DIGITAL UNIVERSITY KERALA

Ethical Hacking and Penetration Testing

Footprinting and Reconnaissance

0471-2788072 https://ksaac.duk.ac.in info.ksaac@duk.ac.in

LEARNING OBJECTIVES

01 Explain Footprinting Concepts

02 Demonstrate Footprinting through Search Engines

03 Demonstrate Footprinting through Internet Research Services

04 Demonstrate Footprinting through Social Networking Sites

05 Use Different Techniques for Whois Footprinting

06 Use Different Techniques for DNS Footprinting

07 Use Different Techniques for Network and Email Footprinting

08 Demonstrate Footprinting through Social Engineering

09 Automate Footprinting Tasks using Advanced Tools and AI

10 Explain Footprinting Countermeasures

LO#01: Explain Footprinting Concepts

Reconnaissance

Reconnaissance (also known as footprinting) refers to the preparatory phase where an attacker seeks to **gather as much information as possible about a target of evaluation** prior to launching an attack

Types of Reconnaissance

Passive

Gathering information about the target **without direct interaction**

It involves:

- Open-source Intelligence (OSINT) gathering
- Proprietary databases and paid services
- Sharing intelligence with partner organizations or industry groups

Active

Gathering information about the target **with direct interaction**

It involves:

- DNS interrogation
- Social engineering
- Network/port scanning
- User and service enumeration

Information Obtained in Footprinting

Organization information

- Employee details
- Telephone numbers
- Branch and location details
- Background of the organization
- Web technologies
- News articles, press releases, and related documents

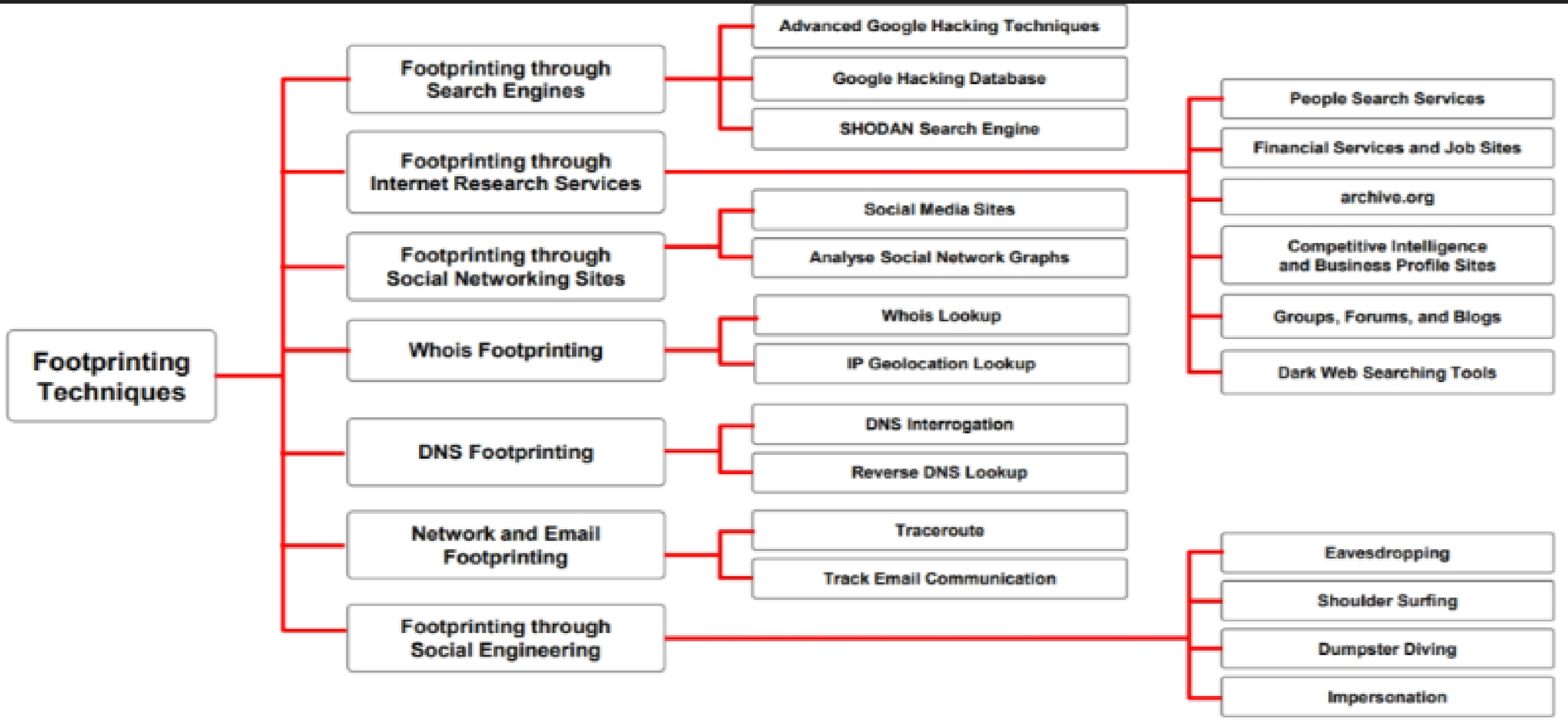
Network information

- Domain and sub-domains
- Network blocks
- Network topology, trusted routers, and firewalls
- IP addresses of the reachable systems
- Whois records
- DNS records

System information

- Web server OS
- Location of web servers
- Publicly available email addresses
- Usernames and passwords

Footprinting Methodology



LO#02: Demonstrate Footprinting through Search Engines

Footprinting through Search Engines

- Attackers use search engines to extract information about a target, such as employed technology platforms, employee details, login pages, and intranet portals, which help the attacker to perform social engineering and other types of advanced system attacks

- Major search engines:

Google Bing YAHOO! Ask Aol. Baidu 百度 DuckDuckGo

- Attackers can use advanced search operators available with these search engines and create complex queries to find, filter, and sort specific information about the target

- Search engines are also used to find other sources of publically accessible information resources, e.g., you can type "top job portals" to find major job portals that provide critical information about the target organization

Footprinting Using Advanced Google Hacking Techniques

- Attackers use search engines to **extract information about a target**, such as employed technology platforms, employee details, login pages, and intranet portals, which help the attacker to perform social engineering and other types of advanced system attacks
- Google hacking refers to the use of advanced Google search operators for **creating complex search queries** to extract sensitive or hidden information that helps attackers **find vulnerable targets**

Popular Google advanced search operators

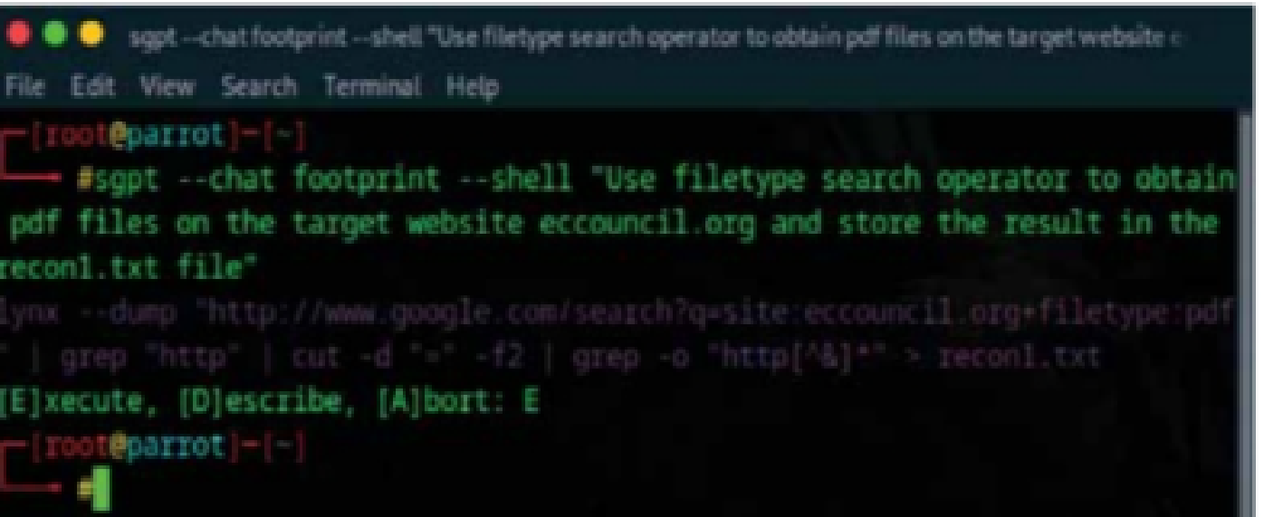
Search Operator	Purpose
[cache:]	Displays the web pages stored in the Google cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are similar to the specified web page
[info:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain

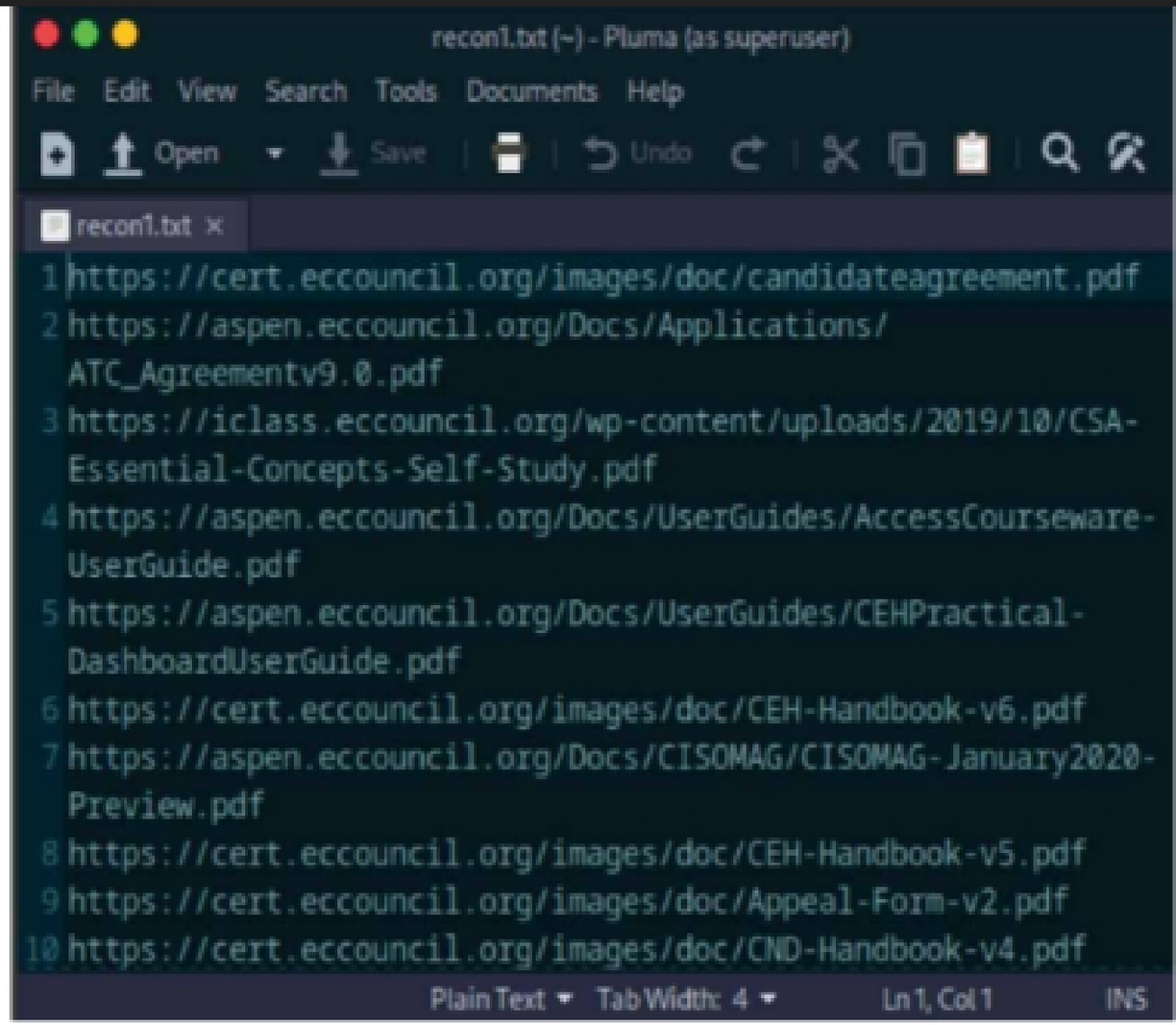
Search Operator	Purpose
[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[location:]	Finds information for a specific location

Footprinting Using Advanced Google Hacking Techniques with AI

- An attacker can also leverage **AI-powered ChatGPT** or other generative AI technology to perform this task by using an appropriate prompt such as:

  "Use filetype search operator to obtain pdf files on the target website eccouncil.org and store the result in the recon1.txt file"

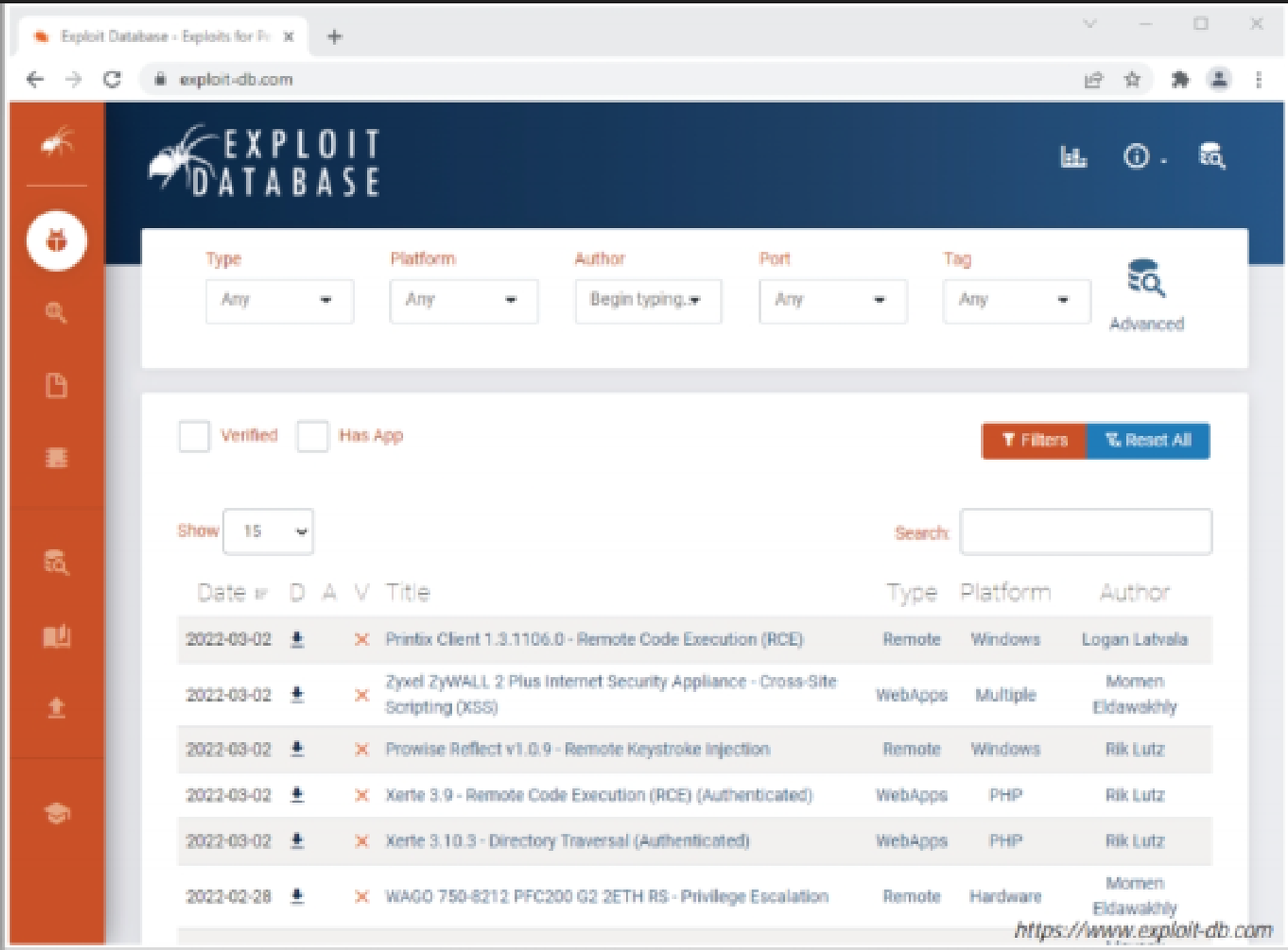




Google Hacking Database

- The Google Hacking Database (GHDB) is an authoritative source for querying the ever-widening reach of the Google search engine
- Attackers use Google dorks in Google advanced search operators to extract sensitive information about their target, such as vulnerable servers, error messages, sensitive files, login pages, and websites

EXPLOIT DATABASE



https://www.exploit-db.com

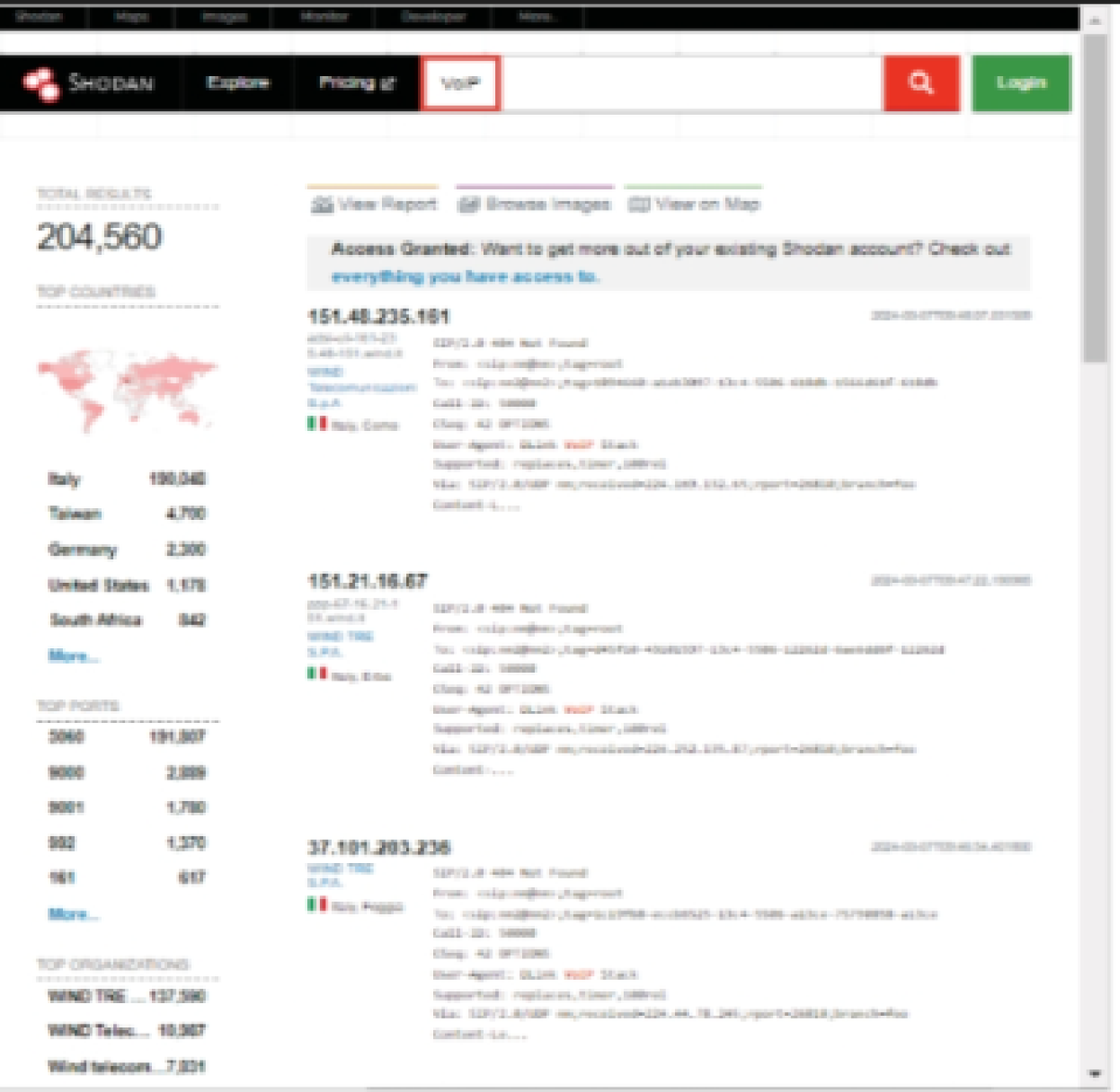
VPN Footprinting through Google Hacking Database

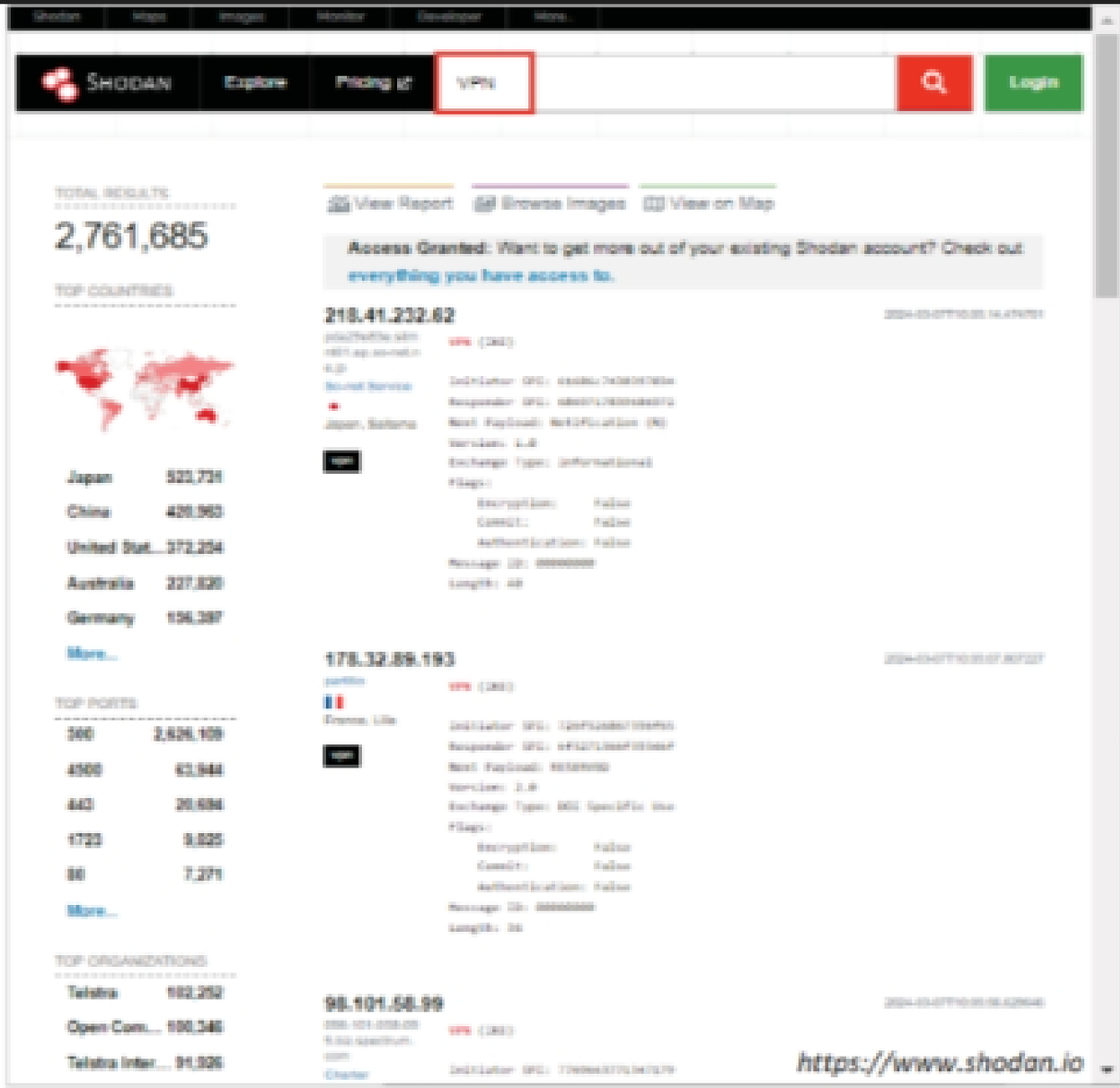
Google Dork	Description
inurl:"/sslvpn_logon.shtml" intitle:"User Authentication" "WatchGuard Technologies"	Finds pages containing login portals
inurl:/sslvpn/Login/Login	Finds VPN login portals
site:vpn.*.*/ intitle:"login"	
intext:Please Login SSL VPN inurl:remote/login intext:FortiClient	Finds Fortinet VPN login pages
site:vpn.*.*/ intext:"login" intitle:"login"	Retrieves various VPN login pages
intitle:"index of" /etc/openvpn/	Retrieves juicy information and sensitive directories
"-----BEGIN OpenVPN Static key V1-----" ext:key	Finds OpenVPN static keys
intitle:"index of" "vpn-config.*"	Retrieves juicy information about the vpn-config file
Index of / *.ovpn	Finds OpenVPN configuration files, some certificates, and keys
inurl:"/vpn/tmindex.html" vpn	Finds Netscaler and Citrix Gateway VPN login portals
intitle:"SSL VPN Service" + intext:"Your system administrator provided the following information to help understand and remedy the security conditions:"	Finds Cisco ASA login web pages

Other Techniques for Footprinting through Search Engines

Footprinting Technique	Description	Information Gathered	Tools Used
Google Advanced Search	Provides the same precision as that achieved with advanced operators but without typing or remembering the operators	List of sites that may link back to the target organization's website	Google Advanced Search
Advanced Image Search			Google Advance Image Search
Reverse Image Search	Uses an image as a search query	Original source and details of images, such as photographs, profile pictures, and memes	Google Image Search, TinEye Reverse Image Search, and Yahoo Image Search
Video Search Engines	Search for video content related to the target	Hidden information such as time/date and thumbnails	YouTube Metadata, YouTube DataViewer, and EZGif
Meta Search Engines	Use other search engines (Google, Bing, Ask.com, etc.) to produce their own results from the Internet	Detailed information about the target, such as images, videos, blogs, and news articles, from different sources	Startpage and MetaGer
FTP Search Engines	Search for files located on FTP servers	Critical files and directories that reveal valuable information, such as business strategy, tax documents, and employees' personal records	NAPALM FTP Indexer and FreewareWeb FTP File Search
IoT Search Engines	Crawl the Internet for IoT devices that are publicly accessible	Manufacturer details, geographical location, IP address, hostname, and open ports of IoT devices	Shodan, Censys, and Thingful

Footprinting through SHODAN Search Engine

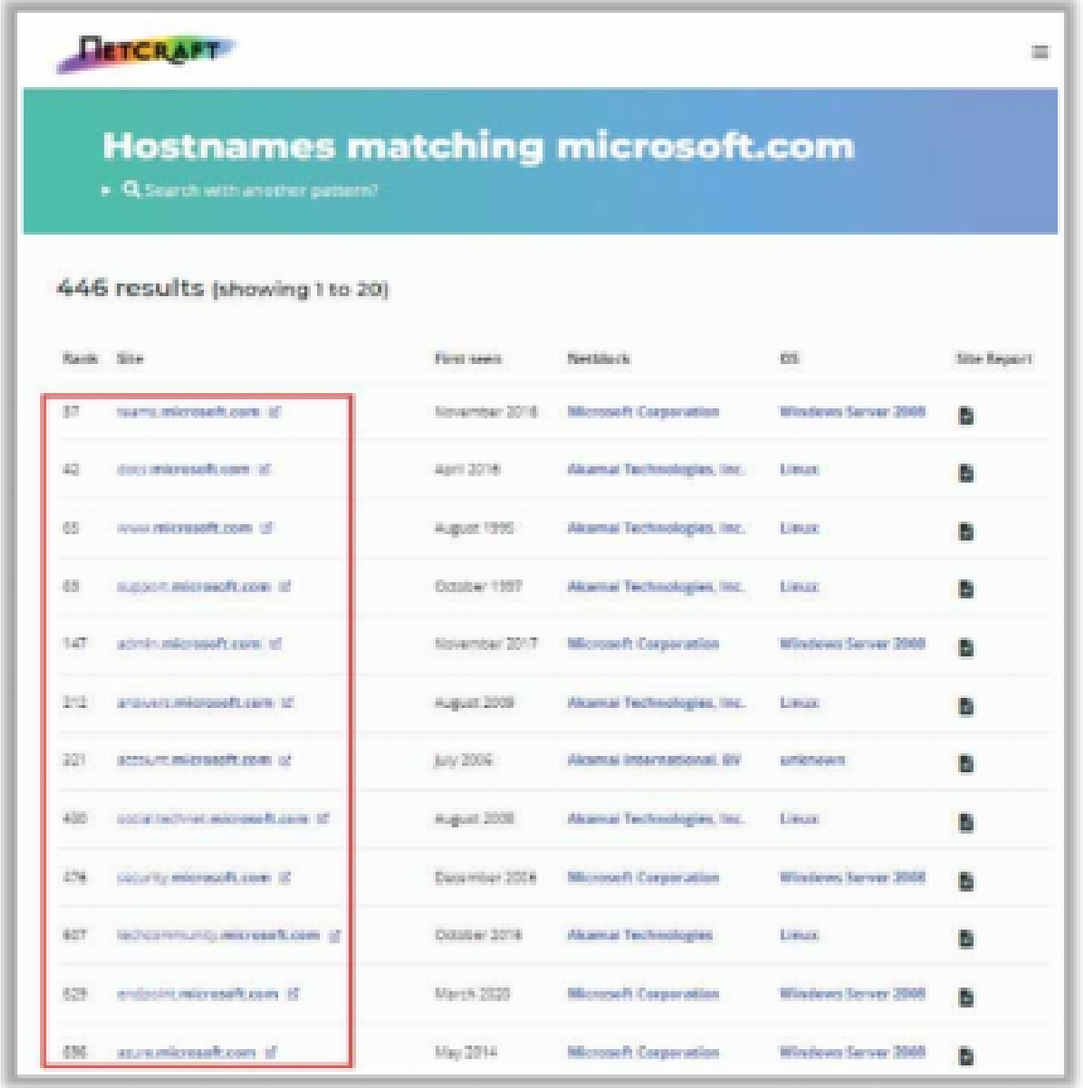




LO#03: Demonstrate Footprinting through Internet Research Services

Finding a Company's Top-Level Domains (TLDs) and Sub-domains

- Search for the target company's external URL in a search engine, such as Google and Bing
- Sub-domains provide an insight into different departments and business units in an organization
- You may find a company's sub-domains by trial and error method or using a service such as https://www.netcraft.com
- You can use the Sublist3r python script, which enumerates subdomains across multiple sources at once



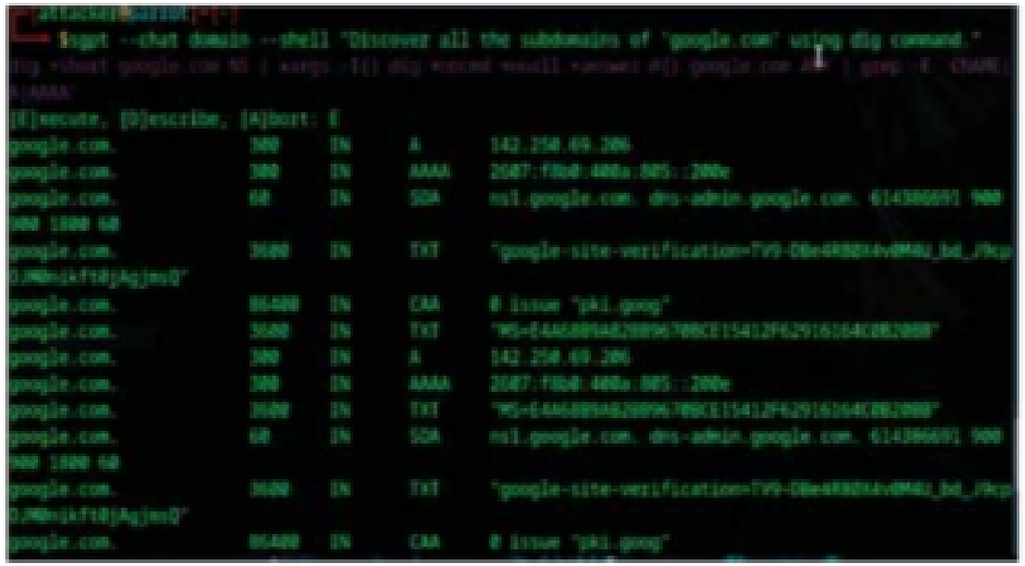
https://www.netcraft.com

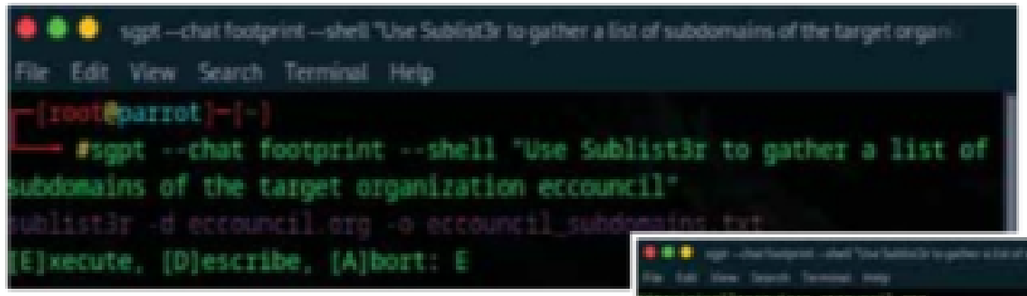
https://github.com

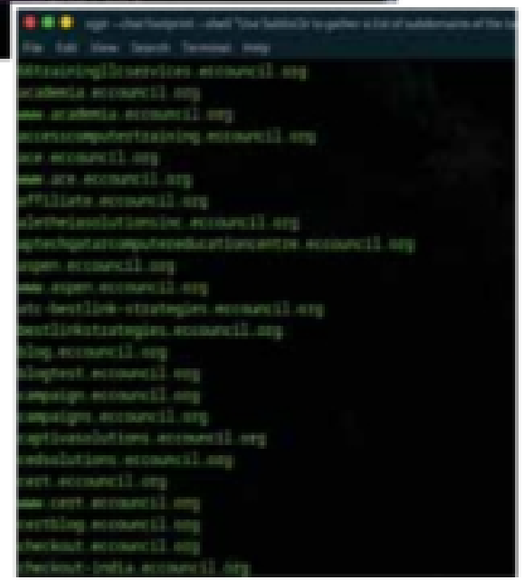
Finding a Company's Top-Level Domains (TLDs) and Sub-domains with AI

An attacker can also leverage **AI-powered ChatGPT** or other generative AI technology to perform this task by using appropriate prompts such as

1. ***"Discover all the subdomains of 'google.com' using dig command"***
2. ***"Use Sublist3r to gather a list of subdomains of the target organization eccouncil"***

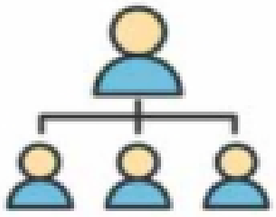


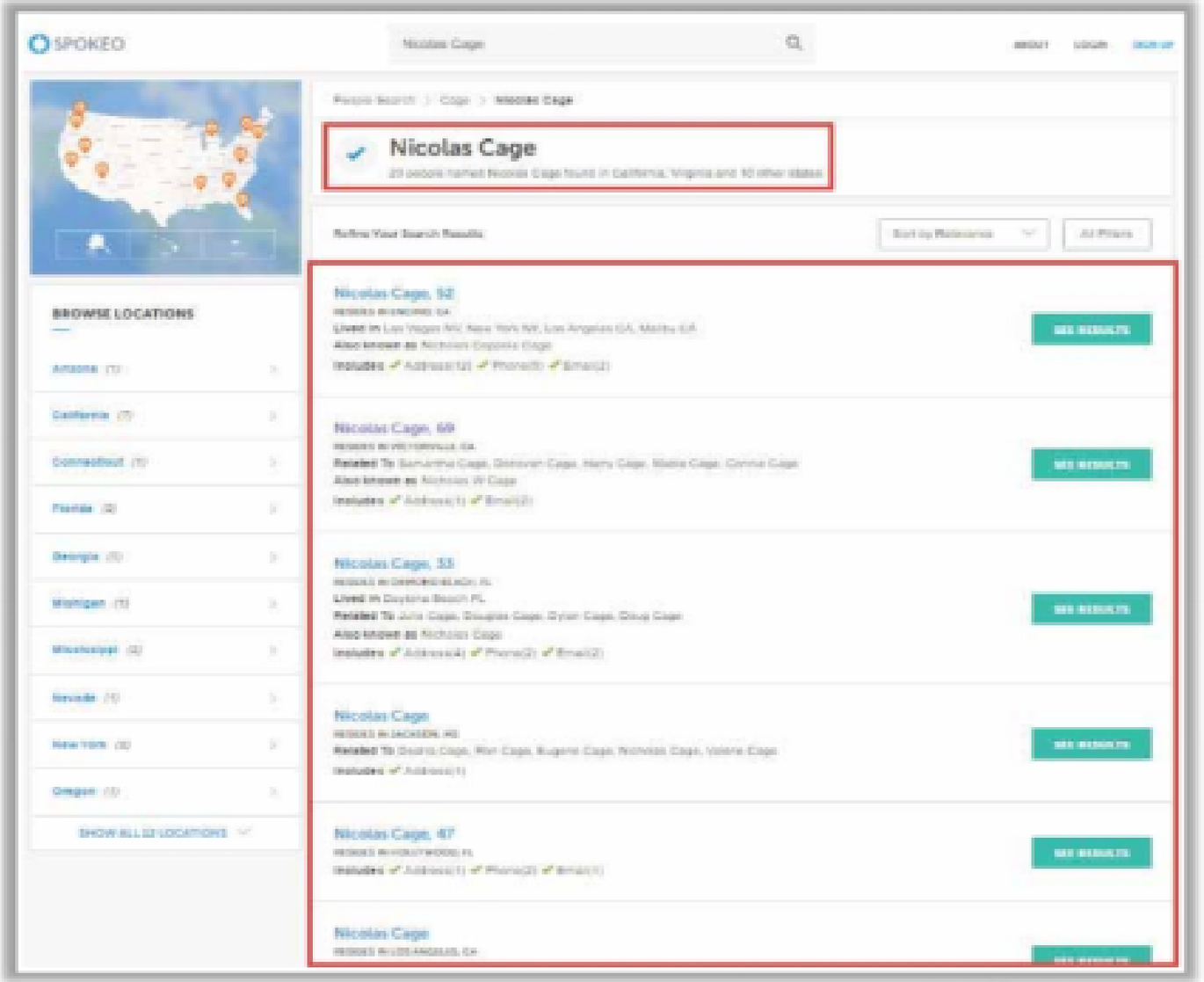




People Search on Social Networking Sites and People Search Services

- Social networking services, such as Facebook, Twitter, and LinkedIn, provide **useful information about the individual** that helps the attacker in performing social engineering and other attacks
- The people search can provide critical **information about a person or an organization**, including location, emails, websites, blogs, contacts, important dates, etc.
- People search online services, such as **Spokeo**, **Intelius**, **pipl**, **BeenVerified**, **Whitepages**, and **PeekYou**, provide people's names, addresses, contact details, date of birth, photographs, videos, profession, and so on

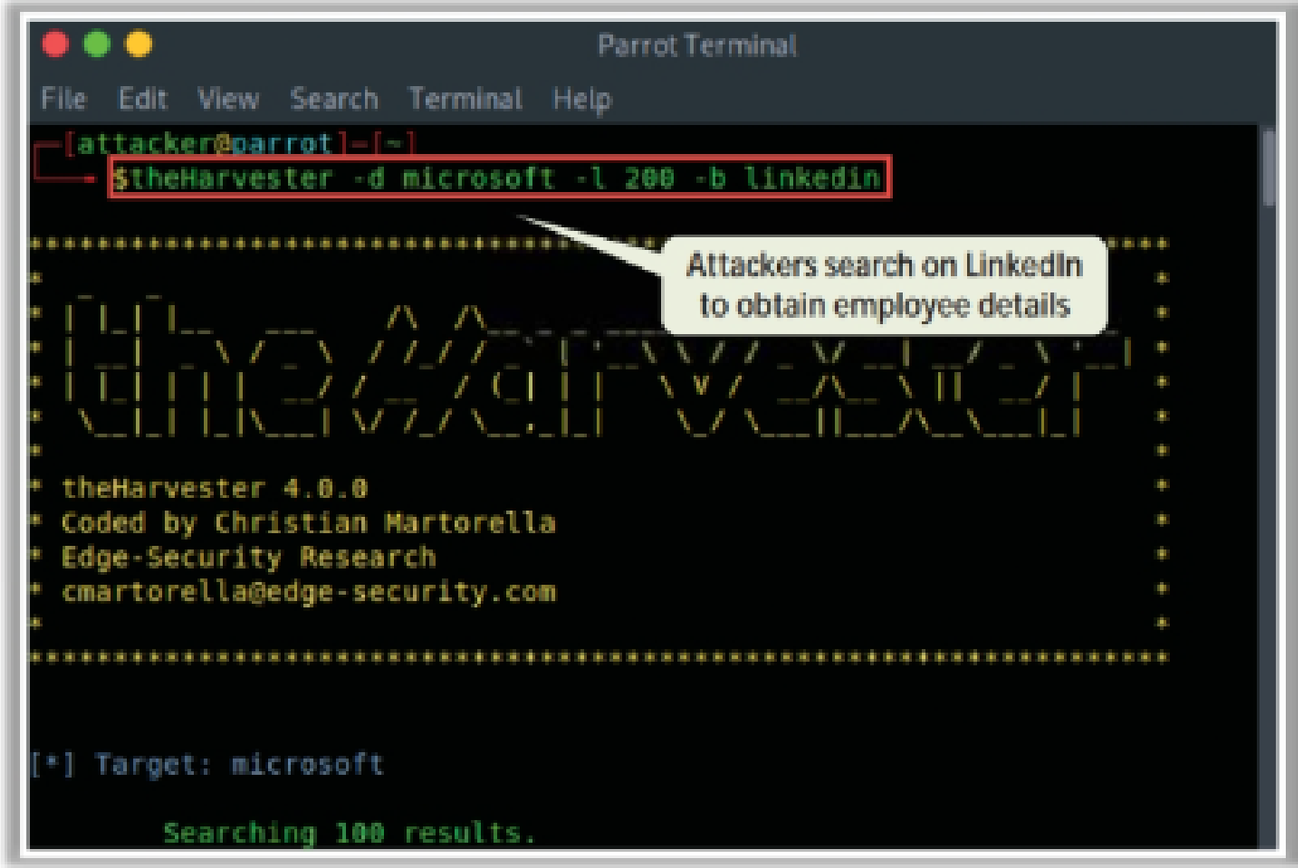


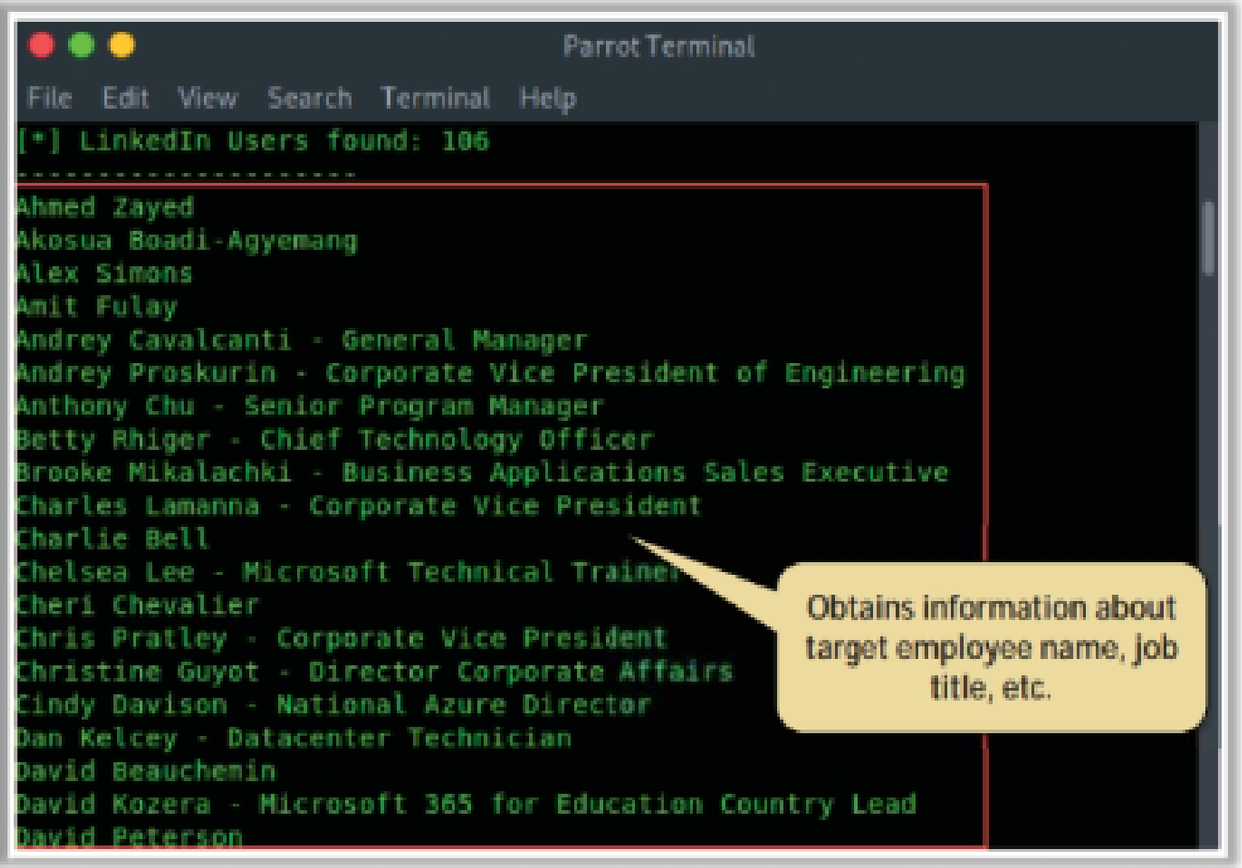


https://www.spokeo.com

Gathering Information from LinkedIn

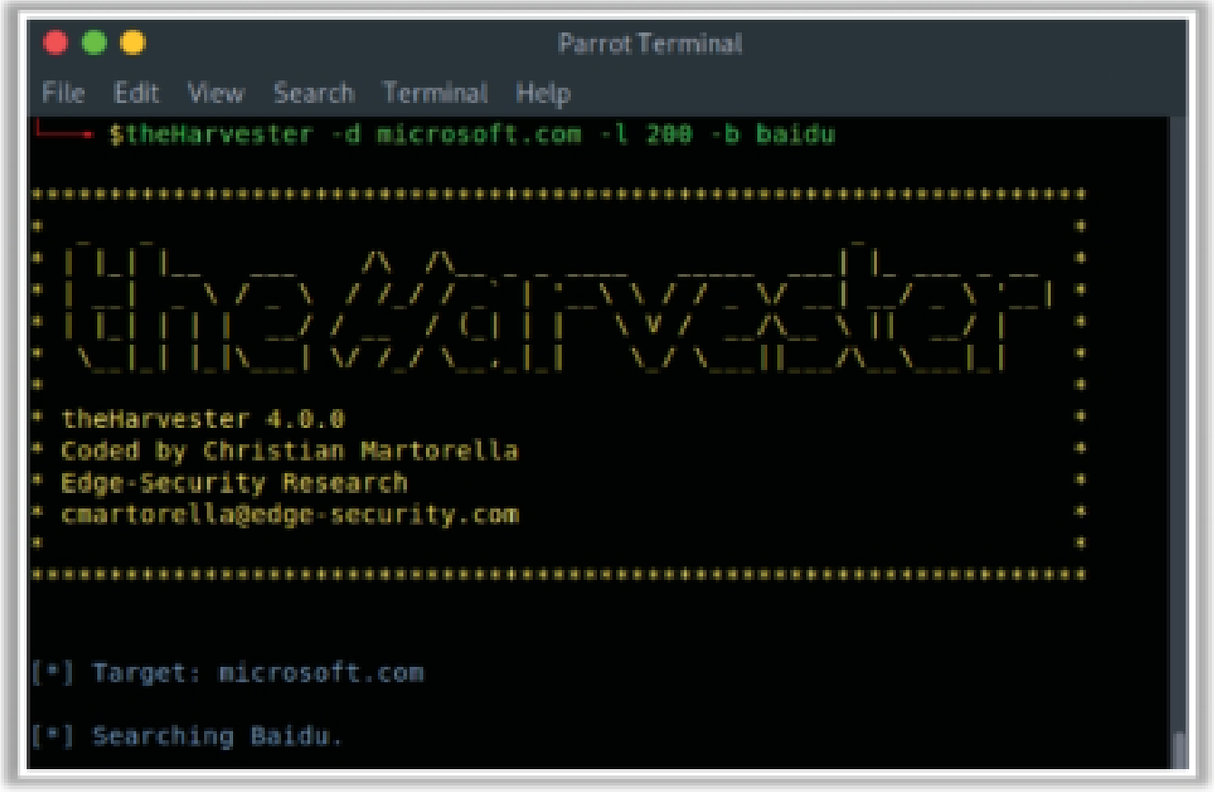
- Attackers use theHarvester tool to perform enumeration on LinkedIn and find employees of the target company along with their job titles
- Attackers can use this information to gather more information, such as current location and educational qualifications, and perform social engineering or other kinds of attacks

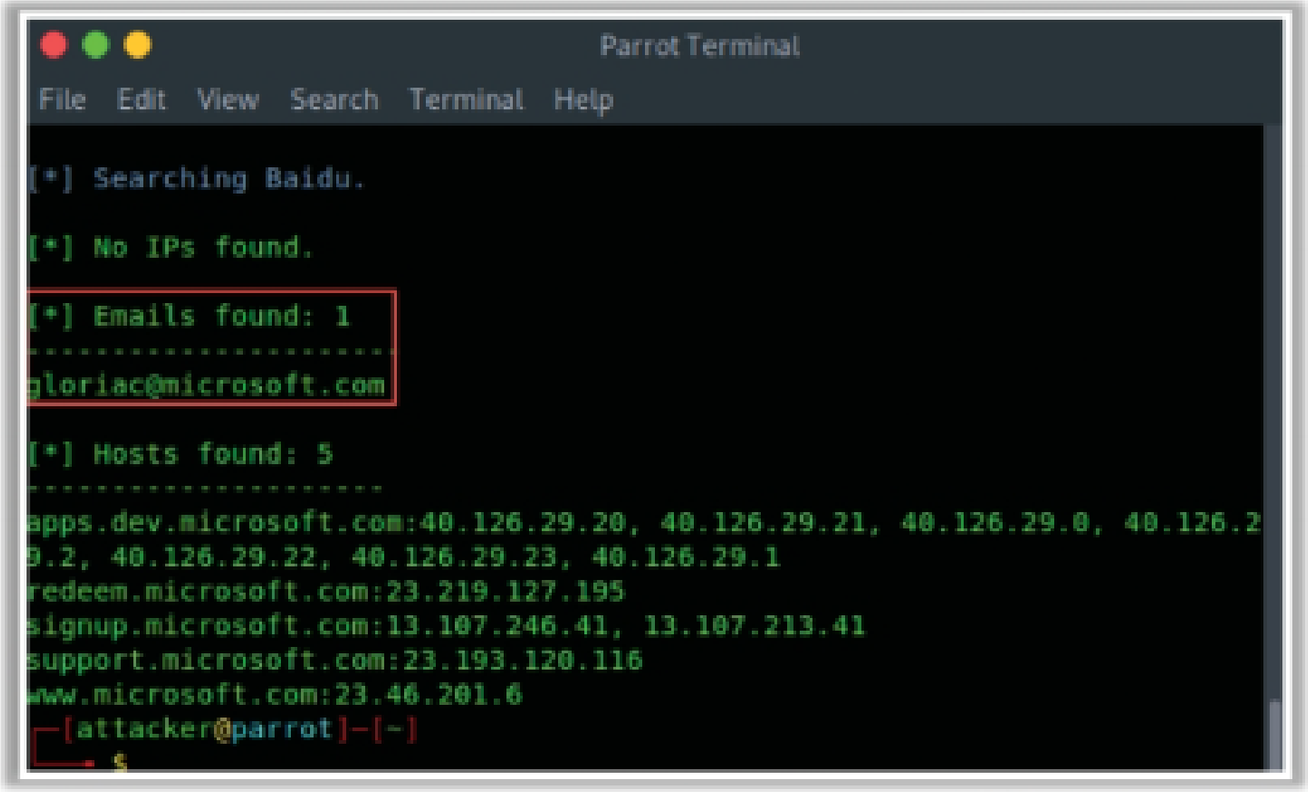




Harvesting Email Lists

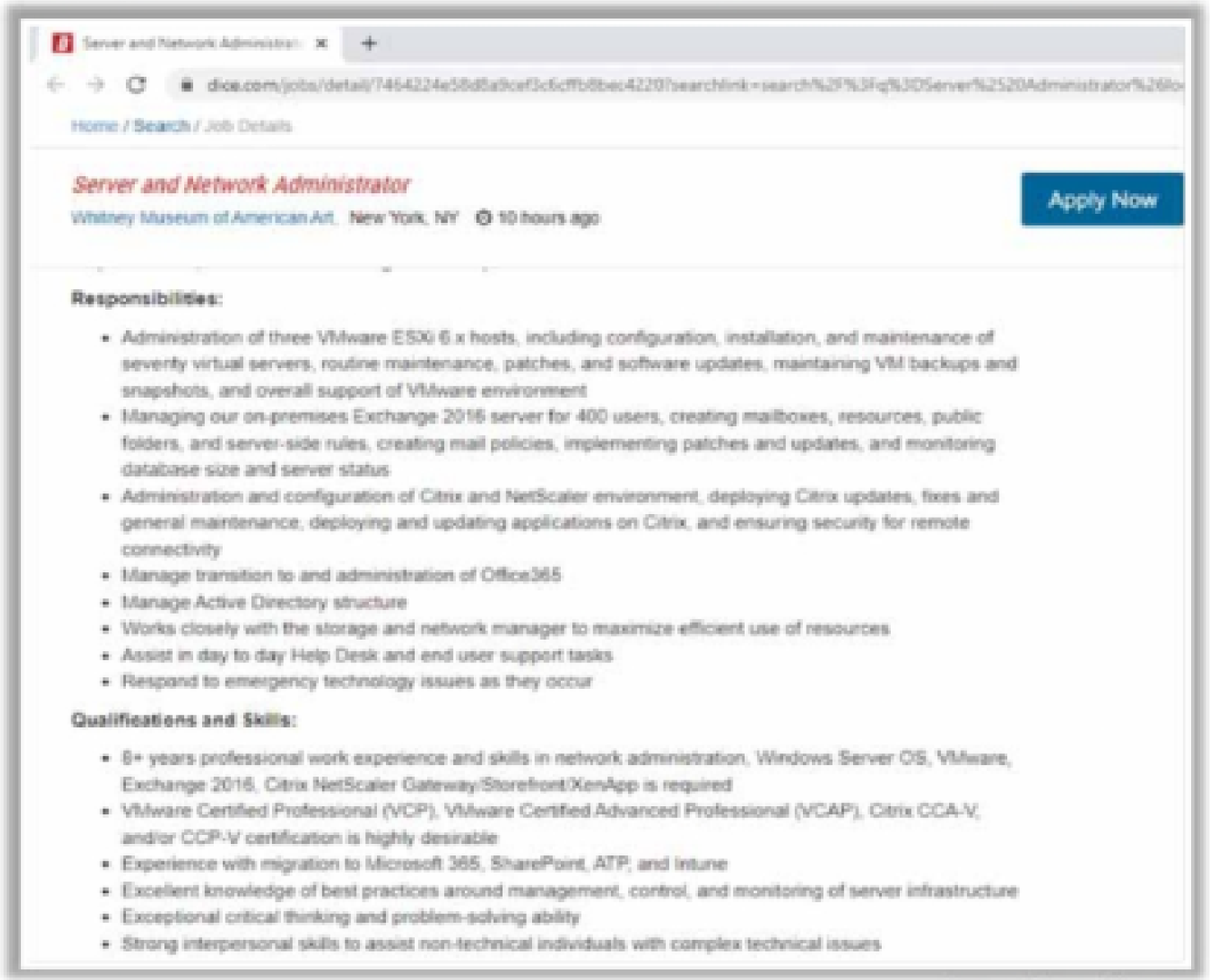
- Gathering email addresses related to the target organization acts as an important attack vector during the later phases of hacking
- Attackers use automated tools such as theHarvester and Email Spider to collect publicly available email addresses of the target organization that helps them perform social engineering and brute-force attacks





Footprinting through Job Sites

company's infrastructure details can be gathered from job postings



https://www.dice.com

Look for these:

- Job requirements
- Employees' profiles
- Hardware information
- Software information

- Attackers use the technical information obtained through job sites, such as Dice, LinkedIn, and Simply Hired, to detect underlying vulnerabilities in the target IT infrastructure

Deep and Dark Web Footprinting

Deep web

- It consists of web pages and contents that are hidden and unindexed and cannot be located using traditional web browsers and search engines
- It can be accessed by search engines like Tor Browser and The WWW Virtual Library

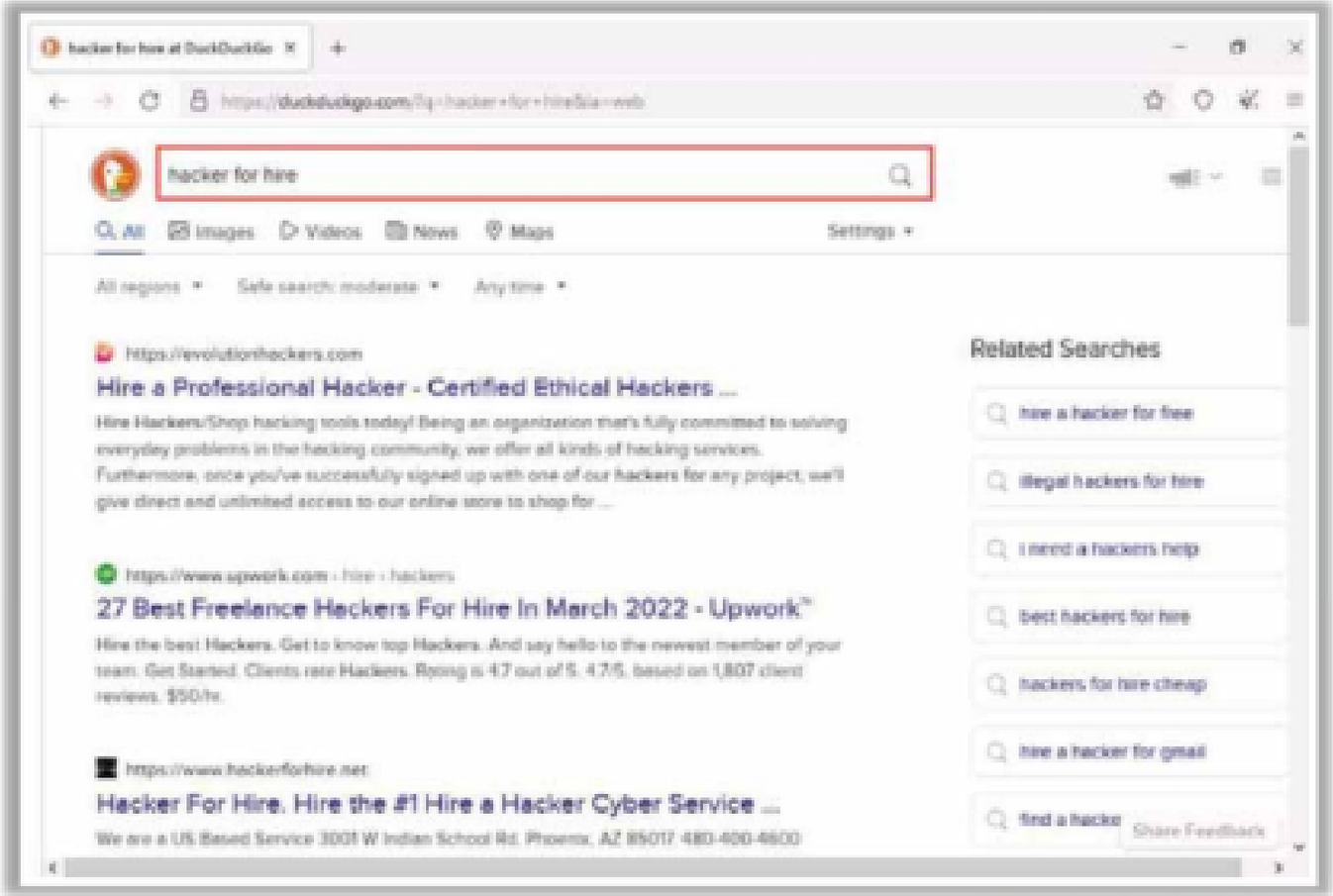
Dark web or Darknet

- It is the subset of the deep web that enables anyone to navigate anonymously without being traced
- It can be accessed by browsers, such as TOR Browser, Freenet, GNUnet, I2P, and Retroshare

- Attackers use deep and dark web searching tools, such as Tor Browser and ExoneraTor, to gather confidential information about the target, including credit card details, passport information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

TOR Browser

It is used to access the deep and dark web where it acts as a default VPN for the user and bounces the network IP address through several servers before interacting with the web



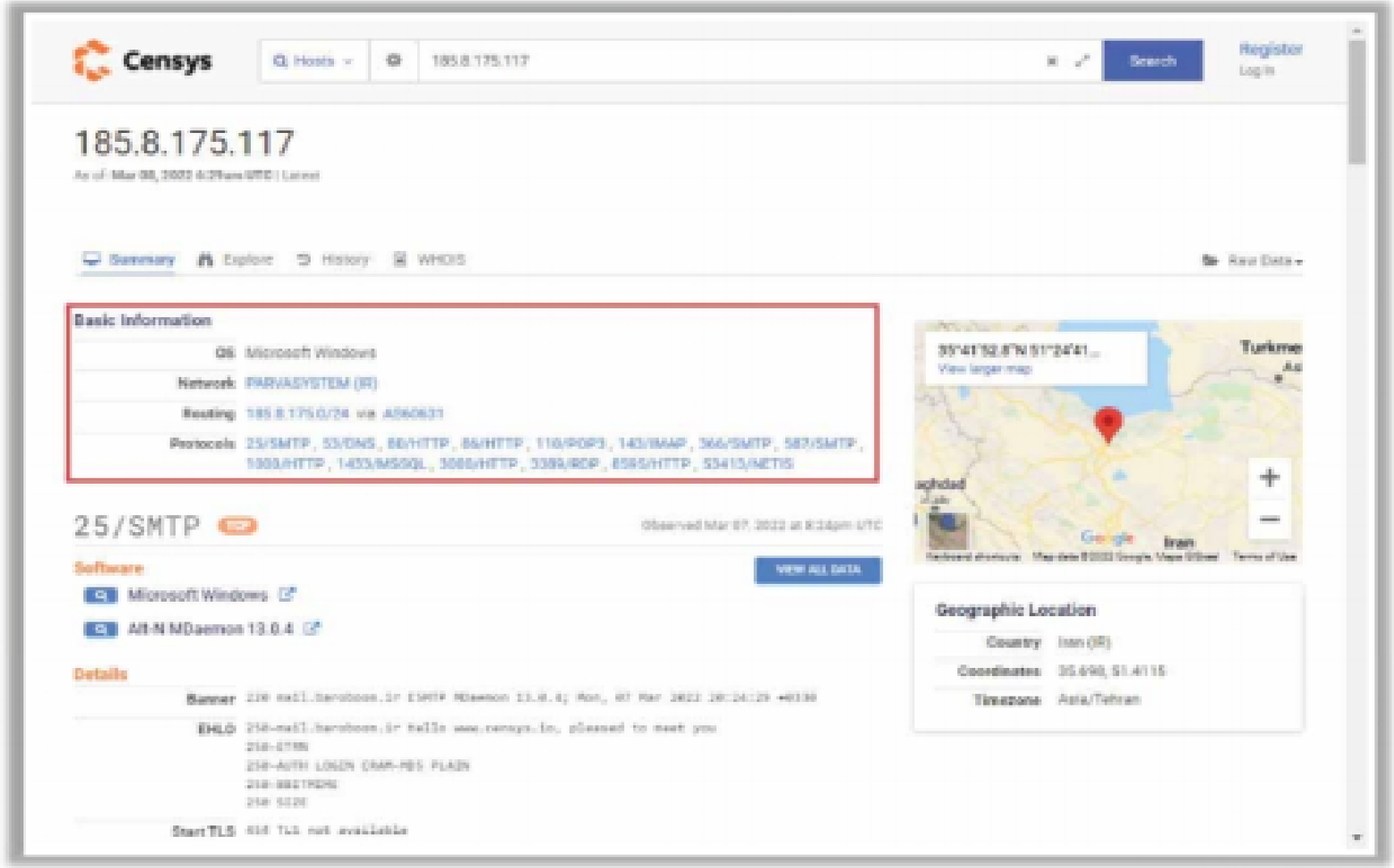
https://www.torproject.org

Determining the Operating System

- SHODAN search engine lets you find connected devices (routers, servers, IoT, etc.) using a variety of filters

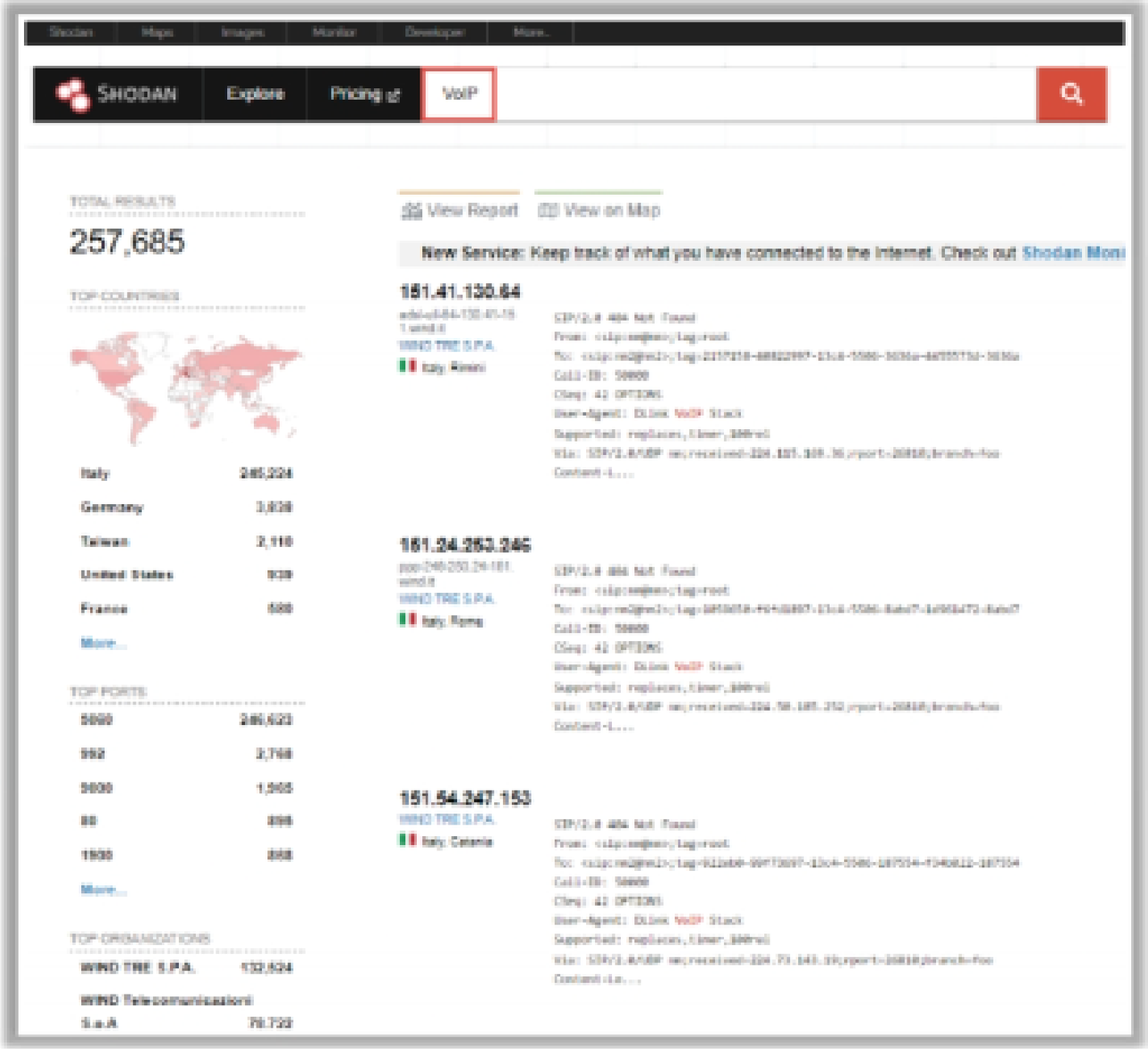
https://www.shodan.io

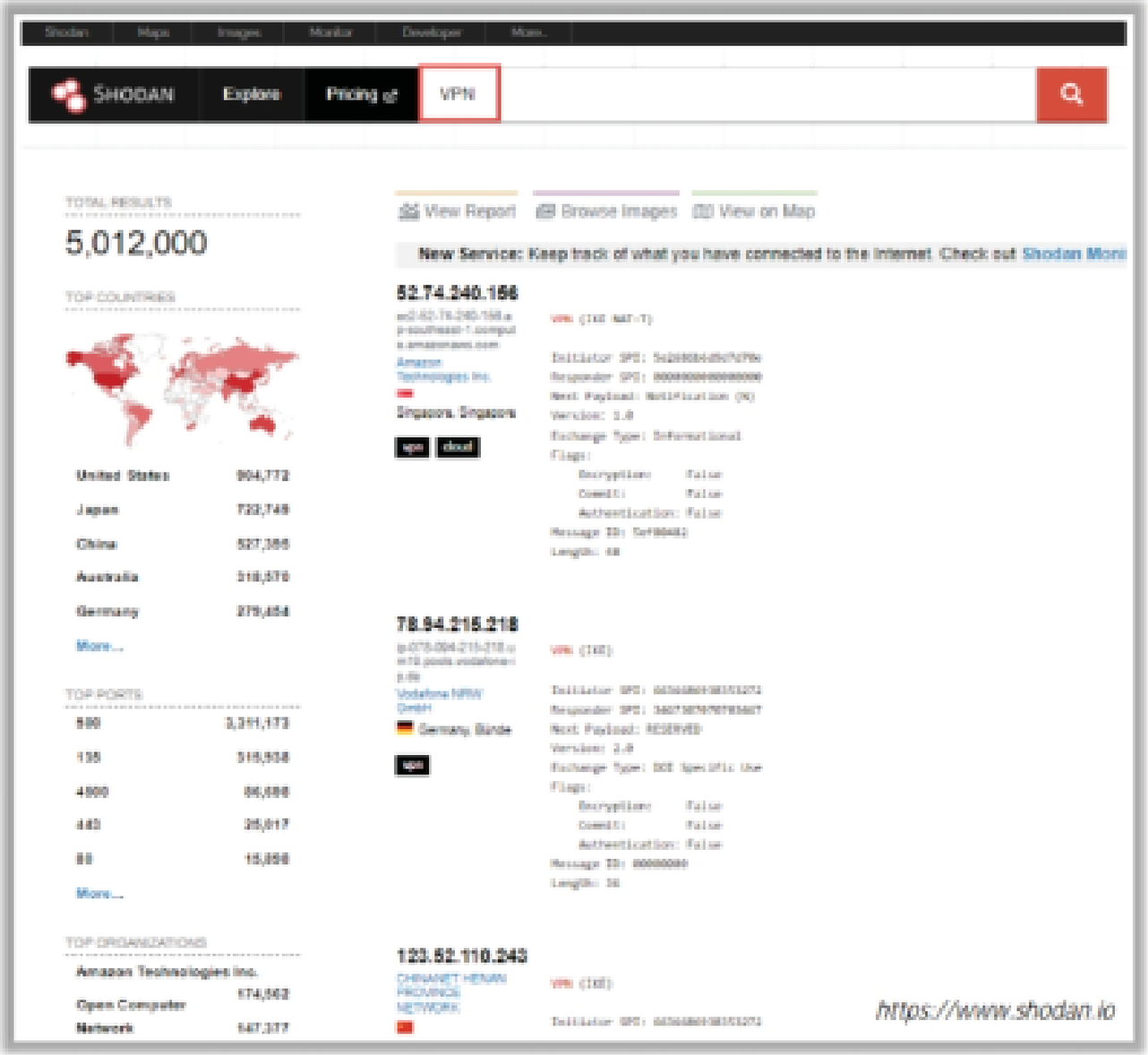
- Censys search engine provides a full view of every server and device exposed to the Internet



https://censys.io

VoIP and VPN Footprinting through SHODAN





Competitive Intelligence Gathering

- Competitive intelligence gathering is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources, such as the Internet
- Competitive intelligence is non-interfering and subtle in nature

Sources of Competitive Intelligence

1. Company websites and employment ads
2. Search engines, Internet, and online database
3. Press releases and annual reports
4. Trade journals, conferences, and newspapers
5. Patent and trademarks
6. Social engineering employees
7. Product catalogs and retail outlets
8. Analyst and regulatory reports
9. Customer and vendor interviews
10. Agents, distributors, and suppliers

Competitive Intelligence Gathering…

When Did this Company Begin? How Did it Develop?

- Information Resource Sites
  - EDGAR Database
    https://www.sec.gov/edgar.shtml
  - D & B Hoovers
    https://www.dnb.com
  - LexisNexis
    https://www.lexisnexis.com
  - Business Wire
    http://www.businesswire.com

What Are the Company's Plans?

- Information Resource Sites
  - MarketWatch
    https://www.marketwatch.com
  - The Wall Street Transcript
    https://www.twst.com
  - Euromonitor
    https://www.euromonitor.com
  - Experian
    https://www.experian.com

What Expert Opinions Say About the Company?

- Information Resource Sites
  - SEMRush
    https://www.semrush.com
  - ABI/INFORM Global
    https://www.proquest.com
  - SimilarWeb
    https://www.similarweb.com
  - SERanking
    https://seranking.com

Other Techniques for Footprinting through Web Services

Footprinting Technique	Description	Information Gathered	Tools Used
Finding the Geographical Location of the Target	Obtain the physical location of the target	Entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, etc.	Google Earth, Google Maps, and Wikimapia
Gathering Information from Financial Services	Search for financial data such as stock quotes and charts, financial news, and portfolios	Market value of a company's shares, company profile, and competitor details	Google Finance, MSN Money, and Yahoo! Finance
Gathering Information from Business Profile Sites	Retrieve business information of companies located in a particular region	Location, addresses, contact information, and employee database of the target organization	opencorporates, Crunchbase, and corporationwiki
Monitoring Targets Using Alerts	Obtain up-to-date information of the target, usually via email or SMS	Mentions of the organization's name, member names, website, or any of its people or projects	Google Alerts, Twitter Alerts, and Giga Alerts
Tracking the Online Reputation of the Target	Monitor a company's reputation on the Internet	Search engine ranking information, email notifications when a company is mentioned online, and social news about the company	Mention, ReviewPush, and Reputology
Gathering Information from Groups, Forums, and Blogs	Join the target organization's employee groups, where they share personal and company information	Public network information, system information, and personal information	Google Groups and Yahoo! Groups
Gathering Information from NNTP Usenet Newsgroups	Retrieve messages on various subjects and topics that are submitted by users over the Internet	Operating systems, software, web servers, etc. used by the target organization	Newshosting, Eweka, and Supernews
Gathering Information from Public Source-Code Repositories	Identify information about the developers and technologies used	Configuration files, private SSH and SSL keys, source-code files, dynamic libraries, and software tools developed by contributors	Recon-ng

LO#04: Demonstrate Footprinting through Social Networking Sites

Collecting Information through Social Engineering on Social Networking Sites

- Attackers use **social engineering tricks** to gather sensitive information from social networking websites
- Attackers create a **fake profile** and then use the false identity to lure employees into revealing their sensitive information
- Attackers collect information about the employees' **interests** and tricks them into revealing more information

What Users Do	What Attacker Gets
Maintain profile	Contact info, location, etc.
Connect to friends, chat	Friends list, friends' info, etc.
Share photos and videos	Identity of family members, interests, etc.
Play games, join groups	Interests
Create events	Activities

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Recruitment	Platform/technology
Background check to hire employees	Type of business

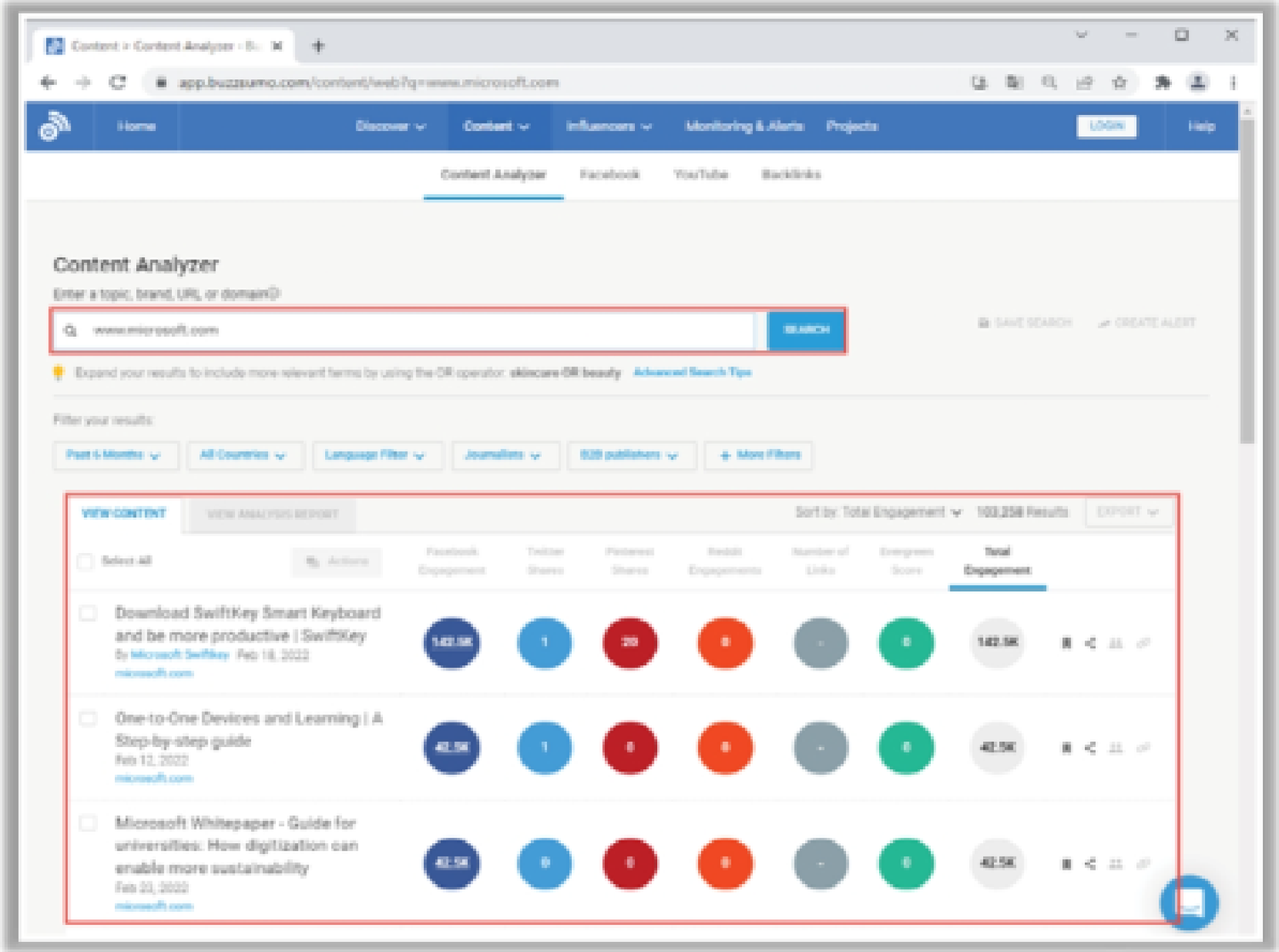
General Resources for Locating Information from Social Media Sites

- Attackers track social media sites using BuzzSumo, Google Trend, Hashatit, etc. to discover most shared content using hashtags or keywords, track accounts and URLs, email addresses, etc.

- Attackers use this information to perform phishing, social engineering, and other types of attacks

BuzzSumo

BuzzSumo's advanced social search engine finds the most shared content for a topic, author or a domain



https://buzzsumo.com

Conducting Location Search on Social Media Sites

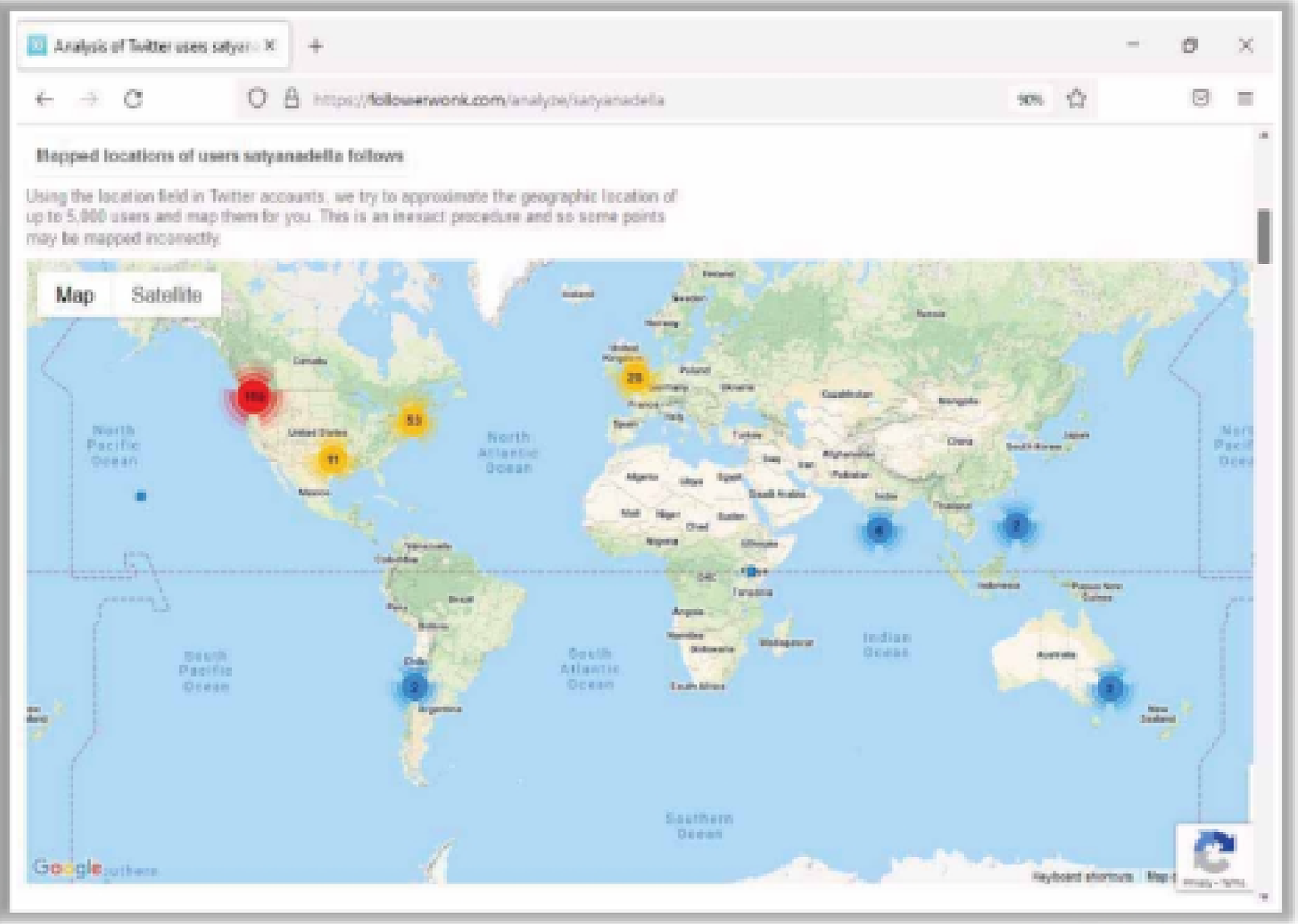
- Conducting location search on social media sites, such as Twitter, Instagram, and Facebook, helps attackers in detecting the geolocation of the target

- Attackers use online tools, such as Followerwonk, Hootsuite, and Meltwater, to search for both geotagged and non-geotagged information about the target on social media sites

- Attackers use this information to perform various social engineering and non-technical attacks

Followerwonk

Followerwonk helps to explore and grow one's social graph by digging deeper into Twitter analytics



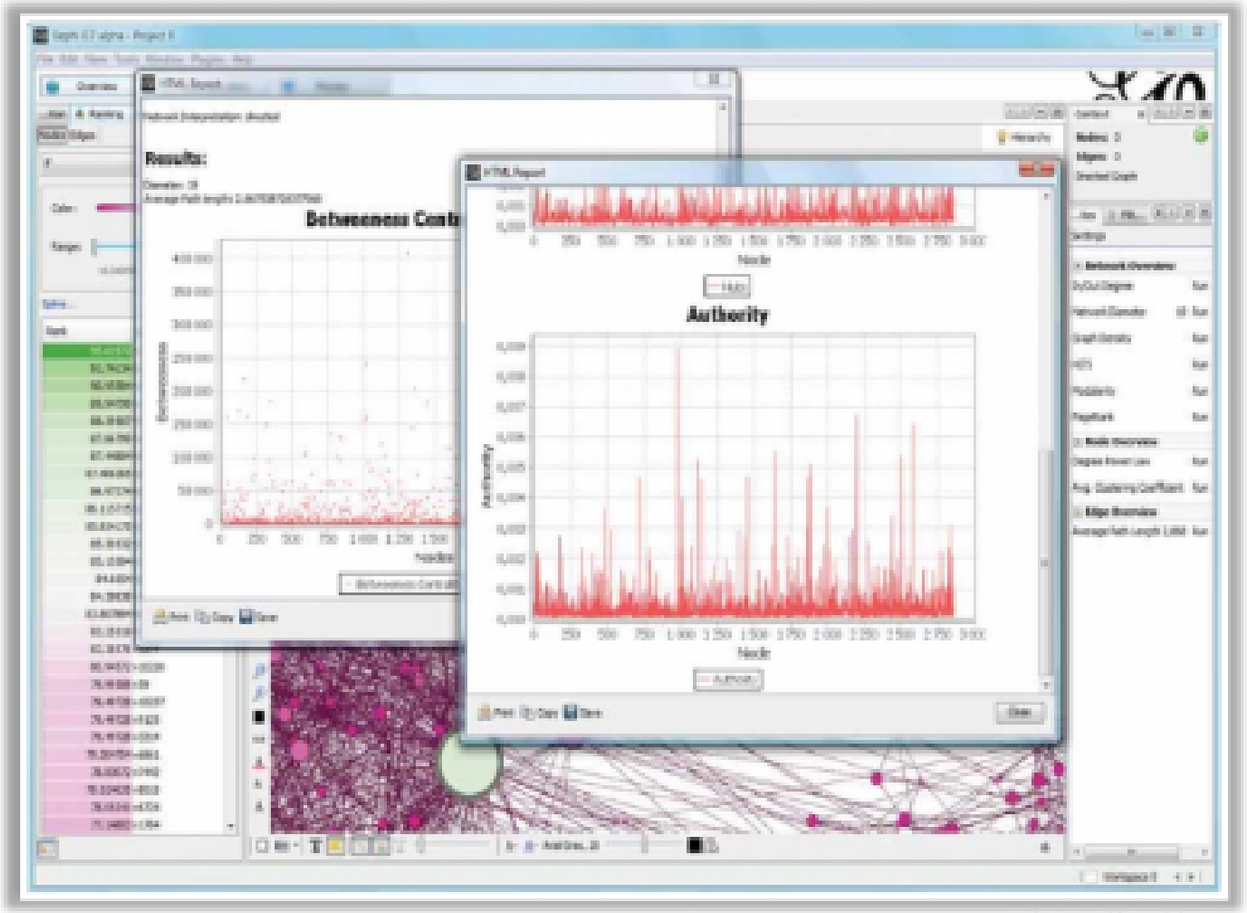
https://followerwonk.com

Constructing and Analyzing Social Network Graphs

- The construction of social network graphs involves representing various connections and relationships between people in the form of graphs to analyze and extract valuable information from various social networking connections

- Using graphical analysis, attackers can identify how a group of users communicate, what information they share, and their personal and professional interests

- Attackers use tools such as Gephi, SocNetV, and NodeXL to construct and analyze social networks and obtain critical information about the target organization/users

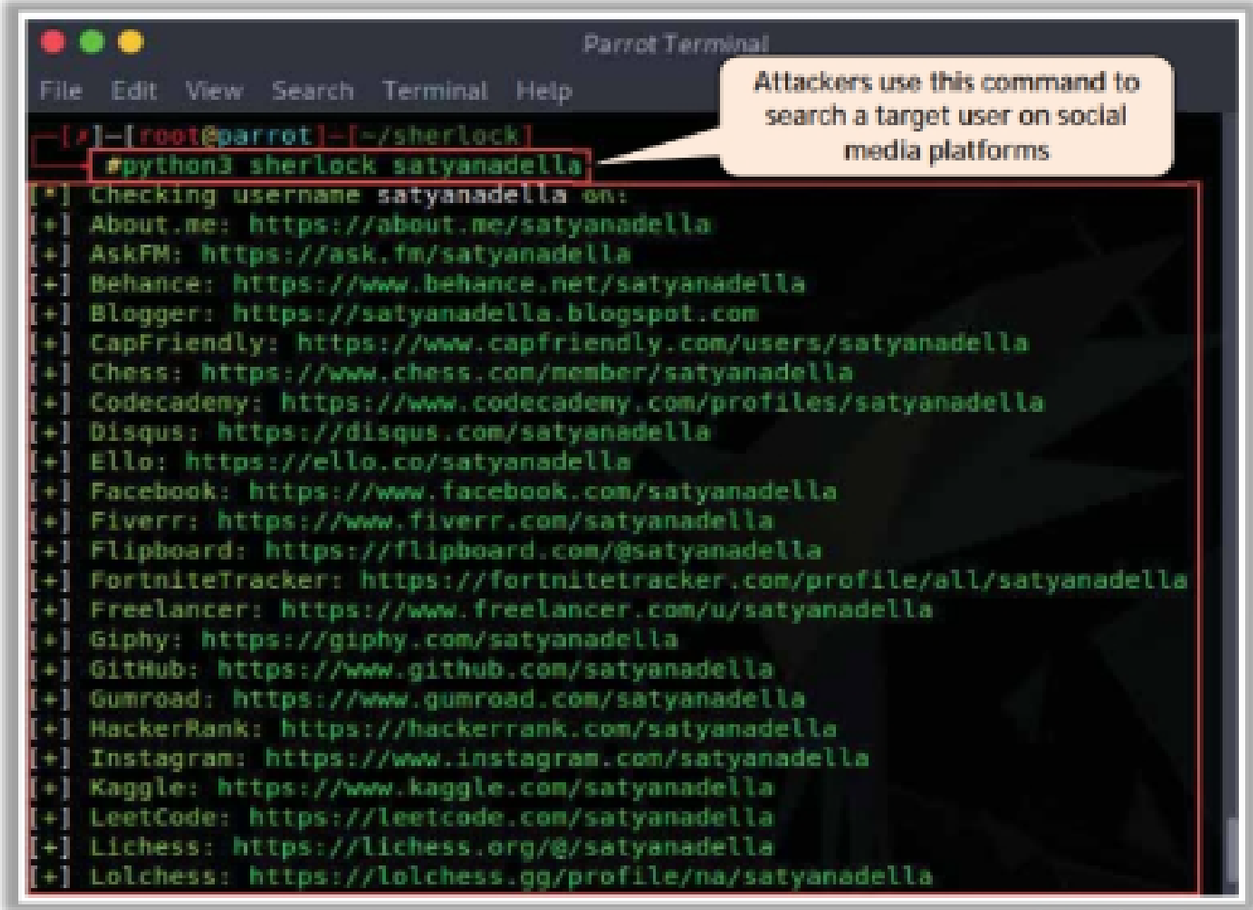


https://gephi.org

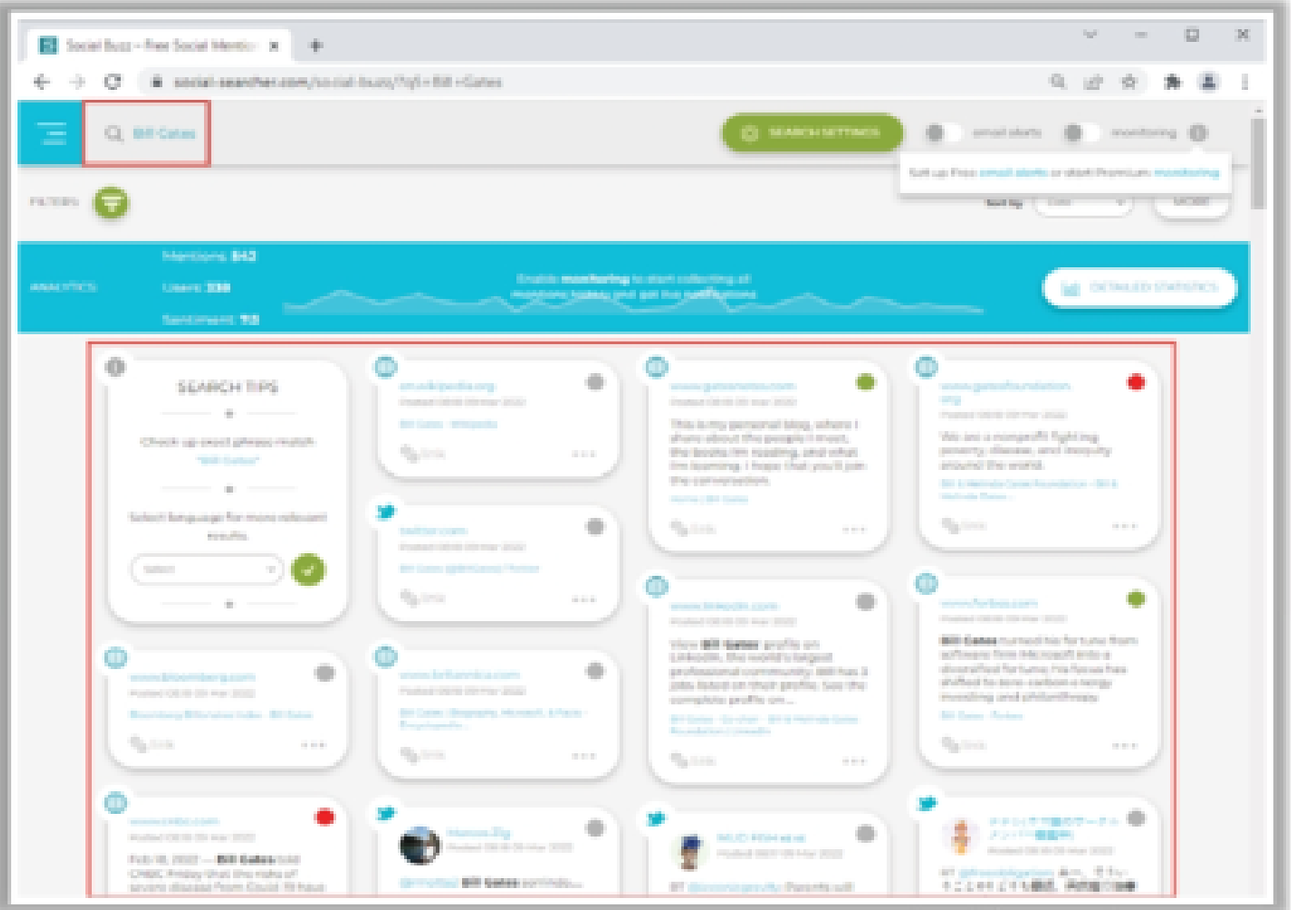
Tools for Footprinting through Social Networking Sites

Sherlock | Sherlock tool is used to search a vast number of social networking sites for a target username

Social Searcher | Social Searcher allows you to search for content in social networks in real-time and provides deep analytics data



https://github.com



https://www.social-searcher.com

LO#05: Use Different Techniques for Website Footprinting

Website Footprinting

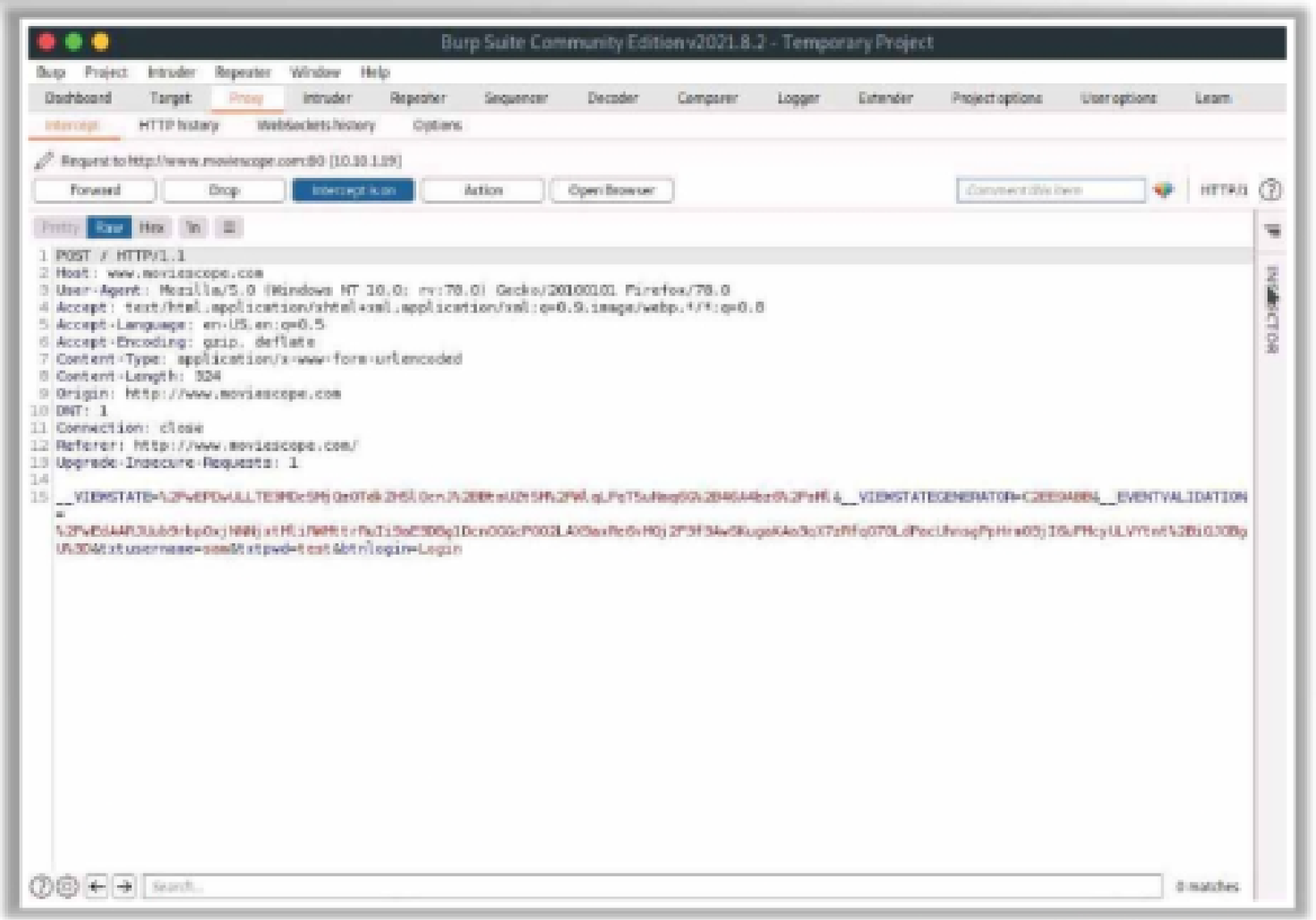
- Website footprinting refers to the monitoring and analysis of the target organization's website for information

Browsing the target website may provide the following information:

- Software used and its version
- Operating system used and its scripting platform
- Sub-directories and parameters
- Filename, path, database field name, or query
- Technologies used
- Contact and CMS details

Attackers use Burp Suite, Zaproxy, Wappalyzer, CentralOps, Website Informer, etc. to view headers that provide the following information:

- Connection status and content-type
- Accept-Ranges and Last-Modified
- X-Powered-By information
- Web server in use and its version



https://pentestlab.net

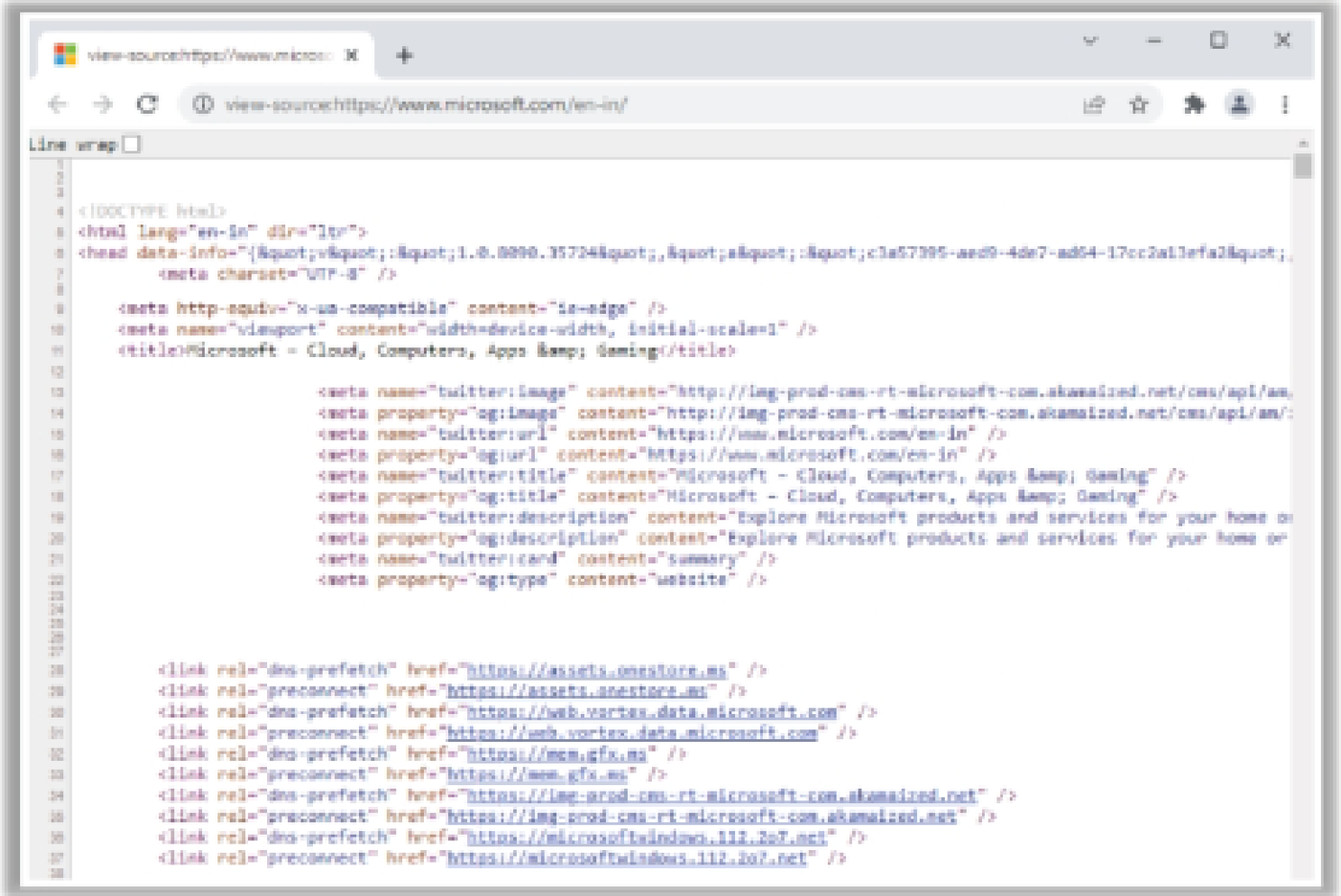
Website Footprinting

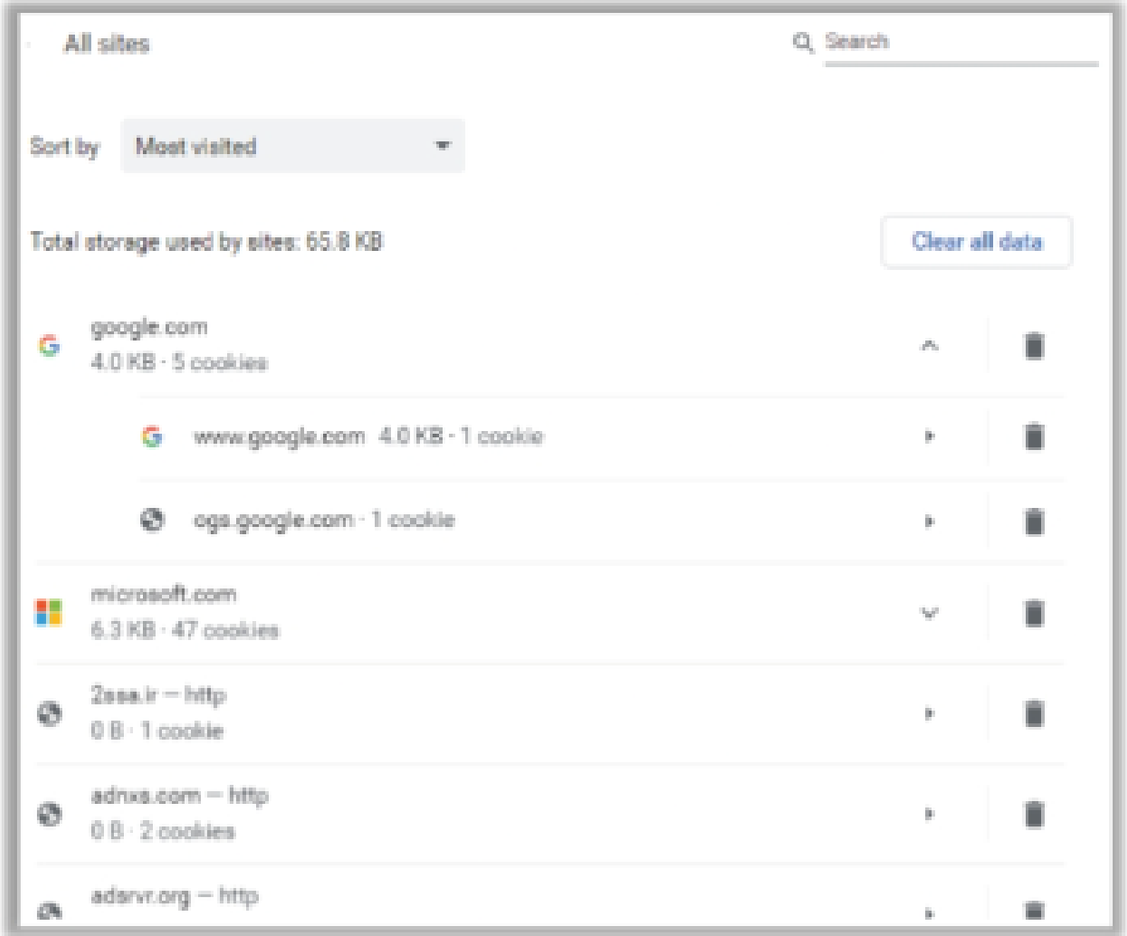
Examining the HTML source code may provide

- Comments present in the source code
- Contact details of the web developer or admin
- File system structure and script type

Examining cookies may provide

- Software in use and its behavior
- Scripting platforms used



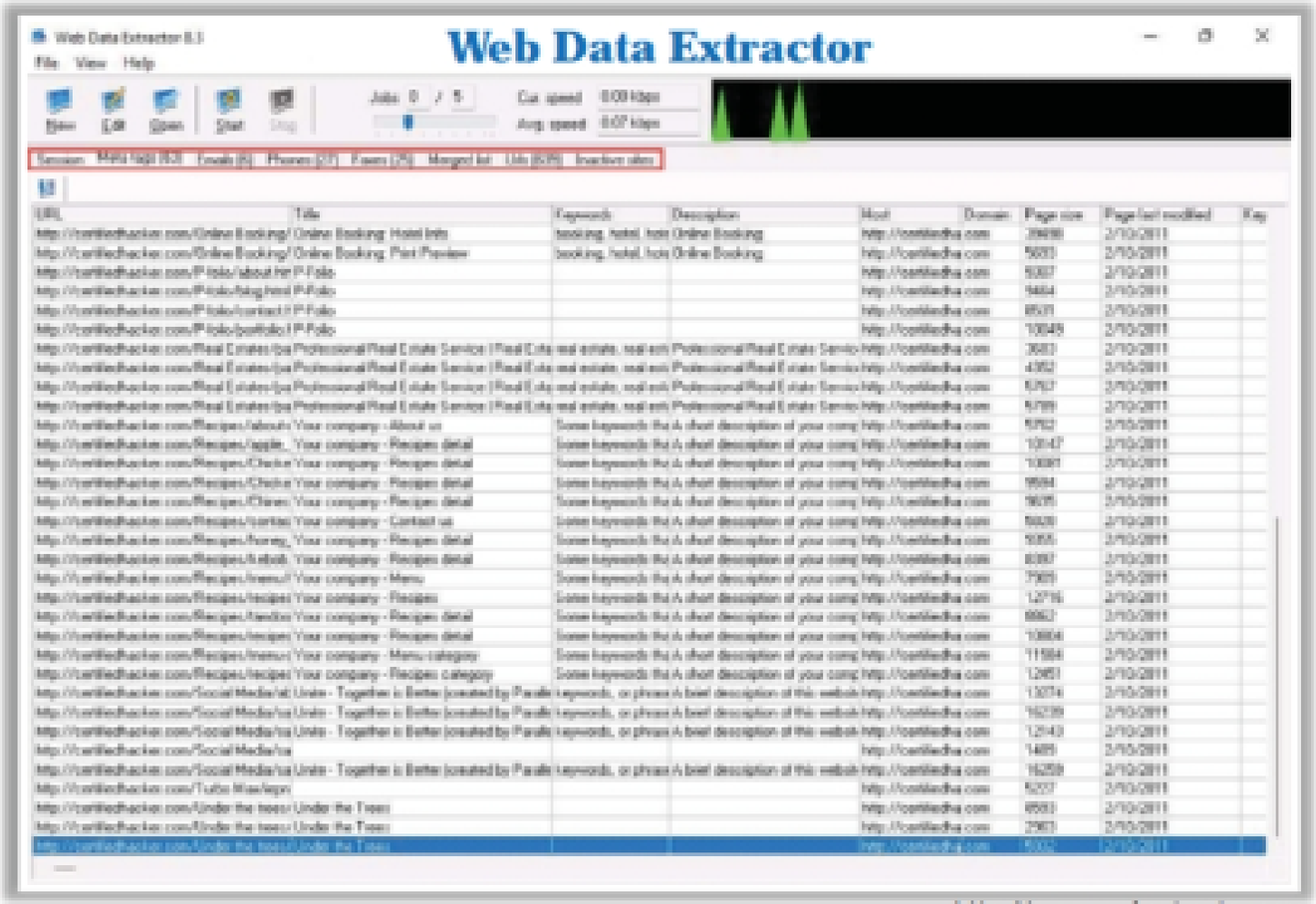


Website Footprinting using Web Spiders

- Web spiders, such as Web Data Extractor and ParseHub, perform automated searches on the target website and collect specified information, such as employee names and email addresses
- Attackers use the collected information to perform footprinting and social engineering attacks

User-Directed Spidering

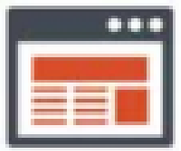
- Attackers use standard web browsers to walk through the target website functionalities
- The incoming and outgoing traffic of the target website is monitored and analyzed by tools that include features of both a web spider and an intercepting proxy
- Attackers use tools such as Burp Suite and WebScarab to perform user-directed spidering



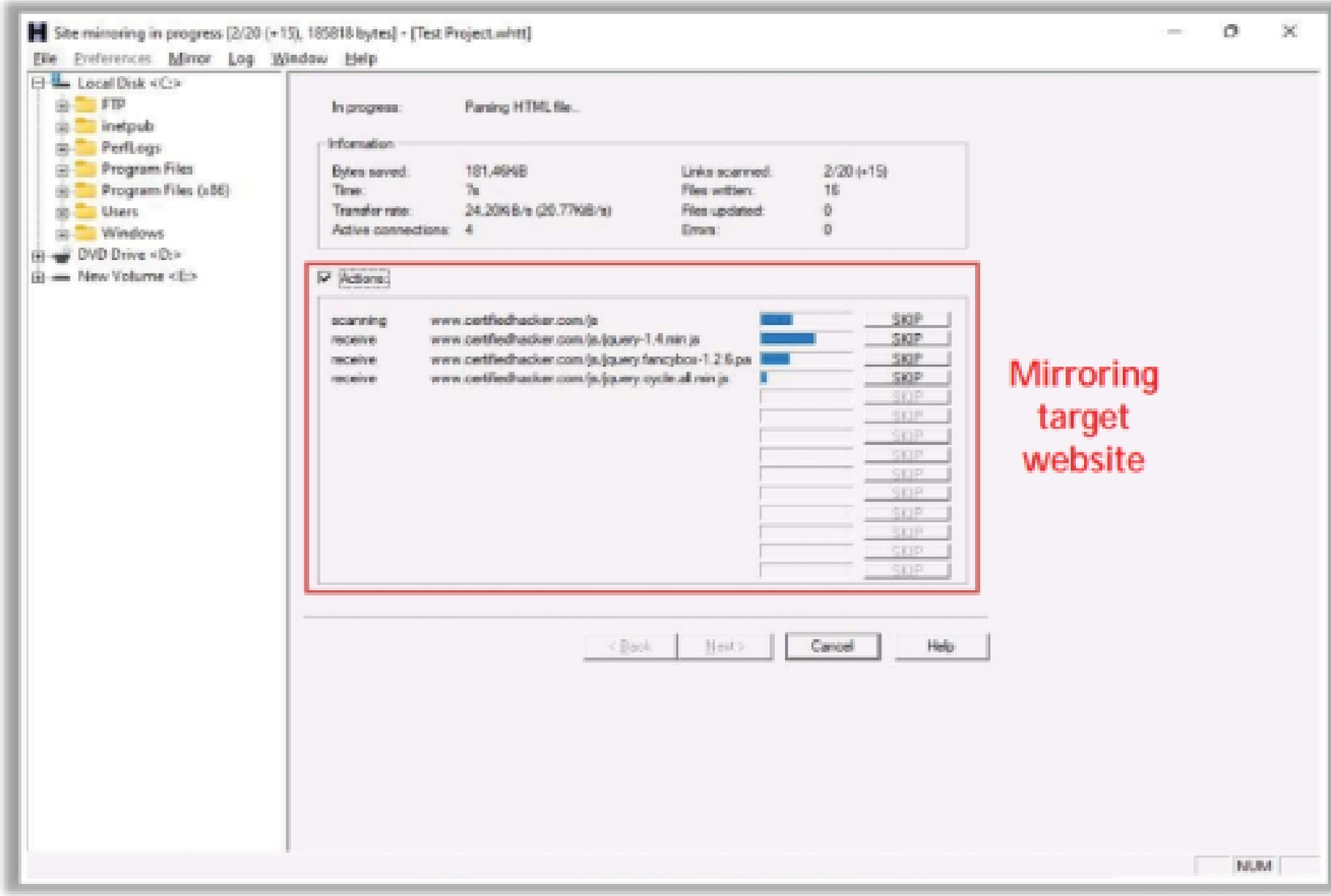
http://www.webextractor.com

Mirroring Entire Website

- Mirroring an entire website onto a local system enables an attacker to browse website offline; it also assists in finding directory structure and other valuable information from the mirrored copy without sending multiple requests to web server
- Web mirroring tools, such as HTTrack Web Site Copier, and Cyotek WebCopy, allow you to download a website to a local directory, recursively building all directories, HTML, images, flash, videos, and other files from the server to your computer



HTTrack Web Site Copier

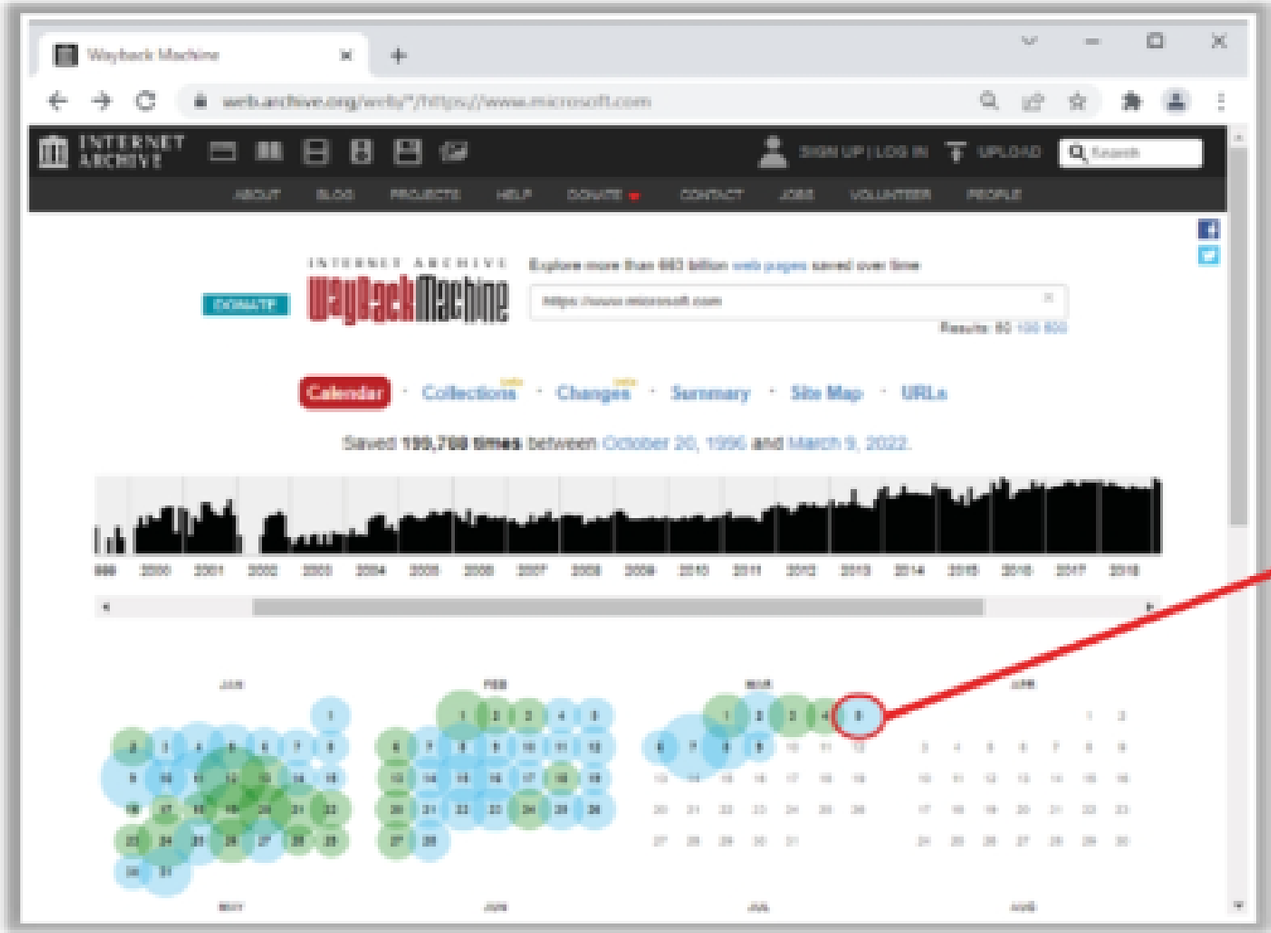


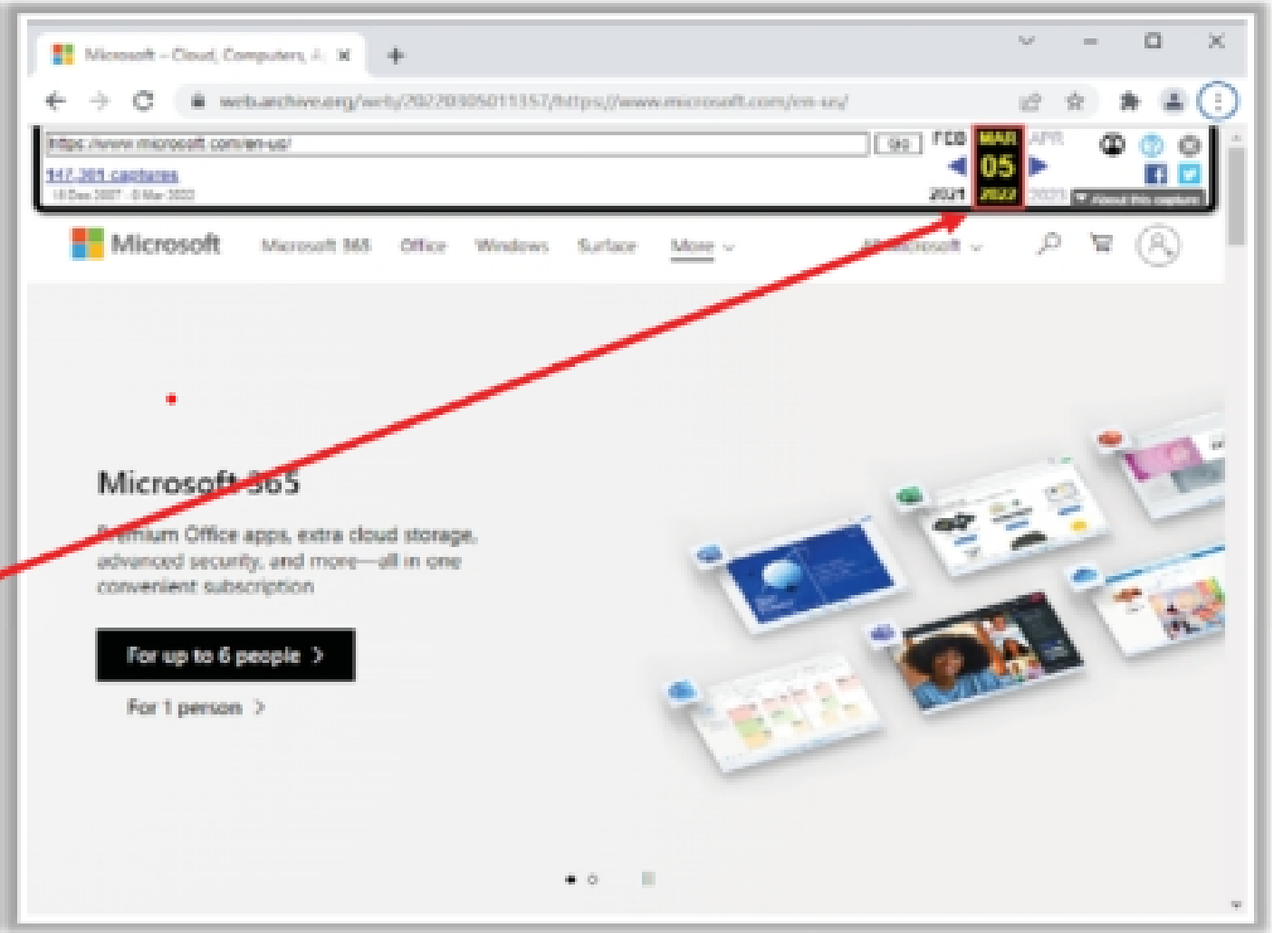
Mirroring target website

https://www.httrack.com

Extracting Website Information from https://archive.org

- Internet Archive's Wayback Machine allows one to visit archived versions of websites





- Attackers can use tools such as Photon to retrieve archived URLs of the target website from archive.org

Other Techniques for Website Footprinting

Footprinting Technique	Description	Information Gathered	Tools Used
Extracting Website Links	Analyze the target website to determine its internal and external links	Linked images, scripts, iframes, and URLs of the target website	Octoparse, Netpeak Spider, and Link Extractor
Gathering the Wordlist from the Target Website	Gather the wordlist available on the target website to brute-force the email addresses gathered through search engines, social networking sites, web spidering, etc.	List of words from the target website	CeWL
Extracting Metadata of Public Documents	Useful information may reside on the target website in the form of pdf documents, Microsoft Word files, etc.	Title of the page, description, keywords, creation/modification date and time of the content, and usernames and e-mail addresses of employees of the target organization	ExifTool, Web Data Extractor, and Metagoofil
Monitoring Web Pages for Updates and Changes	Detect changes or updates in the target website	Changes to the login pages, password-protected pages, software version and driver updates, and images	WebSite-Watcher, Visual Ping, and Follow That Page
Searching for Contact Information, Email Addresses, and Telephone Numbers from Company Website	Search the target company's website to gather crucial information about the company	Contact details, location, partner information, news, and links to other sites	Target website
Searching for Web Pages Posting Patterns and Revision Numbers	Search for copyright notices and revision numbers on the web	Copyright symbol, year of creation, name of the author, and a rights statement	Web search
Monitoring Website Traffic of the Target Company	Collect information about the target's customer base	Total visitors, page views, bounce rate, live visitor map, site ranking, and customer locations	Web-Stat, Rank Tracker, and TeamViewer

Deep and Dark Web Footprinting

Deep web

- It consists of web pages and contents that are hidden and unindexed and cannot be located using traditional web browsers and search engines
- It can be accessed by search engines like Tor Browser and The WWW Virtual Library

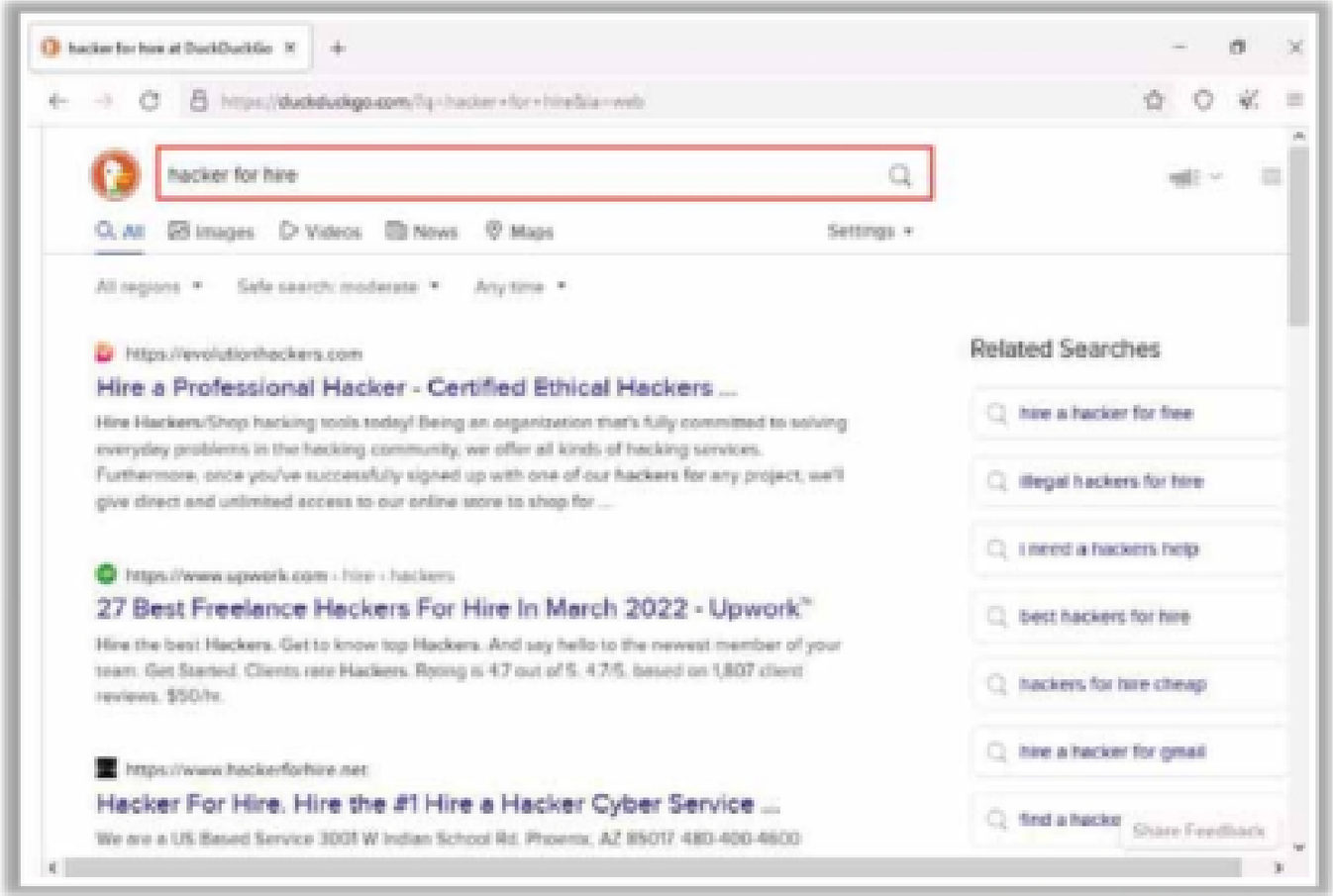
Dark web or Darknet

- It is the subset of the deep web that enables anyone to navigate anonymously without being traced
- It can be accessed by browsers, such as TOR Browser, Freenet, GNUnet, I2P, and Retroshare

- Attackers use deep and dark web searching tools, such as Tor Browser and ExoneraTor, to gather confidential information about the target, including credit card details, passport information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

TOR Browser

It is used to access the deep and dark web where it acts as a default VPN for the user and bounces the network IP address through several servers before interacting with the web

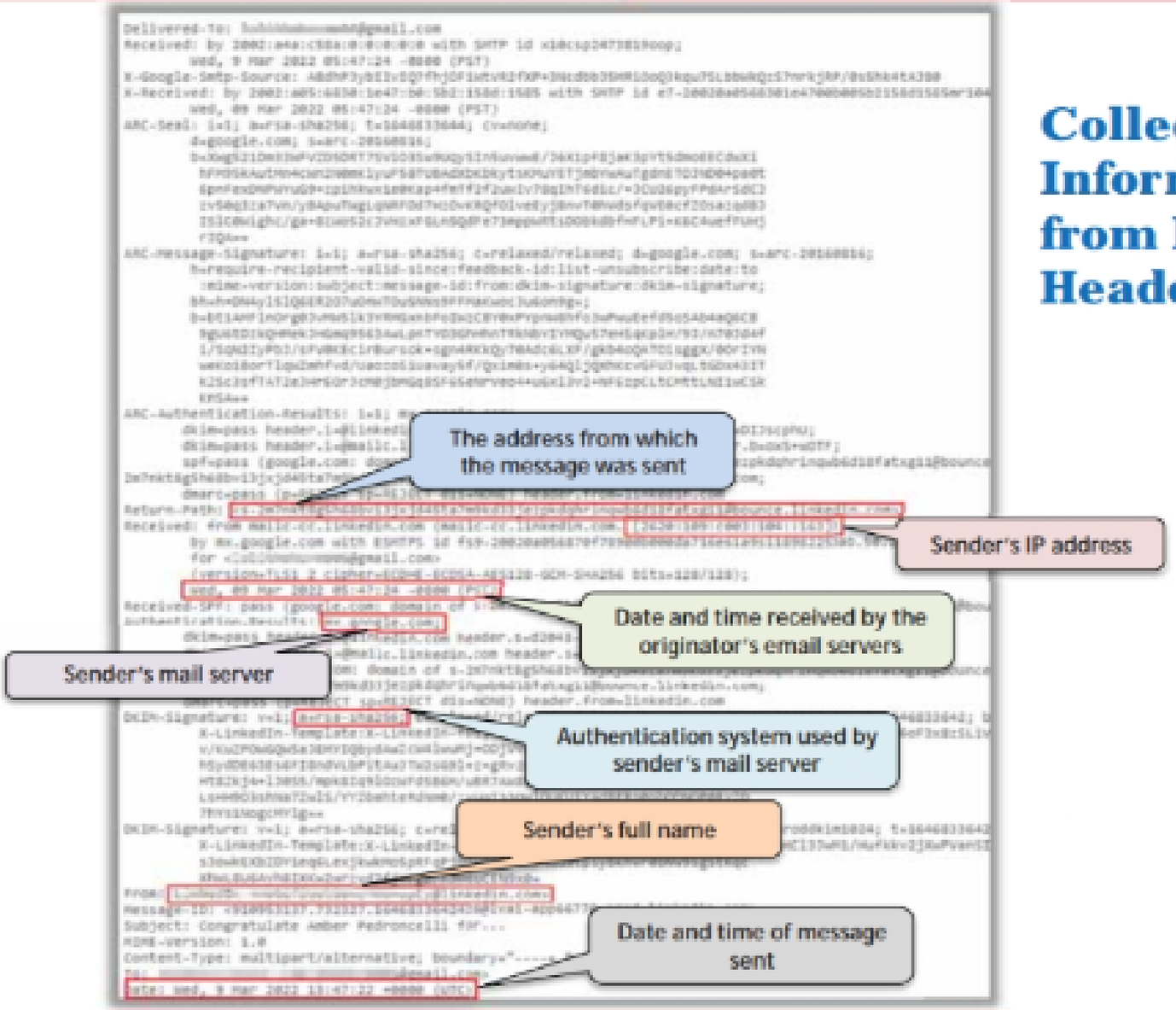


https://www.torproject.org

LO#06: Use Different Techniques for Email Footprinting

Tracking Email Communications

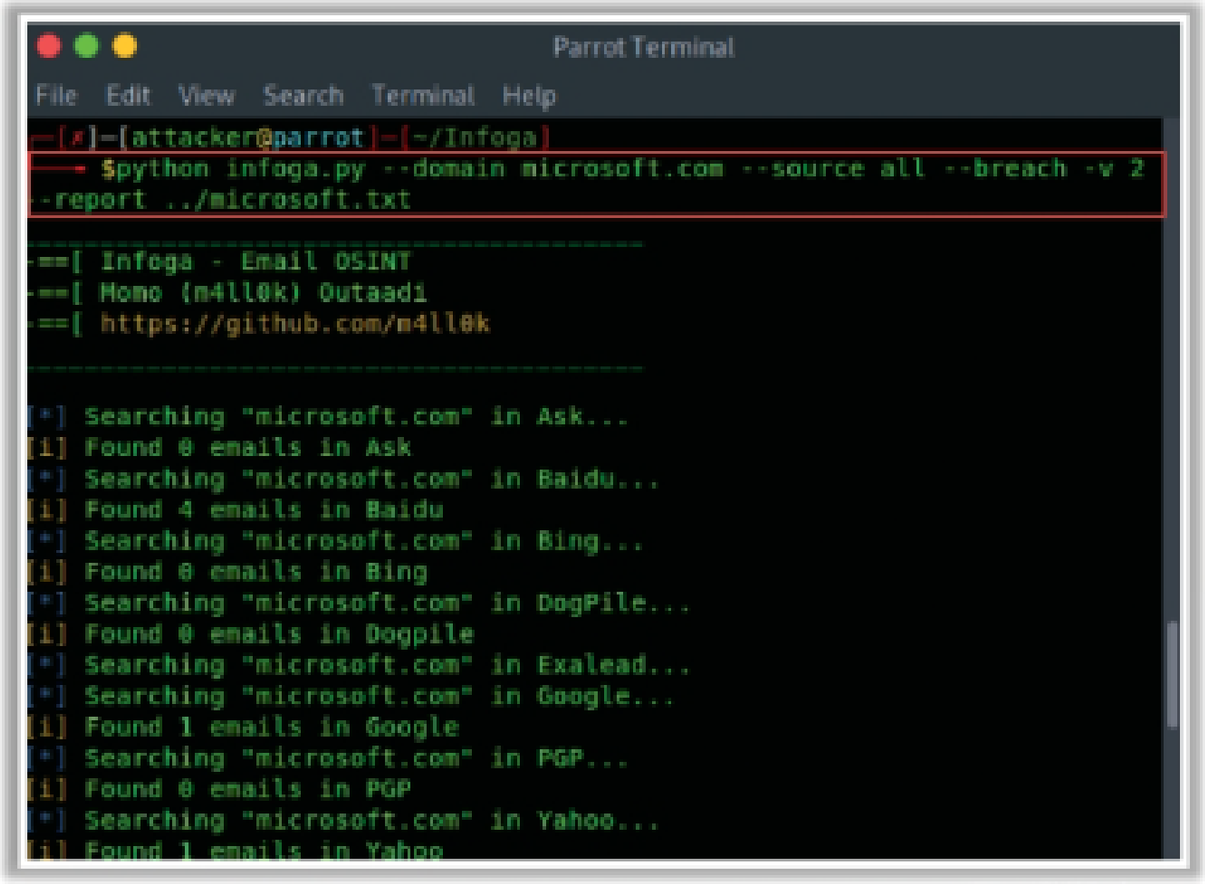
- Email tracking is used to monitor the delivery of emails to an intended recipient
- Attackers track emails to gather information about a target recipient, such as IP addresses, geolocation, browser and OS details, to build a hacking strategy and perform social engineering and other attacks



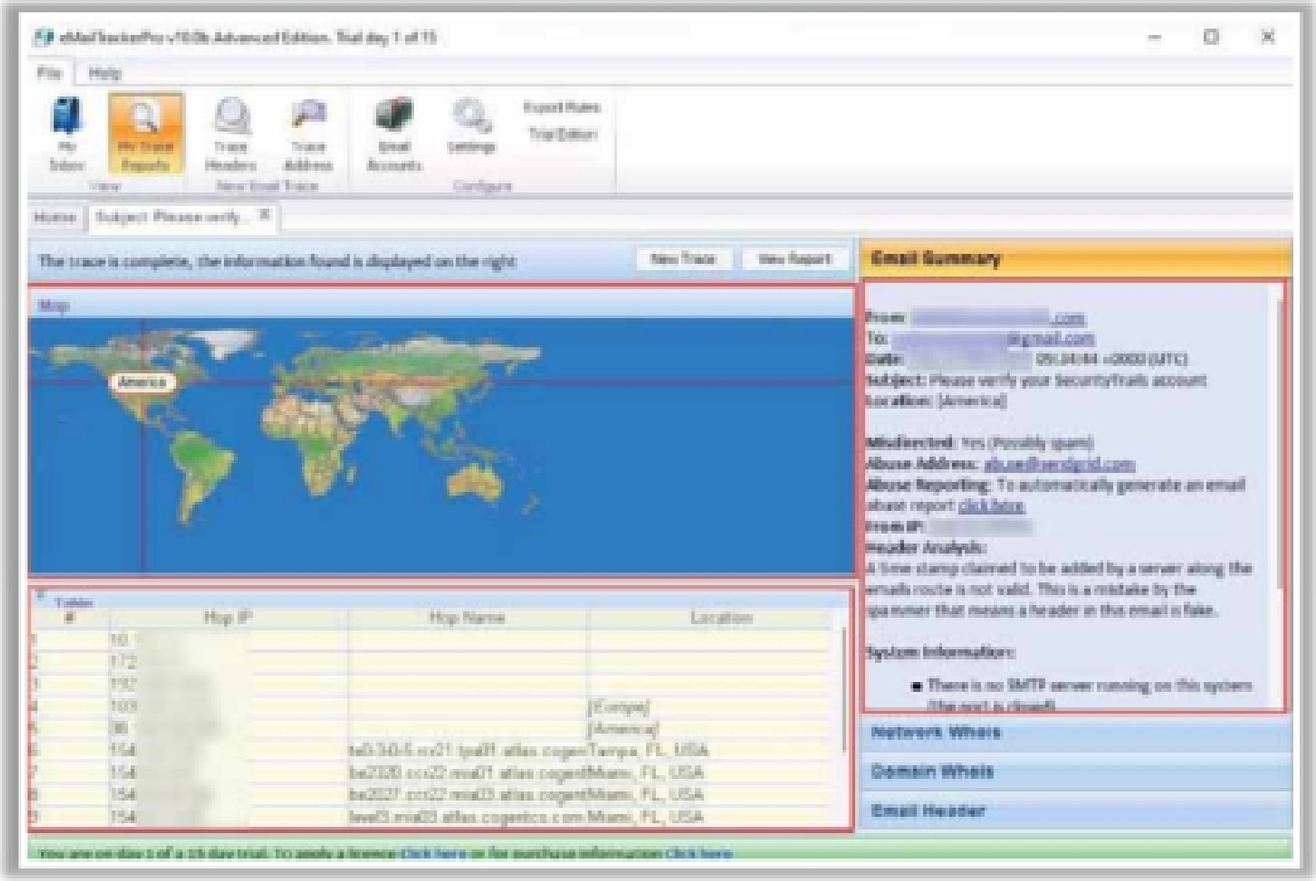
Collecting Information from Email Header

Email Tracking Tools

- Email tracking tools, such as eMailTrackerPro, Infoga, Mailtrack, and PoliteMail, allow an attacker to track an email and extract information, such as sender identity, mail server, sender's IP address, and location
- eMailTrackerPro analyzes email headers and reveals information, such as sender's geographical location and IP address



https://github.com



http://www.emailtrackerpro.com

LO#07: Use Different Techniques for Whois Footprinting

Whois Lookup

Whois databases are maintained by Regional Internet Registries and contain personal information of domain owners

Whois query returns

- Domain name details
- Contact details of domain owners
- Domain name servers
- NetRange
- When a domain was created
- Expiry records
- Last updated record

Information obtained from Whois database assists an attacker to

- Gather personal information that assists in social engineering
- Create a map of the target organization's network
- Obtain internal details of the target network

Regional Internet Registries (RIRs)

ARIN

AFRINIC

RIPE NCC

lacnic

APNIC

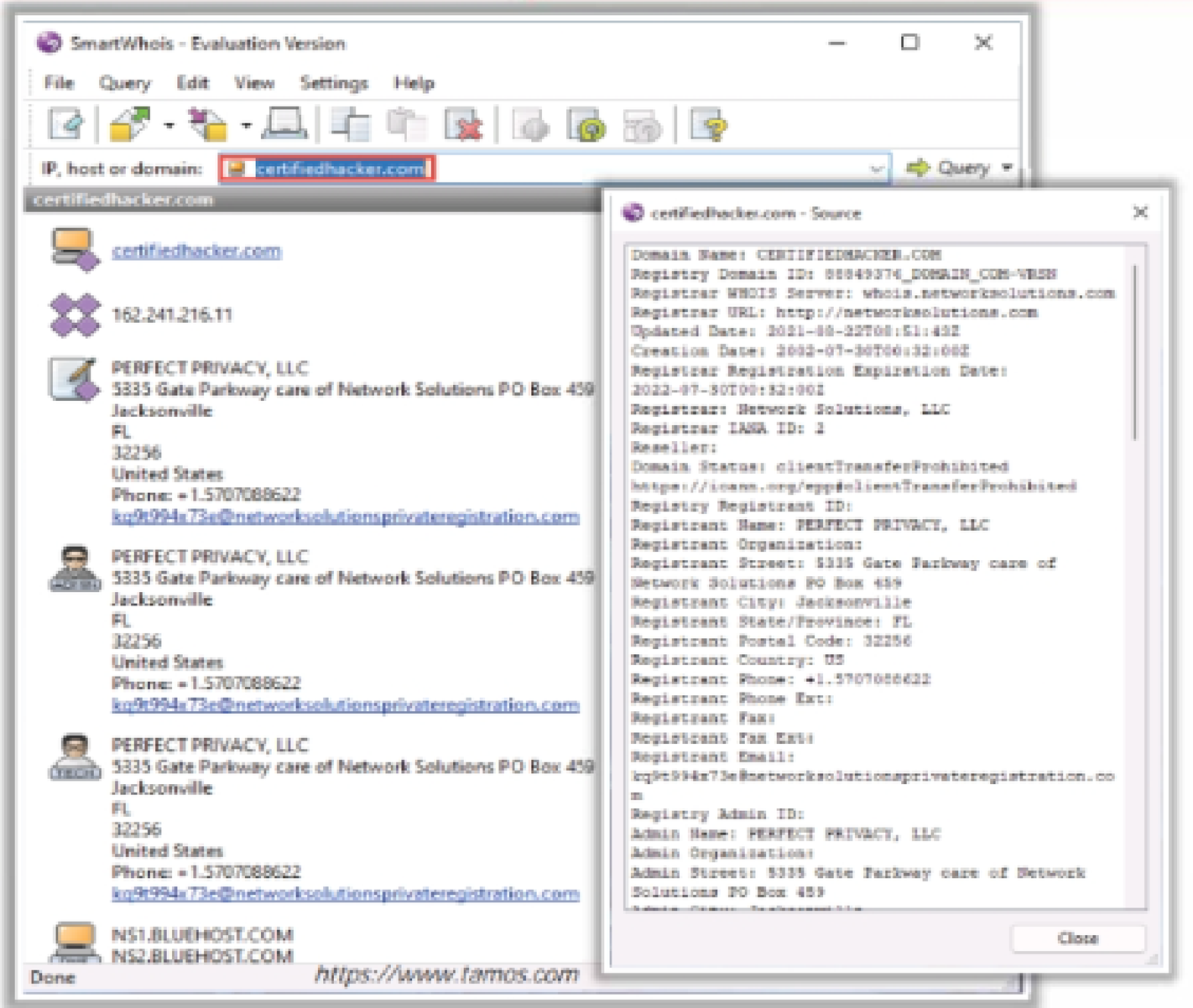
Whois Lookup

Whois Record for CertifiedHacker.com

— Domain Profile

Registrant	PERFECT PRIVACY, LLC
Registrant Country	us
Registrar	Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) 18777228662
Registrar Status	clientTransferProhibited
Dates	7,164 days old Created on 2002-07-29 Expires on 2022-07-29 Updated on 2021-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,681,575 domains) NS2.BLUEHOST.COM (has 2,681,575 domains)
Tech Contact	PERFECT PRIVACY, LLC 5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, FL, 32256, us kq9t994x73e@networksolutionsprivateregistration.com (p) 15707088622
IP Address	162.241.216.11 - 1,745 other sites hosted on this server
IP Location	- Utah - Provo - Unified Layer
ASN	AS26337 OIS1, US (registered Oct 09, 2013)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 16 years
Registrar History	3 registrars with 2 drops
Hosting History	6 changes on 4 unique name servers over 19 years

http://whois.domaintools.com



https://www.tamos.com

Finding IP Geolocation Information

- IP geolocation helps to identify information, such as country, region/state, city, ZIP/postal code, time zone, connection speed, ISP (hosting company), domain name, IDD country code, area code, mobile carrier, and elevation

- IP geolocation lookup tools, such as IP2Location and IP Location Finder, help to collect IP geolocation information about the target, which in turn helps attackers in launching social engineering attacks, such as spamming and phishing

IP2Location

IP Address	207.46.232.182
Country	Singapore [SG]
Region	Singapore
City	Singapore
Coordinates of City	1.289670, 103.850070 (1°17'23"N 103°51'0"E)
ISP	Microsoft Corporation
Local Time	10 Mar, 2022 07:54 PM (UTC +08:00)
Domain	microsoft.com
Net Speed	(COMP) Company/T1
IDD & Area Code	(65) 06
ZIP Code	179431
Weather Station	Singapore (SNXX0006)

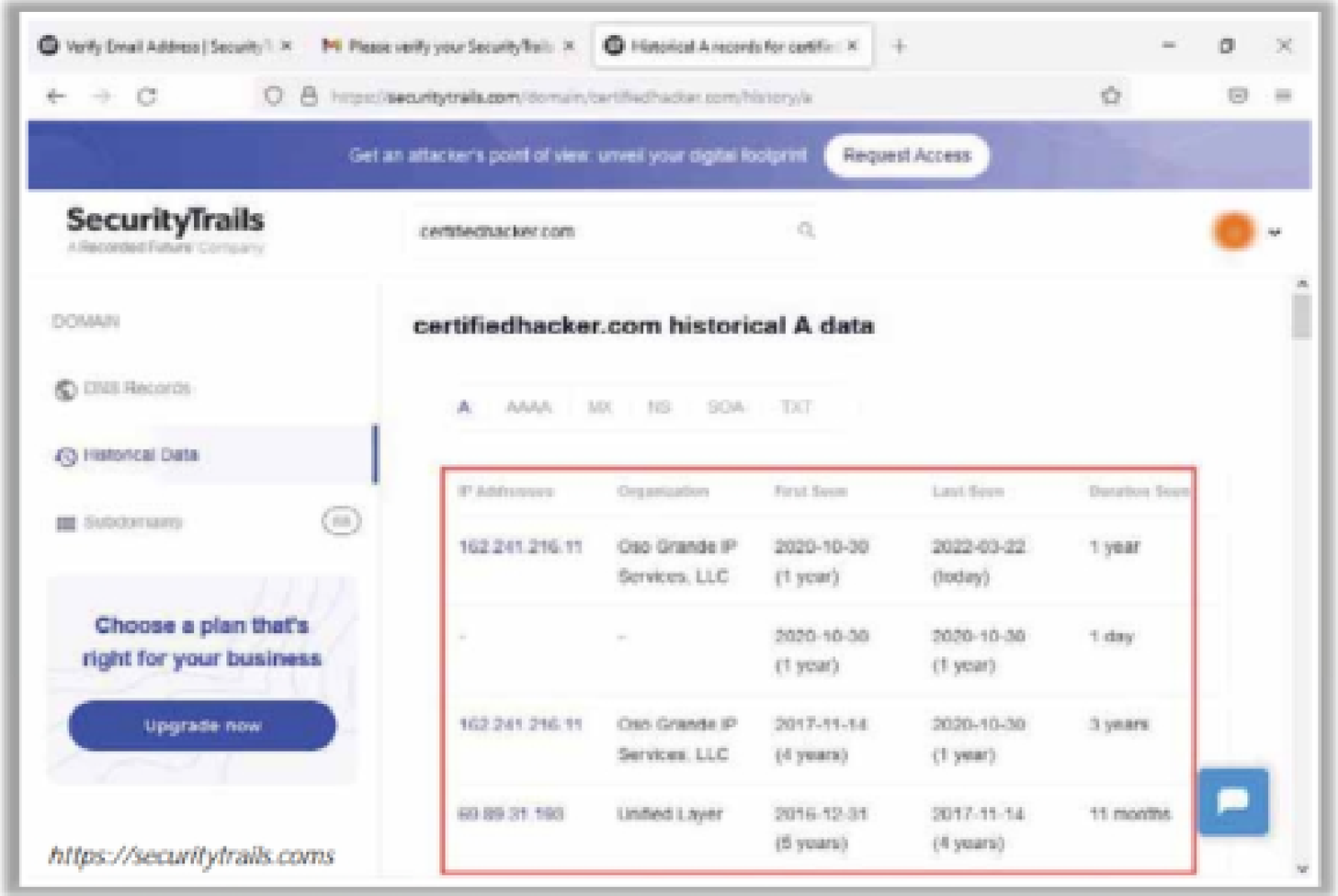
LO#08: Use Different Techniques for DNS Footprinting

Extracting DNS Information

- DNS records provide important information about the location and types of servers
- Attackers can gather DNS information to determine key hosts in the network and can perform social engineering attacks

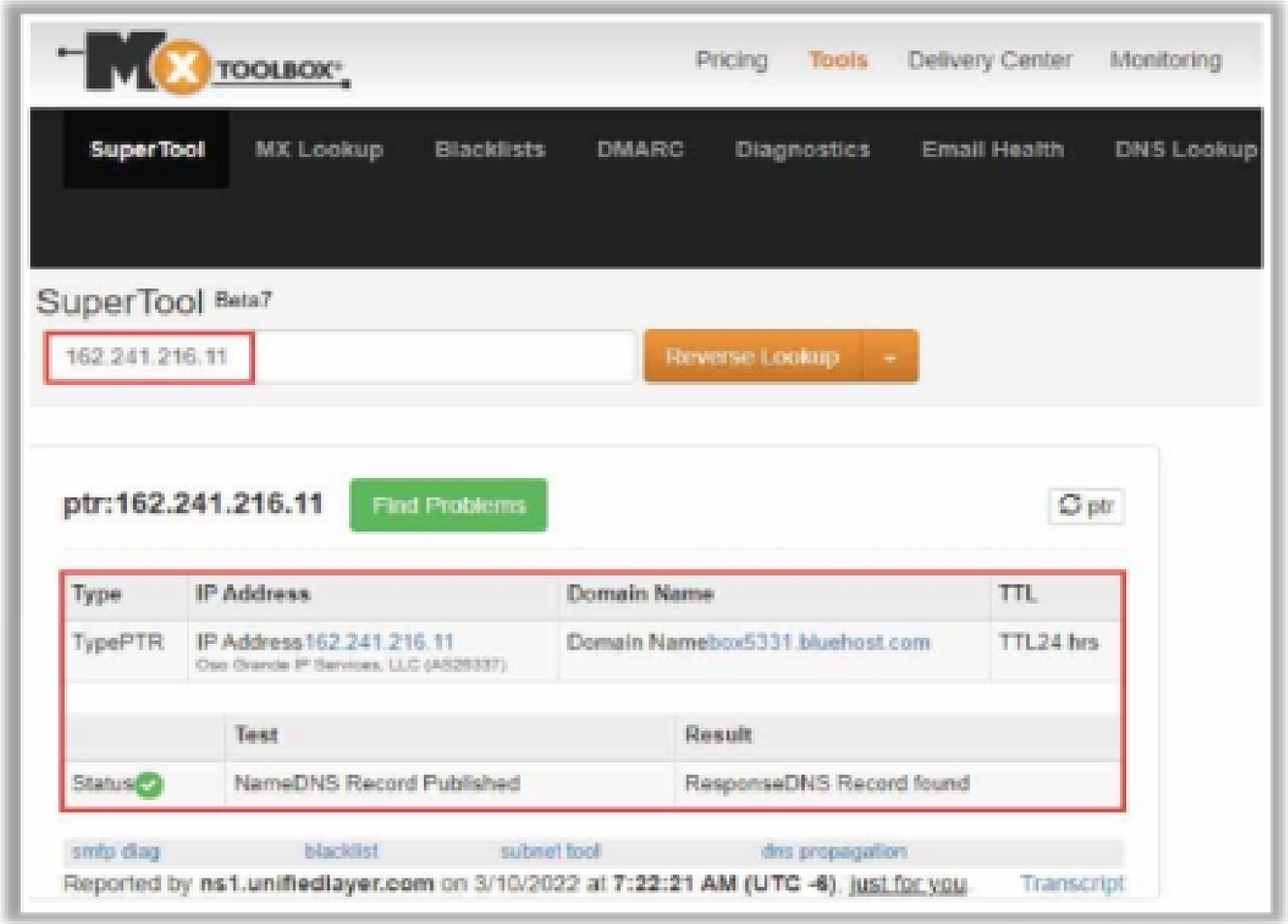
Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for a domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

- Attackers query DNS servers using DNS interrogation tools, such as SecurityTrails, NSLOOKUP, and DNS Records, to retrieve the record structure that contains information about the target DNS

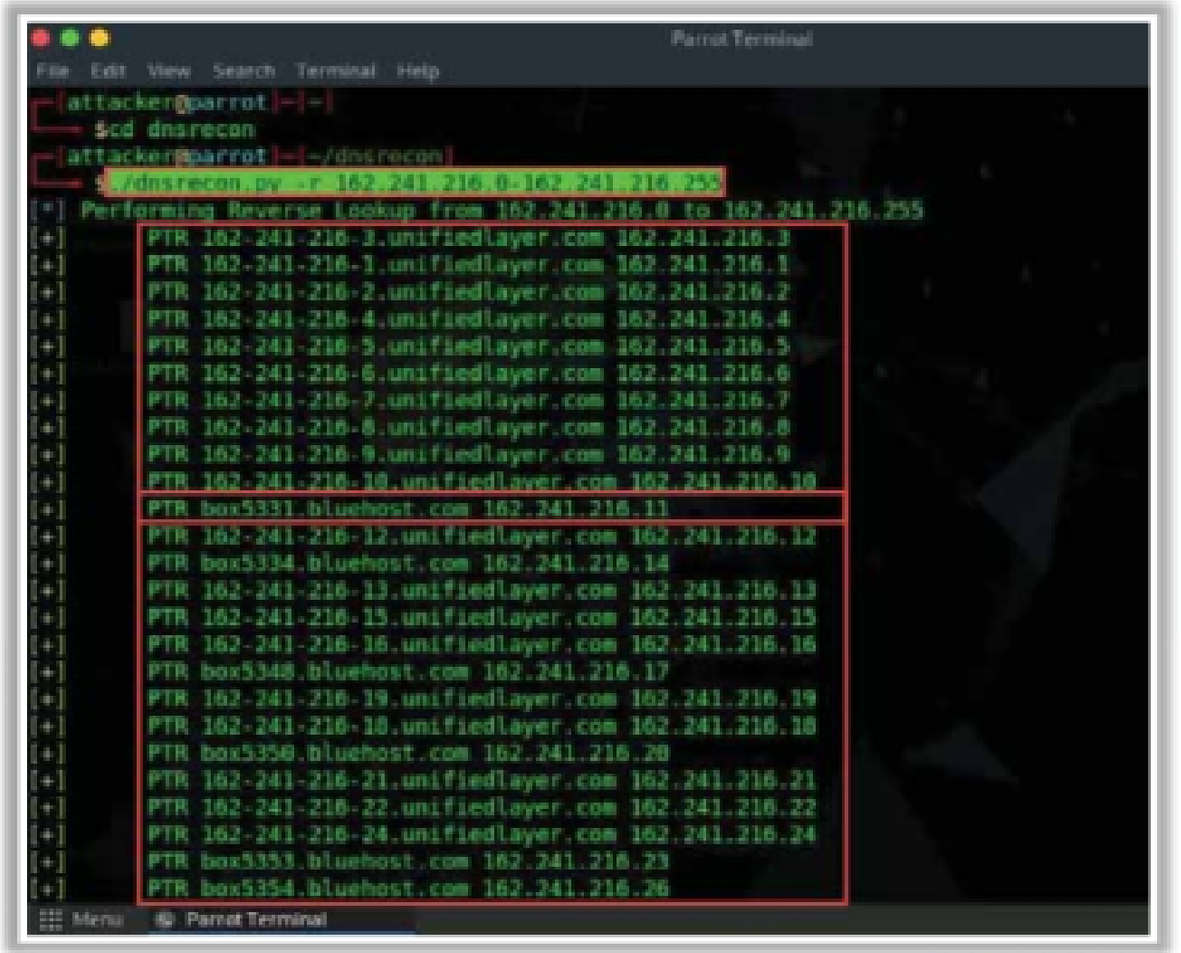


Reverse DNS Lookup

- Attackers perform a reverse DNS lookup on IP ranges in an attempt to **locate a DNS PTR record** for those IP addresses
- Attackers use various tools, such as **DNSRecon** and **Reverse Lookup** to perform the reverse DNS lookup on the target host



https://mxtoolbox.com

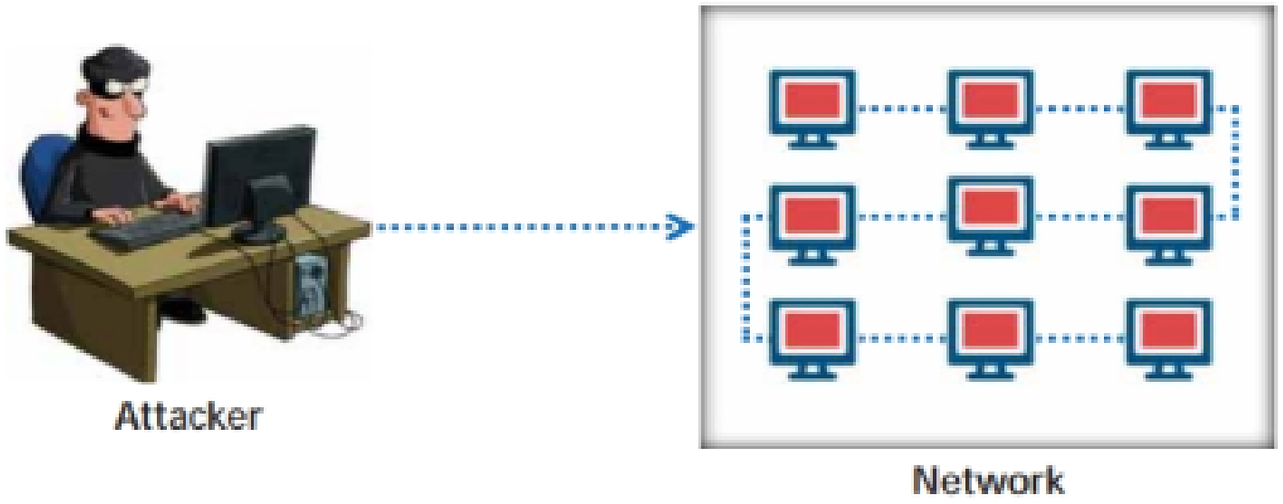


https://github.com

LO#09: Use Different Techniques for Network Footprinting

Locate the Network Range

- Network range information assists attackers in creating a map of the target network
- One can find the range of IP addresses using ARIN whois database search tool
- One can also find the range of IP addresses and the subnet mask used by the target organization from Regional Internet Registry (RIR)



Network: NET-207-46-0-0-1

Source Registry	ARIN
Net Range	207.46.0.0 - 207.46.255.255
CIDR	207.46.0.0/16
Name	MICROSOFT-GLOBAL-NET
Handle	NET-207-46-0-0-1
Parent	NET-207-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	*not provided*
Registration	Mon, 31 Mar 1997 05:00:00 GMT (Mon Mar 31 1997 local time)
Last Changed	Wed, 15 Dec 2021 01:28:40 GMT (Wed Dec 15 2021 local time)
Self	https://rdap.arin.net/registry/ip/207.46.0.0
Alternate	https://whois.arin.net/rest/net/NET-207-46-0-0-1
Port 43 Whois	whois.arin.net

Related Entities	1 Entity
Source Registry	ARIN
Kind	Org
Full Name	Microsoft Corporation
Handle	MSFT
Address	One Microsoft Way Redmond WA 98052 United States
Roles	Registrant
Registration	Fri, 10 Jul 1998 04:00:00 GMT (Fri Jul 10 1998 local time)
Last Changed	Wed, 13 Oct 2021 21:39:04 GMT (Thu Oct 14 2021 local time)
Comments	To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to: * https://cert.microsoft.com.

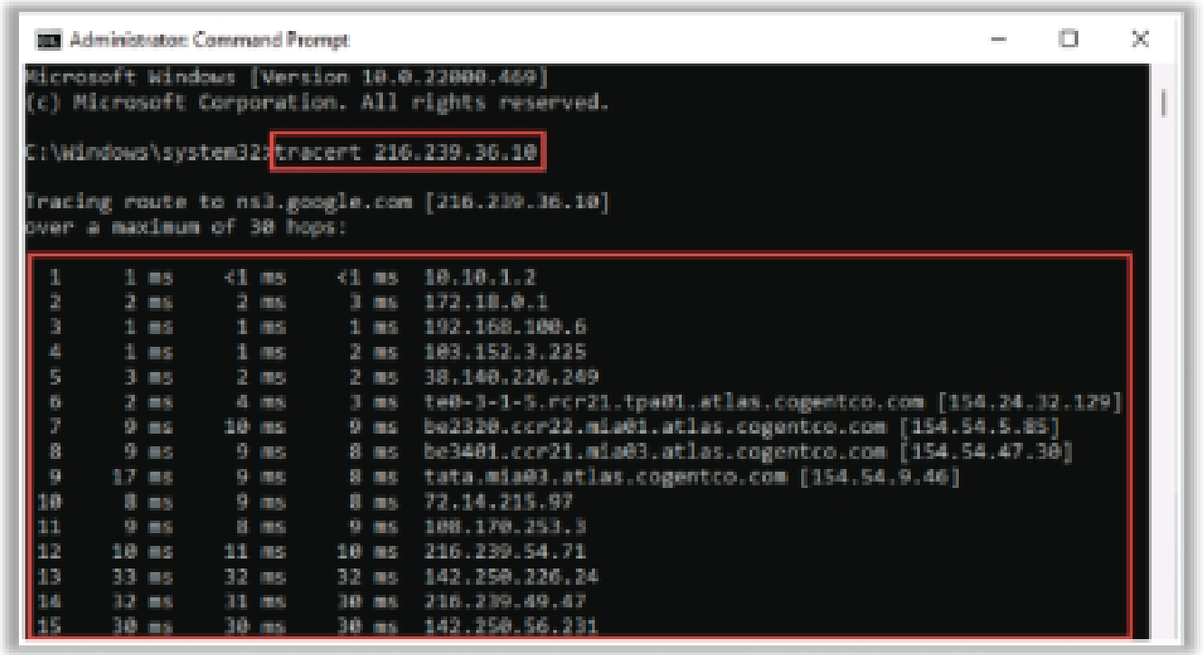
Network Whois Record

Queried search.arin.net with "207.46.232.182"

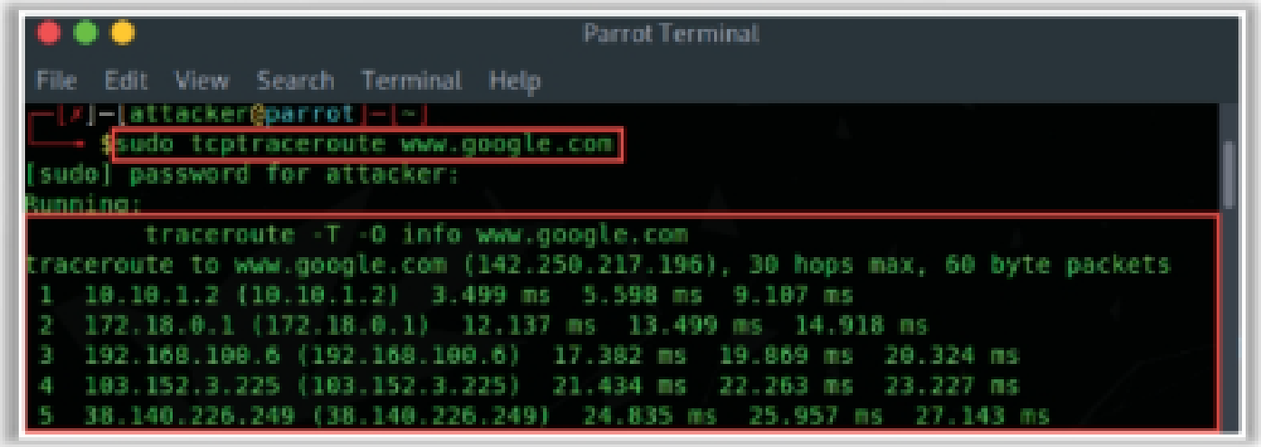
Traceroute

- Traceroute programs work on the concept of ICMP protocol and use the TTL field in the header of ICMP packets to discover the routers on the path to a target host

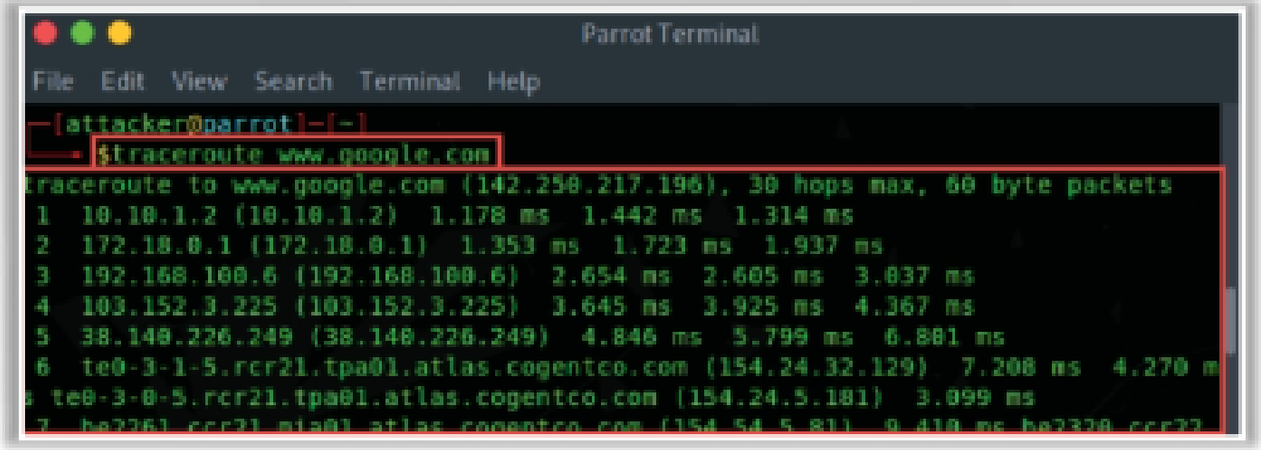
IMCP Traceroute



TCP Traceroute



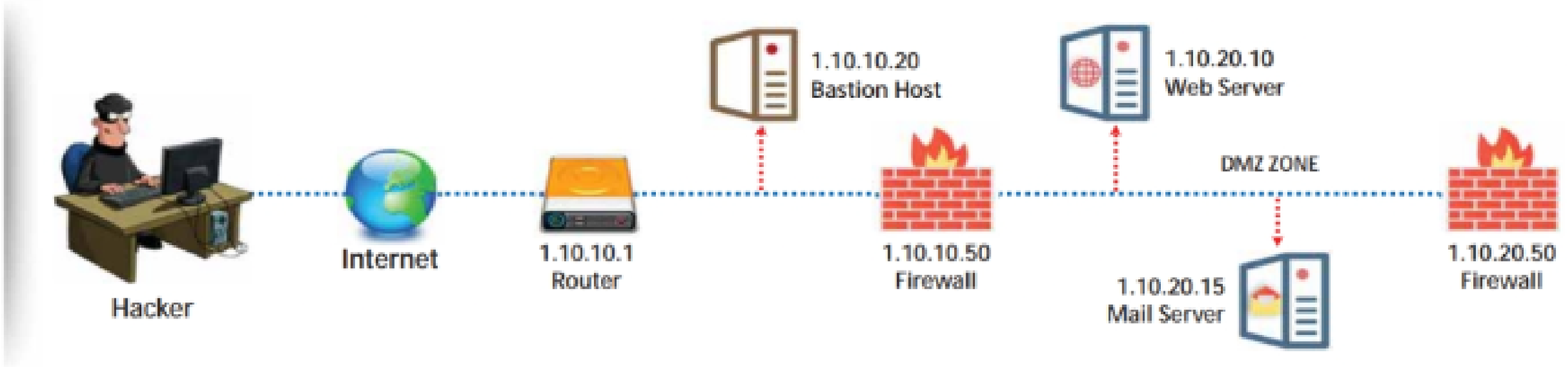
UDP Traceroute



Traceroute Analysis

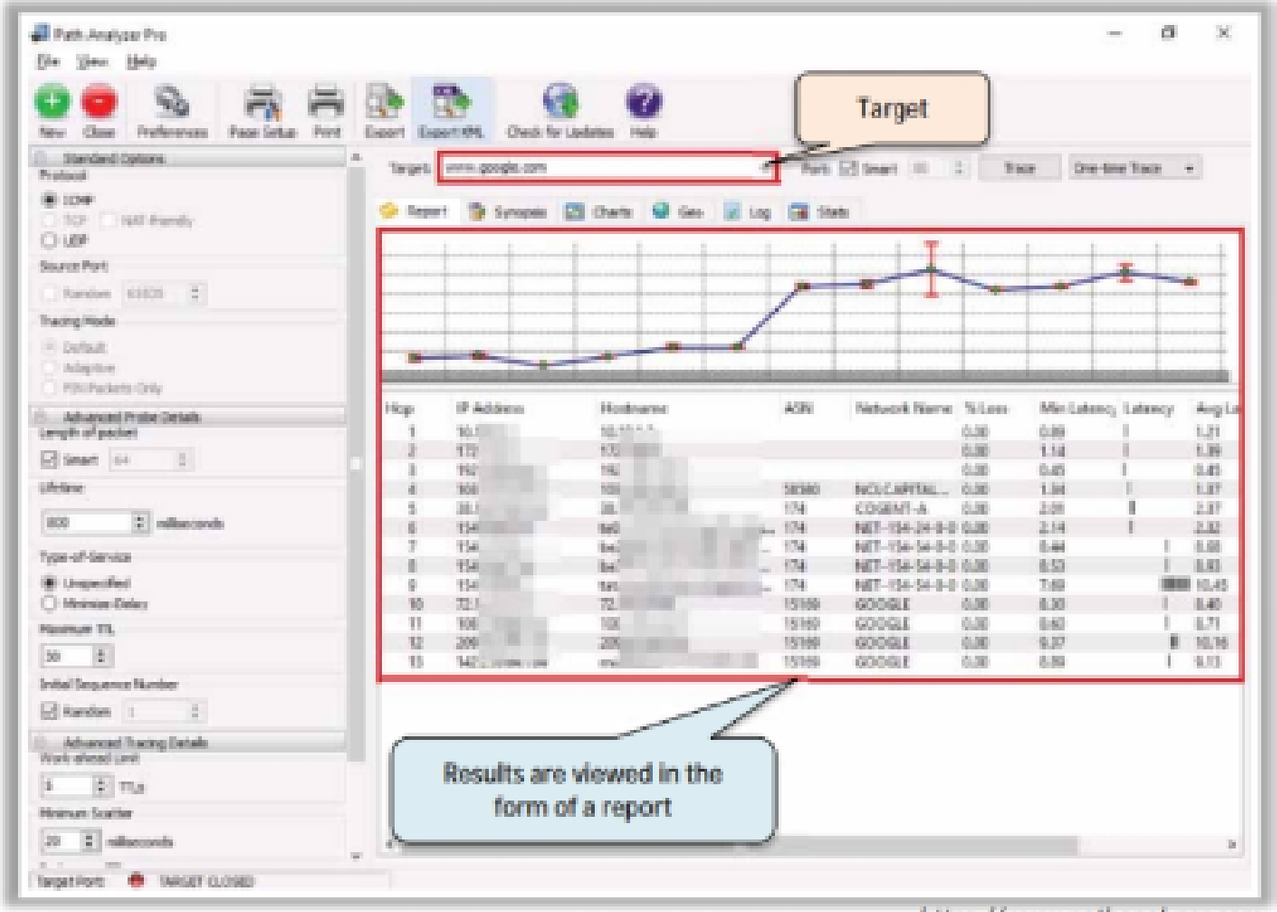
- Attackers execute traceroute to find the IP addresses of intermediate devices such as routers and firewalls present between a source and its destination
- For example, after running several traceroutes, an attacker might obtain the following information:
  - traceroute 1.10.10.20, second to last hop is 1.10.10.1
  - traceroute 1.10.20.10, third to last hop is 1.10.10.1
  - traceroute 1.10.20.10, second to last hop is 1.10.10.50
  - traceroute 1.10.20.15, third to last hop is 1.10.10.1
  - traceroute 1.10.20.15, second to last hop is 1.10.10.50
- By compiling this information, attackers can identify the intermediate devices or hosts in the path to the target network

Attack Process

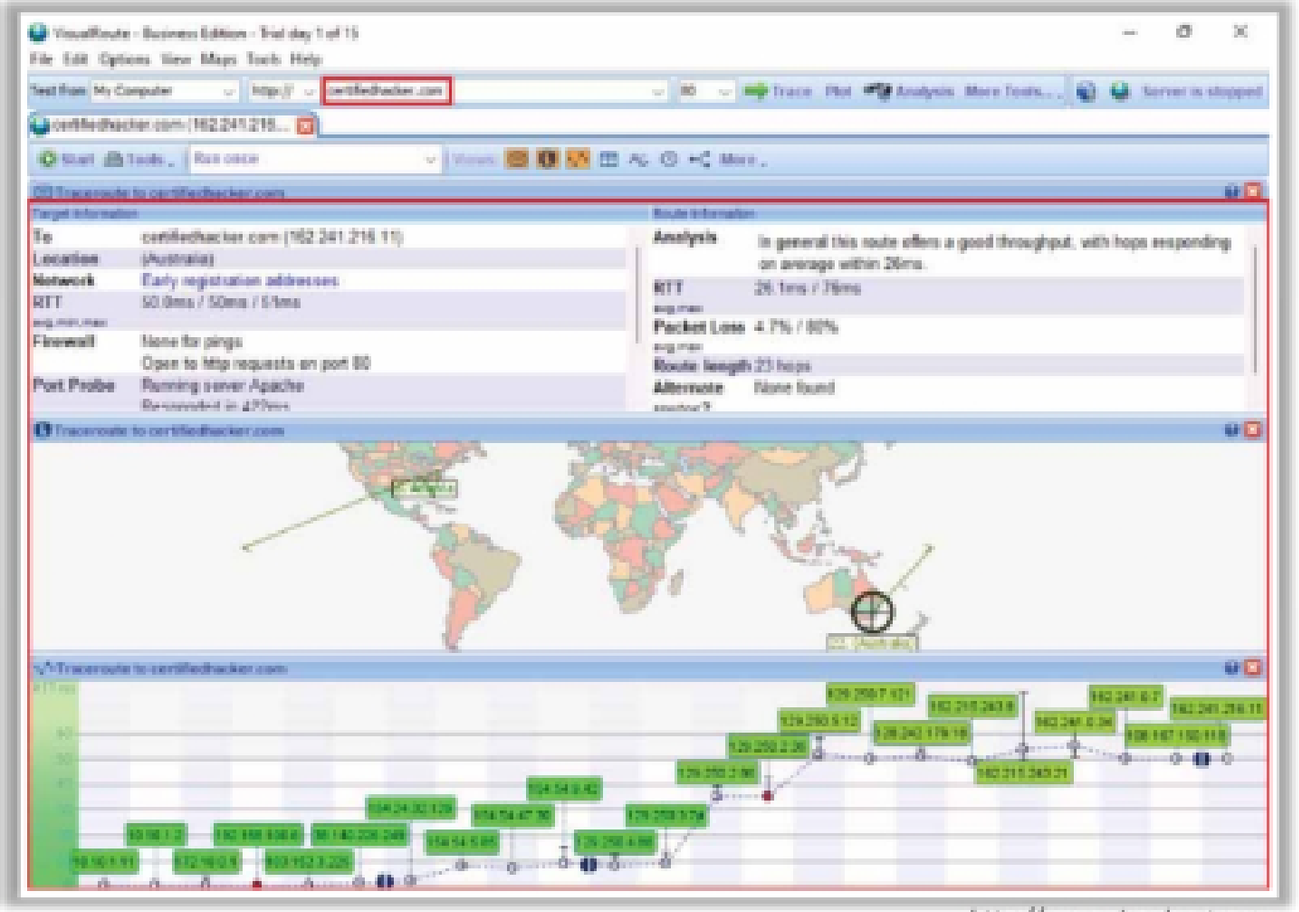


Traceroute Tools

Path Analyzer Pro	It delivers network route tracing with performance tests, DNS, Whois, and network resolution to investigate network issues
VisualRoute	It is a traceroute and network diagnostic tool that identifies the geographical location of routers, servers, and other IP devices



https://www.pathanalyzer.com



http://www.visualroute.com

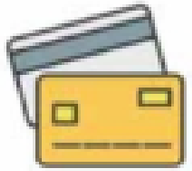
LO#10: Demonstrate Footprinting through Social Engineering

Footprinting through Social Engineering

- Social engineering is an art of exploiting human behaviour to extract confidential information
- Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it

Social engineers attempt to gather

- Credit card details and social security number
- Usernames and passwords
- Security products in use
- Operating systems and software versions
- Network layout information
- IP addresses and names of servers



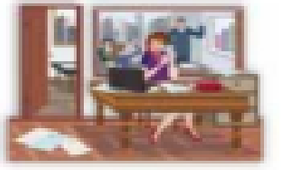
Social engineering techniques include

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation

Collecting Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving, and Impersonation

Eavesdropping

- Unauthorized listening of conversations or reading of messages
- It is the interception of any form of communication, such as audio, video, or text



Shoulder Surfing

- Secretly observing the target to gather critical information, such as passwords, personal identification number, account numbers, and credit card information

Dumpster Diving

- Looking for treasure in someone else's trash
- It involves the collection of phone bills, contact information, financial information, operations-related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

Impersonation

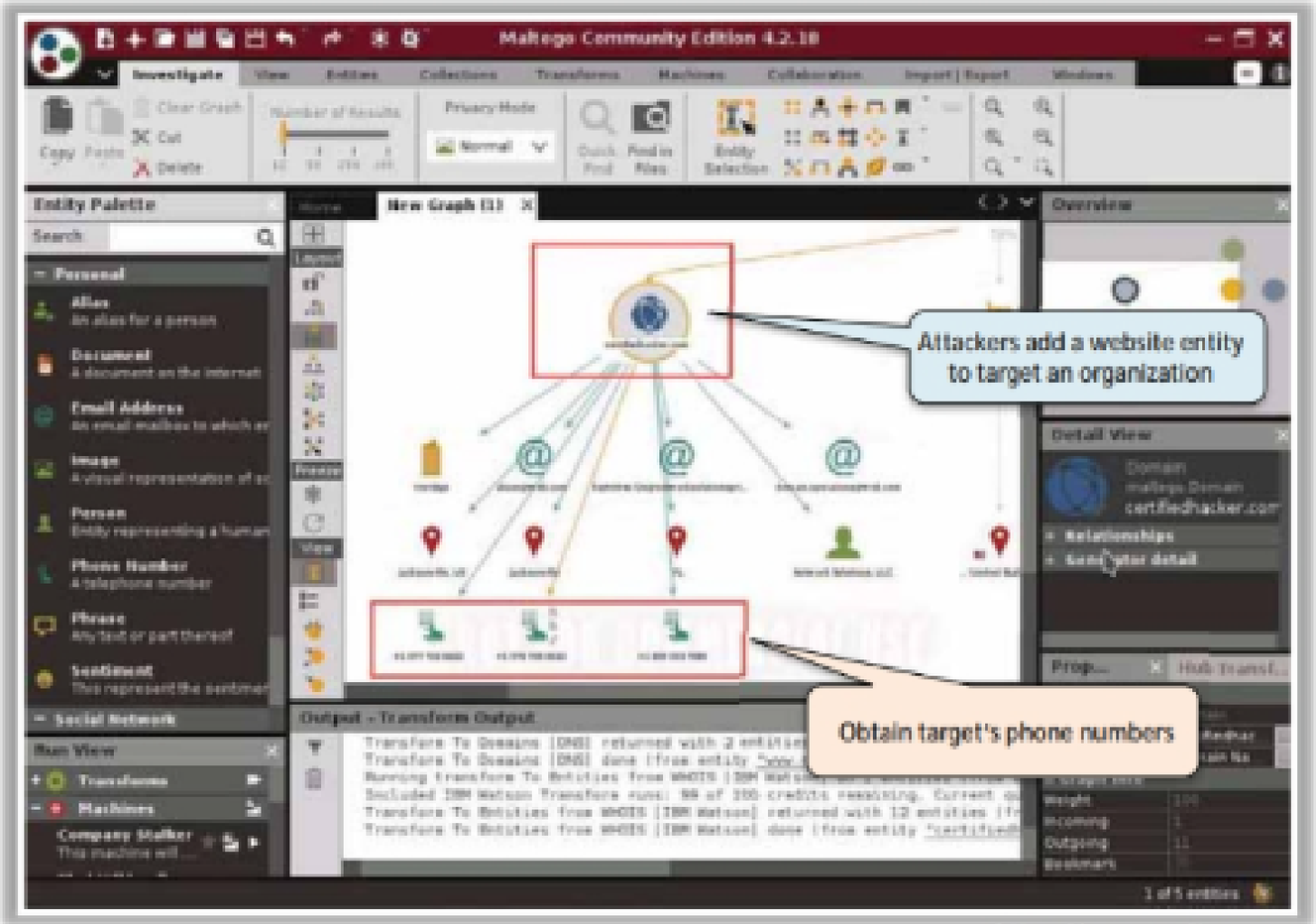
- Pretending to be a legitimate or authorized person and using the phone or other communication medium to mislead targets and trick them into revealing information

LO#11: Use Various Footprinting Tools

Footprinting Tools: Maltego and Recon-ng

Maltego

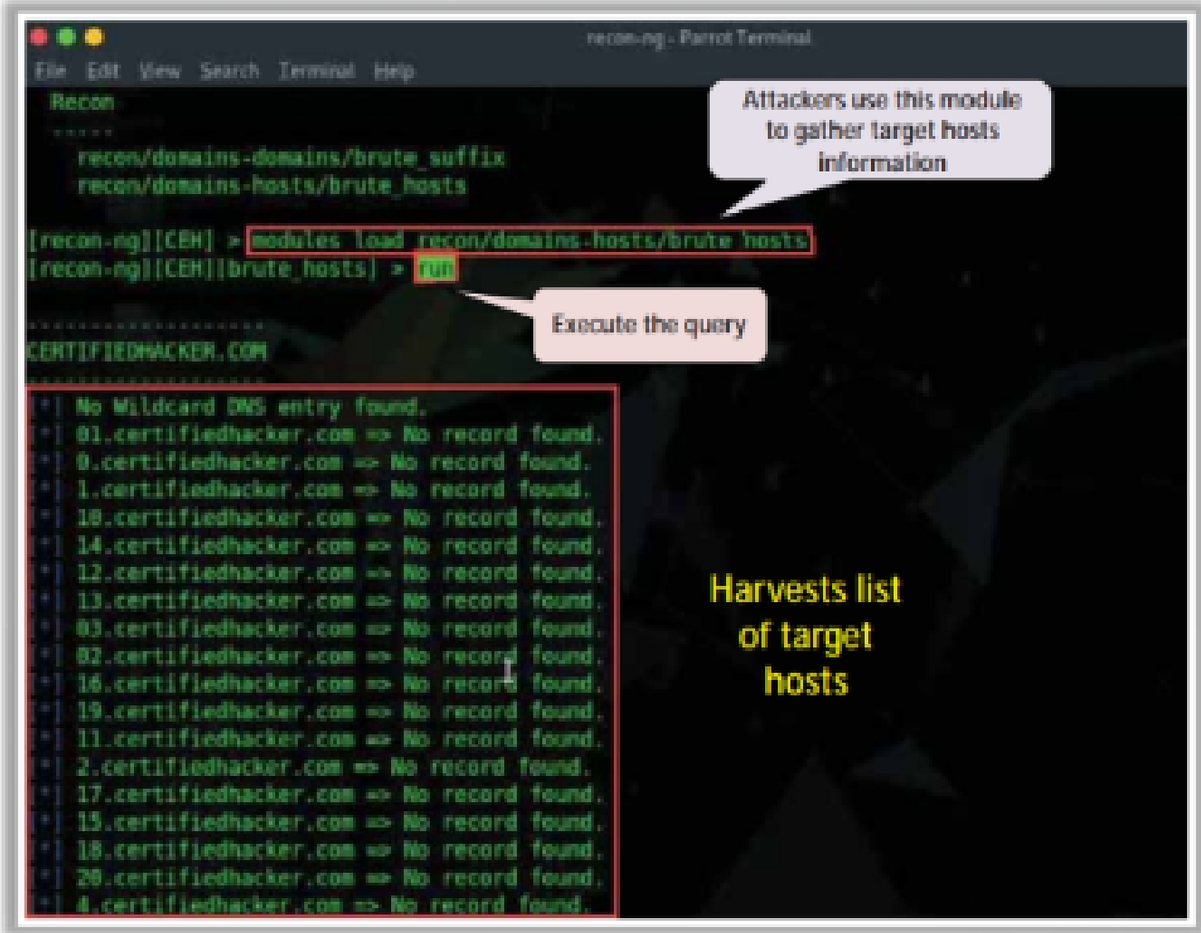
Maltego can be used to determine the relationships and real world links between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.



https://www.maltego.com

Recon-ng

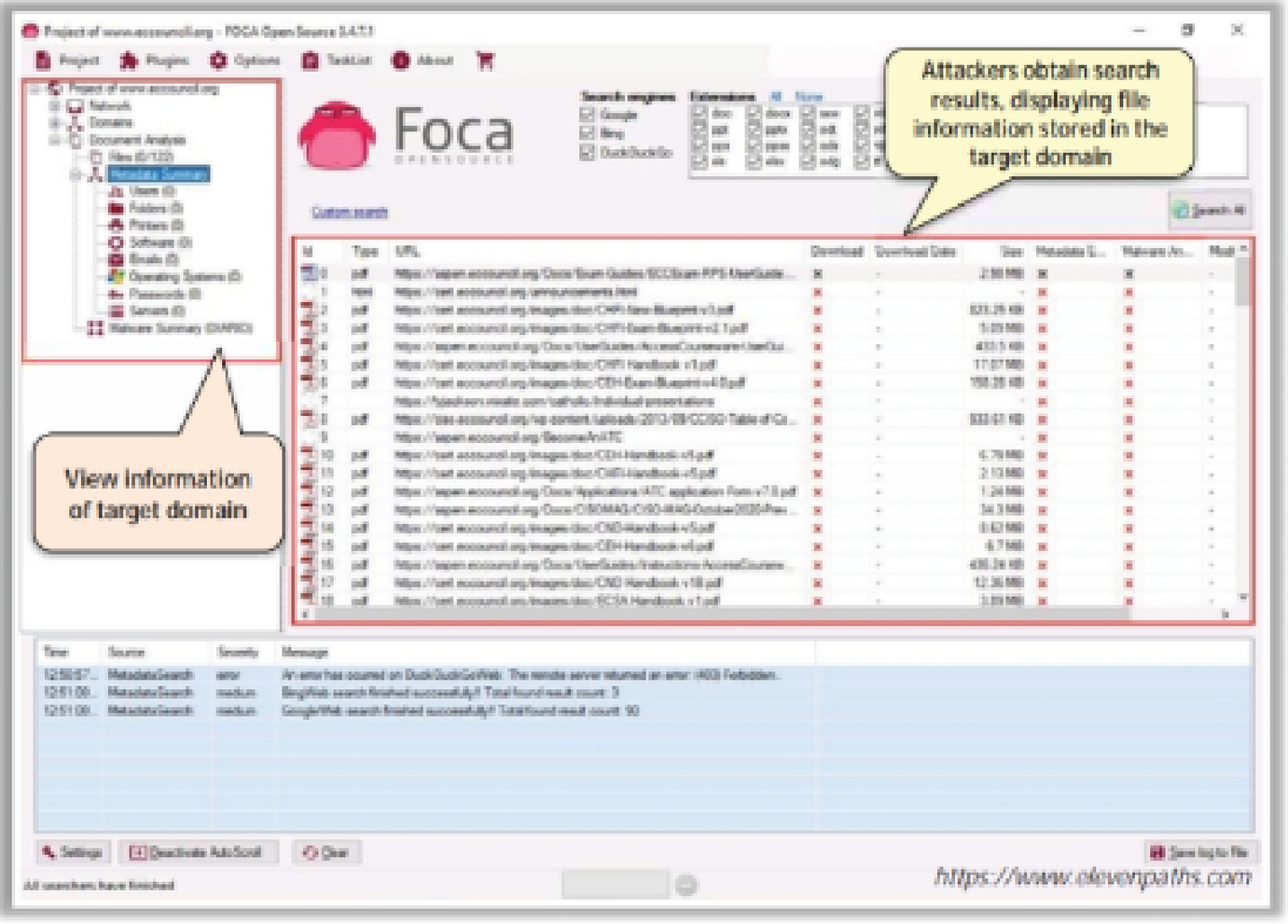
Recon-ng is a Web Reconnaissance framework with independent modules and database interaction, which provides an environment in which open source, web-based reconnaissance can be conducted



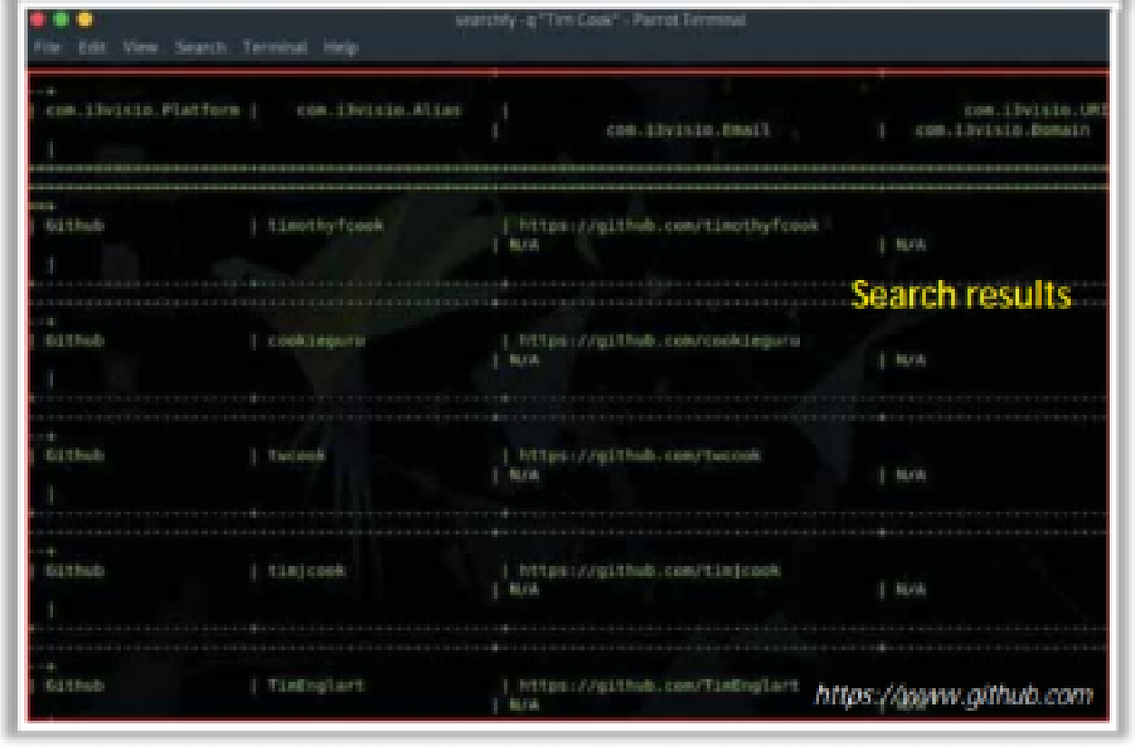
https://github.com

Footprinting Tools: FOCA and OSRFramework

FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents it scans

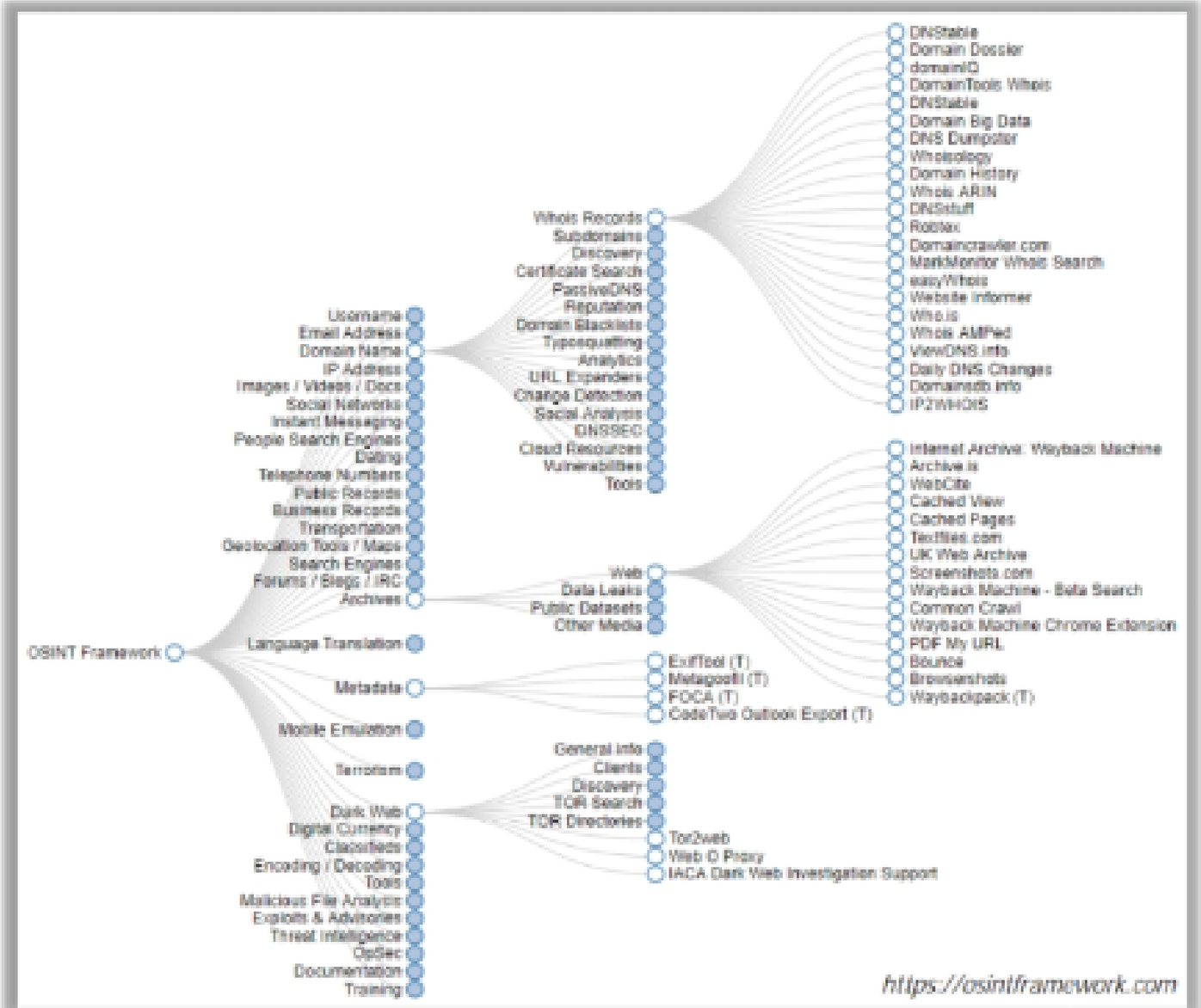


OSRFramework includes applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, etc.



Footprinting Tools: OSINT Framework

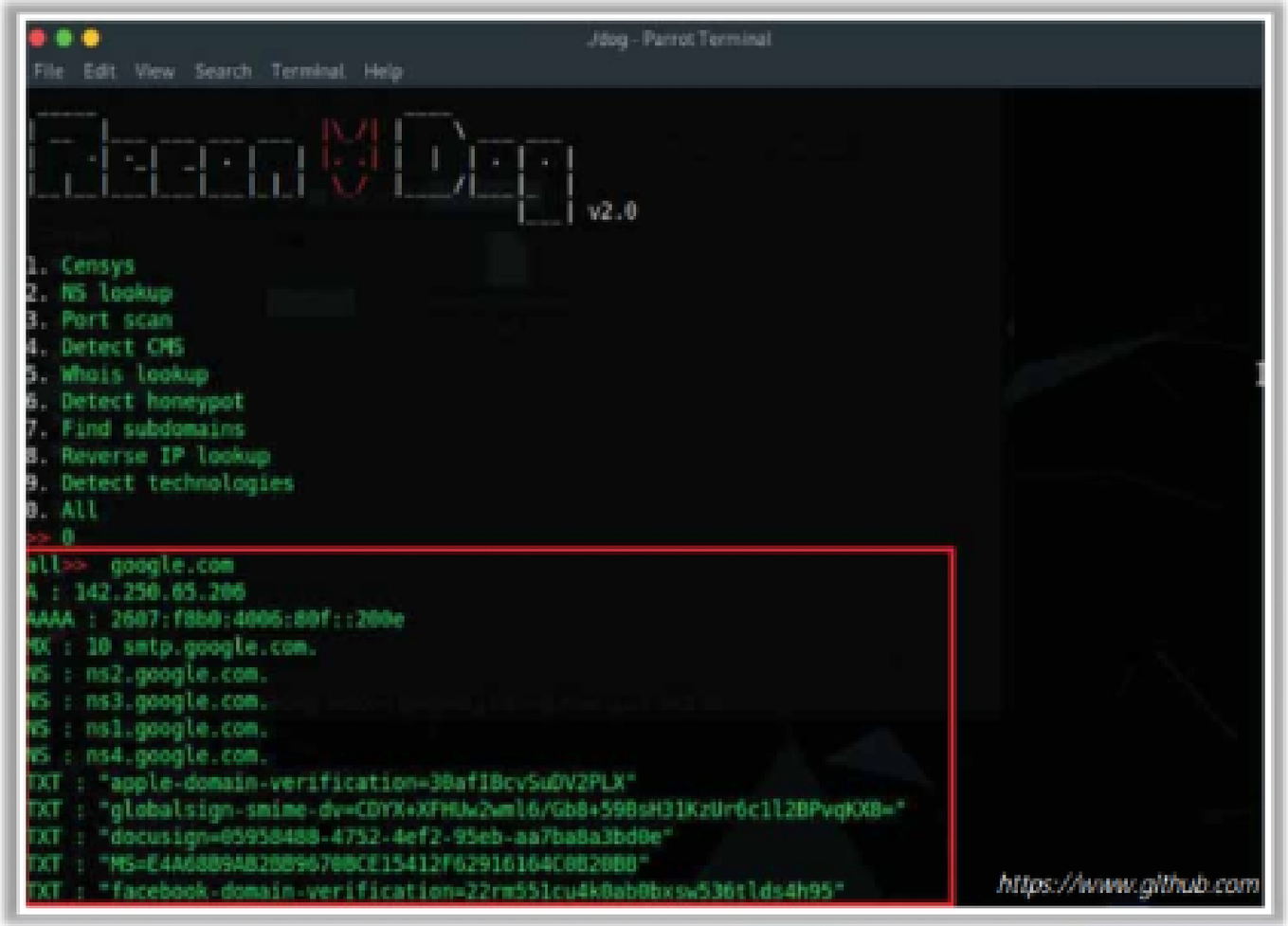
- OSINT Framework is an **open source intelligence gathering framework** that is focused on gathering information from free tools or resources
- It provides a simple web interface that lists various OSINT tools arranged by categories and is shown as **OSINT tree structure** on the web interface
- Tools listed includes the following indicators:
  - (T) - Indicates a link to a tool that must be installed and run locally
  - (D) - Google Dork
  - (R) - Requires registration
  - (M) - Indicates a URL that contains the search term and the URL itself must be edited manually



Footprinting Tools: Recon-Dog and BillCipher

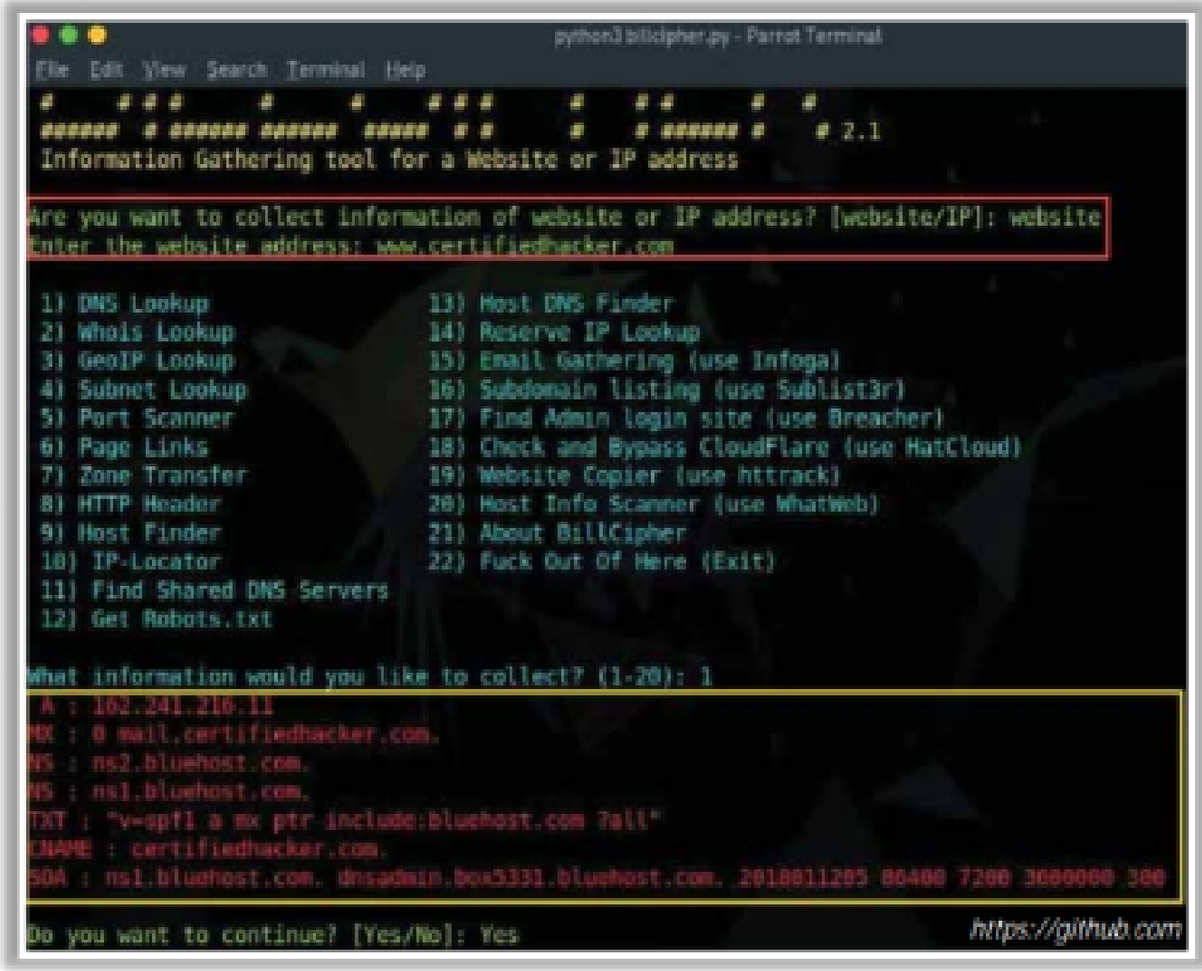
Recon-Dog

- Recon-Dog is an all-in-one tool for information gathering needs, which uses APIs to collect information about the target system



BillCipher

- BillCipher is an information gathering tool for a website or IP address



Footprinting Tools…

Spyse

Attackers can use different parameters available in this tool to identify information such as subdomains, certificates, and vulnerabilities risk scores

https://spyse.com

Grecon
https://github.com

theHarvester
http://www.edge-security.com

Th3Inspector
https://github.com

Raccoon
https://github.com

Orb
https://github.com

LO#12: Explain Footprinting Countermeasures

Footprinting Countermeasures

- Restrict the employees' access to social networking sites from the organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums
- Do not reveal critical information in press releases, annual reports, product catalogues, etc.
- Limit the amount of information published on a website or the Internet
- Use footprinting techniques to discover and remove any sensitive information that is publicly available
- Prevent search engines from caching a web page and use anonymous registration services

Footprinting Countermeasures…

1. Develop and enforce security policies to regulate the information that employees can reveal to third parties
2. Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers
3. Disable directory listings in the web servers
4. Conduct security awareness training periodically to educate employees about various social engineering tricks and risks
5. Opt for privacy services on a Whois Lookup database
6. Avoid domain-level cross-linking for critical assets
7. Encrypt and password-protect sensitive information
8. Place critical documents, such as business plans and proprietary documents offline to prevent exploitation
9. Train employees to thwart social engineering techniques and attacks
10. Sanitize the details provided to Internet registrars to hide the direct contact details of the organization
11. Disable the geo-tagging functionality on cameras to prevent geolocation tracking
12. Avoid revealing one's location or travel plans on social networking sites
13. Turn off geolocation access on all mobile devices when not required
14. Ensure that no critical information is displayed on notice boards or walls


DIGITAL
UNIVERSITY
KERALA
Curating a responsible digital world