the lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

Overview of Firebug

Firebug is an add-on tool for Mozilla Firefox. Running Firebug displays information such as directory structure, internal URLs, cookies, session IDs, etc.

Lab Tasks

Firebug includes a lot of features such as debugging, HTML inspecting, profiling and etc. which are very useful for web development.

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

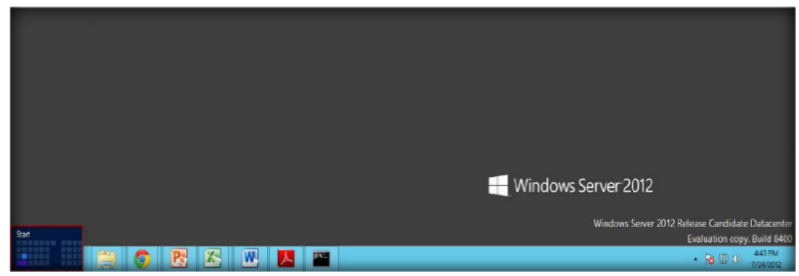


FIGURE 8.1: Windows Server 2012 – Desktop view

2. On the **Start** menu, click **Mozilla Firefox** to launch the browser

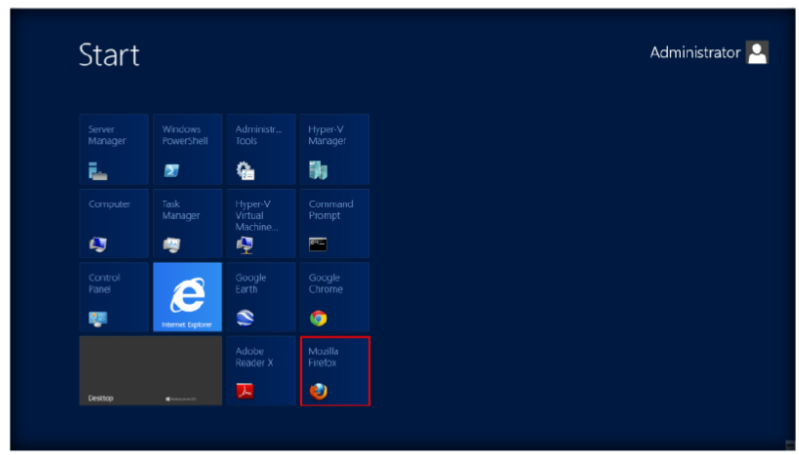


FIGURE 8.2: Windows Server 2012 – Apps

Firebug features:

- Javascript debugging
- Javascript CommandLine
- Monitor the Javascrit Performance and XmlHttpRequest
- Logging
- Tracing
- Inspect HTML and Edit HTML
- Edit CSS

3. Type the URL **https://getfirebug.com** in the Firefox browser and click **Install Firebug**

TASK 1

Installing Firebug

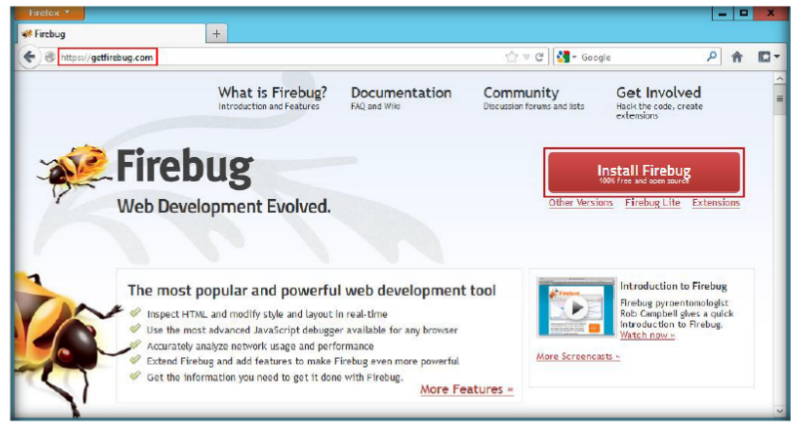


FIGURE 8.3: Windows Server 2012 – Apps

4. Clicking **Install Firebug** will redirect to the **Download Firebug** page. Click the **Download** link to install Firebug

Firebug inspects HTML and modify style and layout in real-time

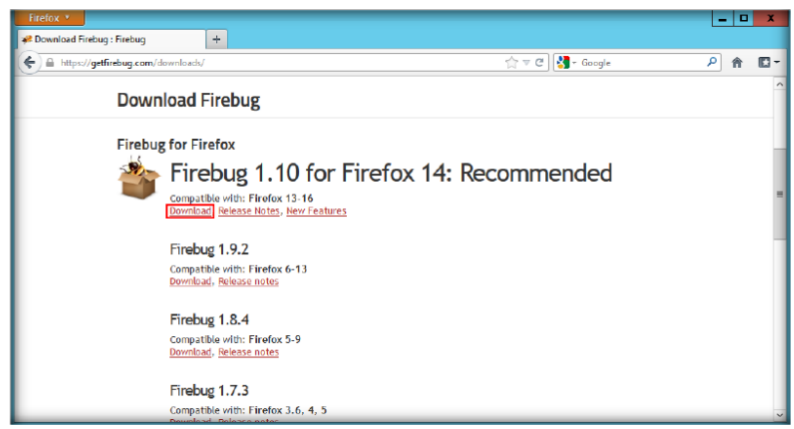


FIGURE 8.4: Windows Server 2012 – Apps

5. On the **Add-Ons** page, click the button **Add to Firefox** to initiate the Add-On installation

Firebug adds several configuration options to Firefox. Some of these options can be changed through the UI, others can be manipulated only via about:config.

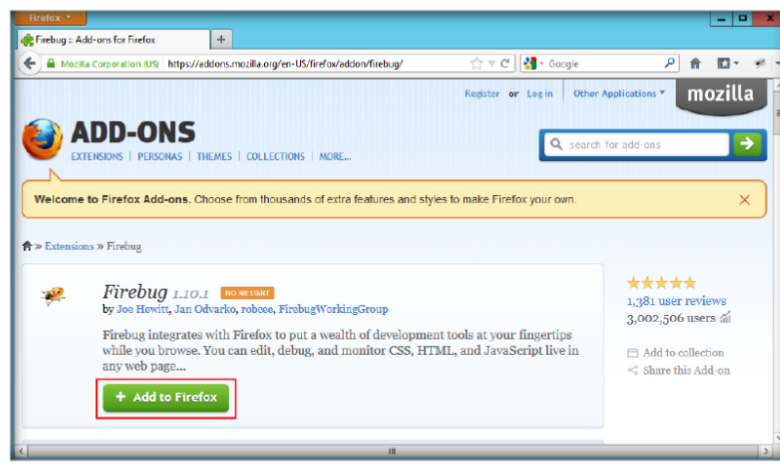


FIGURE 8.5: Windows Server 2012 – Apps

6. Click the **Install Now** button in the **Software Installation** window

panelTabMinWidth describes minimal width in pixels of the Panel tabs inside the Panel Bar when there is not enough horizontal space.

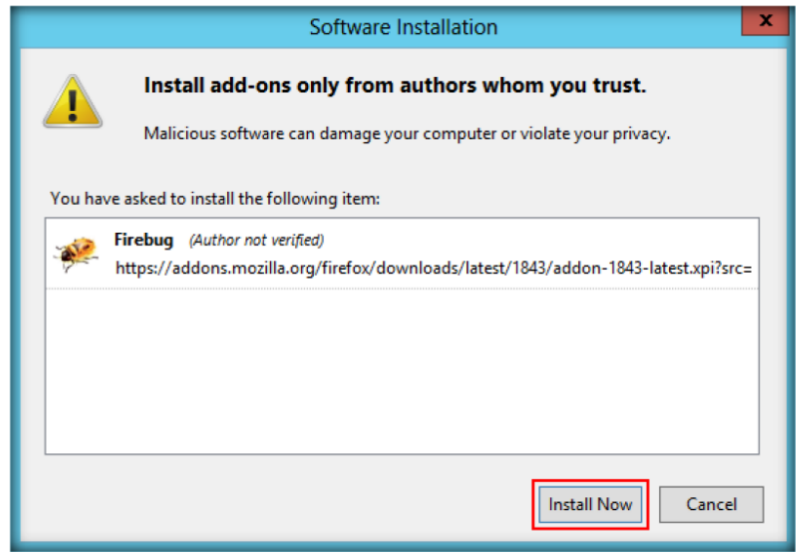


FIGURE 8.6: Windows Server 2012 – Apps

7. Once the Firebug Add-On is installed, it will appear as a **grey colored bug** on the **Navigation Toolbar** as highlighted in the following screenshot

showFirstRunPage specifies whether to show the first run page.

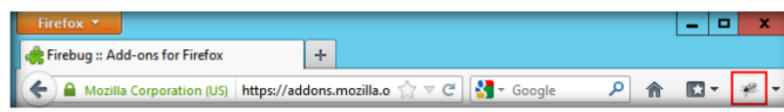


FIGURE 8.7: Windows Server 2012 – Apps

8. Click the **Firebug** icon to view the Firebug pane.
9. Click the **Enable** link to view the detailed information for Console panel. Perform the same for the Script, Net, and Cookies panels

The console panel offers a JavaScript command line, lists all kinds of messages and offers a profiler for JavaScript commands.

FIGURE 8.8: Windows Server 2012 – Apps

10. Enabling the Console panel displays all the requests by the page. The one highlighted in the screenshot is the **Headers** tab
11. In this lab, we have demonstrated http://www.microsoft.com
12. The **Headers** tab displays the Response Headers and Request Headers by the website

The CSS panel manipulates CSS rules. It offers options for adding, editing and removing CSS styles of the different files of a page containing CSS. It also offers an editing mode, in which you can edit the content of the CSS files directly via a text area..

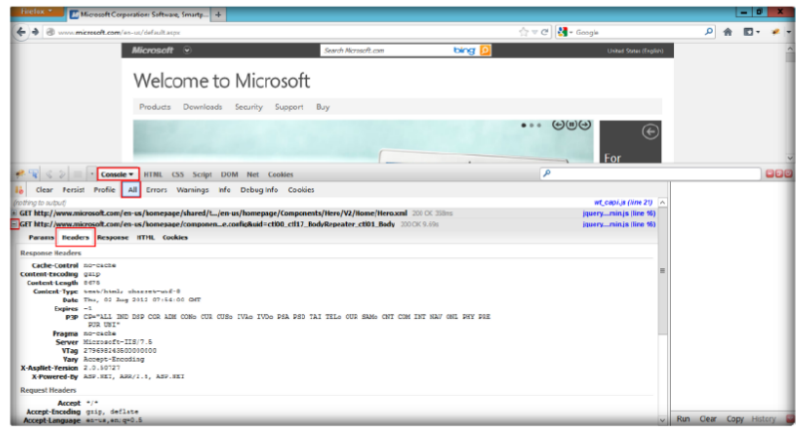


FIGURE 8.9: Windows Server 2012 – Apps

13. Similarly, the rest of the tabs in the Console panel like **Params**, **Response**, **HTML**, and **Cookies** hold important information about the website
14. The HTML panel displays information such as source code, internal URLs of the website, etc.

The HTML panel displays the generated HTML/XML of the currently opened page. It differs from the normal source code view, because it also displays all manipulations on the DOM tree. On the right side it shows the CSS styles defined for the currently selected tag, the computed styles for it, layout information and the DOM variables assigned to it in different tabs.

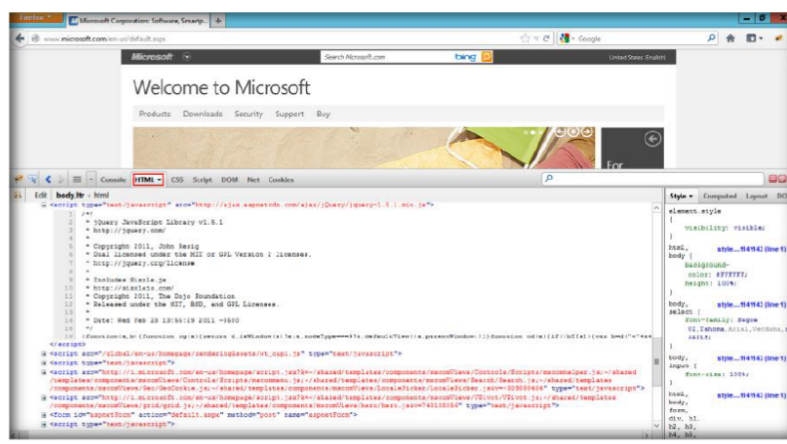


FIGURE 8.10: Windows Server 2012 – Apps

15. The **Net** panel shows the **Request start** and **Request phases start and elapsed time relative to the Request start** by hovering the mouse cursor on the Timeline graph for a request

Net Panel's purpose is to monitor HTTP traffic initiated by a web page and present all collected and computed information to the user. Its content is composed of a list of entries where each entry represents one request/response round trip made by the page..

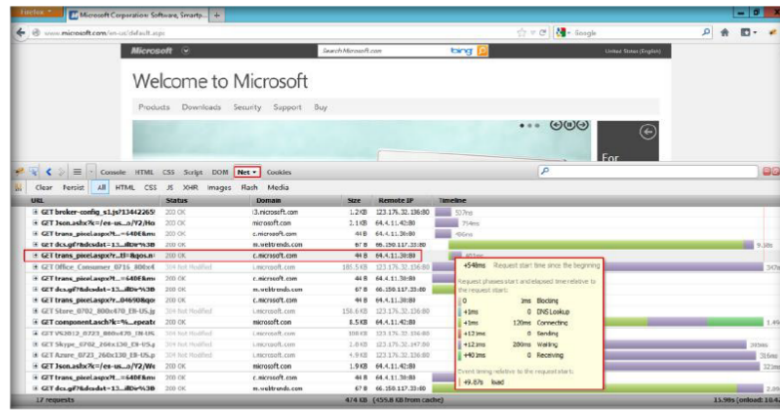


FIGURE 8.11: Windows Server 2012 – Apps

16. Expand a request in the Net panel to get detailed information on Params, Headers, Response, Cached, and Cookies. The screenshot that follows shows the Cache information

Script panel debugs JavaScript code. Therefore the script panel integrates a powerful debugging tool based on features like different kinds of breakpoints, step-by-step execution of scripts, a display for the variable stack, watch expressions and more..

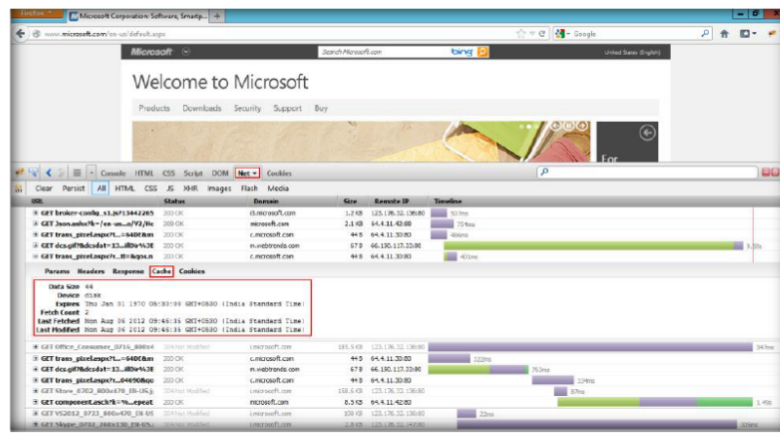


FIGURE 8.12: Windows Server 2012 – Apps

17. Expand a request in the Cookies panel to get information on a cookie Value, Raw data, JSON, etc.

Export cookies for this site - exports all cookies of the current website as text file. Therefore the Save as dialog is opened allowing you to select the path and choose a name for the exported file.

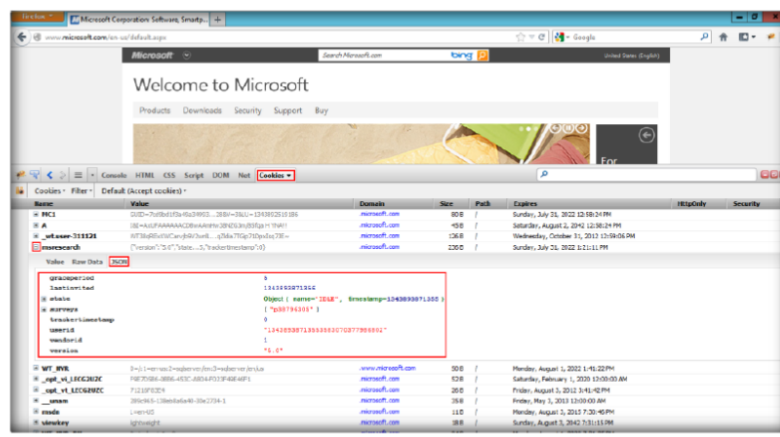


FIGURE 8.13: Windows Server 2012 – Apps

Note: You can find information related to the CSS, Script, and DOM panel on the respective tabs.

Lab Analysis

Collect information such as internal URLs, cookie details, directory structure, session IDs, etc. for different websites using Firebug.

Tool/Utility	Information Collected/Objectives Achieved
Firebug	**Server on which the website is hosted:** Microsoft –IIS/7.5
	Development Framework: ASP.NET
	HTML Source Code using JavaScript, jQuery, Ajax
	Other Website Information: ▪ Internal URLs ▪ Cookie details ▪ Directory structure ▪ Session IDs

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine the Firebug error message that indicates a problem.
2. After editing pages within Firebug, how can you output all the changes that you have made to a site's CSS?
3. In the Firebug DOM panel, what do the different colors of the variables mean?
4. What does the different color line indicate in the Timeline request in the Net panel?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 9

Mirroring Websites Using the HTTrack Web Site Copier Tool

HTTrack Web Site Copier is an Offline browser utility that allows you to download a World Wide Web site through the Internet to your local directory.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Website servers set cookies to help authenticate the user if the user logs in to a secure area of the website. Login information is stored in a cookie so the user can enter and leave the website without having to re-enter the same authentication information over and over.

You have learned in the previous lab to extract information from a web application using Firebug. As cookies are transmitted back and forth between a browser and website, if an attacker or unauthorized person gets in between the data transmission, the sensitive cookie information can be intercepted. An attacker can also use Firebug to see what JavaScript was downloaded and evaluated. Attackers can modify a request before it's sent to the server using Tamper data. If they discover any SQL or cookie vulnerabilities, attackers can perform a SQL injection attack and can tamper with cookie details of a request before it's sent to the server. Attackers can use such vulnerabilities to trick browsers into sending sensitive information over insecure channels. The attackers then siphon off the sensitive data for unauthorized access purposes. Therefore, as a penetration tester, you should have an updated antivirus protection program to attain Internet security.

In this lab, you will learn to mirror a website using the HTTrack Web Site Copier Tool and as a penetration tester you can prevent D-DoS attack.

Lab Objectives

The objective of this lab is to help students learn how to mirror websites.

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

- Web Data Extractor located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Website Copier**
- You can also download the latest version of **HTTrack Web Site Copier** from the link http://www.httrack.com/page/2/en/index.html
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- Follow the **Wizard driven installation** process
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8, Window Server 2008**, and **Windows 7**
- To run this tool Administrative privileges are required

Lab Duration

Time: 10 Minutes

Overview of Web Site Mirroring

WinHTTrack arranges the original site's relative link-structure.

Web mirroring allows you to download a website to a local directory, building recursively all **directories**, **HTML**, **images**, **flash**, **videos**, and other files from the server to your computer.

Lab Tasks

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

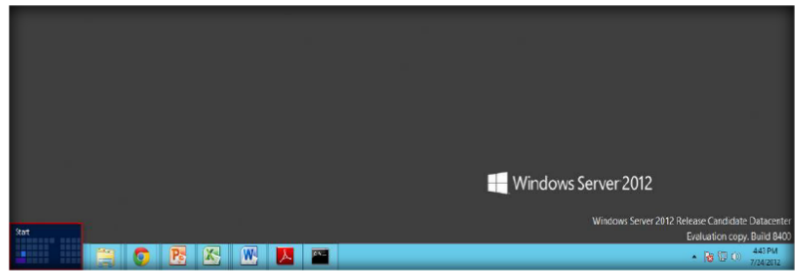


FIGURE 9.1: Windows Server 2012 – Desktop view

WinHTTrack works as a command-line program or through a shell for both private (capture) and professional (on-line web mirror) use.

2. In the **Start** metro apps, click **WinHTTrack** to launch the application **WinHTTrack**

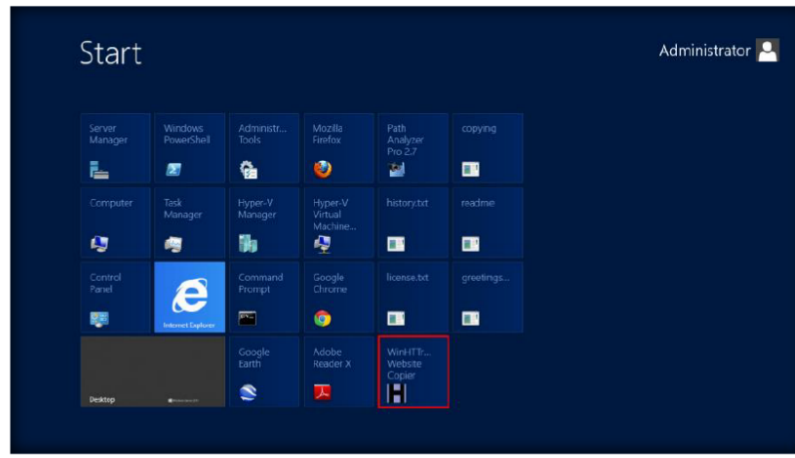


FIGURE 9.2: Windows Server 2012 – Apps

TASK 1

Mirroring a Website

3. In the WinHTTrack main window, click **Next** to create a **New Project**

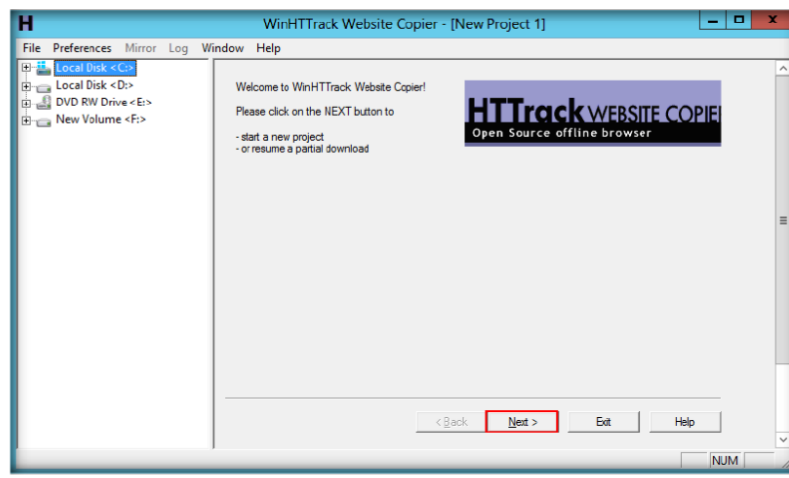


FIGURE 9.3: HTTrack Website Copier Main Window

Quickly updates downloaded sites and **resumes** interrupted downloads (due to connection break, crash, etc.)

4. Enter the **project name** in the **Project name** field. Select the Base path to store the copied files. Click **Next**

Wizard to specify which links must be loaded (accept/refuse: link, all domain, all directory)

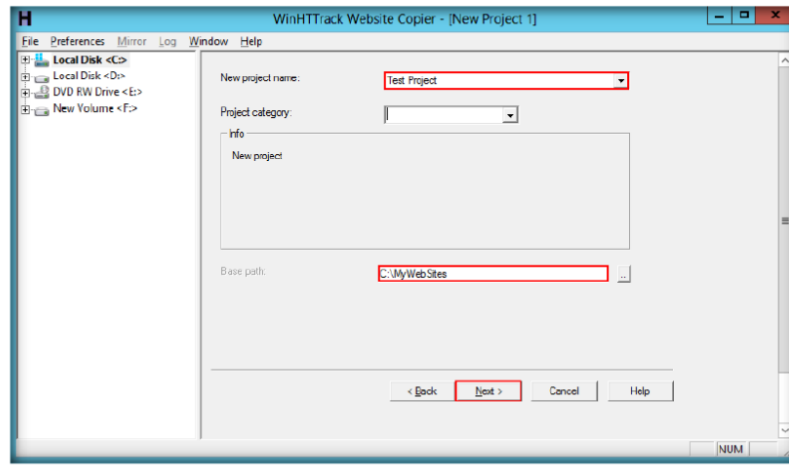


FIGURE 9.4: HTTrack Website Copier selecting a New Project

5. Enter **www.certifiedhacker.com** under **Web Addresses: (URL)** and then click the **Set options** button

Timeout and minimum transfer rate manager to abandon slowest sites

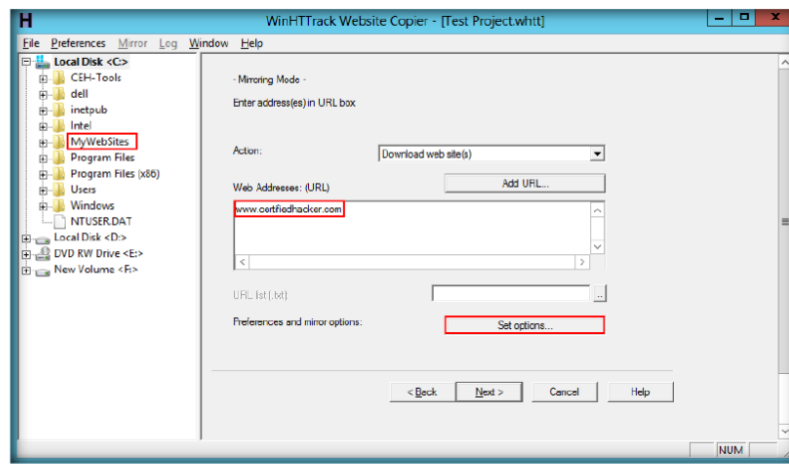


FIGURE 9.5: HTTrack Website Copier Select a project a name to organize your download

Downloading a site can overload it, if you have a fast pipe, or if you capture too many simultaneous cgi (dynamically generated pages)

6. Clicking the **Set options** button will launch the **WinHTTrack** window
7. Click the **Scan Rules** tab and select the check boxes for the file types as shown in the following screenshot and click **OK**

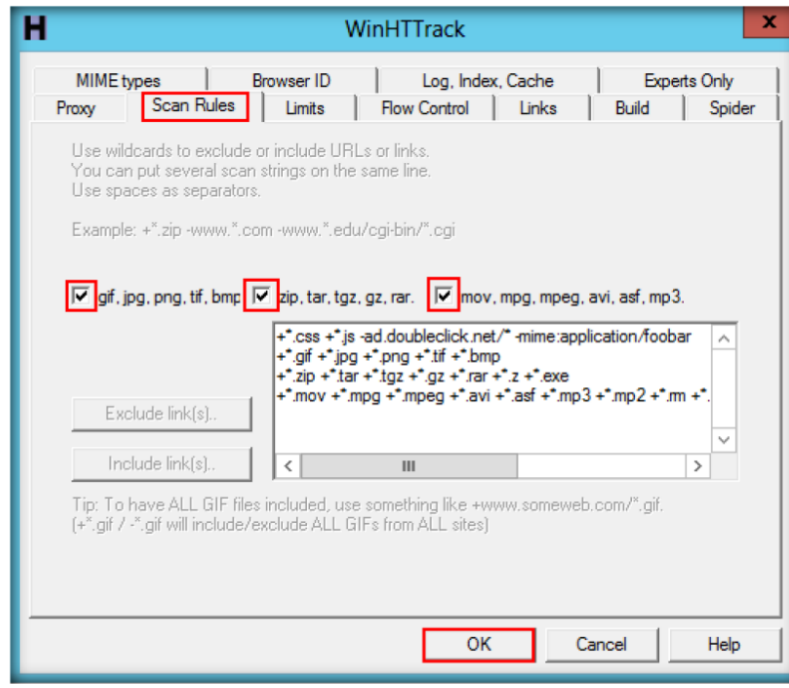


FIGURE 9.6: HTTrack Website Copier Select a project a name to organize your download

8. Then, click **Next**

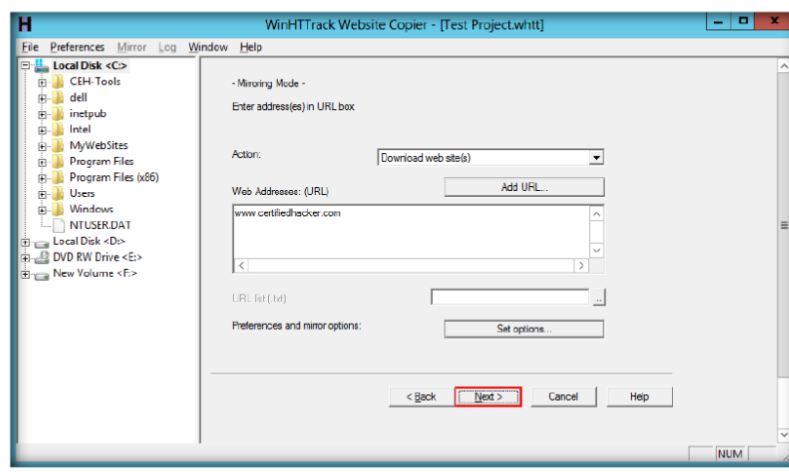


FIGURE 9.7: HTTrack Website Copier Select a project a name to organize your download

9. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation**
10. Click **Finish** to start mirroring the website

File names with original structure kept or splitted mode (one html folder, and one image folder), dos 8-3 filenames option and user-defined structure

HTML parsing and tag analysis, including javascript code/embedded HTML code

Proxy support to maximize speed, with optional authentication

🗀 The tool has integrated DNS cache and native https and ipv6 support

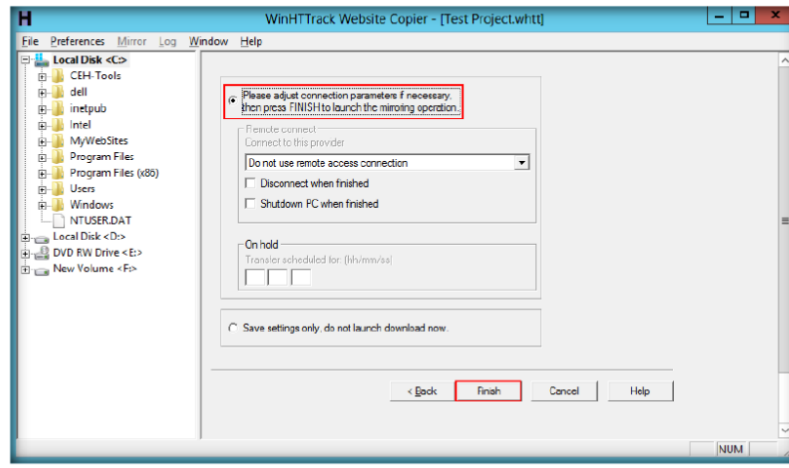


FIGURE 9.8: HTTrack Website Copier Type or drop and drag one or several Web addresses

🗀 HTTrack can also update an existing mirrored site and resume interrupted downloads. HTTrack is fully configurable by options and by filters

11. Site mirroring progress will be displayed as in the following screenshot

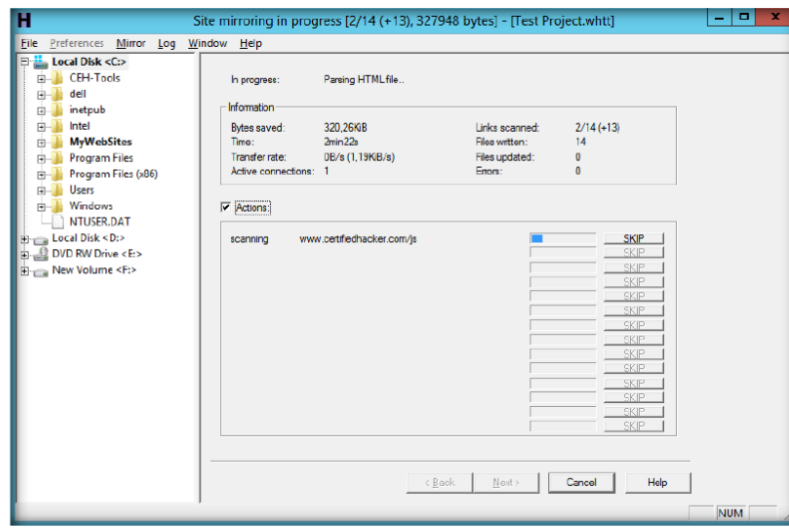


FIGURE 9.9: HTTrack Website Copier displaying site mirroring progress

🗀 Filter by file type, link location, structure depth, file size, site size, accepted or refused sites or filename (with advanced wild cards)..

12. WinHTTrack shows the message **Mirroring operation complete** once the site mirroring is completed. Click **Browse Mirrored Website**

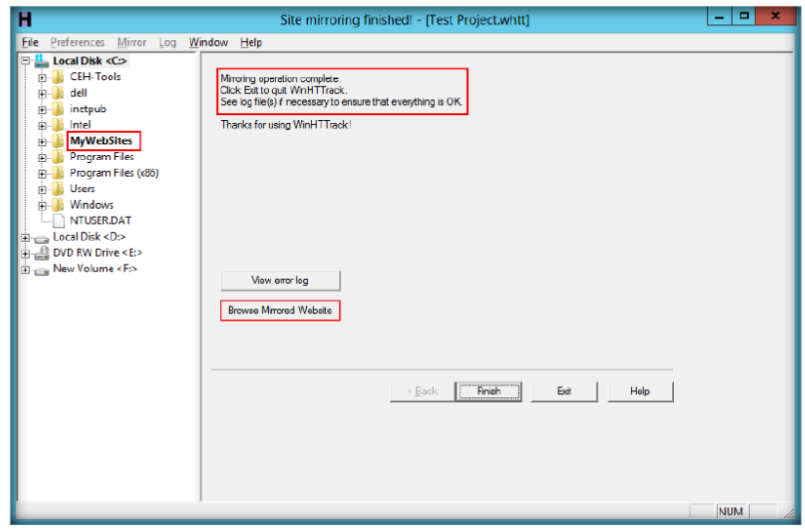


FIGURE 9.10: HTTrack Website Copier displaying site mirroring progress

13. Clicking the **Browse Mirrored Website** button will launch the mirrored website for www.certifiedhacker.com. The URL indicates that the site is located at the local machine

🗀 Optional log file with error-log and comments-log.

Note: If the web page does not open for some reasons, navigate to the directory where you have mirrored the website and open index.html with any web browser

🗀 Use bandwidth limits, connection limits, size limits and time limits

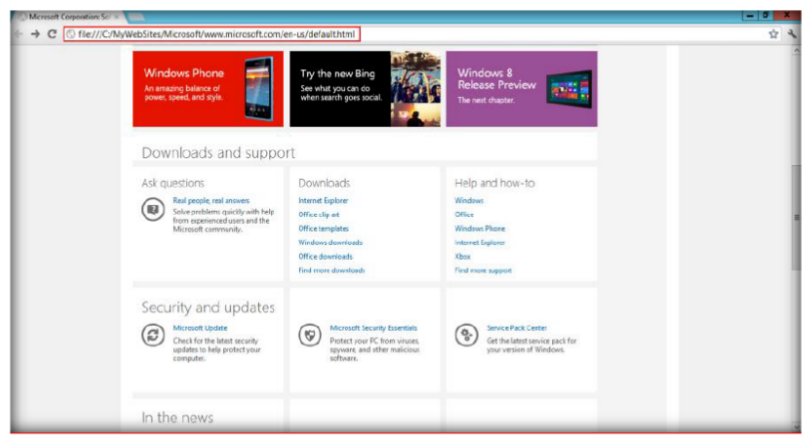


FIGURE 9.11: HTTrack Website Copier Mirrored Website Image

14. A few websites are very large and will take a long time to mirror the complete site

🗀 Do not download too large websites: use filters; try not to download during working hours

15. If you wish to stop the mirroring process prematurely, click **Cancel** in the **Site mirroring progress** window
16. The site will work like a **live hosted website**.

Lab Analysis

Document the mirrored website directories, getting HTML, images, and other files.

Tool/Utility	Information Collected/Objectives Achieved
HTTrack Web Site Copier	▪ Offline copy of the website www.certifiedhacker.com is created

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

5. How do you retrieve the files that are outside the domain while mirroring a website?
6. How do you download ftp files/sites?
7. Can HTTrack perform form-based authentication?
8. Can HTTrack execute HP-UX or ISO 9660 compatible files?
9. How do you grab an email address in web pages?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 10

Extracting a Company's Data Using Web Data Extractor

Web Data Extractor is used to extract targeted company(s) contact details or data such as emails, fax, phone through web for responsible b2b communication.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers continuously look for the easiest method to collect information. There are many tools available with which attackers can extract a company's database. Once they have access to the database, they can gather employees' email addresses and phone numbers, the company's internal URLs, etc. With the information gathered, they can send spam emails to the employees to fill their mailboxes, hack into the company's website, and modify the internal URLs. They may also install malicious viruses to make the database inoperable.

As an expert **penetration tester**, you should be able to think from an attacker's perspective and try all possible ways to gather information on **organizations**. You should be able to collect all the **confidential information** of an organization and implement security features to prevent company data leakage. In this lab, you will learn to use Web Data Extractor to extract a company's data.

Lab Objectives

The objective of this lab is to demonstrate how to extract a company's data using **Web Data Extractor**. Students will learn how to:

- Extract Meta Tag, Email, Phone/Fax from the web pages

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out the lab you need:

- Web Data Extractor located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Additional Footprinting Tools\Web Data Extractor**
- You can also download the latest version of **Web Data Extractor** from the link http://www.webextractor.com/download.htm
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

WDE send queries to search engines to get matching website URLs

Overview of Web Data Extracting

WDE will query 18+ popular search engines, extract all matching URLs from search results, remove duplicate URLs and finally visits those websites and extract data from there

Web data extraction is a type of information retrieval that can extract automatically unstructured or semi-structured web data sources in a structured manner.

Lab Tasks

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

FIGURE 10.1: Windows 8 – Desktop view

TASK 1

Extracting a Website

2. In the **Start** menu, click **Web Data Extractor** to launch the application **Web Data Extractor**

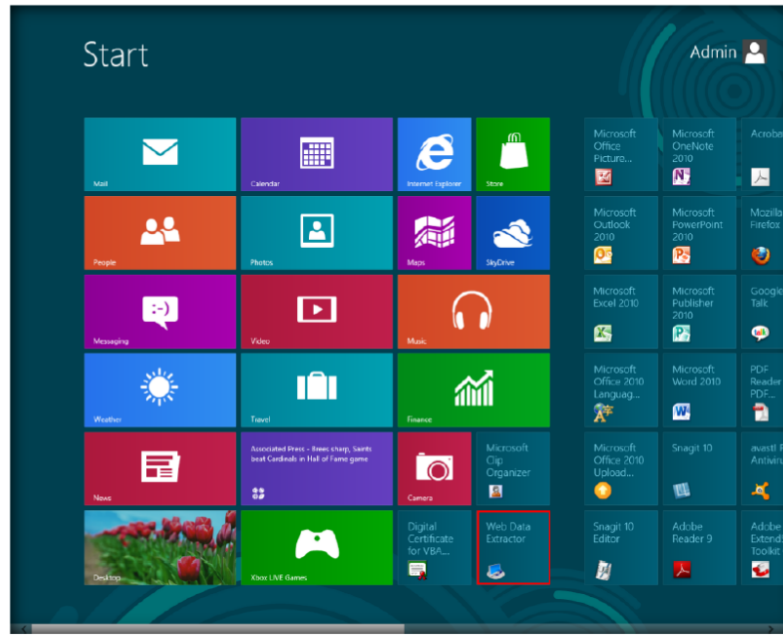


FIGURE 10.2: Windows 8 – Apps

WDE - Phone, Fax Harvester module is designed to spider the web for fresh Tel, FAX numbers targeted to the group that you want to market your product or services to

3. Web Data Extractor's main window appears. Click **New** to start a new session

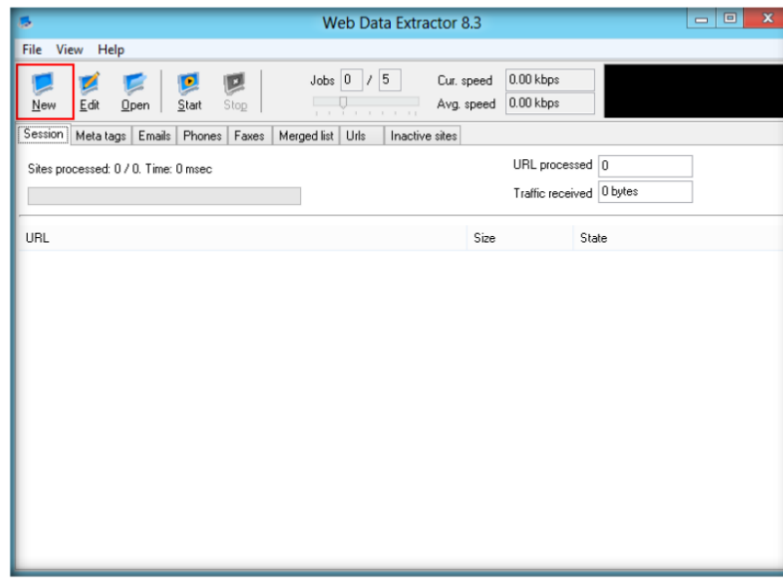


FIGURE 10.3: The Web Data Extractor main window

It has various limiters of scanning range - url filter, page text filter, domain filter - using which you can extract only the links or data you actually need from web pages, instead of extracting all the links present there, as a result, you create your own custom and targeted data base of urls/links collection

4. Clicking **New** opens the **Session settings** window.
5. Type a URL (www.certifiedhacker.com) in the **Starting URL** field. Select the check boxes for all the options as shown in the screenshot and click **OK**

Web Data Extractor automatically get lists of meta-tags, e-mails, phone and fax numbers, etc. and store them in different formats for future use

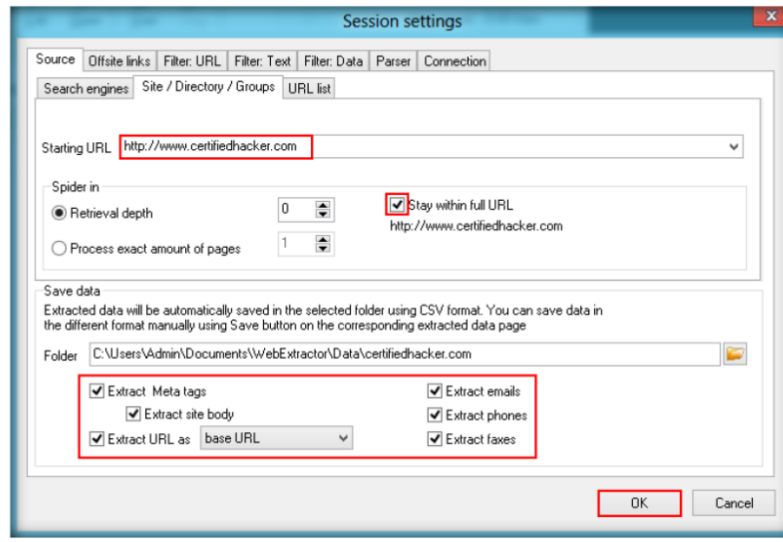


FIGURE 10.4: Web Data Extractor the Session setting window

Fixed "Stay with full url" and "Follow offsite links" options which failed for some sites before

6. Click **Start** to initiate the data extraction

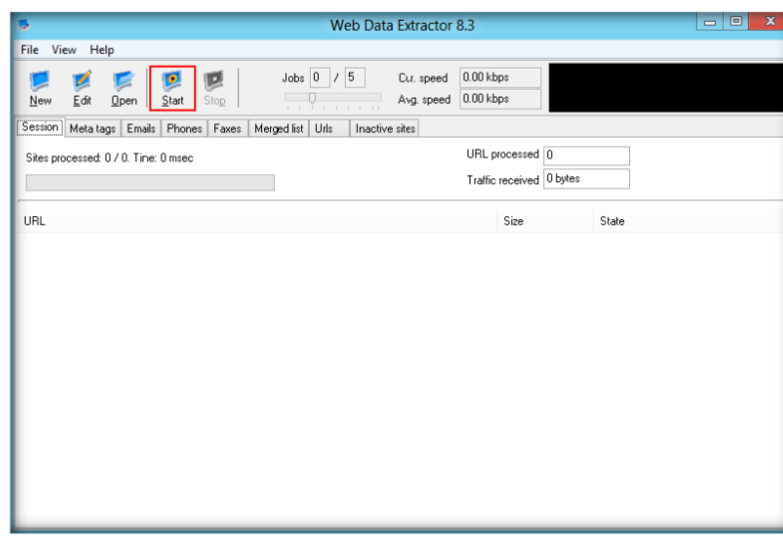
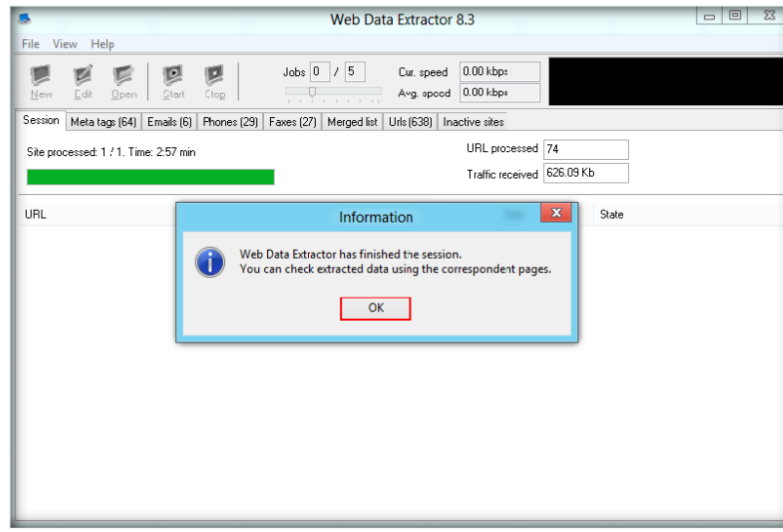


FIGURE 10.5: Web Data Extractor initiating the data extraction windows

It supports operation through proxy-server and works very fast, as it is able of loading several pages simultaneously, and requires very few resources. Powerful, highly targeted email spider harvester

7. Web Data Extractor will start collecting the information (**emails**, **phones**, **faxes,** etc.). Once the data extraction process is completed, an **Information** dialog box appears. Click **OK**



🗁 Meta Tag Extractor module is designed to extract URL, meta tag (title, description, keyword) from web-pages, search results, open web directories, list of urls from local file

FIGURE 10.6: Web Data Extractor Data Extraction windows

8. The extracted information can be viewed by clicking the tabs

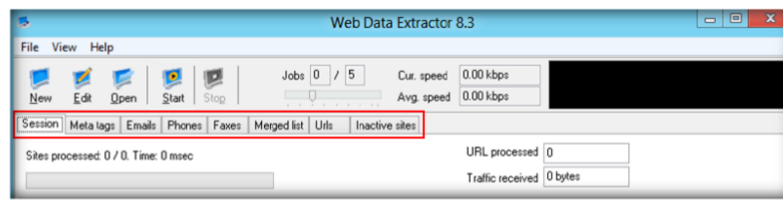
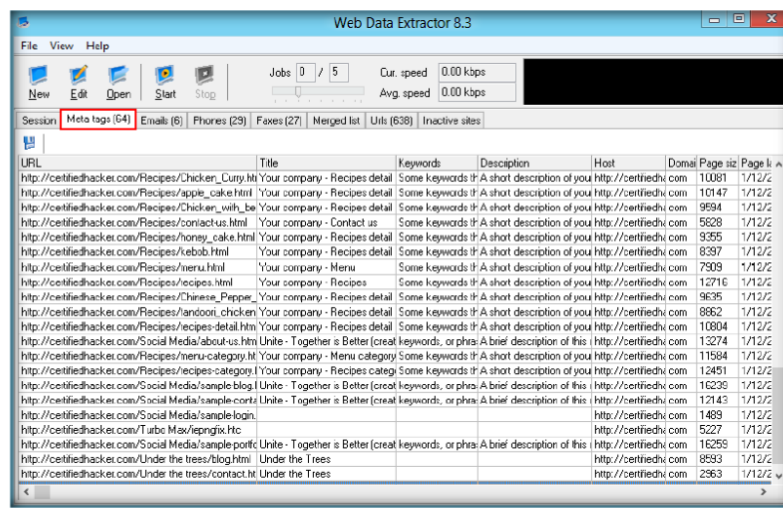


FIGURE 10.7: Web Data Extractor Data Extraction windows

9. Select the **Meta tags** tab to view the URL, Title, Keywords, Description, Host, Domain, and Page size information



🕮 If you want WDE to stay within first page, just select "Process First Page Only". A setting of "0" will process and look for data in whole website. A setting of "1" will process index or home page with associated files under root dir only.

FIGURE 10.8: Web Data Extractor Extracted emails windows

10. Select **Emails** tab to view the Email, Name, URL, Title, Host, Keywords density, etc. information related to emails

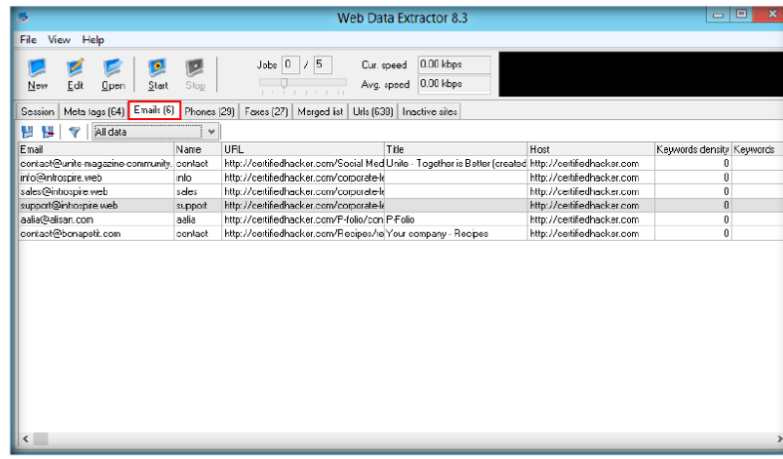


FIGURE 10.9: Web Data Extractor Extracted Phone details window

WDE send queries to search engines to get matching website URLs. Next it visits those matching websites for data extraction. How many deep it spiders in the matching websites depends on "Depth" setting of "External Site" tab

11. Select the **Phones** tab to view the information related to phone like Phone number, Source, Tag, etc.

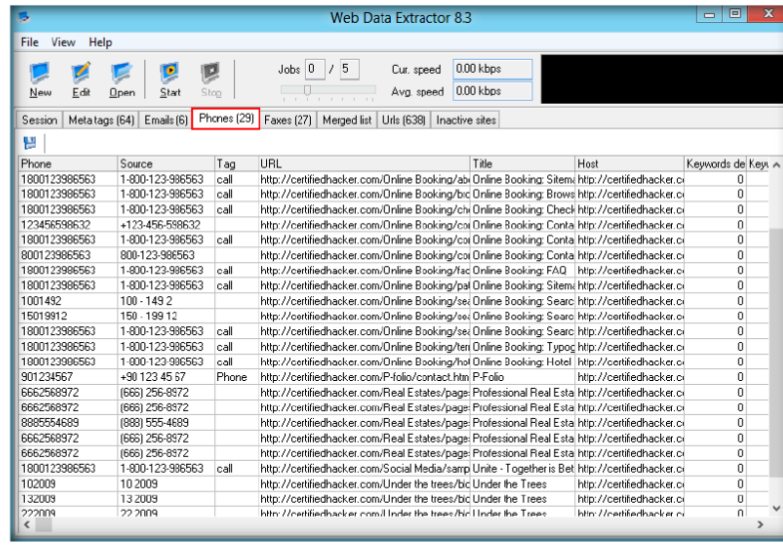


FIGURE 10.10: Web Data Extractor Extracted Phone details window

12. Similarly, check for the information under Faxes, Merged list, Urls (638), Inactive sites tabs

13. To save the session, go to **File** and click **Save session**

Save extracted links directly to disk file, so there is no limit in number of link extraction per session. It supports operation through proxy-server and works very fast, as it is able of loading several pages simultaneously, and requires very few resources

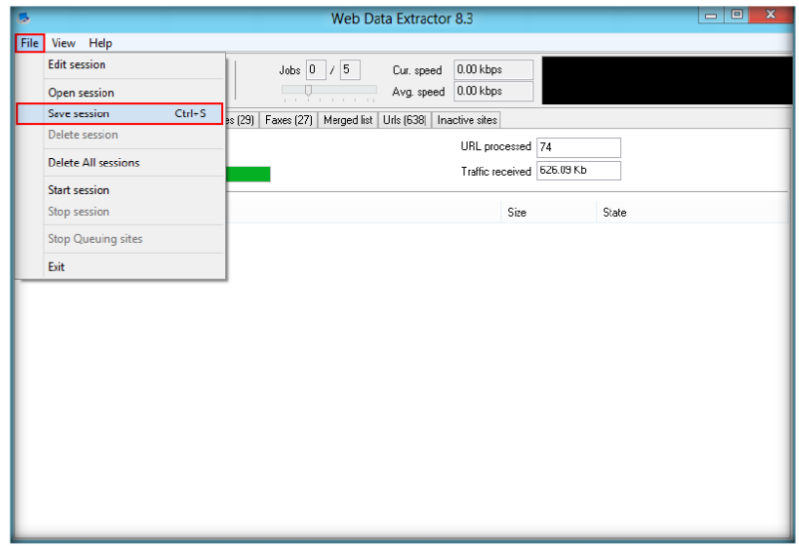


FIGURE 10.11: Web Data Extractor Extracted Phone details window

14. Specify the session name in the **Save session** dialog box and click **OK**

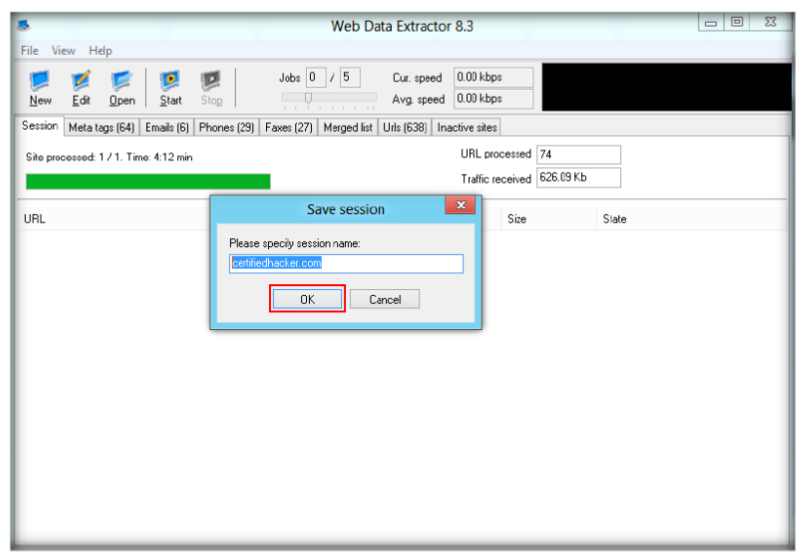


FIGURE 10.12: Web Data Extractor Extracted Phone details window

15. By default, the session will be saved at **D:\Users\admin\Documents\WebExtractor\Data**

Lab Analysis

Document all the Meta Tags, Emails, and Phone/Fax.

Tool/Utility	Information Collected/Objectives Achieved
Web Data Extractor	**Meta tags Information:** URL, Title, Keywords, Description, Host, Domain, Page size, etc.
	Email Information: Email Address, Name, URL, Title, Host, Keywords density, etc.
	Phone Information: Phone numbers, Source, Tag, etc.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. What does Web Data Extractor do?
2. How would you resume an interrupted session in Web Data Extractor?
3. Can you collect all the contact details of an organization?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Lab 11

Identifying Vulnerabilities and Information Disclosures in Search Engines using Search Diggity

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Search Diggity is the primary attack tool of the Google Hacking Diggity Project. It is an MS Windows GUI application that serves as a front-end to the latest versions of Diggity tools: GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.

Lab Scenario

An easy way to find vulnerabilities in websites and applications is to Google them, which is a simple method adopted by attackers. Using a Google code search, hackers can identify crucial vulnerabilities in application code strings, providing the entry point they need to break through application security.

As an expert **ethical hacker**, you should use the same method to identify all the vulnerabilities and patch them before an attacker identifies them to exploit vulnerabilities.

Lab Objectives

The objective of this lab is to demonstrate how to identify vulnerabilities and information disclosures in search engines using Search Diggity. Students will learn how to:

- Extract Meta Tag, Email, Phone/Fax from the web pages

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out the lab, you need:

- Search Diggity is located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Google Hacking Tools\SearchDiggity**

- You can also download the latest version of **Search Diggity** from the link http://www.stachliu.com/resources/tools/google-hacking-diggity-project/attack-tools
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

GoogleDiggity is the primary Google hacking tool, utilizing the Google JSON/ATOM Custom Search API to identify vulnerabilities and information disclosures via Google searching.

Overview of Search Diggity

Search Diggity has a predefined query database that runs against the website to scan the related queries.

Lab Tasks

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

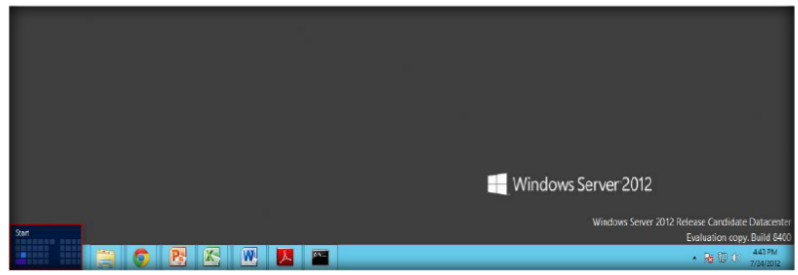


FIGURE 11.1: Windows Server 2012 – Desktop view

TASK 1

Launch Search Diggity

2. In the **Start** menu, to launch **Search Diggity** click the **Search Diggity** icon

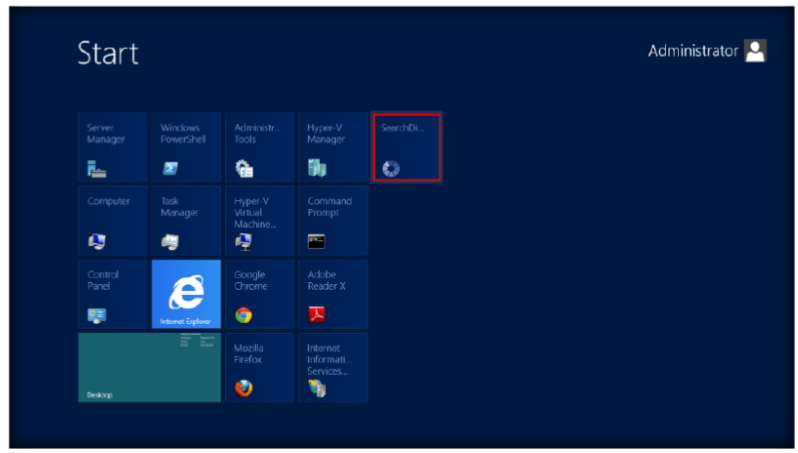


FIGURE 11.2: Windows Server 2012 – Start menu

3. The **Search Diggity** main window appears with **Google Diggity** as the default

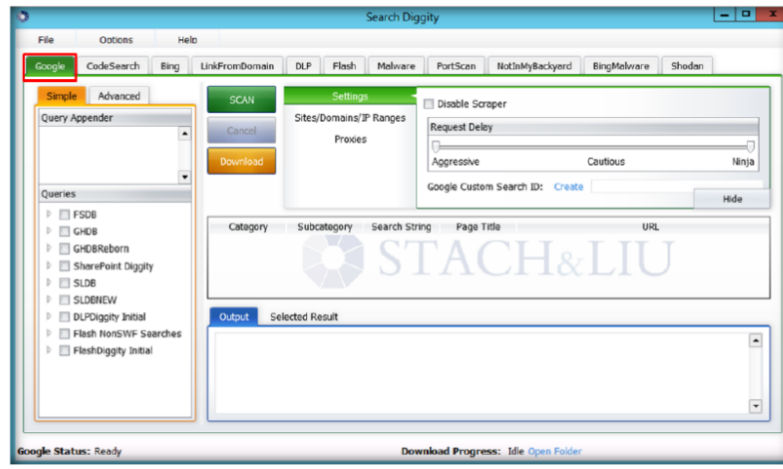


FIGURE 11.3: Search Diggity – Main window

Queries – Select Google dorks (search queries) you wish to use in scan by checking appropriate boxes.

4. Select **Sites/Domains/IP Ranges** and type the domain name in the domain field. Click **Add**

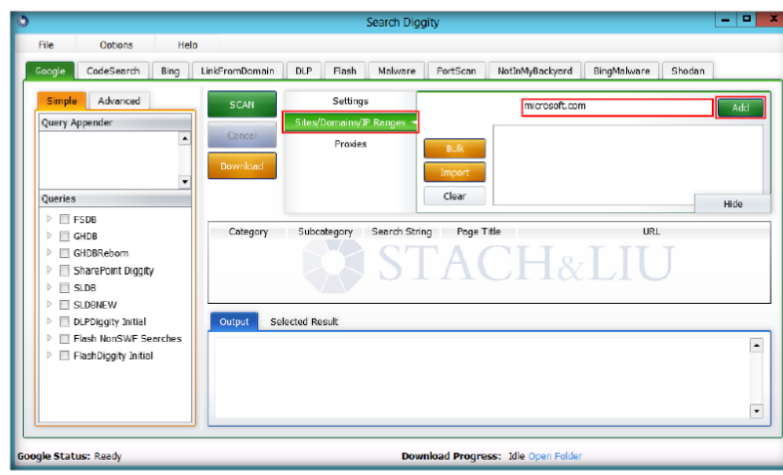


FIGURE 11.4: Search Diggity – Selecting Sites/Domains/IP Ranges

Download_Button – Select (highlight) one or more results in the results pain, then click this button to download the search result files locally to your computer. By default, downloads to `D:\DiggityDownloads\`.

Import Button – Import a text file list of domains/IP ranges to scan. Each query will be run against Google with `site:yourdomainname.com` appended to it.

5. The added domain name will be listed in the box below the **Domain** field

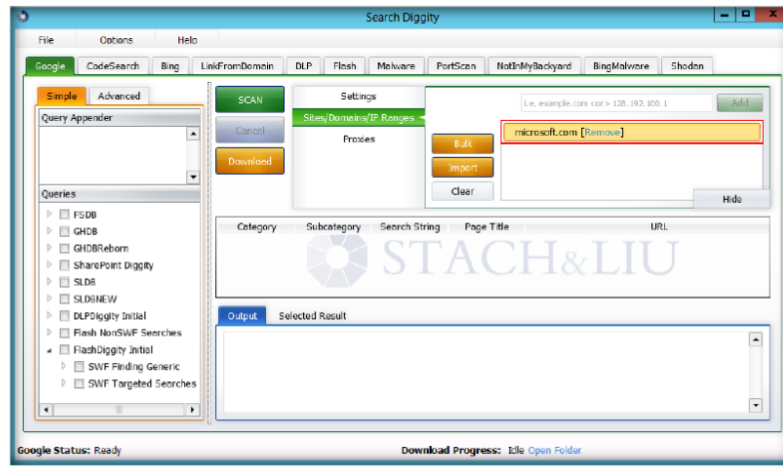


FIGURE 11.5: Search Diggity – Domain added

6. Now, select a **Query** from left pane you wish to run against the website that you have added in the list and click **Scan**

TASK 2

Run Query against a website

Note: In this lab, we have selected the query **SWF Finding Generic**. Similarly, you can select other queries to run against the added website

When scanning is kicked off, the selected query is run against the complete website.

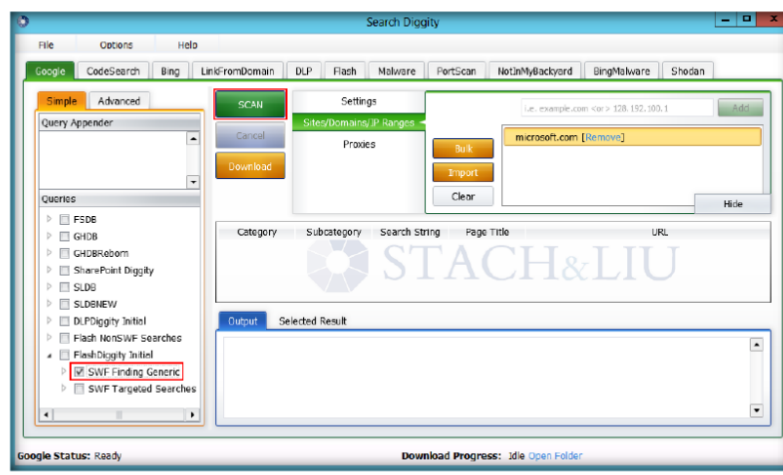


FIGURE 11.6: Search Diggity – Selecting query and Scanning

Results Pane - As scan runs, results found will begin populating in this window pane.

7. The following screenshot shows the **scanning process**

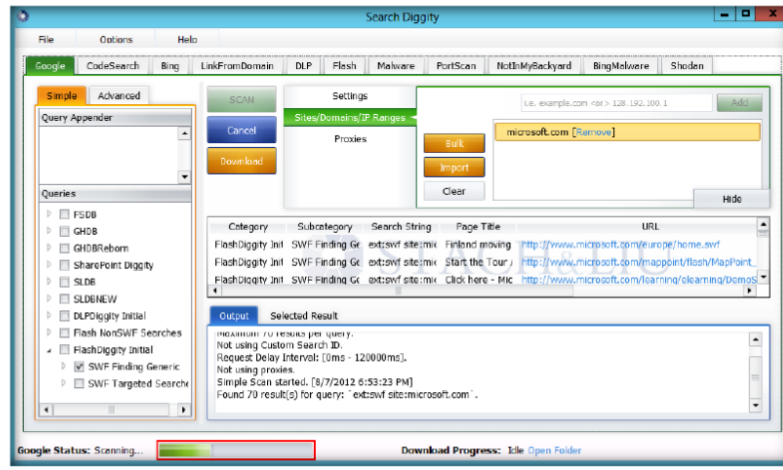


FIGURE 11.7: Search Diggity – Scanning in progress

Simple – Simple search text box will allow you to run one simple query at a time, instead of using the Queries checkbox dictionaries.

8. All the URLs that contain the SWF extensions will be listed and the output will show the query results

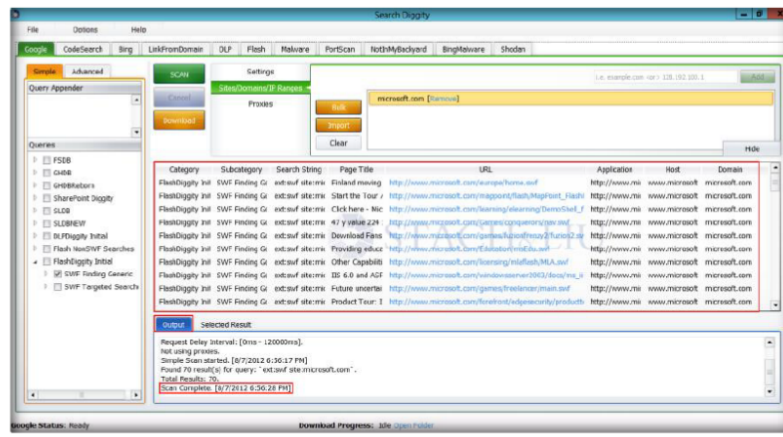


FIGURE 11.8: Search Diggity – Output window

Output – General output describing the progress of the scan and parameters used..

Lab Analysis

Collect the different error messages to determine the vulnerabilities and note the information disclosed about the website.

Tool/Utility	Information Collected/Objectives Achieved
Search Diggity	Many error messages found relating to vulnerabilities

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Is it possible to export the output result for Google Diggity? If yes, how?

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs