knowledge C. Pentesting with partial knowledge D. Pentesting performed by Black Hat

12. What does TOE stand for? A. Type of Evaluation B. Time of Evaluation C. Term of Evaluation D. Target of Evaluation

13. The term “Vulnerability” refers to: A. A virus
B. A malware
C. An attack
D. A weakness

Chapter 2: Footprinting & Reconnaissance

Technology Brief

In previous chapter “Introduction to Ethical Hacking”, we have discussed about phases of ethical hacking. Let’s being with its first step i.e. Footprinting and Reconnaissance. The Footprinting phase allows the attacker to gather information regarding the internal and external security architecture of the target; this collection of information helps to identify the vulnerabilities within a system, which can be used to exploit the system to gain access. Attaining in-depth information reduces the focus area and brings the attacker closer to the target. The attacker lists the range of IP addresses he/she has to go through, either to hack or footprint the domain information of the target.

Footprinting Concepts

The first step in ethical hacking is Footprinting. Footprinting means gathering every possible piece of information related to the target and target network. The collected information helps in identifying different possible ways to enter into the target network. Usually, information is gathered from both public and secret sources. Footprinting and reconnaissance are the most common techniques used to perform social engineering, system, and network attacks. Active and passive methods of reconnaissance are also well-known for gathering information about a target. The overall purpose of this phase is to

maintain interaction with the target in order to gain information without being detected or alerting the target.

Note: Reconnaissance is an attack in which an intruder engages with the targeted system to gather information about vulnerabilities. The term is borrowed from its military use, where it refers to a mission into enemy territory to obtain information.

Pseudonymous Footprinting

Pseudonymous Footprinting is the collection of information about a target through online sources. In Pseudonymous footprinting, information about a target is published over the internet by anyone other than the target. This type of information is shared without real credentials in order to avoid begin traced to the actual source of the information. The author may be a corporate or government official and be prohibited from posting under his or her original name.

Internet Footprinting

Internet Footprinting includes footprinting and reconnaissance methods for collecting information through the internet. Popular options for internet footprinting include the Google hacking database, Google Advanced Search, and some other search engines.

Objectives of Footprinting

The significant footprinting objectives are:

1. To know security posture
2. To reduce the focus area
3. To identify vulnerabilities
4. To draw network map

Footprinting Methodology

The internet, social media, official websites and a few other similar sources have made it very easy for hackers to get information about whomever they want. It does not require much effort to gather information from these sources. The information available on public

sources may not be sensitive, but it might be enough to fulfill the hacker's requirements. Hackers often use the following techniques for gathering information:

- Footprinting through Search Engines
- Footprinting through Advanced Google Hacking Techniques
- Footprinting through Social Networking Sites
- Footprinting through Websites
- Footprinting through Email
- Footprinting through Competitive Intelligence
- Footprinting through WHOIS
- Footprinting through DNS
- Footprinting through Network
- Footprinting through Social Engineering

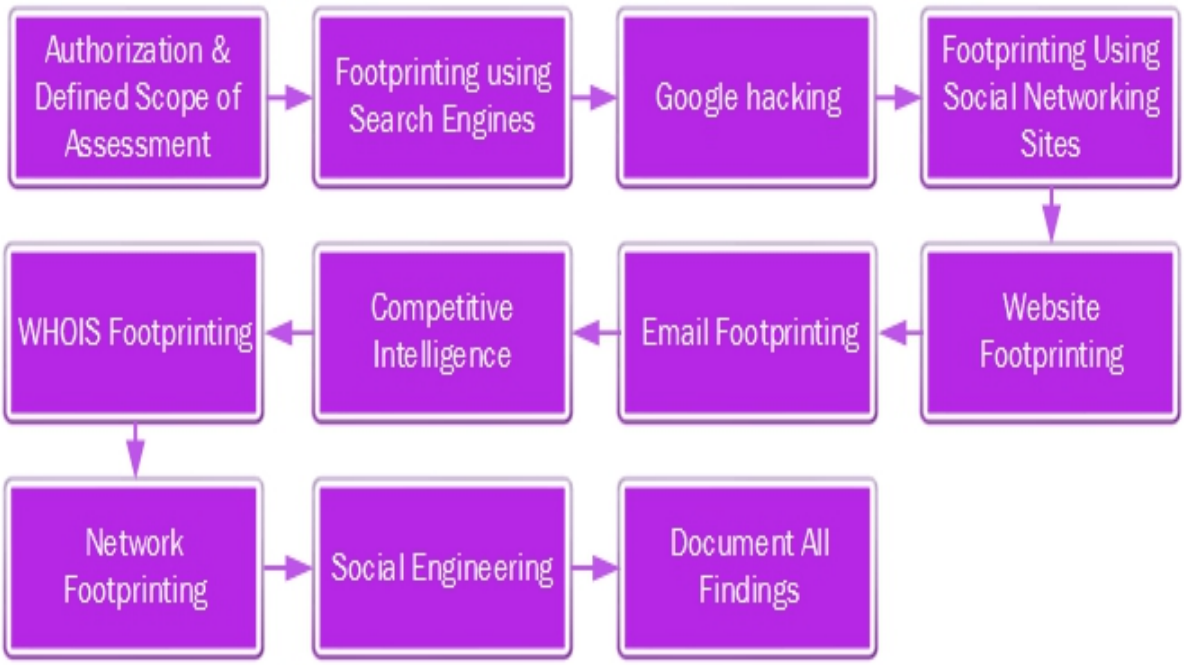


Figure 2-01: Footprinting Methodology

Footprinting through Search Engines

The most basic and responsive option is Footprinting through search engines. Search engines extract information from the internet about anything subject. You can open a web browser and use a search

engine, such as Google or Bing, to search for anything you want. The search engine generates results showing every piece of information available on the internet.

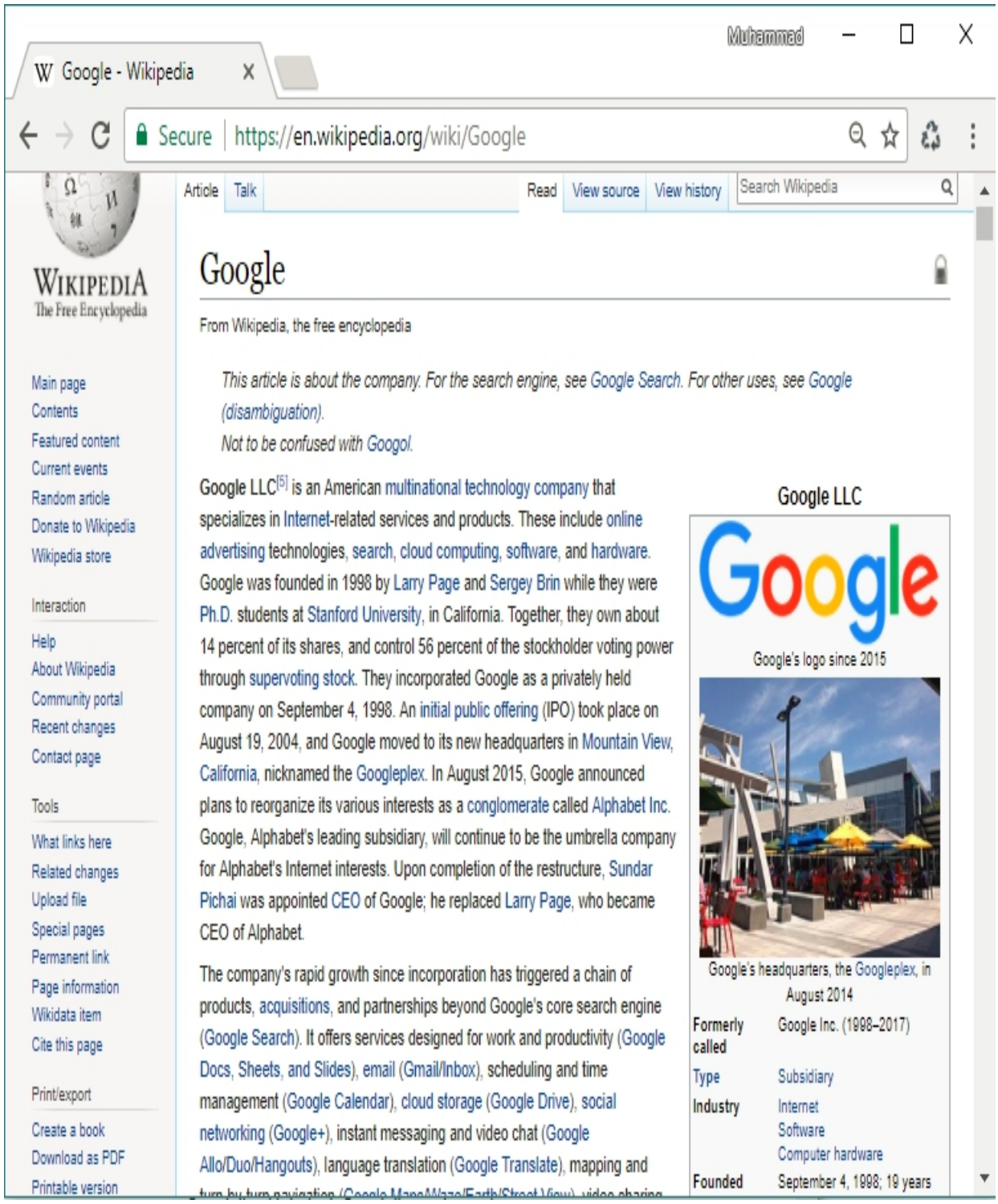


Figure 2-02: Footprinting

For example, Figure 2-02 shows the information generated about the world's most popular search engine when searching for Google. This information includes the location of the headquarters, the date on which the organization was found, the names of founders, the number of employees, the parent organization, the link of the official website, etc. To get more information about Google, you can access its official website from the given link.

As well as this publically available information, website and search engine caches can also provide information that is not available, updated, or modified on the official website.

Finding a Company's Public and Restricted Websites

During the process of collecting information, an attacker also collects information of an organization's official website including its public and restricted URLs. The official website's URL can simply be obtained through search engines as previously explained. However, to find the restricted URL of an organization's website, the attacker will have to use different services that can fetch information from websites. One of these services includes using online tools such as www.netcraft.com .

Figure 2. 02: Netcraft Webpage

Figure 2-03: Netcraft webpage

Collect Location Information

After collecting the necessary information through search engines and different services like Netcraft and Shodan, an attacker can start collecting location information. Information like the physical location of the headquarters, what surrounds it, the location of branch offices, and other related information can be collected from online location and map services.

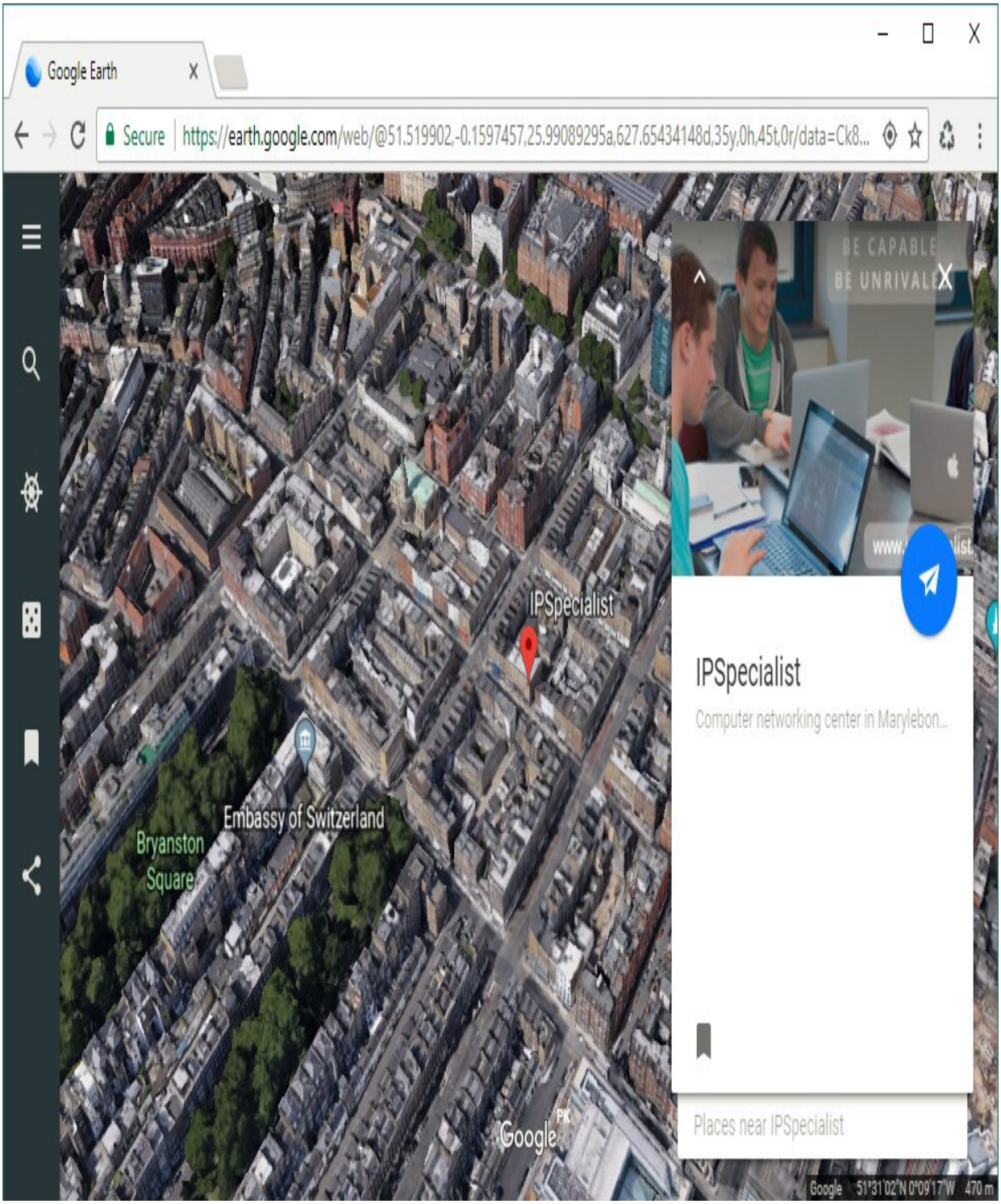


Figure 2-04: Collection of Location Information

Some of the most popular online services are:

- Google Earth
- Google Map

- Bing Map
- Wikimapia
- Yahoo Map

Online People Search Services

Online services are available for looking up people's phone numbers and addresses. Some of these websites include:

- www.privateeye.com
- www.peoplesearchnow.com
- www.publicbackgroundchecks.com
- www.anywho.com
- www.intelius.com
- www.4 1 1 1.com
- www.peoplefinders.com

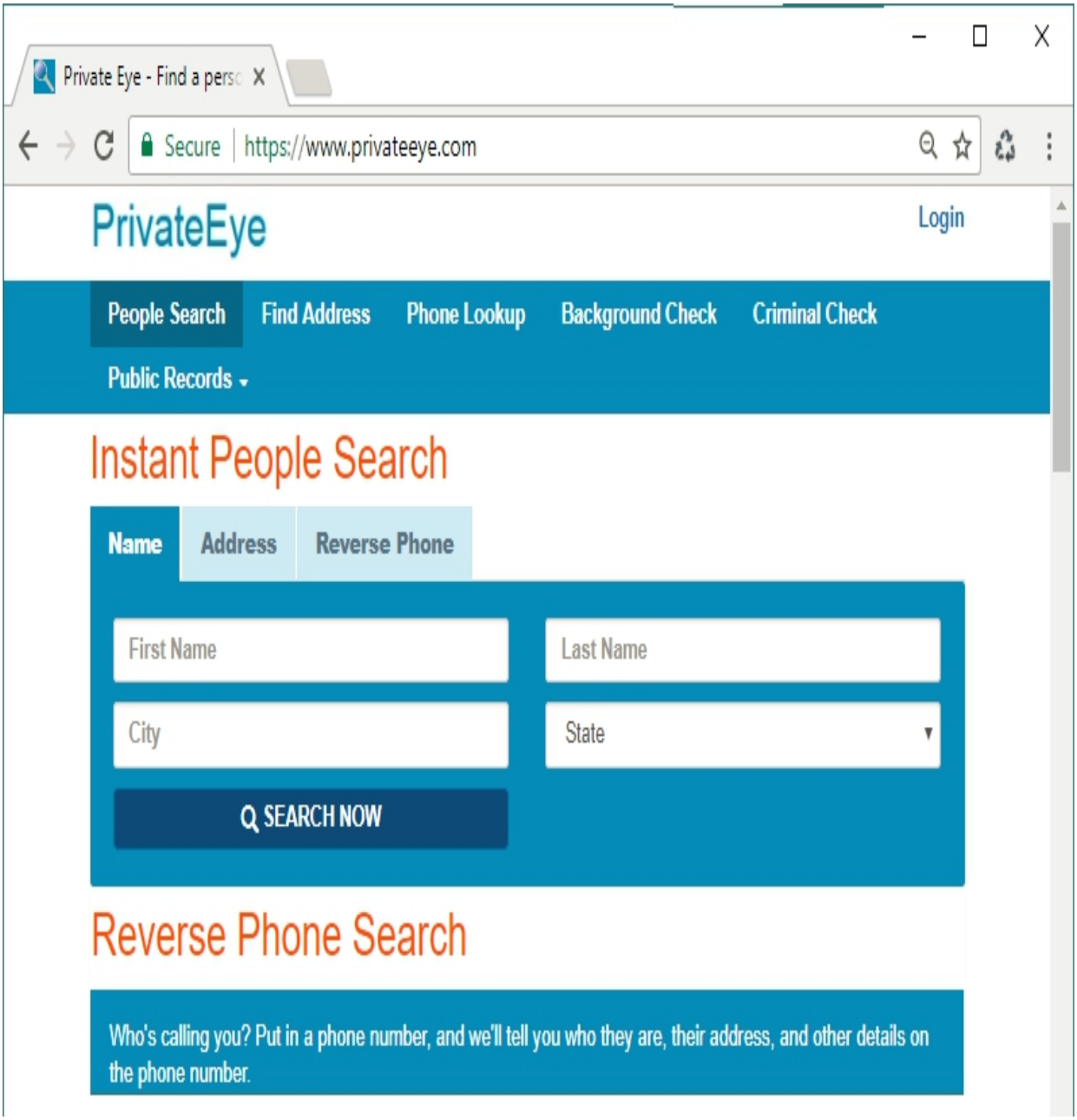


Figure 2-05: Online People Search Service

Gathering Information from Financial Services

There are some Financial Services available online, powered by different search engines, that provide financial information about internationally known organizations. By just searching for your target organization, you can obtain their financial information. The most popular Online Financial Service providers are Google (www.google.com/finance) and Yahoo (finance.yahoo.com).

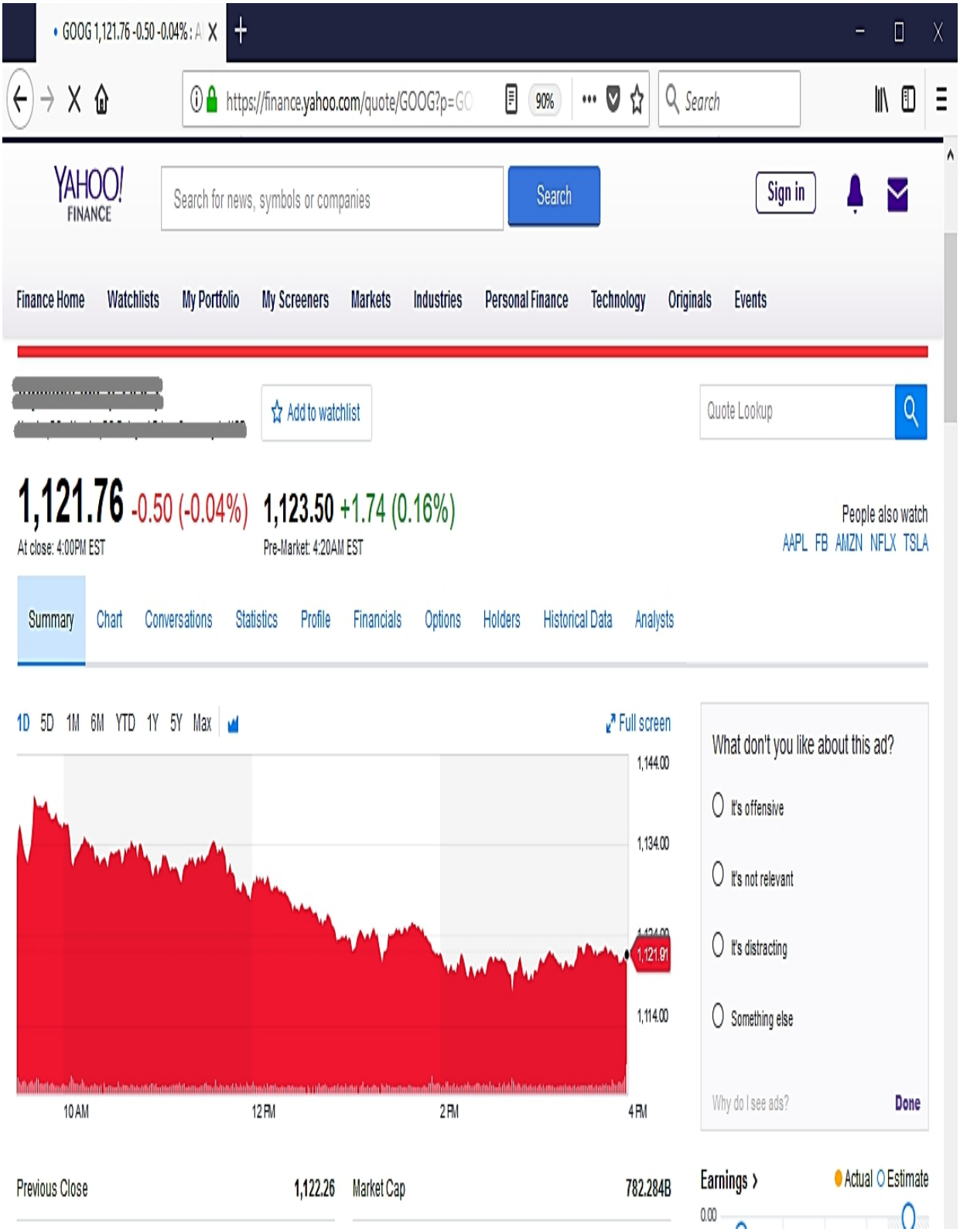


Figure 2-06: Financial Services

Footprinting through Job Sites

On Job Sites, organizations that offer job vacancies provide their organization's information and portfolio as well as the job post. This information includes the company's location, industry information, contact information, the number of employees, job requirements, and hardware and software information. Similarly, personal information can be collected from a targeted individual by posting a fake job vacancy on such sites. Some of the most popular job sites are:

- www.linkedIn.com
- www.monster.com
- www.indeed.com
- www.careerbuilder.com

Monitoring a Target Using Alerts

Google, Yahoo, and other alert services offer content monitoring services through an alert feature that notifies the subscriber about the latest and up-to-date information related to the subscribed topic.

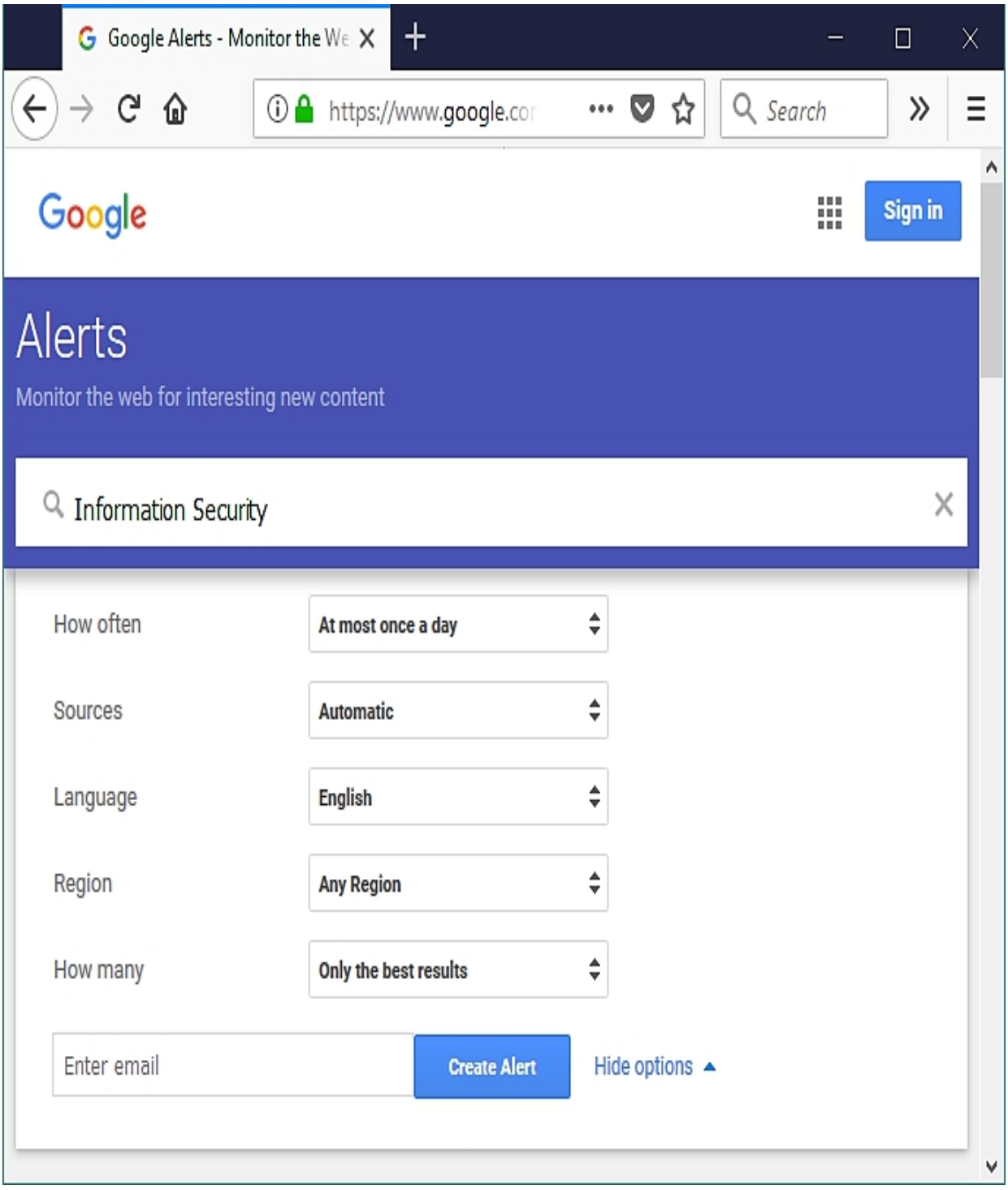


Figure 2-07: Alert Service by Google

Gathering Information Using Groups, Forums, and Blogs

Groups, forums, blogs, and communities can be a great source of sensitive information. Joining these platforms using a fake ID and accessing the target organization's group is not difficult for anyone

these days. Any official and non-official group can become a source for the leakage of sensitive information.

Footprinting Using Advanced Google Hacking Techniques

Google Advanced Search Operators

Some advanced operators can be used to modify a search for a specific topic using search engines. These advanced search operators make the search more focused and appropriate to a task. Google's advanced search operators are as follows:

Advanced Operators

site :
related : cache :
link :
allintext : intext :
allintitle : intitle :
allinurl : inurl :
Search Description

Search for the result in the given domain
Search for similar web pages
Display the web pages stored in the cache
List the websites with a link to a specific web page Search for websites containing a specific keyword Search for documents containing a specific keyword Search for websites containing a specific keyword in the title Search for documents containing a specific keyword in the title Search for websites containing a specific keyword in URL Search for documents containing a specific keyword in URL

Table 2-01: Google Advanced Search Operators

For Google Advanced Search, you can also go to the following URL:
https://www.google.com/advanced_search

Google

Advanced Search

Find pages with...		To do this in the search box.
all these words:		Type the important words: `tri-colour rat terrier`
this exact word or phrase:		Put exact words in quotes: `"rat terrier"`
any of these words:		Type `OR` between all the words you want: `miniature OR standard`
none of these words:		Put a minus sign just before words that you don't want: `-rodent, -"Jack Russell"`
numbers ranging from:	to	Put two full stops between the numbers and add a unit of measurement: `10..35 kg, £300..£500, 2010..2011`

Then narrow your results by...

language:	any language	Find pages in the language that you select.
region:	any region	Find pages published in a particular region.
last update:	anytime	Find pages updated within the time that you specify.
site or domain:		Search one site (like `wikipedia.org`) or limit your results to a domain like `.edu`, `.org` or `.gov`
terms appearing:	anywhere in the page	Search for terms in the whole page, page title or web address, or links to the page you're looking for.
SafeSearch:	Show most relevant results	Tell SafeSearch whether to filter sexually explicit content.
file type:	any format	Find pages in the format that you prefer.
usage rights:	not filtered by licence	Find pages that you are free to use yourself.

Advanced Search

Figure 2-08: Footprinting with Google Advanced Search

Google Hacking Database (GHDB)

Google hacking, also known as "Google Dorking", is a combination of computer hacking techniques for finding security holes within an organization's network and systems using Google search and other applications powered by Google. Google Hacking was popularized by Johnny Long. He categorized the internet search engine queries in a database known as the Google Hacking Database (GHDB). This categorized database of queries is designed to uncover information, such as sensitive information and information related to updates, which can be used for exploiting different frameworks. This information might be confidential and not publically available. Google hacking is used to speed up searches. As shown in Figure 2-09, through www.exploit-db.com, you can search GHDB or browse the category of GHDB. Similarly, www.hackersforcharity.org is also an online platform for GHDB.

Enter the following URL:
https://www.exploit-db.com/google-hacking-database/

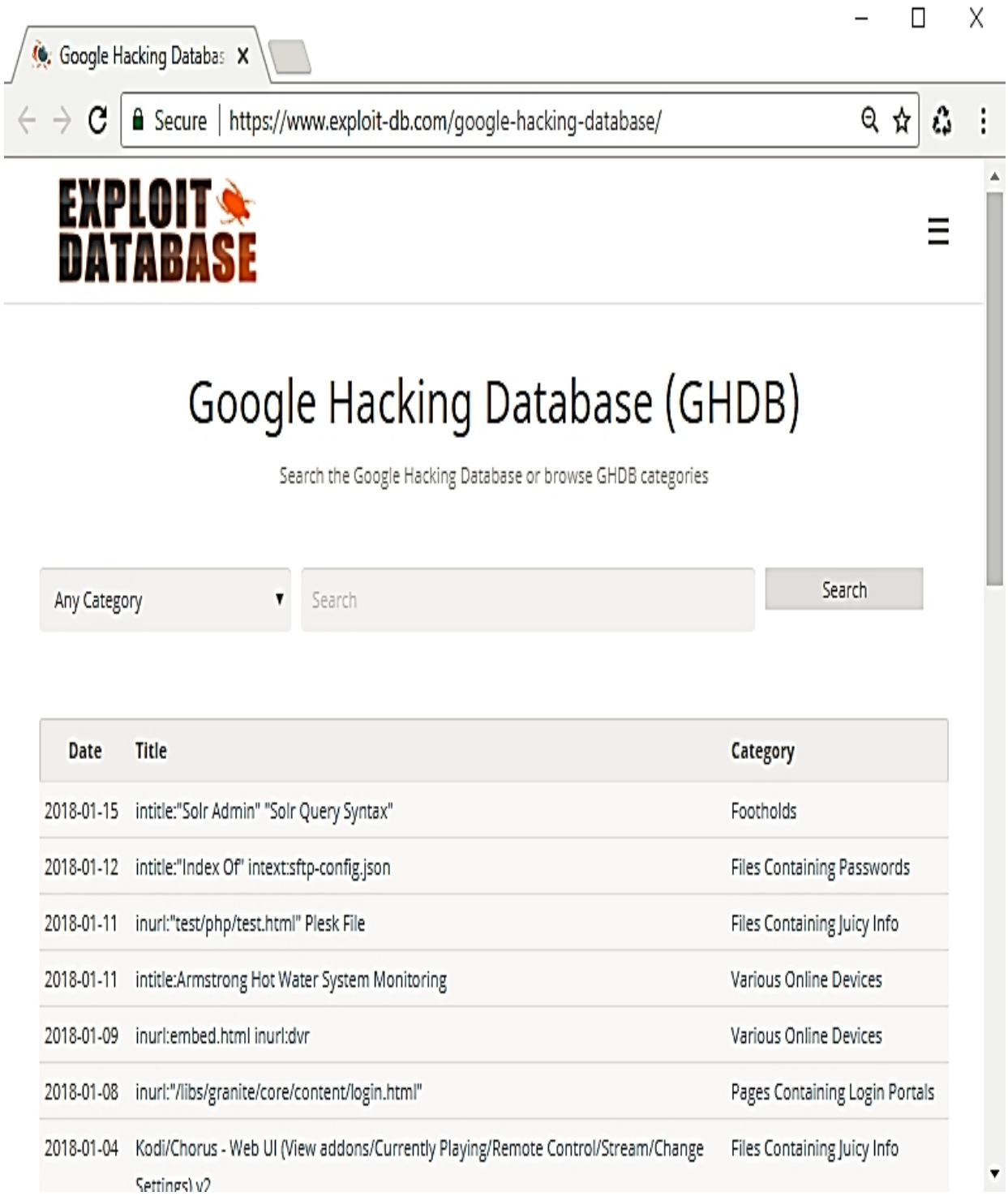


Figure 2-09: Google Hacking Database

The Google hacking database provides updated information that is useful for exploitation such as footholds, sensitive directories, vulnerable files, error messages and much more.

Footprinting through Social Networking Sites

Social Engineering

Social Engineering in information security refers to the technique of psychological manipulation. This trick is used to gather information from people through different social networking platforms for hacking and using the information to get close to the target.

Footprinting using Social Engineering on Social Networking Sites

Social Networking is one of the best information sources. Popular and most widely used social networking sites have made it quite easy to find information about someone. This information includes both personal and sensitive information. Advanced features on these social networking sites also provide up-to-date information. An example of footprinting through social networking is finding someone on Facebook, Twitter, LinkedIn, Instagram, and many more similar platforms.

Figure 2-10: Social Networking Sites

Social Networking is not only a source of entertainment, but it also connects people personally, professionally, and traditionally. Social networking platforms can provide plenty of information about an individual. Simply searching for an organization's or individual's name on social networking sites generates results which show the target's photo, personal information, contact details, etc.

What Users Do People maintain their profiles
People update their statuses
Information

• Photo of the target • • Contact number
• Email address
• Date of birth
• Location • • Work details

• Most recent personal information • • Most recent location
• Information about family & •

friends • • Activities & Interests
• Technology related information • • Upcoming events information

Table 2-02: Social Engineering
What attacker achieves

Personal information about a target including personal details, photo, etc.
Social engineering

Platform & Technology related information Target location
List of Employees / Friends / Family
Nature of business

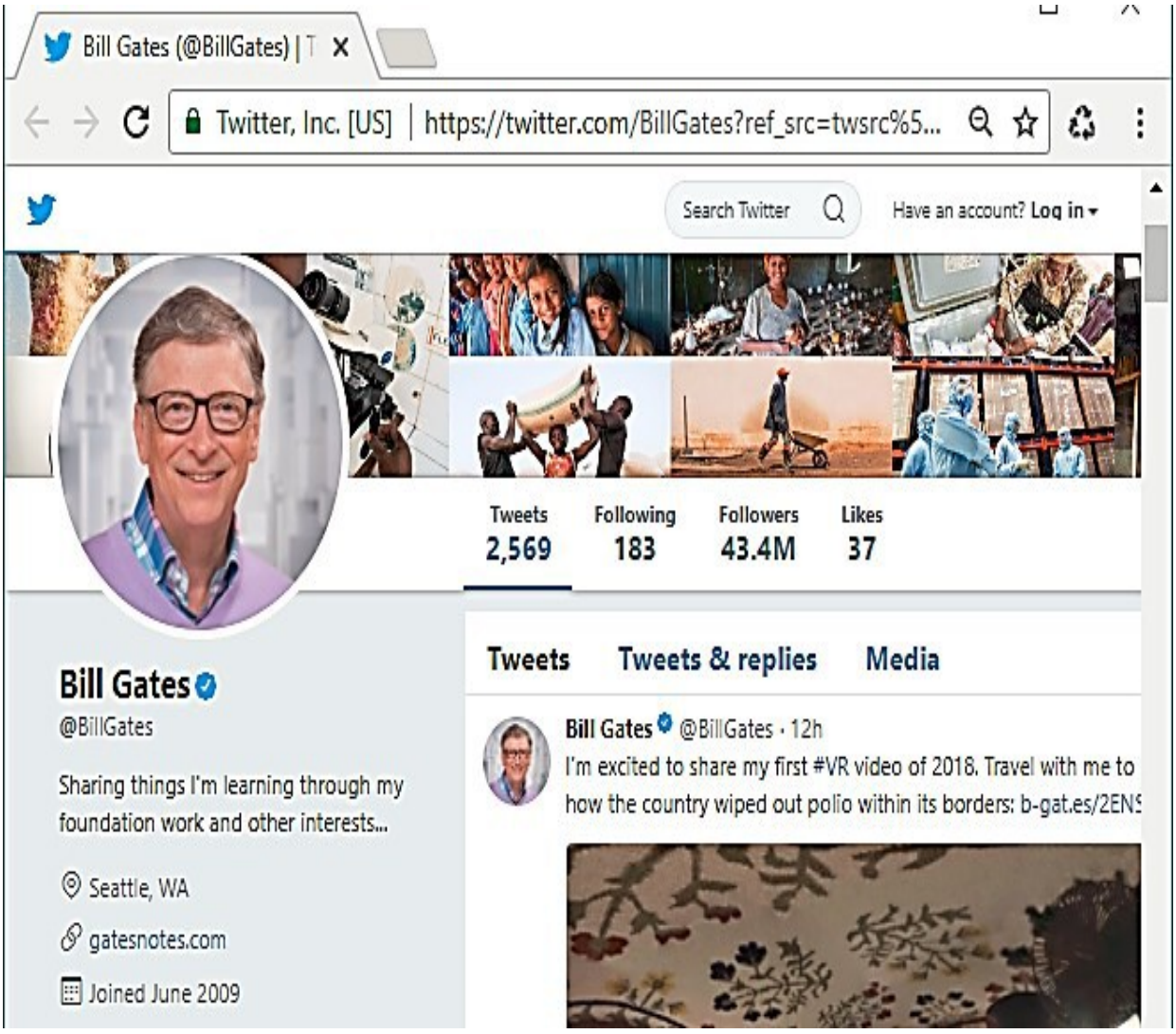
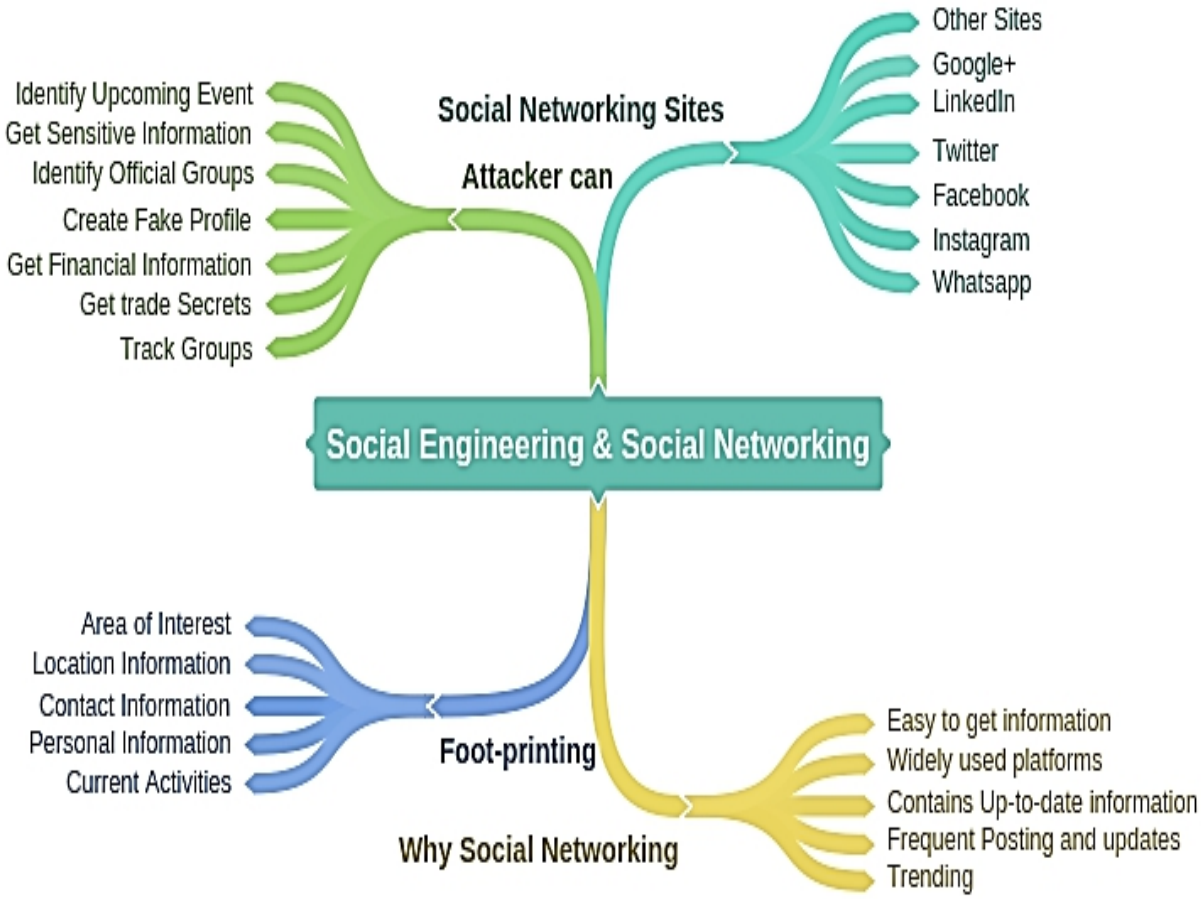


Figure 2-11: Collection of Information from Social Networking

A profile picture can help in identifying a target and personal information can be collected from the target's profile. By using this personal information, an attacker can create a fake profile using the same information. Posts have location links, pictures and other information, which helps in identifying the target's location. Timelines and stories can also reveal sensitive information. By collecting information about interests and activities, an attacker can join several groups and forums for more footprinting. Furthermore, information that can be extracted easily from social media posts includes the type of business, technology in use, platforms used by the target, etc. People do not think before they post something on social media platforms. Their posts

may contain enough information for an attacker to gain access to their systems.

Mind Map



Website Footprinting

Website Footprinting includes monitoring and investigating the target organization's official website for gaining information such as the software being used, the versions of this software, Operating Systems, sub-directories, database, scripting information, and other details. This information can be gathered with the help of online services like netcraft.com as defined earlier or by using software such as Burp Suite, Zaproxy, Website Informer, Firebug, and others. These tools can extract information such as connection type and connection status, and information on recent modifications done on a website. By getting this type of information, an attacker can examine source code, developer's details, file system structure, and scripting.

Determining the Operating System

Using websites such as Netcraft.com can also help in searching for Operating Systems that are in use by the targeted organizations. Simply go to the website www.netcraft.com and enter the target organization's official URL. The results in the figure below are hidden to avoid legal issues.

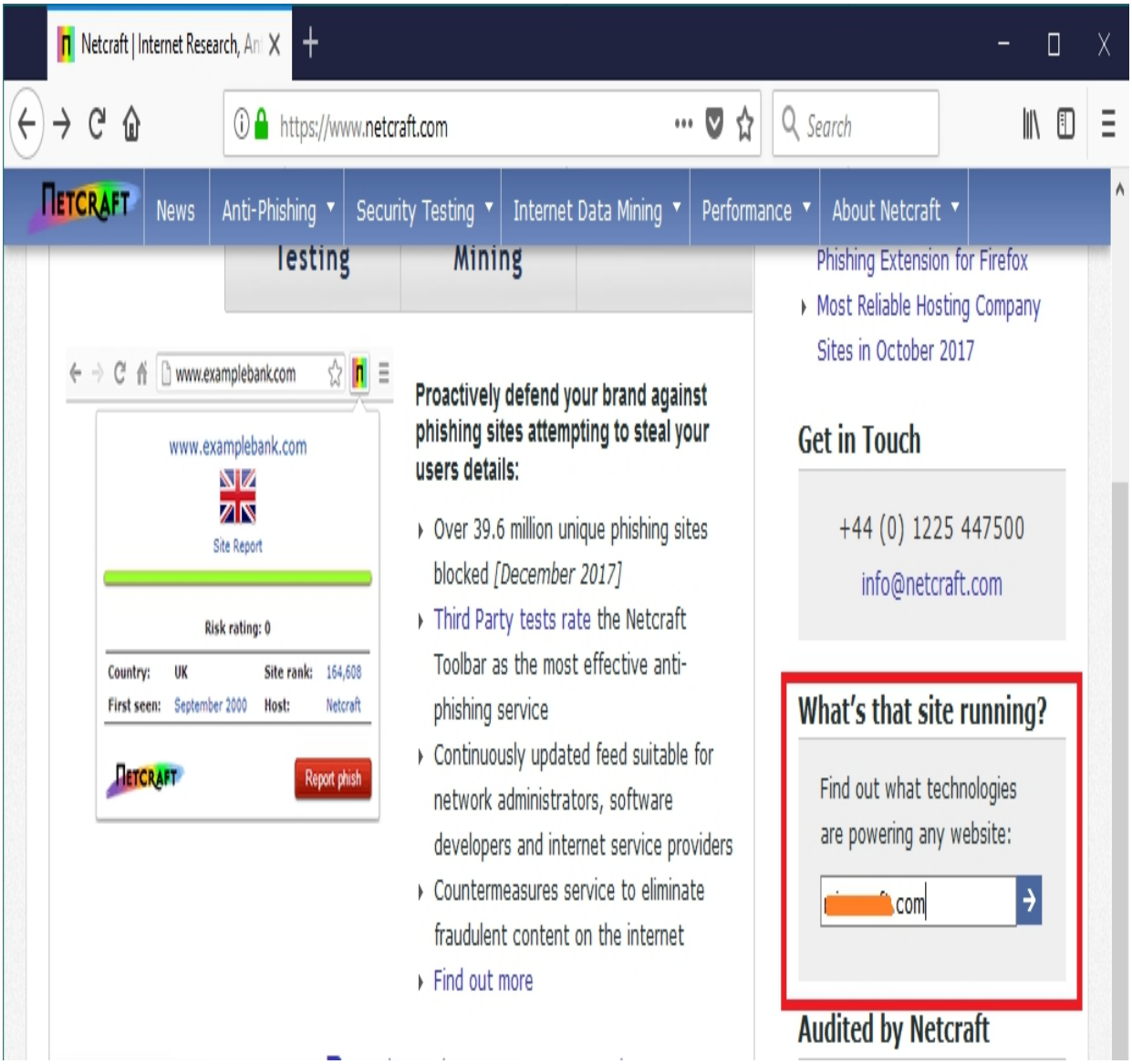


Figure 2-12: Determination of Website Information

The result includes all websites related to the domain of that organization, including Operating System information and other

information. If you enter a complete URL, it shows the in-depth detail of that particular website.

Figure 2-13: Determination of Operating System Information

Another popular online option for searching the detailed information of websites is Shodan, i.e., www.shodan.io . The SHODAN search engine lets you find connected devices such as routers, servers, IoT, and other devices by using a variety of filters. Go to the following URL:

www.shodan.io

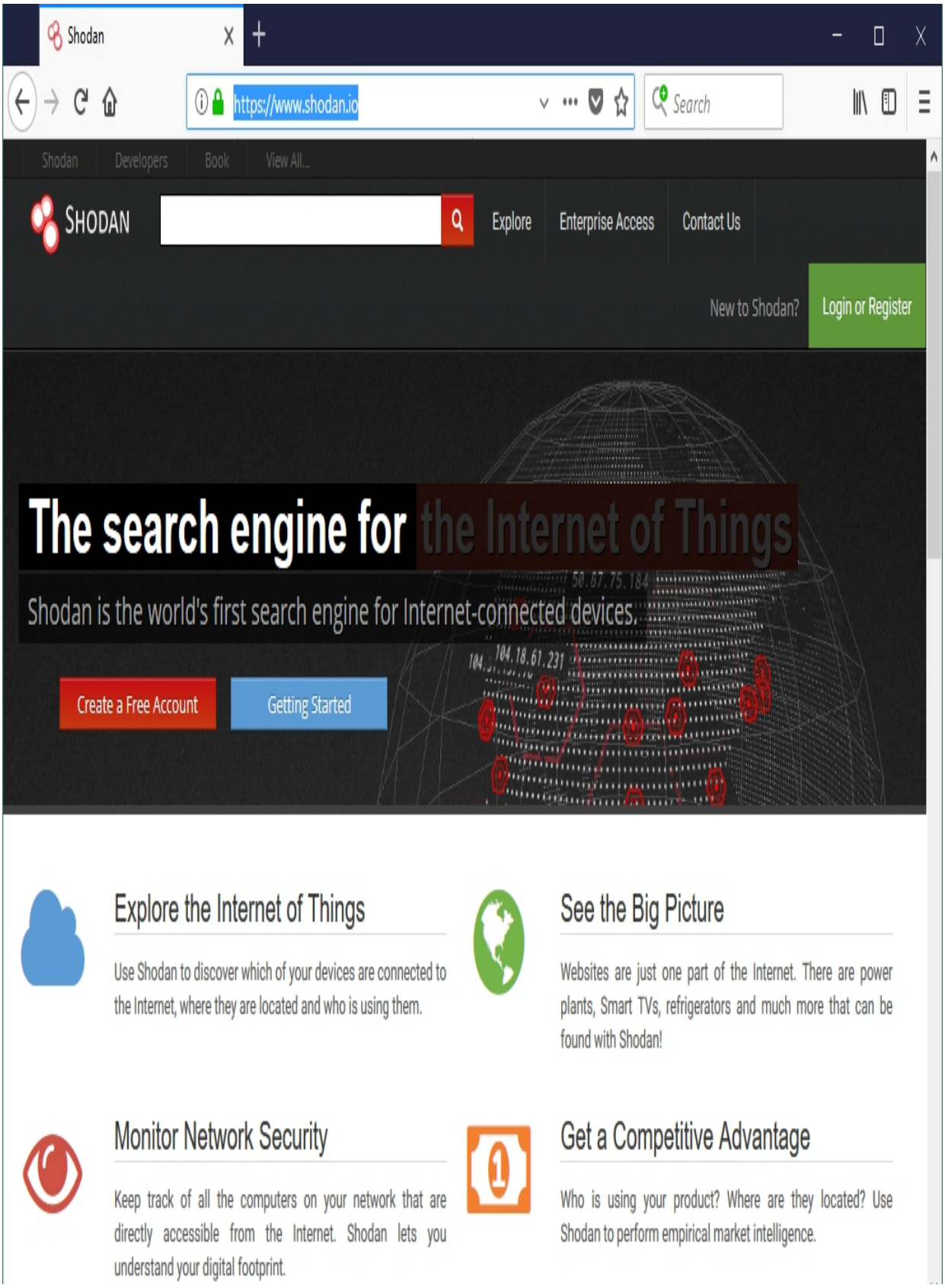


Figure 2-14: Determination of Website Information

Now, search for any device such as CSR 1000v, as shown in figure 2-15:

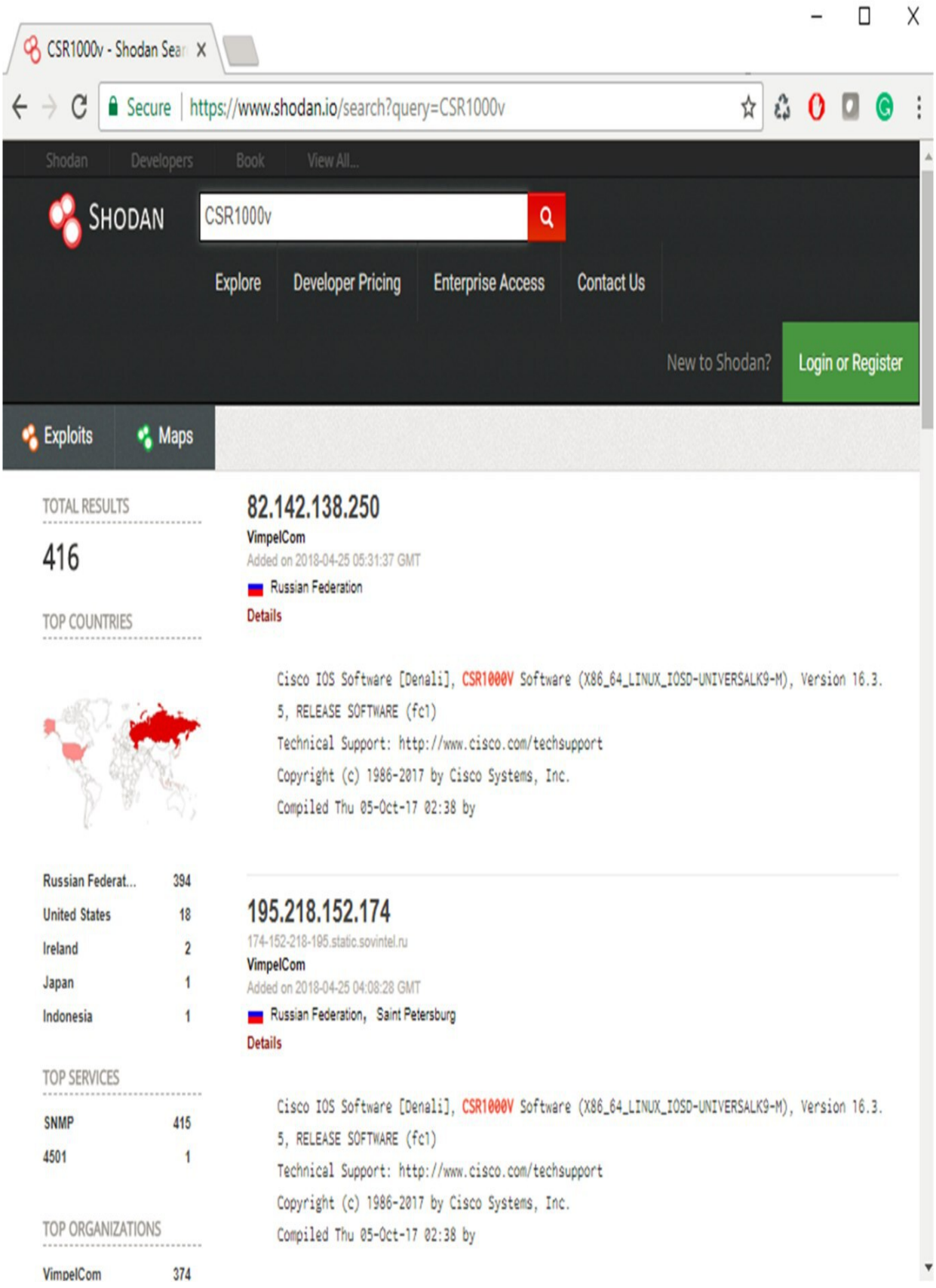

CSR1000v - Shodan Sear
Secure
https://www.shodan.io/search?query=CSR1000v
Shodan
Developers
Book
View All...
SHODAN
CSR1000v
Explore
Developer Pricing
Enterprise Access
Contact Us
New to Shodan?
Login or Register
Exploits
Maps
TOTAL RESULTS
416
TOP COUNTRIES
Russian Federat... 394
United States 18
Ireland 2
Japan 1
Indonesia 1
TOP SERVICES
SNMP 415
4501 1
TOP ORGANIZATIONS
VimpelCom 374
82.142.138.250
VimpelCom
Added on 2018-04-25 05:31:37 GMT
Russian Federation
Details
Cisco IOS Software [Denali], CSR1000V Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.3.
5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 05-Oct-17 02:38 by
195.218.152.174
174-152-218-195.static.sovintel.ru
VimpelCom
Added on 2018-04-25 04:08:28 GMT
Russian Federation, Saint Petersburg
Details
Cisco IOS Software [Denali], CSR1000V Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.3.
5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 05-Oct-17 02:38 by

Figure 2-15: Shodan Search Engine

The search of the CSR 1000v device listed 4 16 results along with IP addresses, Cisco IOS software version information, location information, and other details.

Website Footprinting Using Web Spiders

Web Spiders or *Web Crawlers* are the internet bots used to perform regular and automated browsing on the World Wide Web. This crawling on a targeted website gathers specific information such as names and email addresses.

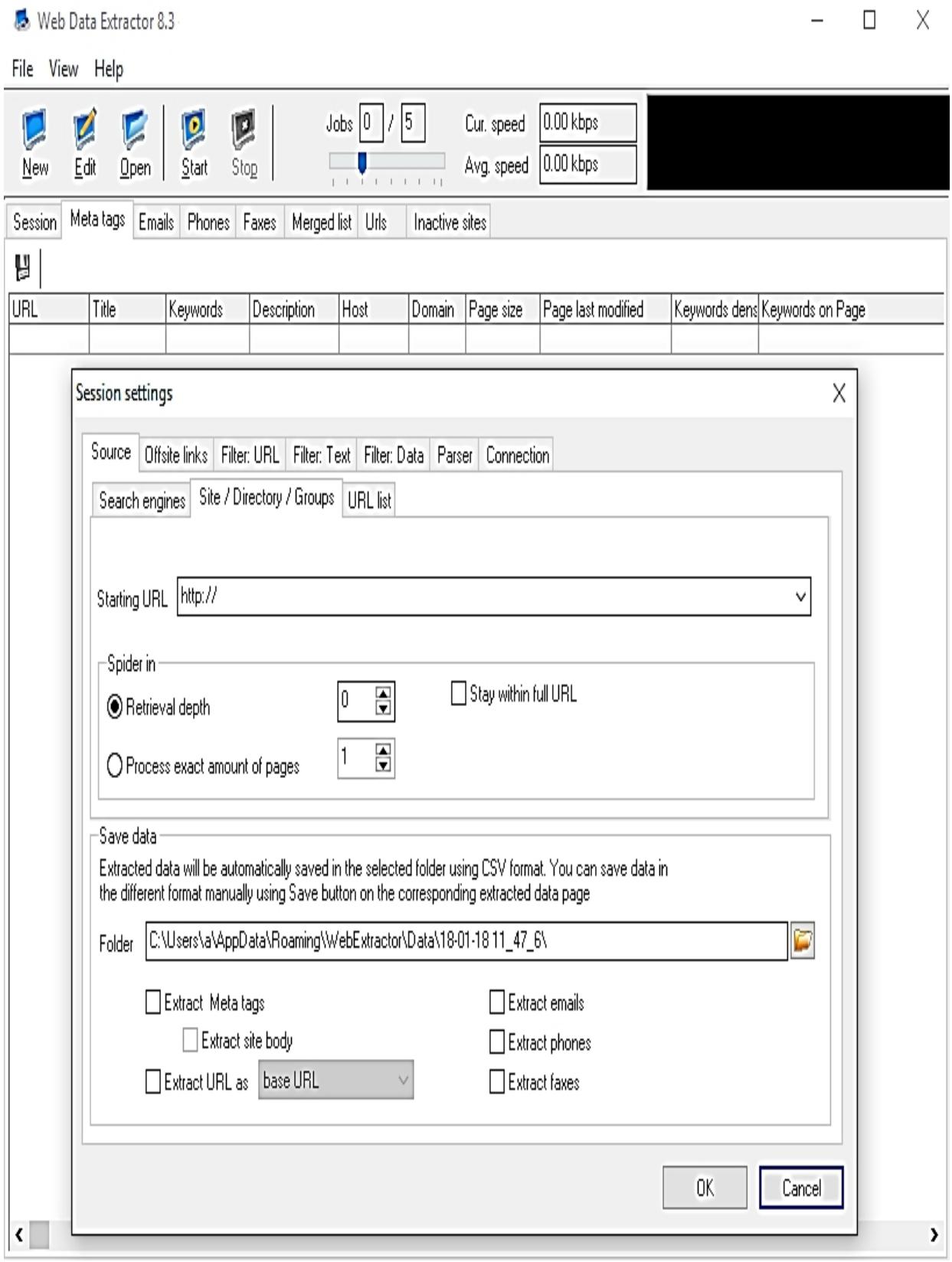


Figure 2-16: Web Data Extractor Application (Web Spider)

Mirroring an Entire Website

Mirroring a website is the process of replicating the entire website in a local directory. Downloading an entire website onto a local directory enables the attacker to use and inspect the website, its directories, and its structure. It also enables the attacker to find

other vulnerabilities from this downloaded copy in an offline environment. Several mirroring tools are available that can download a website. Additionally, they are capable of mirroring all directories, HTML, and other files from the server to a local directory.

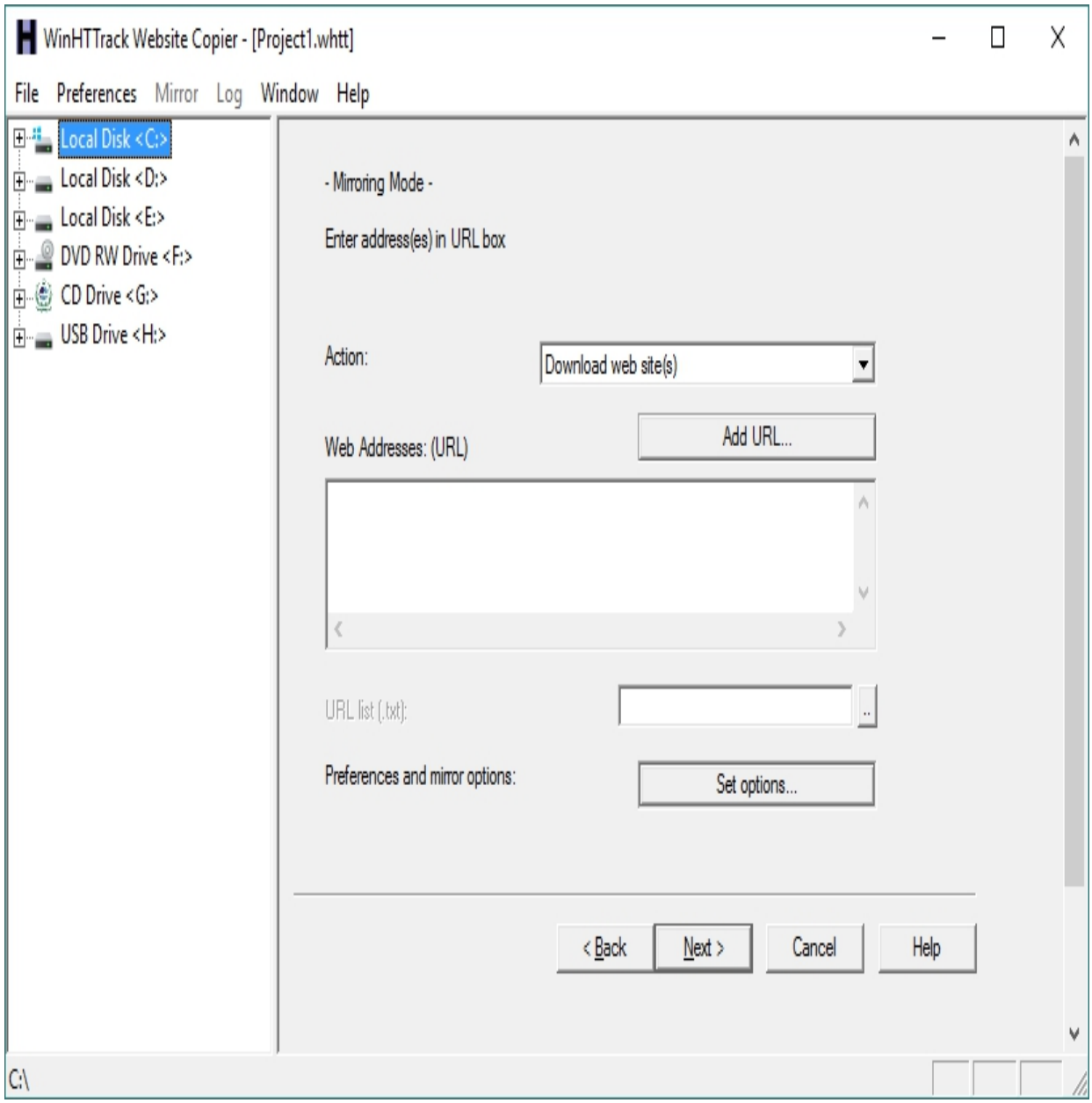


Figure 2-17: WinHTTrack Website Copier

Website Mirroring Tools Website mirroring tools include:

Software

Win HTTrack Website Copier Surf offline Professional
Black Widow
NCollector Studio
Website Ripper Copier
Teleport Pro
Portable Offline Browser

PageNest
Backstreet Browser
Offline Explorer Enterprise
GNU Wget
Hooeey Webprint

Websites https://www.httrack.com/page/2/
http://www.surfoffline.com/ http://softbytelabs.com
http://www.calluna-software.com http://www.tensons.com
http://www.tenmax.com http://www.metaproducts.com
http://www.pagenest.com http://www.spadixbd.com
http://www.metaproducts.com http://www.gnu.org.com
http://www.hooeeywebprint.com

Table 2-03: Website Mirroring Tools

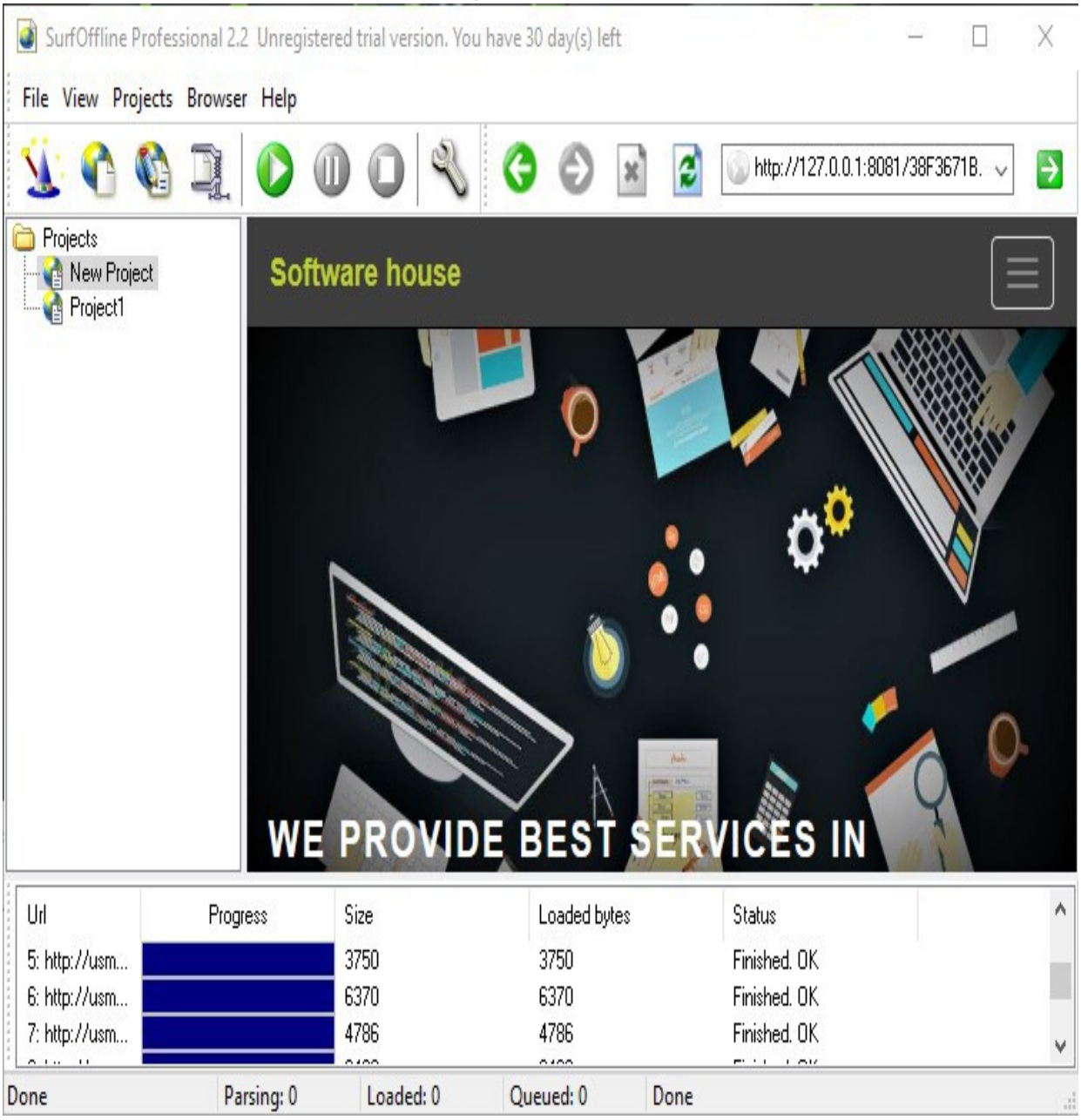


Figure 2-18: Surf Offline Professional Application

Extract Website Information

Archive.com is an online service that provides an archived version of websites. The result consists of a summary of the website including a summary on the MIME-type count, summary for TLD/HOST/Domain, a sitemap of the website and dates, calendar views, and other information.

Extracting Information Using the Wayback Machine

1. Go to the following URL:
https://web.archive.org
2. Search for a target website.
3. Select the year from the calendar.

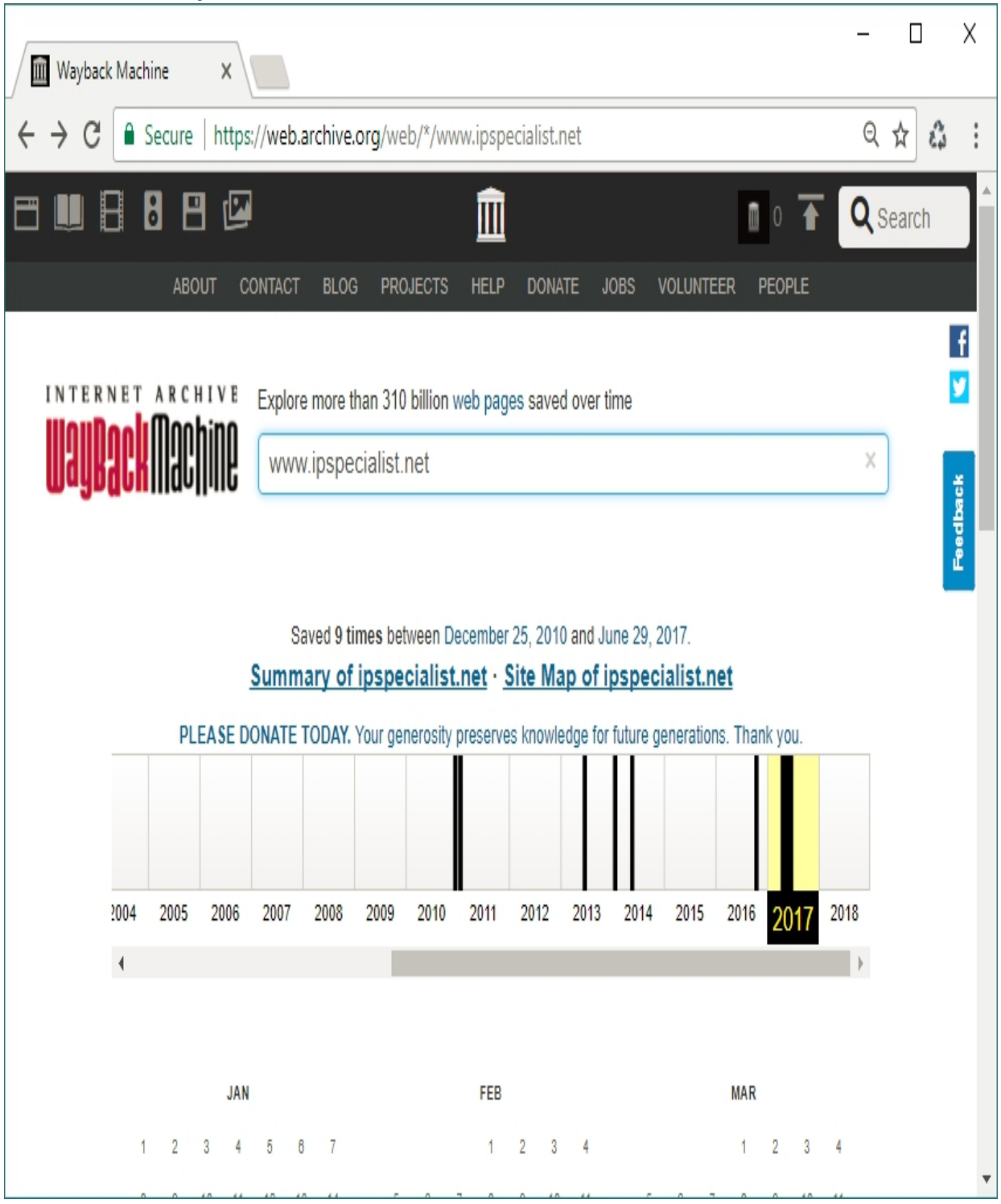


Figure 2-19: Archive.com Wayback Machine

4. Select a date from the highlighted dates on the calendar.

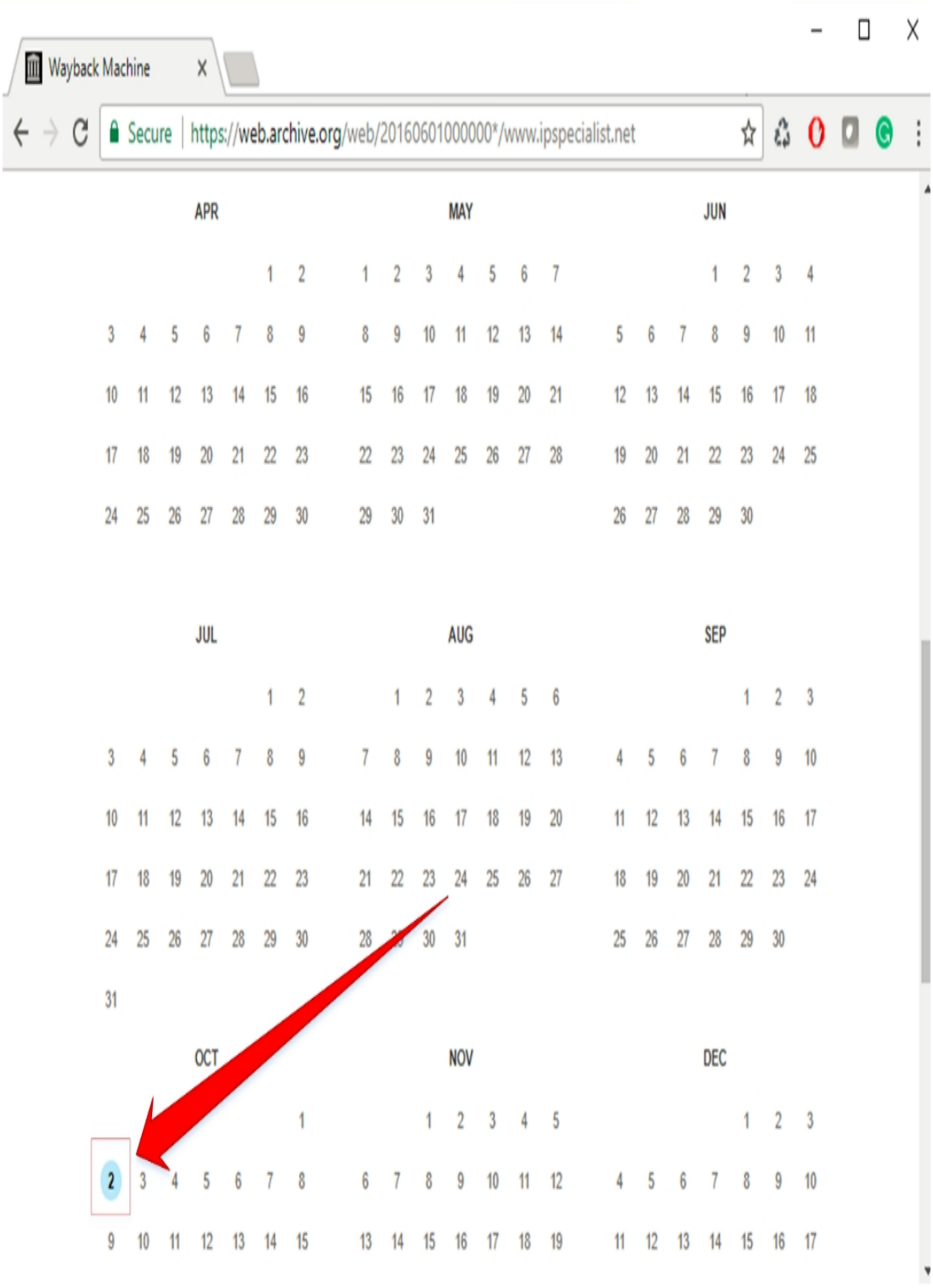

Wayback Machine
Secure
https://web.archive.org/web/20160601000000*/www.ipspecialist.net
APR
1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
MAY
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31
JUN
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30
JUL
1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
AUG
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 30 31
SEP
1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30
OCT
1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
NOV
1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
DEC
1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17

Figure 2-20: Select Date

5. Following is a snapshot of the website on October 2, 20 16.

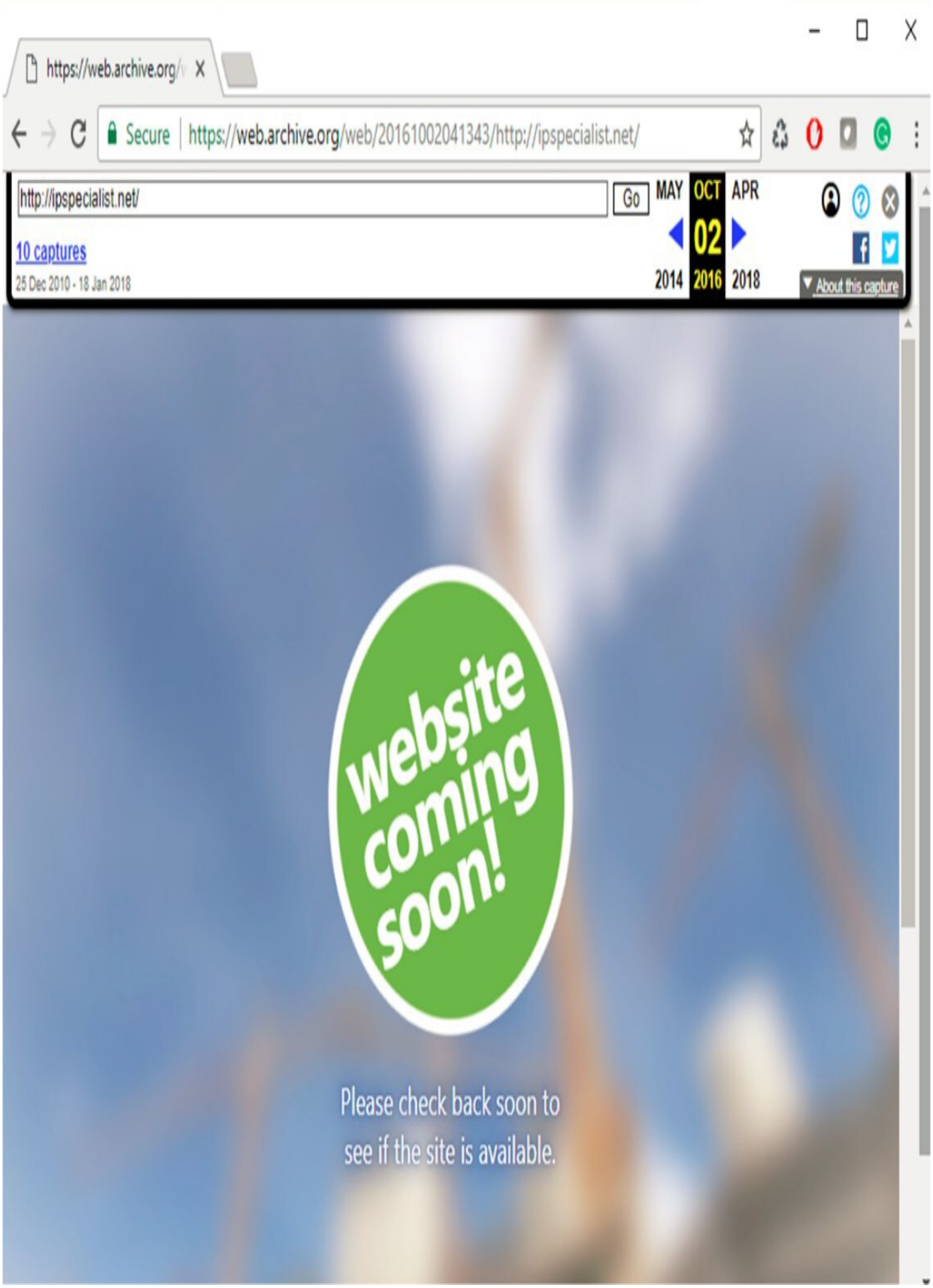

https://web.archive.org/
Secure
https://web.archive.org/web/20161002041343/http://ipspecialist.net/
http://ipspecialist.net/
Go
MAY
OCT
APR
02
10 captures
25 Dec 2010 - 18 Jan 2018
2014
2016
2018
About this capture
website coming soon!
Please check back soon to see if the site is available.

Figure 2-21: Archived Snapshot of a Website

Monitoring Web Updates

Website-Watcher and other similar available tools offer website monitoring. These tools automatically check for updates and changes made to target websites.

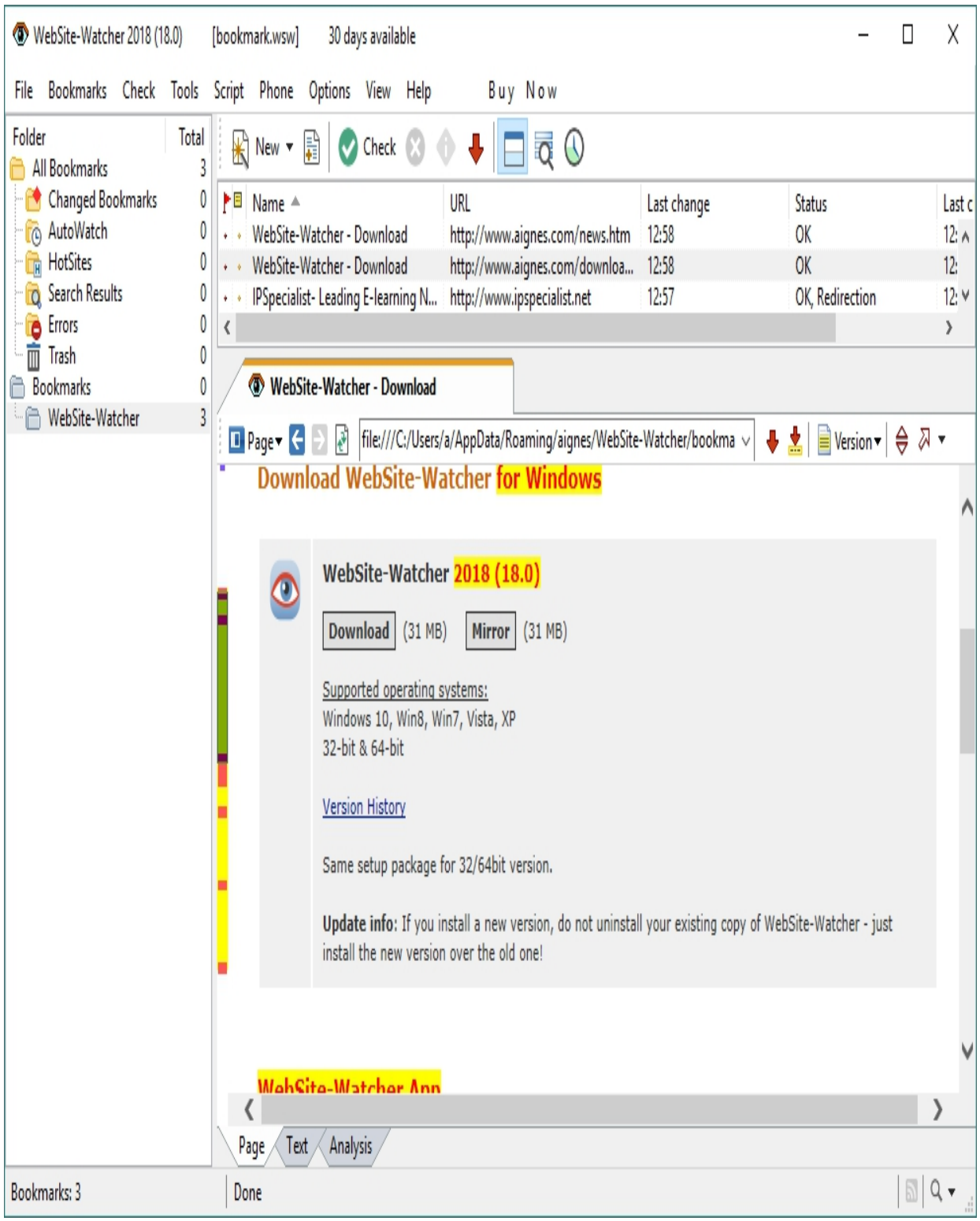


Figure 2-22: Website Watcher Application

Some other Website Monitoring Tools are:

Monitoring Tools Websites Change Detection http://www.changedetection.com Follow That Page

http://www.followthatpage.com Page2RSS http://page2rss.com Watch That Page http://www.watchthatpage.com Check4Change https://addons.mozilla.org OnWebChange http://onwebchange.com Infominder http://www.infominder.com TrackedContent http://trackedcontent.com Websnitcher https://websnitcher.com Update Scanner *Table*

https://addons.mozilla.org *2-04: Website Monitoring Tools*

Email Footprinting

Email plays an essential role in the running an organization's business. Email is one of the most popular, widely used, professional methods of communication and is used by every organization for communicating with partners, employees, competitors, contractors, and other people involved in the organization's daily business. The content or the body of an email is extremely valuable to attackers. This content may include hardware and software information, user credentials, network and security device information, financial information, etc. These details are valuable for penetration testers and attackers.

Polite Mail is a handy tool for email footprinting. *Polite Mail* tracks email communication with Microsoft Outlook. It is a flexible tool that can list a number of email addresses of a target organization, send a malicious link to all of them and track all the events individually. Tracing an email using an email header can reveal the following information:

- Destination address
- Sender's IP address
- Sender's Mail server
- Time and Date information
- Authentication system information of sender's mail server

Tracking Email from an Email Header

An email is tracked by its header. You can track an email from its header and trace the email hop by hop along with IP addresses, Hop Name, and location. Several online and software applications offer email

header tracking. *Email Tracker Pro* is one of the most popular tools for email tracking.

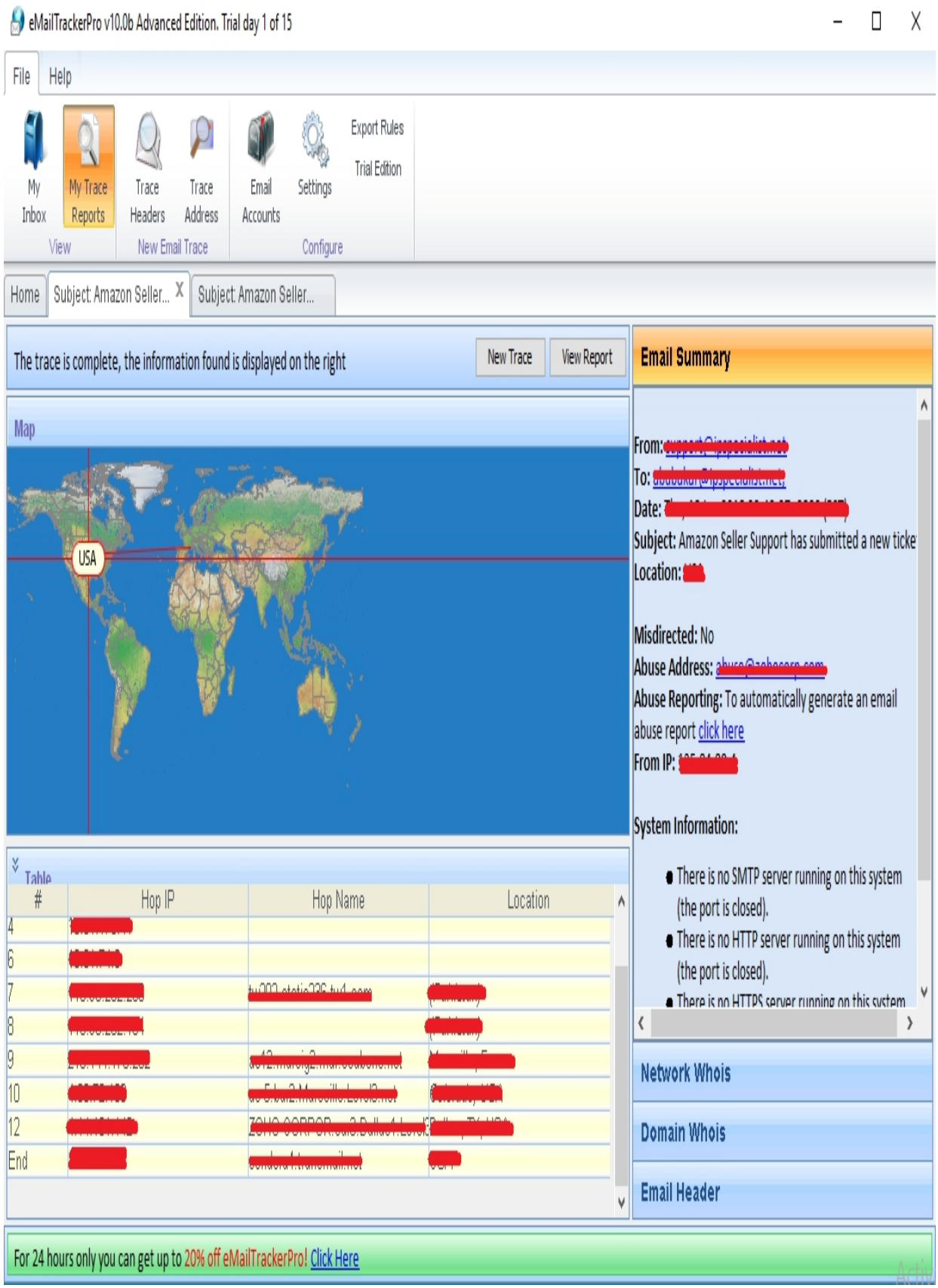


Figure 2- 22: Email Tracker Pro

Figure 2-23: Email Tracker Pro

Email Tracking Tools

Popular Email Tracking tools are as follows:

- Polite Mail
- Email Tracker Pro
- Email Lookup
- Yesware
- Who Read Me
- Contact Monkey
- Read Notify
- Did They Read It
- Get Notify
- Point of Mail
- Trace Email
- G-Lock Analytics

Competitive Intelligence

Competitive Intelligence is an approach to collecting information and analyzing and gathering competitors' statistics. Competitive Intelligence is non-interfering as it is the process of collecting information through different resources. Some primary sources of competitive intelligence are:

- Official Websites
- Job Advertisements
- Press Releases
- Annual Reports
- Product Catalogs
- Analysis Reports
- Regulatory Reports
- Agents, Distributors, and Suppliers

Competitive Intelligence Gathering

For competitive information, you should visit websites like EDGAR, LexisNexis, Business Wire, and CNBC. These websites gather information and reports of companies including legal news, press

releases, financial information, analysis reports, and upcoming projects and plans as well. For more information, visit the following websites:

Websites URL EDGAR https://www.sec.gov/edgar.shtml LexisNexis https://risk.lexisnexis.com Business Wire www.businesswire.com/portal/site/home/ CNBC www.cnbc.com Hoovers www.hoovers.com *Table 2-05: Competitive Intelligence Sources*

Penetration testers or attackers can identify the following information with the help of the above mentioned competitive intelligence tools:

- When the company was established
- Evolution of the company
- Authority of the company
- Background of the organization
- Strategies and planning
- Financial statistics
- Other information

Monitoring a Target Company's Website Traffic

There are some website monitoring tools that are being widely used by developers, attackers, and penetration testers to check the statistics of websites. These tools include Web-Stat and Alexa as popular tools for monitoring website traffic. Results show a website's ranking in the United States, its global ranking, a graphical view of users from all over the world, the number of users from different countries, the pages viewed daily, the time spent on the website, the number of sites linked with it, and other associated information.

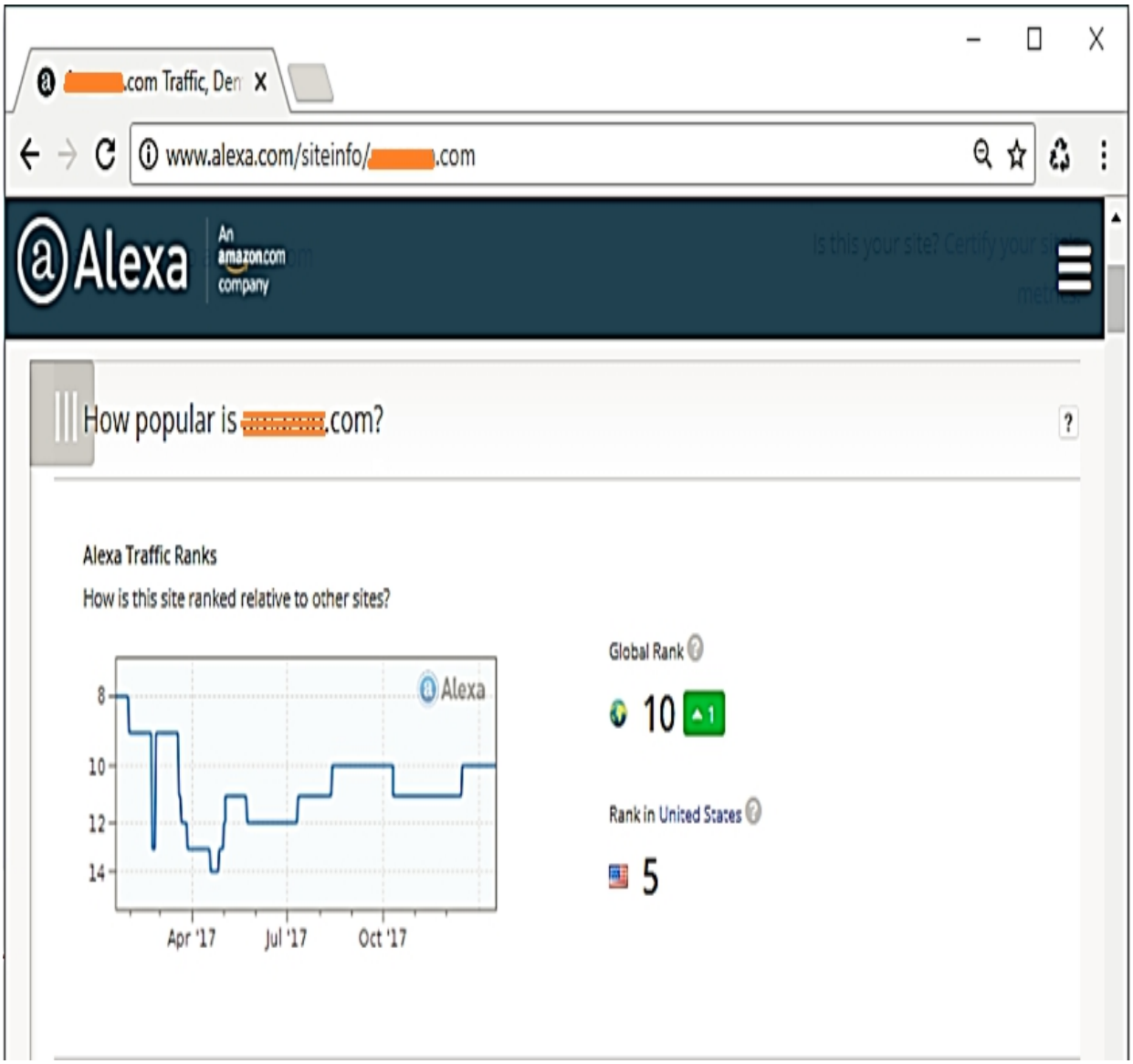


Figure 2-24: Website Statistics Using Alexa

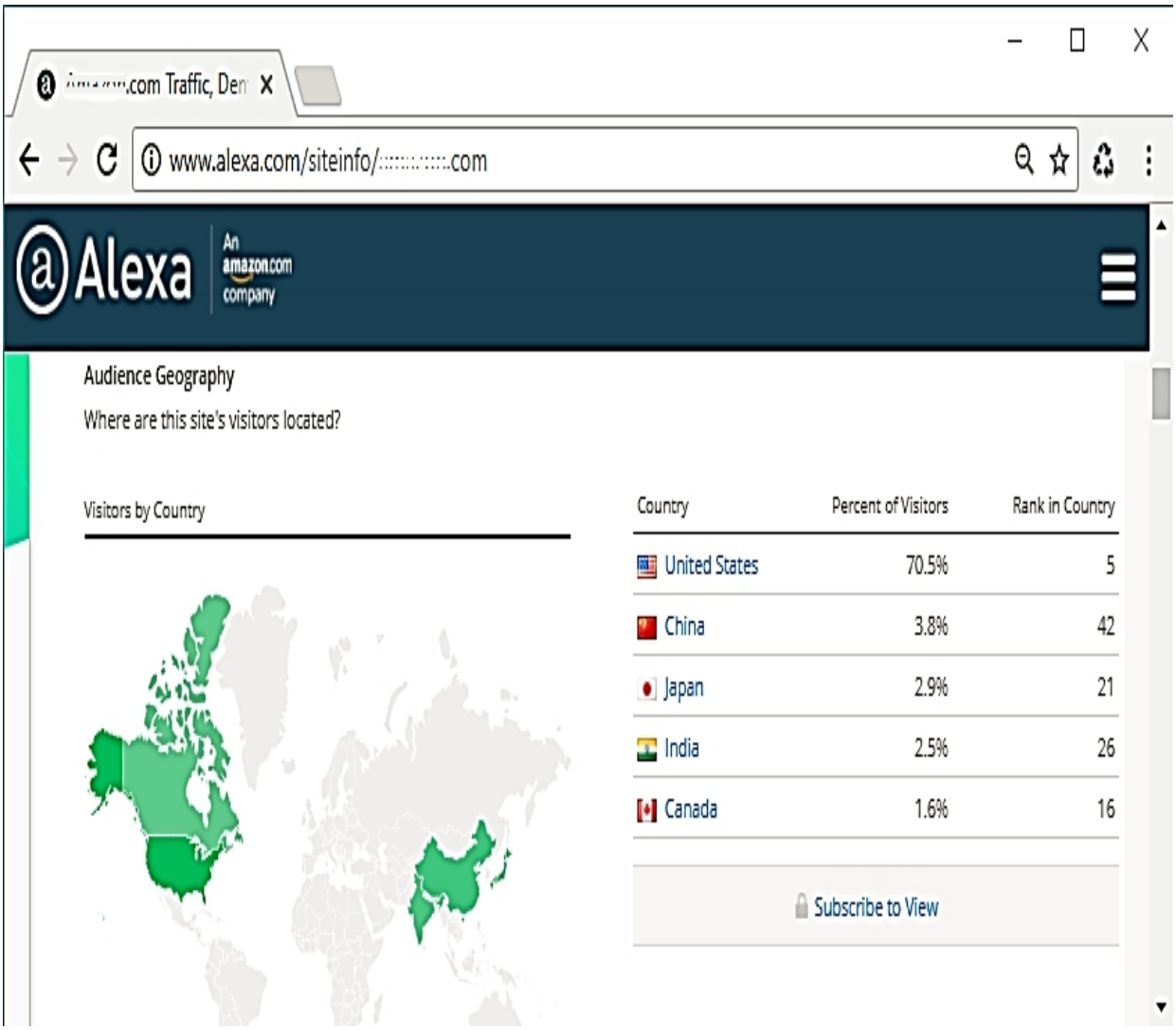


Figure 2-25: Website Statistics Using Alexa

In the figure above, the very popular site Amazon.com is searched by using the tool, Alexa. The results show its website ranking according to Alexa, the global ranking of the website and its rank in the United States. Scrolling down the page shows further results such as a geographical view of the audience, percentage, and ranking in every country, and much more.

Website Traffic Monitoring Tools

Tools URL Monitis http://www.monitis.com/ Web-Stat https://www.web-stat.com/ Alexa https://www.alexa.com/ *Table 2-06: Website Traffic Monitoring Tools*

Similarly, other tools like Web-stat and Monitis monitor website traffic for

collecting bounce rate, live visitors' map, and other information.

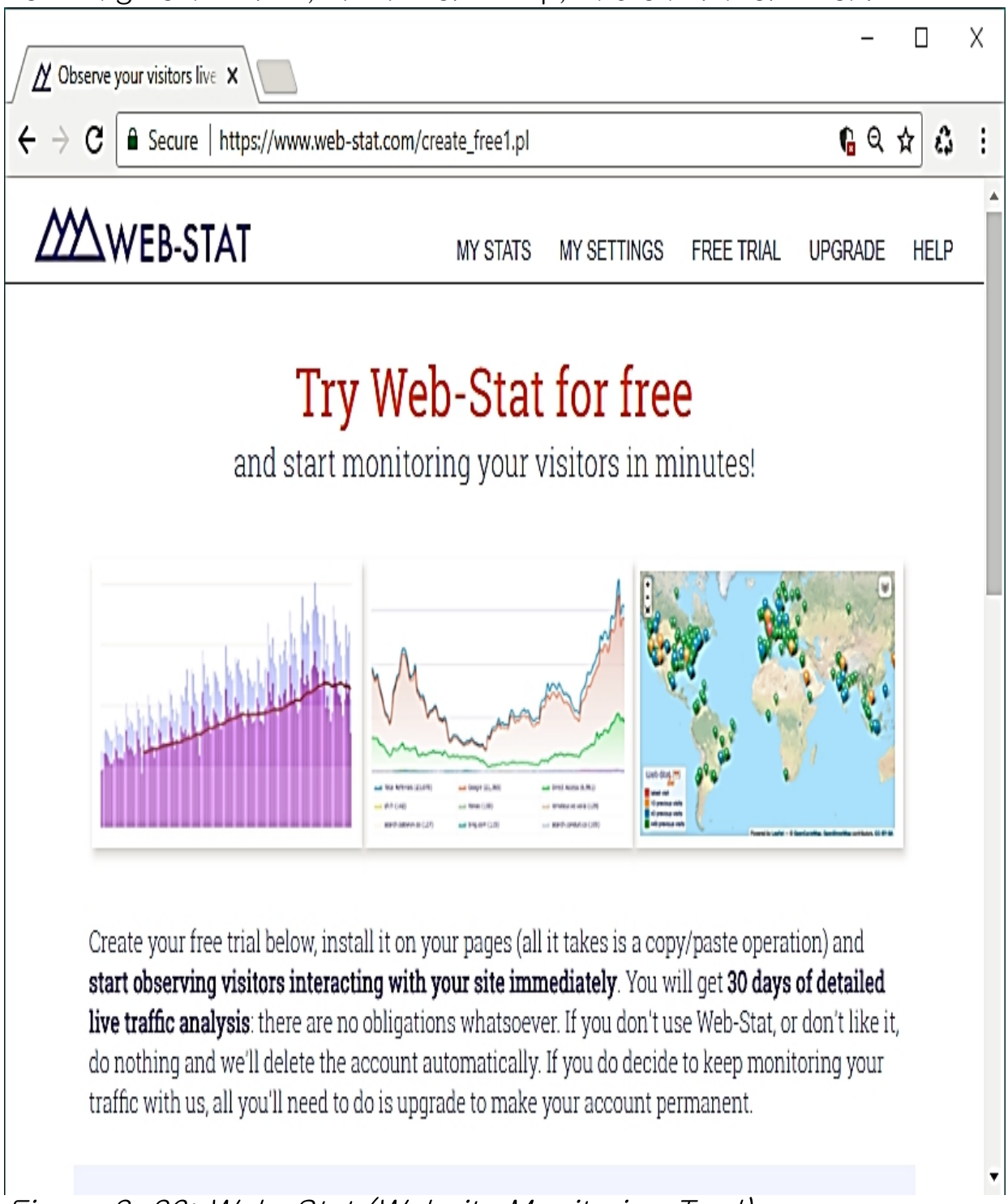


Figure 2-26: Web-Stat (Website Monitoring Tool)

Tracking the Online Reputation of the Target

The reputation of an organization can be monitored through online services. Online Reputation Management (ORM) offers to monitor an organization's reputation. These tools are used to track the reputation and ranking of a site, and sets up a notification alert for a well-known organization to get the latest news and updates. One popular monitoring tool is Trackur (www.trackur.com). Here you can search any keyword such as those shown in figure 2-08, which shows the results. Different icons are used to identify results collected from different sources; you can review the result by selecting an entry.

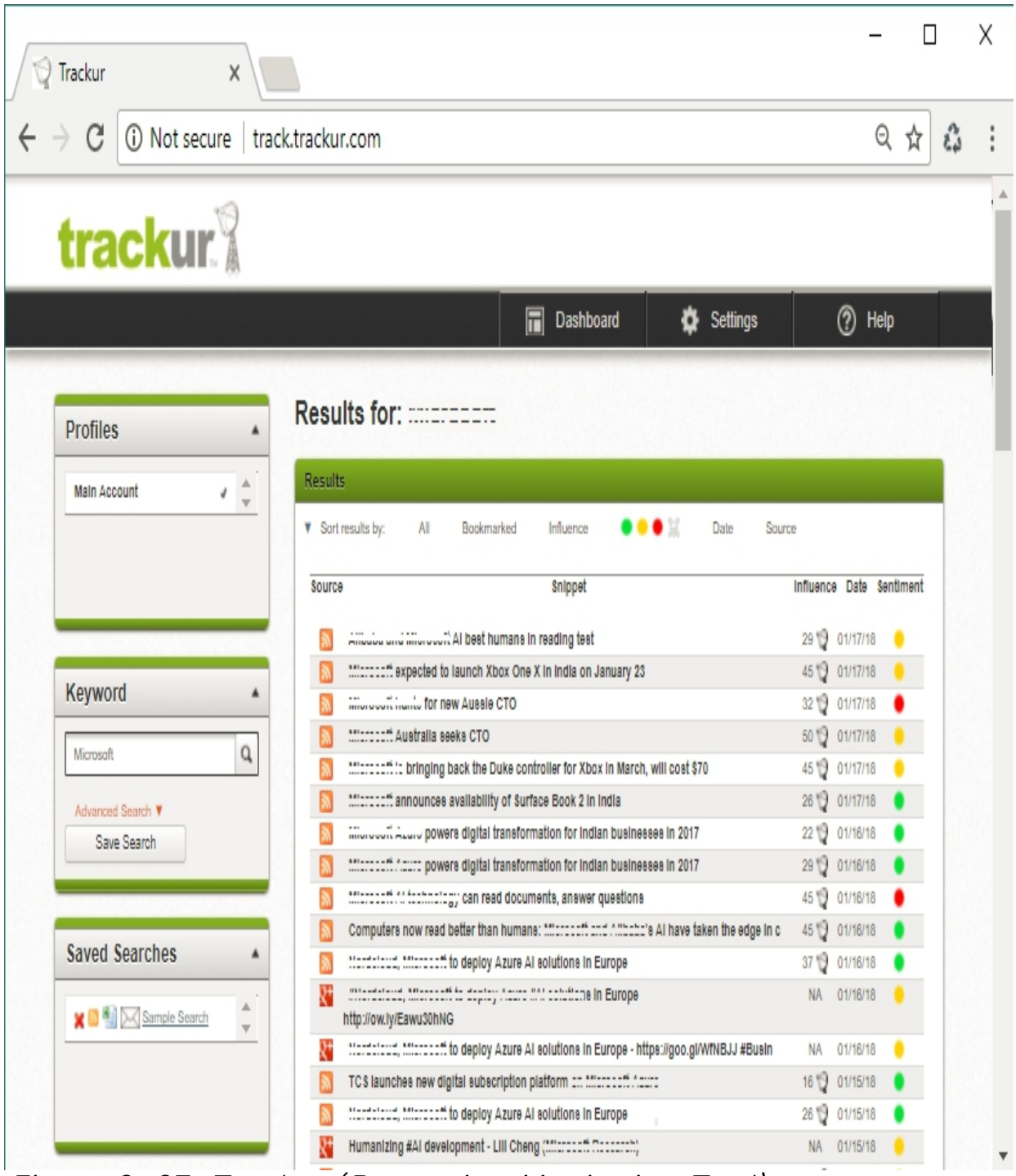


Figure 2-27: Trackur (Reputation Monitoring Tool)

Tools for Tracking Online Reputation

Tool URL Google Alerts https://www.google.com

WhosTalkin

Rankur

PR Software
Social Mention
Reputation Defender http://www.whostalkin.com http://rankur.com
http://www.cision.com
http://www.socialmention.com https://www.reputation.com

Table 2-07: Reputation Monitoring Tools

WHOIS Footprinting

WHOIS Lookup

"WHOIS" finds information regarding domain name and ownership from its database, IP Address, Netblock data, Domain Name Servers and other information. Regional Internet Registries (RIR) maintain the WHOIS database. WHOIS Lookup helps to find out the owner of the target domain name.

The evolvement of the Regional Internet Registry eventually divided the world into five RIRs:
RIRs Acronym Location African Network Information Centre
American Registry for Internet Numbers
Asia-Pacific Network Information Centre
Latin America and Caribbean Network Information Centre Réseaux IP Européens Network Coordination Centre
AFRINIC Africa
ARIN
APNIC
LACNIC

RIPE NCC United States, Canada, several parts of the Caribbean region, and Antarctica

Asia, Australia, New Zealand, and neighboring countries
Latin America and parts of the Caribbean region
Europe, Russia, the Middle East, and Central Asia
Table 2-08: Regional Internet Registry System

WHOIS Lookup Result Analysis

Lookup Results show a complete domain profile, including:

- Registrant information
- Registrant organization
- Registrant country
- Domain name server information
- IP address
- IP location
- ASN
- Domain status
- WHOIS history
- IP history
- Registrar history
- Hosting history

It also includes other information like contact details, the email and postal address of the registrar. You can go to https://whois.domaintools.com and enter the targeted URL.

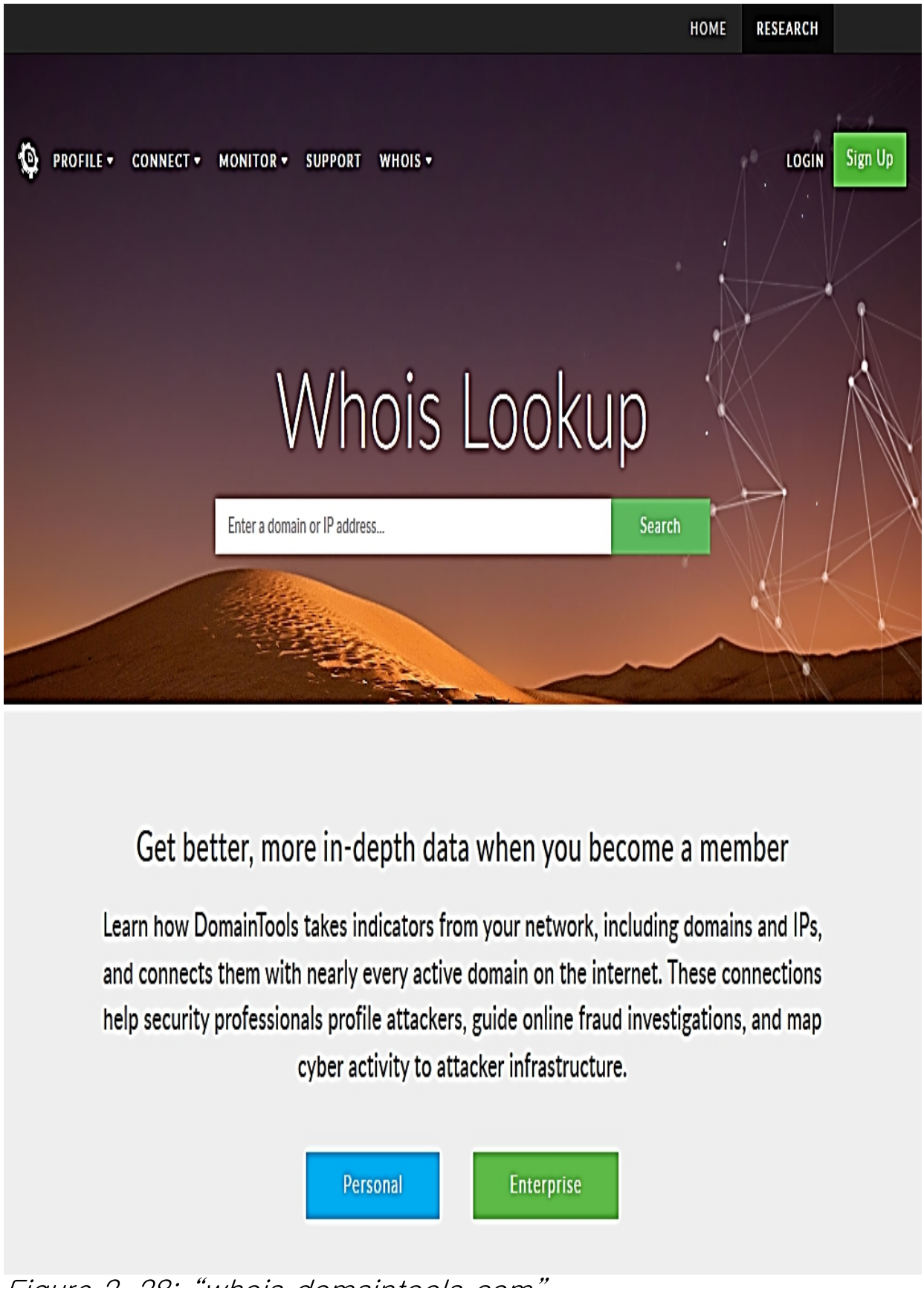


Figure 2. 28: "whois.domaintools.com"

Figure 2-28: whois.domaintools.com

You can download software called SmartWhois from www.tamos.com for Whois Lookup, as shown in the figure below:

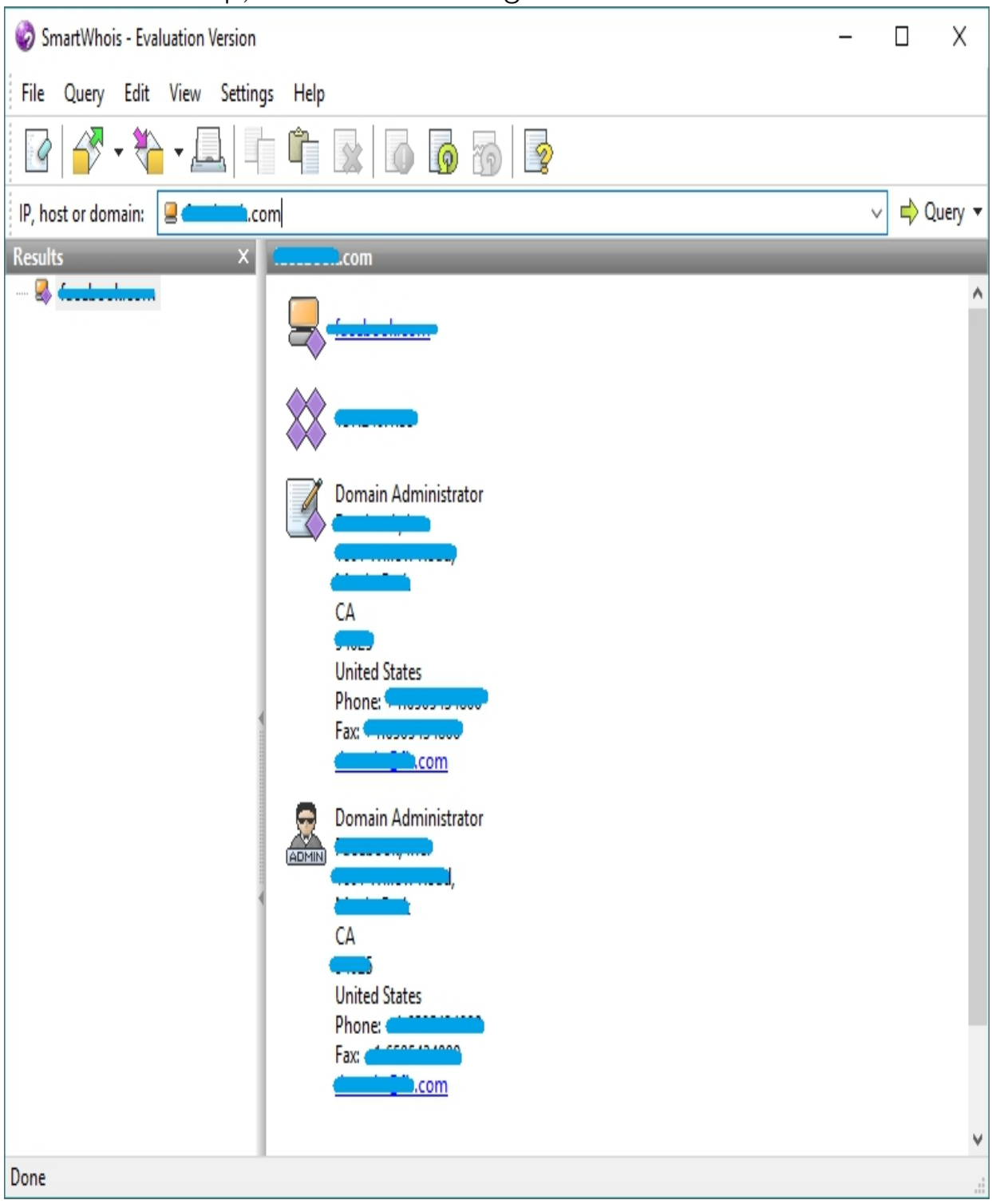


Figure 2-29: SmartWhois Lookup Application

WHOIS Lookup Tools

Tools powered by different developers on WHOIS Lookup are listed below:

- http://lantricks.com
- http://www.networkmost.com
- http://tialsoft.com
- http://www.johnru.com
- https://www.callerippro.com
- http://www.nirsoft.net
- http://www.sobolsoft.com
- http://www.softfuse.com

WHOIS Lookup Tools for Mobile

"DNS Tools", an application launched by www.dnssniffers.com, is available on Google play store. It includes features like DNS Report, Blacklist Check, Email Validation, WHOIS, Ping, and Reverse DNS.

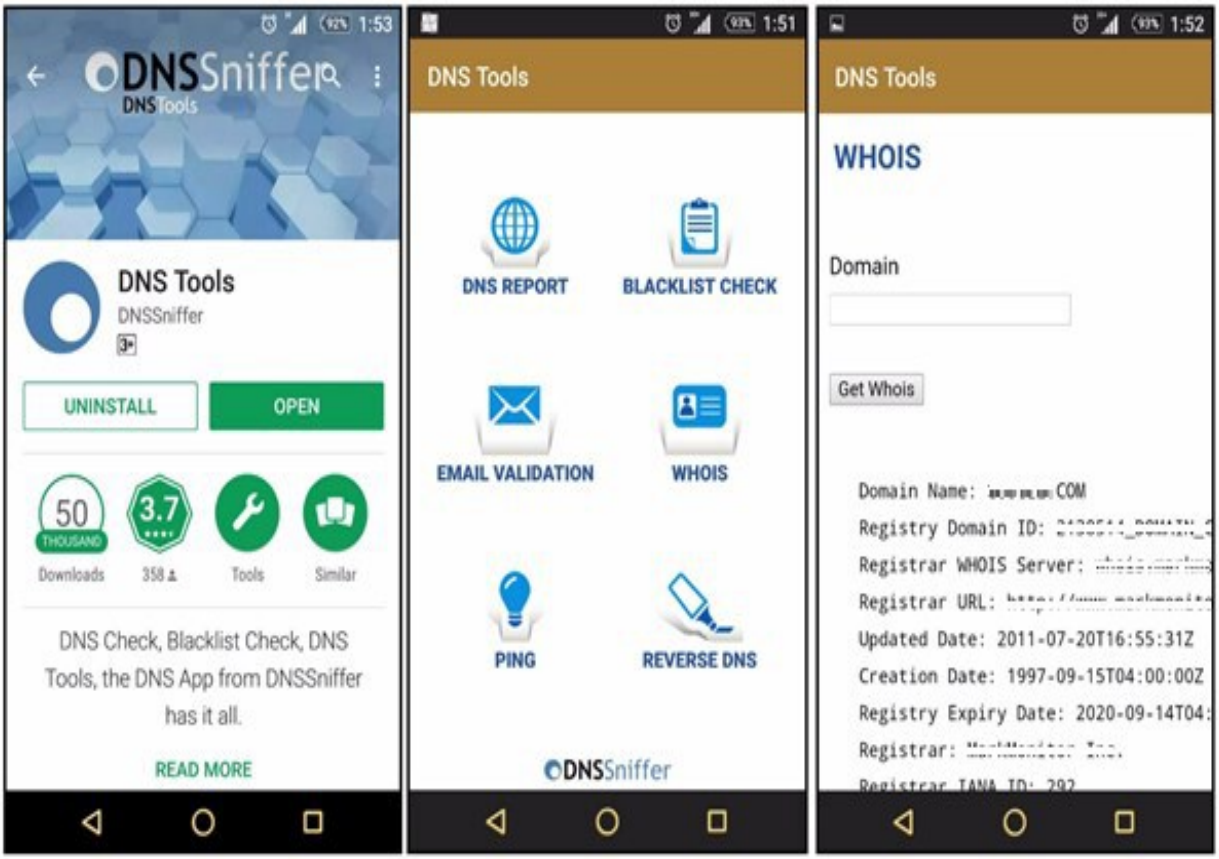


Figure 2-30: DNS Tool Application

Whois®, an application launched by www.whois.com.au , is also available on Google play store. There are several lookup tools powered by www.whois.com.au , such as:

- WHOIS Lookup
- DNS Lookup
- RBL Lookup
- Traceroute
- IP Lookup
- API/Bulk Data Access

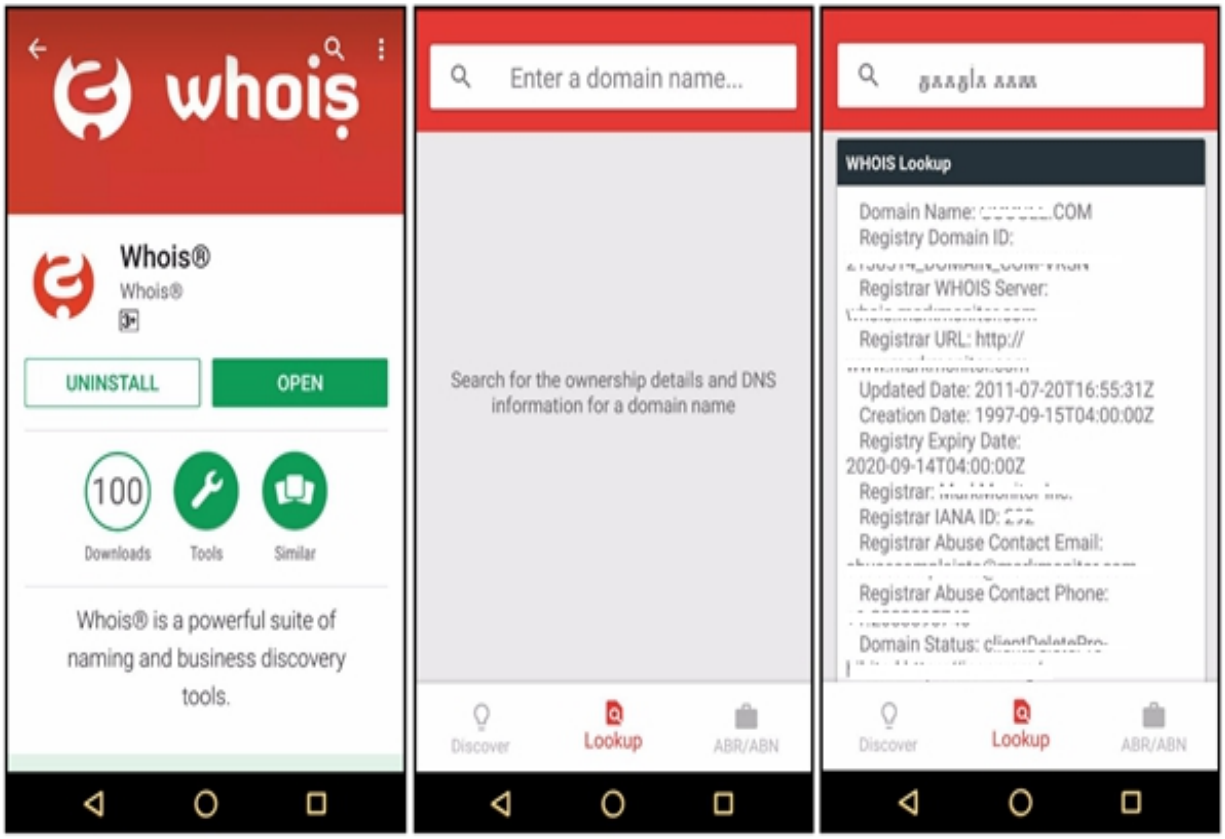


Figure 2-31: Whois Application

www.ultratools.com launched an application called UltraTools Mobile. This application offers multiple features like a domain health report, a DNS Speed test, DNS lookup, Whois Lookup, ping, and several other options.

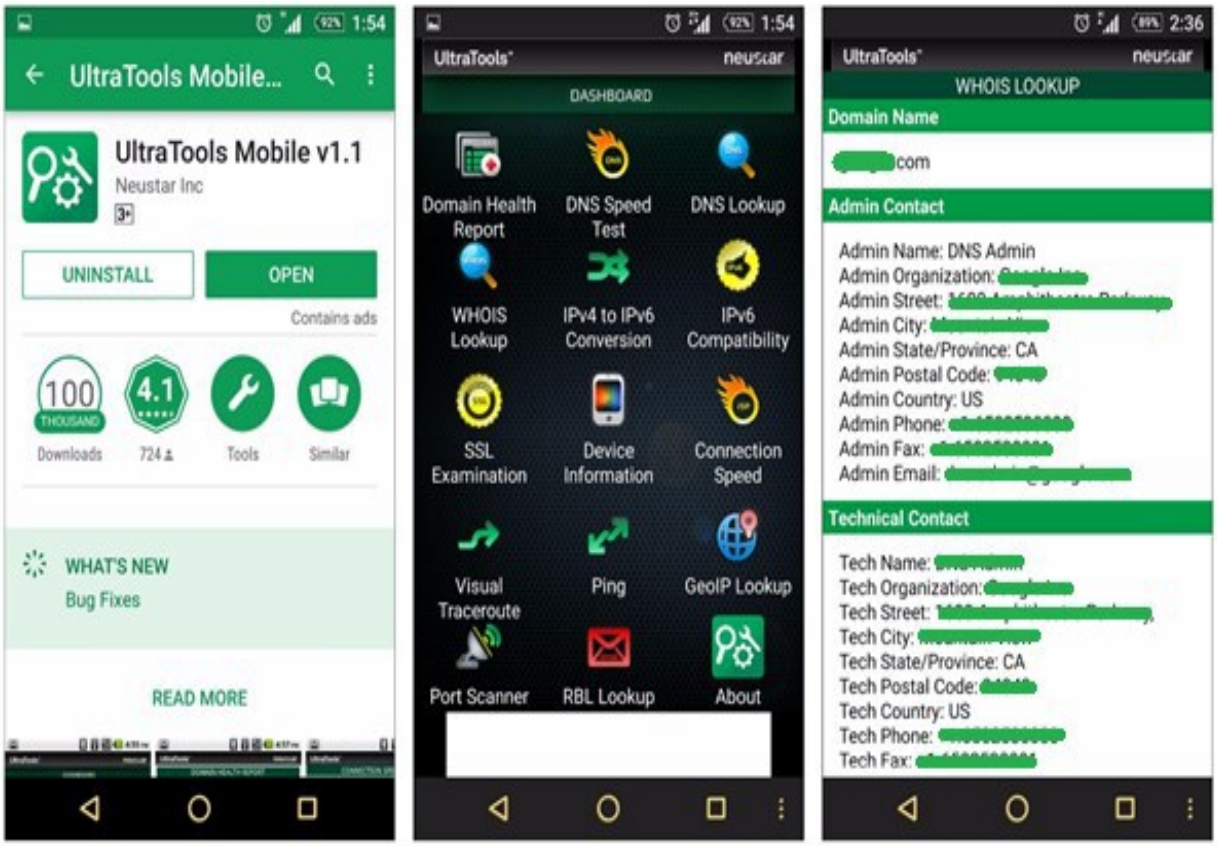


Figure 2-32: UltraTools Mobile Application

Performing WHOIS Footprinting

1. Go to the URL https://www.whois.com/

Figure 2-33: WHOIS Footprinting Engine

2. A search of Target Domain:

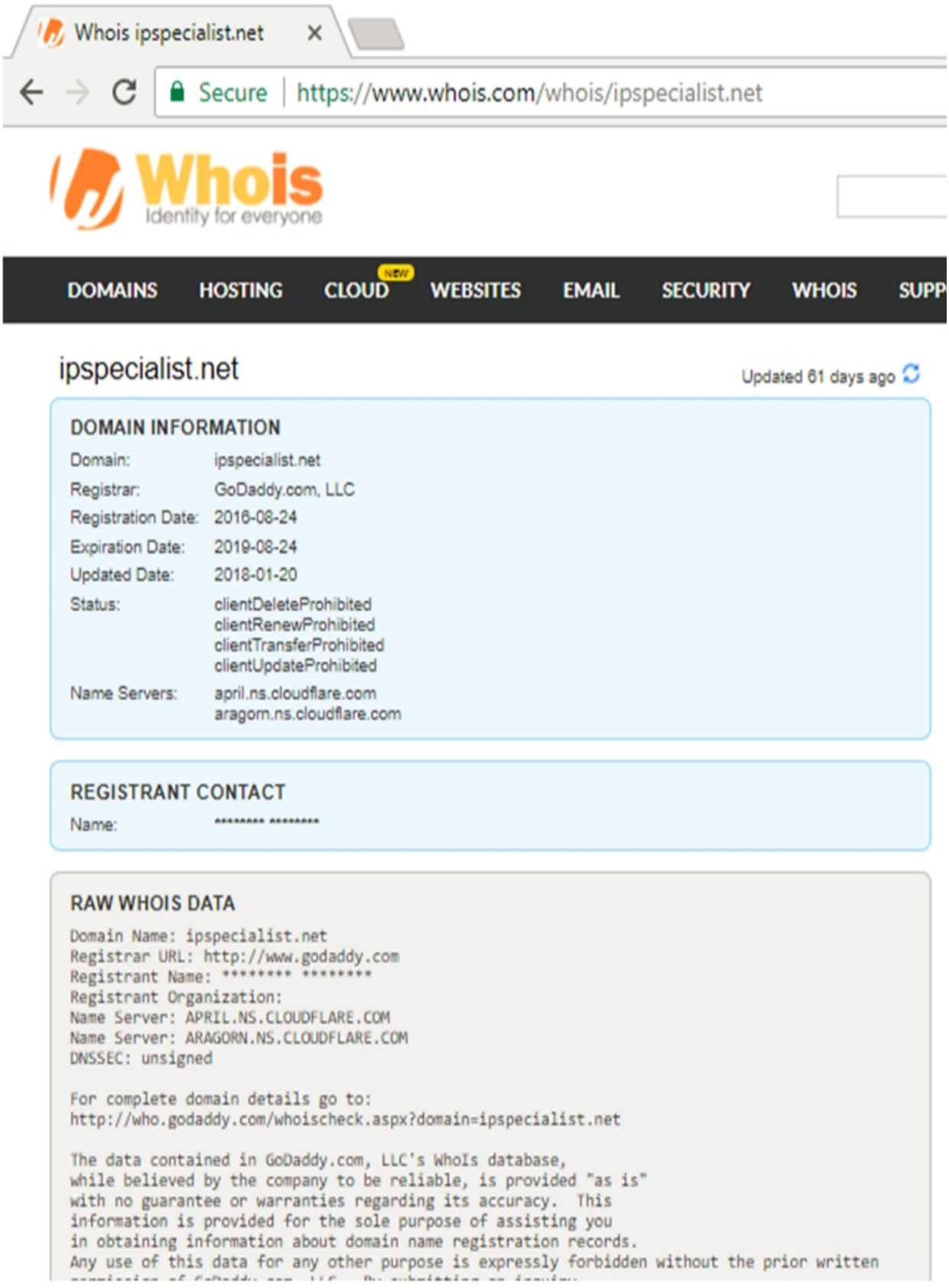

Whois ipspecialist.net
Secure
https://www.whois.com/whois/ipspecialist.net
Whois
Identity for everyone
DOMAINS
HOSTING
CLOUD
NEW
WEBSITES
EMAIL
SECURITY
WHOIS
SUPP
ipspecialist.net
Updated 61 days ago
DOMAIN INFORMATION
Domain: ipspecialist.net
Registrar: GoDaddy.com, LLC
Registration Date: 2016-08-24
Expiration Date: 2019-08-24
Updated Date: 2018-01-20
Status: clientDeleteProhibited
clientRenewProhibited
clientTransferProhibited
clientUpdateProhibited
Name Servers: april.ns.cloudflare.com
aragorn.ns.cloudflare.com
REGISTRANT CONTACT
Name: ******** ********
RAW WHOIS DATA
Domain Name: ipspecialist.net
Registrar URL: http://www.godaddy.com
Registrant Name: ******** ********
Registrant Organization:
Name Server: APRIL.NS.CLOUDFLARE.COM
Name Server: ARAGORN.NS.CLOUDFLARE.COM
DNSSEC: unsigned
For complete domain details go to:
http://who.godaddy.com/whoischeck.aspx?domain=ipspecialist.net
The data contained in GoDaddy.com, LLC's WhoIs database,
while believed by the company to be reliable, is provided "as is"
with no guarantee or warranties regarding its accuracy. This
information is provided for the sole purpose of assisting you
in obtaining information about domain name registration records.
Any use of this data for any other purpose is expressly forbidden without the prior written

Figure 2-34 WHOIS Footprinting

DNS Footprinting

DNS lookup information is helpful for identifying a host within a targeted network. There are several tools available on the internet that perform DNS lookup. Before proceeding to the DNS lookup tools and a result overview, you need to know the DNS record type symbols and what they mean:

Record Type Description
A The Host's IP Address
MX Domain's Mail Server
NS Host Name Server
CNAME Canonical Naming that allows aliases to a host
SDA Indicate Authority for the Domain
SRV Service Records
PTR IP-Host Mapping RP Responsible Person HINFO Host Information
TXT Unstructured Records

Table 2-09: DNS Record Type

Extracting DNS Information Using DNSStuff

Go to the URL: https://www.dnsstuff.com


Toolbox | DNSstuff | DNS
Secure
https://www.dnsstuff.com/tools#dnsReport|type=domain&&value=example.com
DNSreport Results for example.com
Export
Share
Overall Results:
1
FAIL
2
WARNING
25
PASS
2
INFO
PARENT
NS
SOA
MX
WWW
DNSSEC
SPF

Figure 2-35: DNSStuff.com

The above figure shows the output for example. com. You can expand the fields to extract information.

You can expand the desired fields to gain detailed information as shown below:

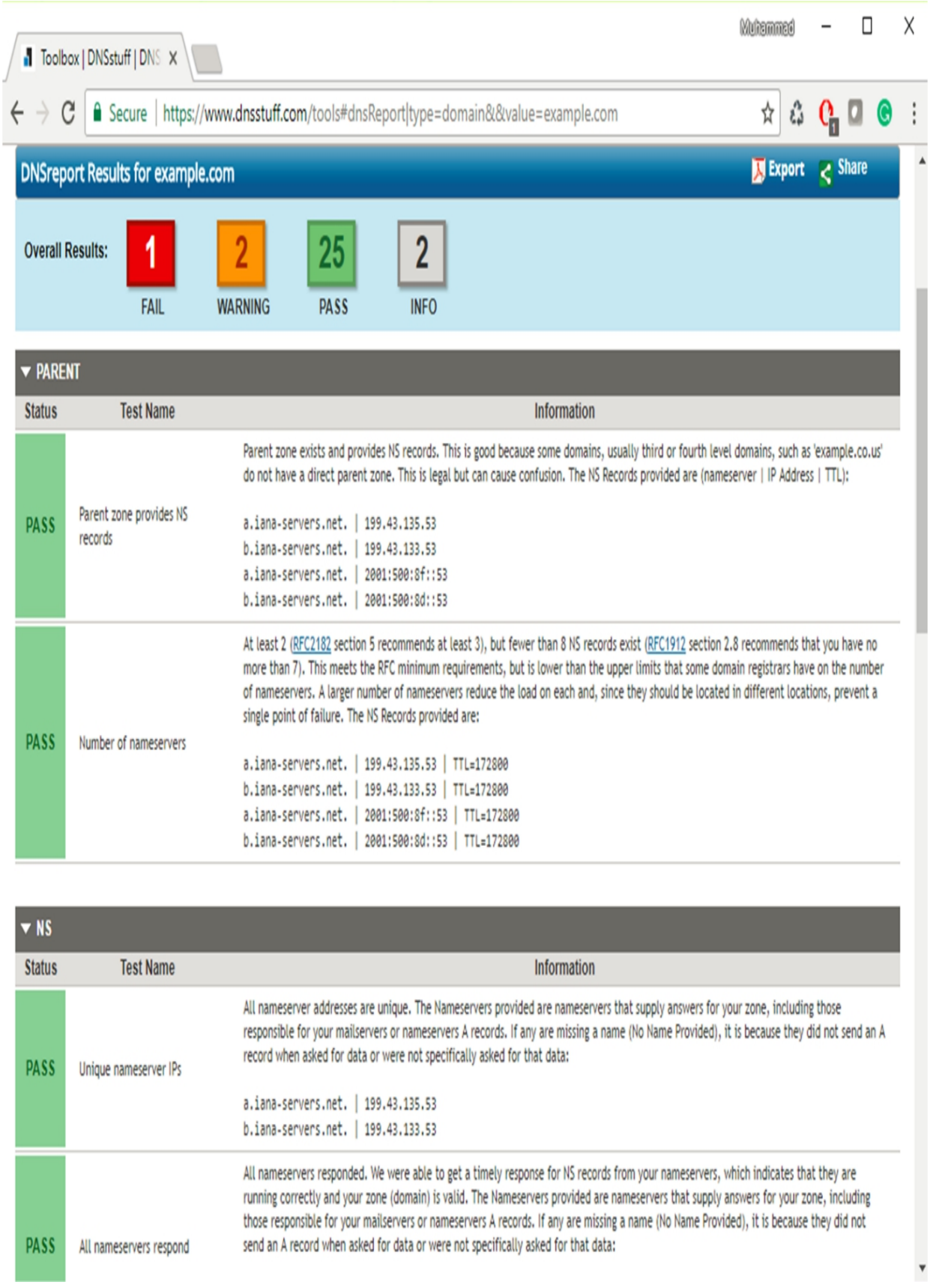

Muhammad
Toolbox | DNSstuff | DNS
Secure | https://www.dnsstuff.com/tools#dnsReport|type=domain&&value=example.com
DNSreport Results for example.com
Export
Share
Overall Results:
1
FAIL
2
WARNING
25
PASS
2
INFO
▼ PARENT
Status
Test Name
Information
PASS
Parent zone provides NS records
Parent zone exists and provides NS records. This is good because some domains, usually third or fourth level domains, such as 'example.co.us' do not have a direct parent zone. This is legal but can cause confusion. The NS Records provided are (nameserver | IP Address | TTL):
a.iana-servers.net. | 199.43.135.53
b.iana-servers.net. | 199.43.133.53
a.iana-servers.net. | 2001:500:8f::53
b.iana-servers.net. | 2001:500:8d::53
PASS
Number of nameservers
At least 2 (RFC2182 section 5 recommends at least 3), but fewer than 8 NS records exist (RFC1912 section 2.8 recommends that you have no more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain registrars have on the number of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are:
a.iana-servers.net. | 199.43.135.53 | TTL=172800
b.iana-servers.net. | 199.43.133.53 | TTL=172800
a.iana-servers.net. | 2001:500:8f::53 | TTL=172800
b.iana-servers.net. | 2001:500:8d::53 | TTL=172800
▼ NS
Status
Test Name
Information
PASS
Unique nameserver IPs
All nameserver addresses are unique. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:
a.iana-servers.net. | 199.43.135.53
b.iana-servers.net. | 199.43.133.53
PASS
All nameservers respond
All nameservers responded. We were able to get a timely response for NS records from your nameservers, which indicates that they are running correctly and your zone (domain) is valid. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:

Figure 2-36: DNS Footprinting

Extracting DNS Information Using Domain Dossier

Go to https://centralops.net/co/ and enter the IP address of the domain you want to search.

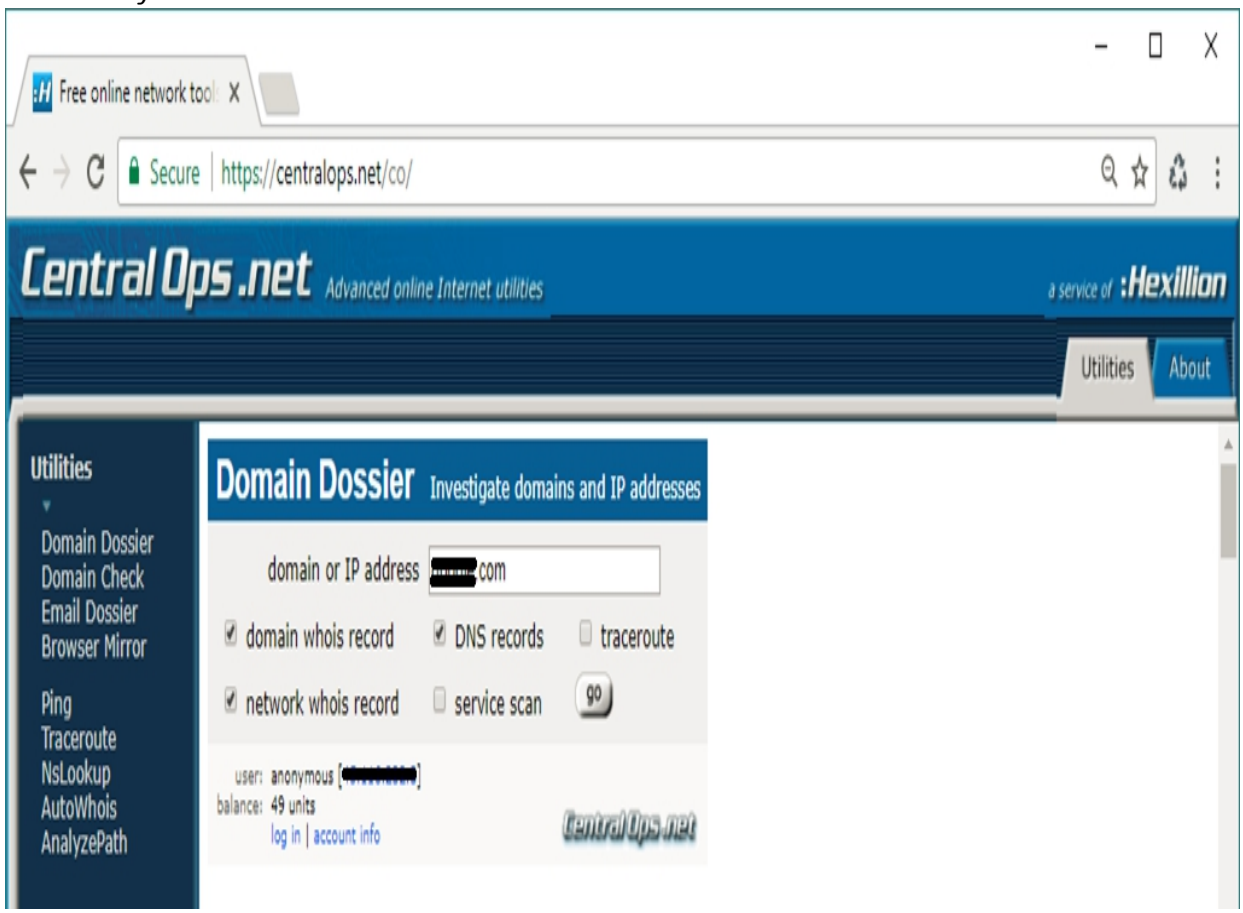


Figure 2-37: Domain Dossier Tool

The result shows the canonical name, aliases, IP address, Domain whois records, Network whois records, and DNS records. Consider the figure given below:

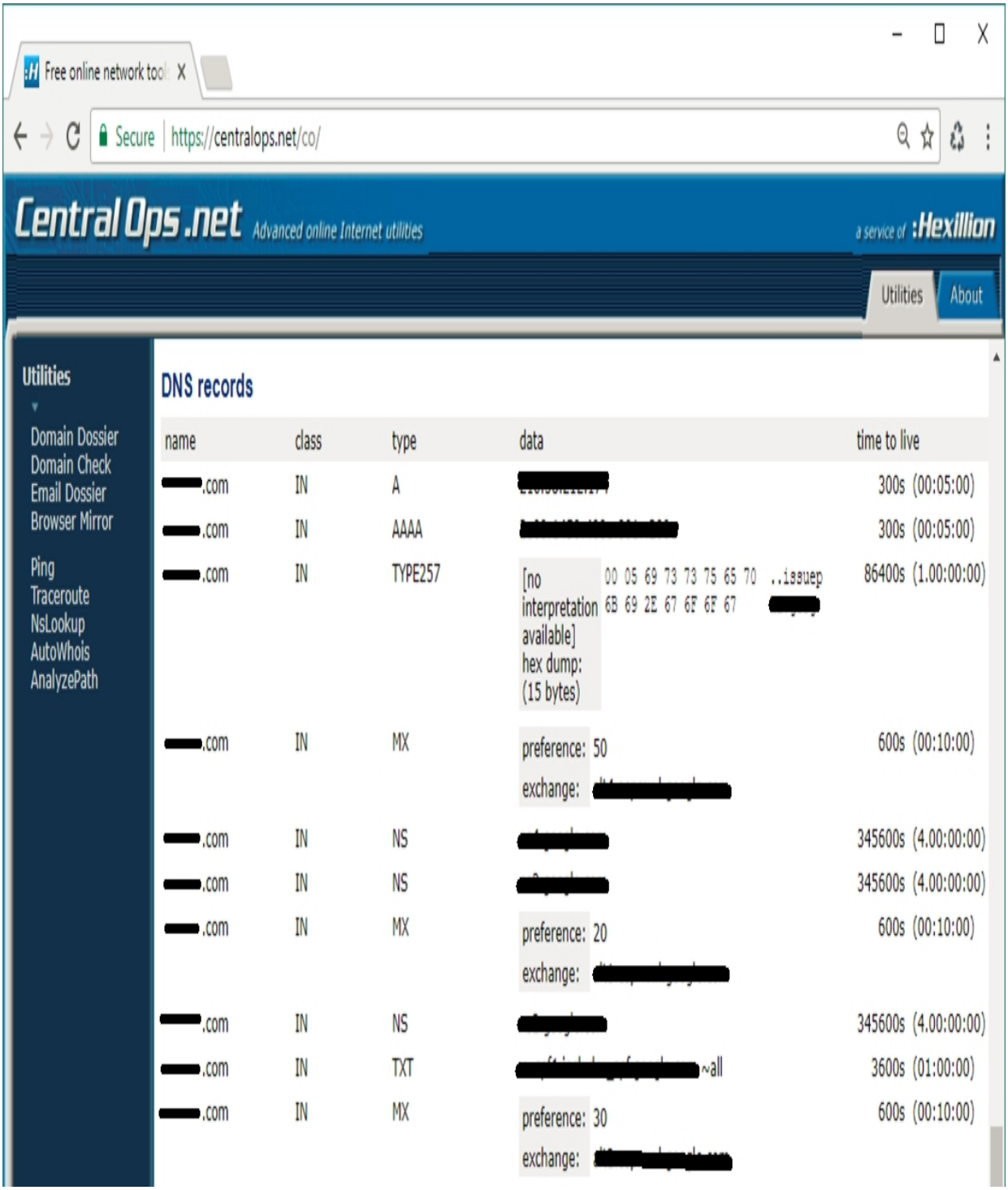


Figure 2-38: Domain Dossier Search Results

DNS Interrogation Tools

There are a lot of online tools available for DNS lookup, some of them are listed below:

- http://www.dnsstuff.com
- http://network-tools.com
- http://www.kloth.net
- http://www.mydnstools.info
- http://www.nirsoft.net
- http://www.dnswatch.info
- http://www.domaintools.com
- http://www.dnsqueries.com
- http://www.ultratools.com
- http://www.webmaster-toolkit.com

Network Footprinting

One of the most important types of footprinting is Network Footprinting. Fortunately, there are several tools available that can be used for network footprinting to gain information about the target network. Using these tools, an information seeker can create a map of the targeted network and can extract information such as: • Network address ranges
- Hostnames
- Exposed hosts
- OS and application version information
- The patch state of the host and the applications
- The structure of the applications and back-end servers

Tools for network footprinting are listed below:

- Whois
- Ping
- NsLookup
- Tracert

Traceroute

Tracert options are available in all Operating Systems as a command line feature. Visual traceroute, graphical, and other GUI-based traceroute applications are also available. Traceroute or Tracert command traces the path information from source to destination in the

hop by hop manner. The result includes all hops between source and destination. The result also includes latency between these hops.

Traceroute Analysis

Consider an example in which an attacker is trying to get network information by using Tracert. After observing the following result, you can identify the network map.

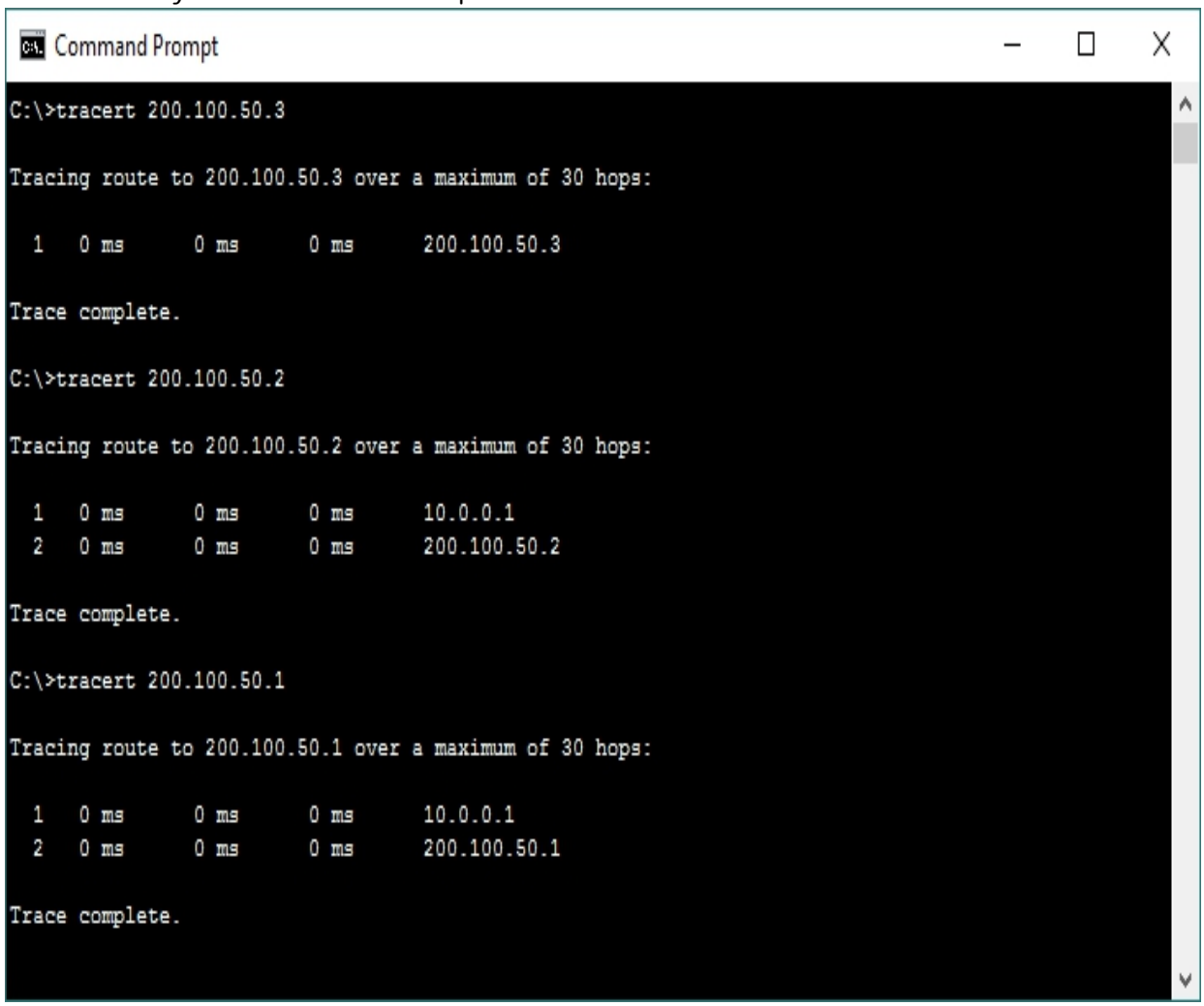


Figure 2-39: Tracert

10 .0.0. 1 is the first hop, which means it is the gateway. The Tracert result of 200. 100.50.3 shows 200. 100.50.3, which is another interface of the first hop device whereas connected IP includes 200. 100.50.2 and 200. 100.50. 1.

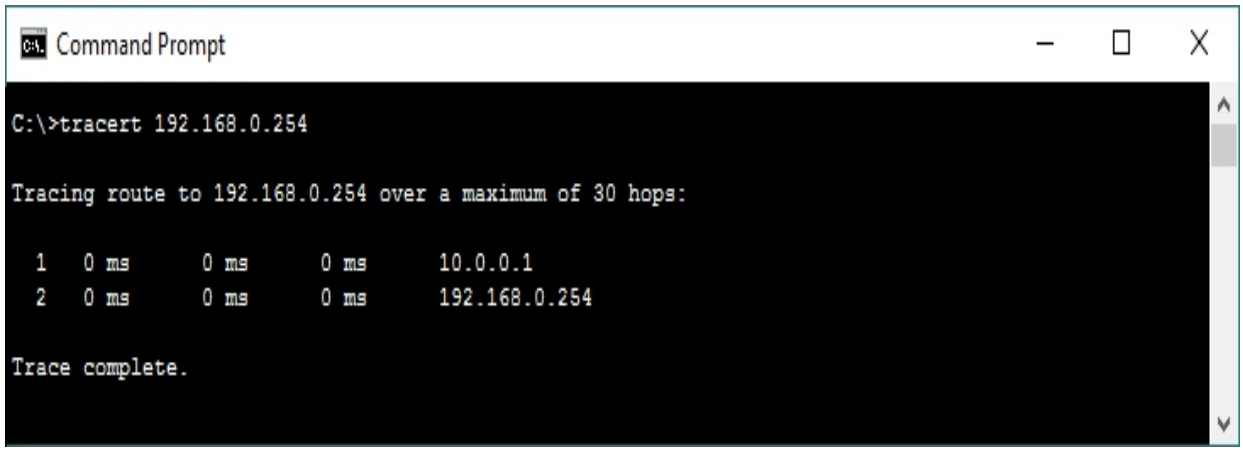


Figure 2-40: Tracert

192. 168.0.254 is the next to last hop 10.0.0. 1. It can either be connected to 200. 100.50. 1 or 200. 100.50.2 to verify and trace the next route.

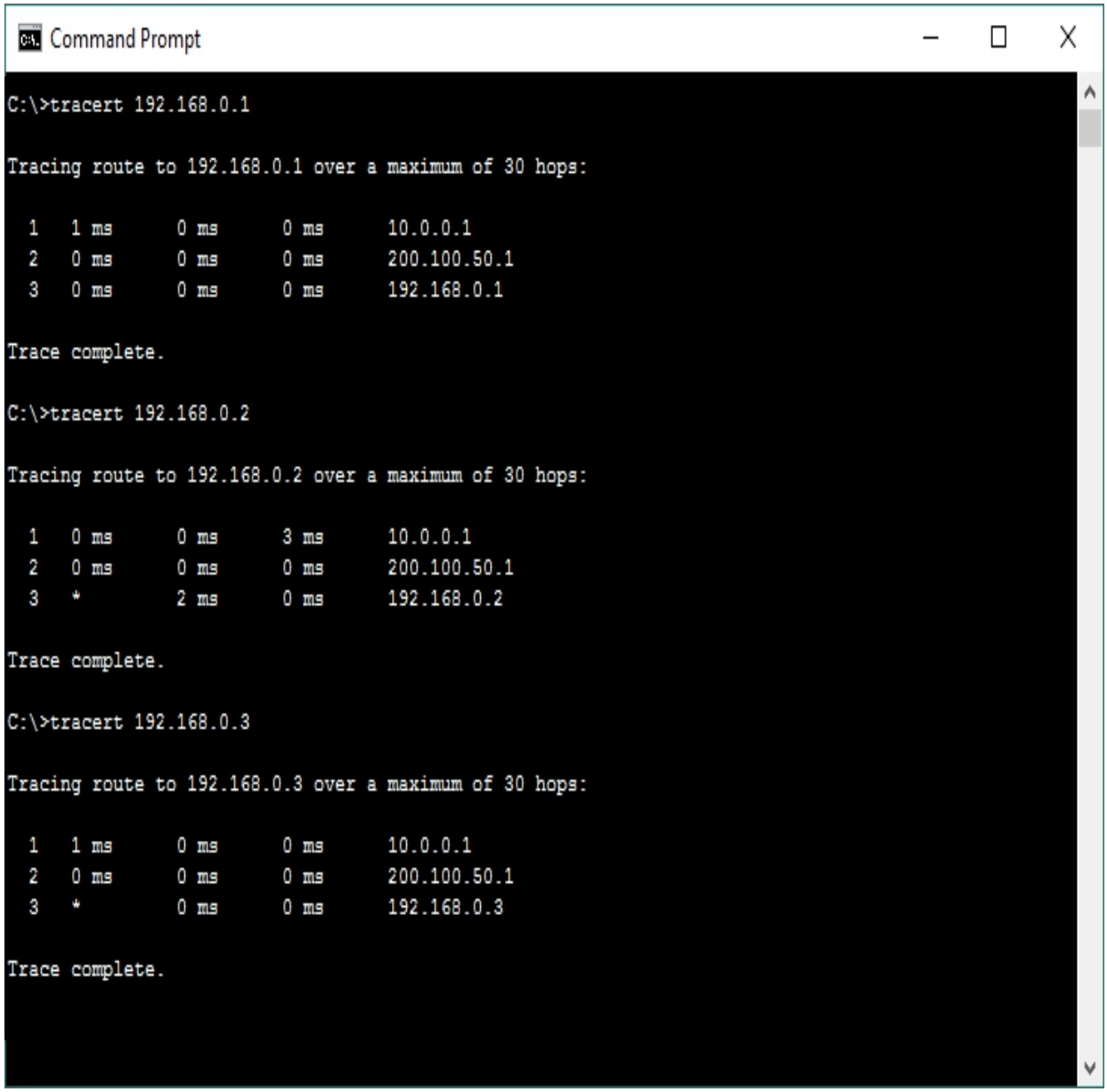


Figure 2-41: Tracert

192. 168.0.254 is another interface of the network device, i.e. 200. 100.50. 1 is connected next to 10.0.0. 1.

192. 168.0. 1, 192. 168.0.2 and 192. 168.0.3 are connected directly to 192. 168.0.254.

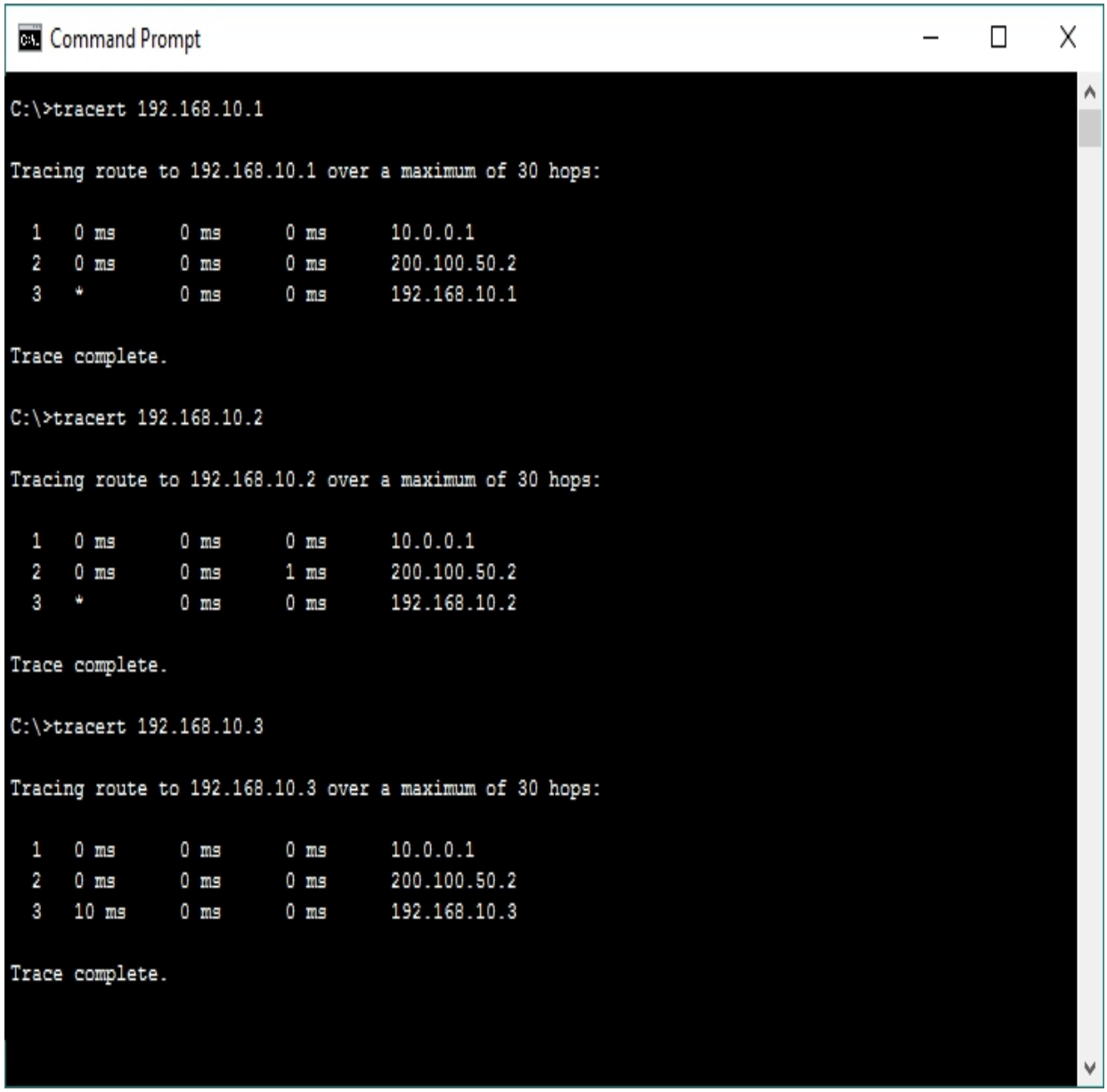


Figure 2-42: Tracert

192. 168. 10.254
next to 10.0.0. 1. 192. 168. 10. 1, 192. 168. 10.
is another interface of the network device, i.e., 200. 100.50.2
connected 2, and 192. 168. 10.3 are connected directly to 192. 168. 10.254.

Traceroute Tools

Traceroute tools have been listed below:

Traceroute Tools
Path Analyzer Pro

Visual Route
Troute
3D Traceroute

Website
www.pathanalyzer.com www.visualroute.com www.mcafee.com www.d3tr.de

Table 2-10: Traceroute Tools

The following figure shows a graphical view and traces information generated by using Visual Route Tool.

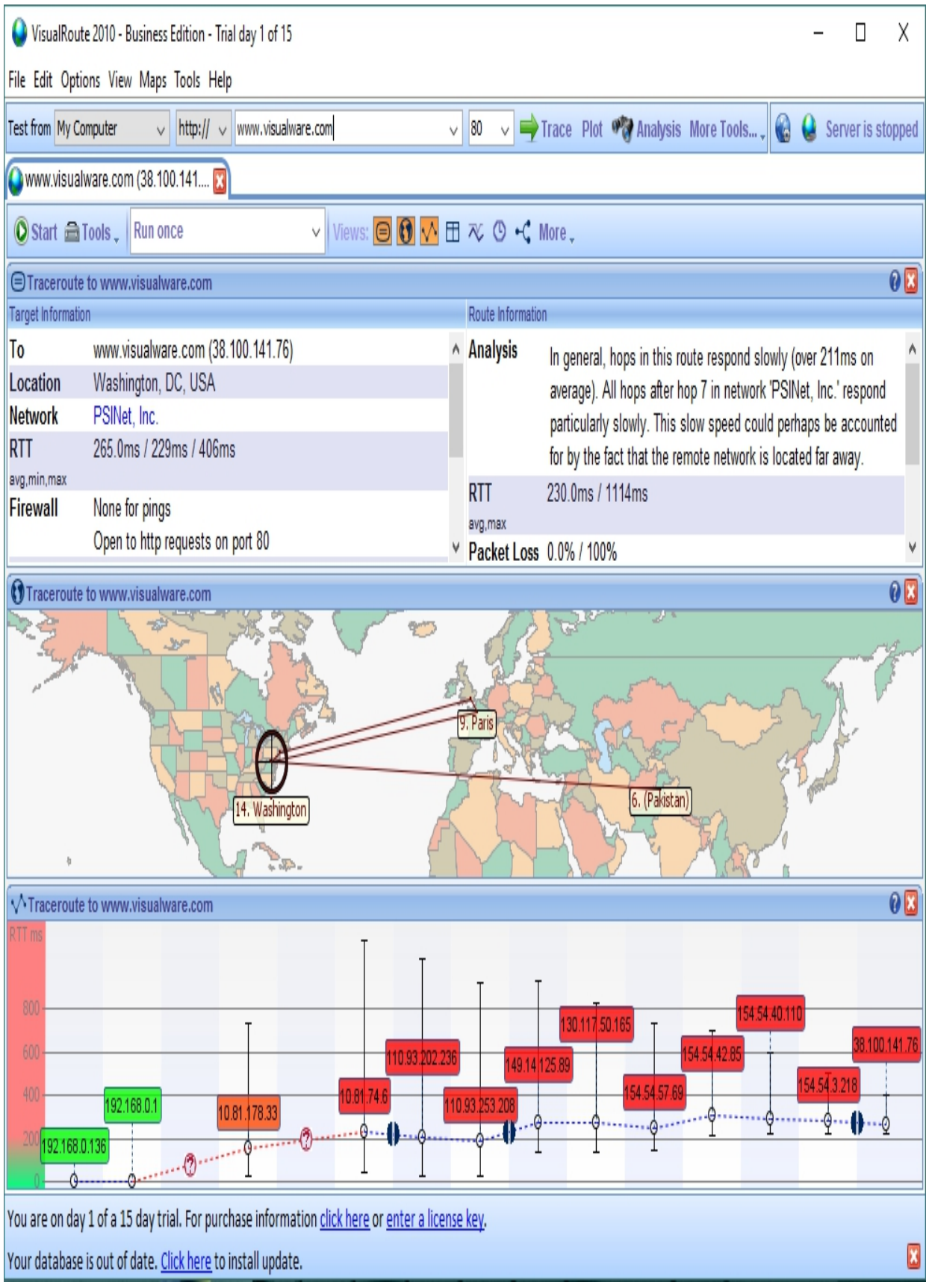

VisualRoute 2010 - Business Edition - Trial day 1 of 15
File Edit Options View Maps Tools Help
Test from My Computer
http://
www.visualware.com
80
Trace Plot Analysis More Tools...
Server is stopped
www.visualware.com (38.100.141....
Start Tools
Run once
Views:
More
Traceroute to www.visualware.com
Target Information
To www.visualware.com (38.100.141.76)
Location Washington, DC, USA
Network PSINet, Inc.
RTT avg,min,max 265.0ms / 229ms / 406ms
Firewall None for pings
Open to http requests on port 80
Route Information
Analysis In general, hops in this route respond slowly (over 211ms on average). All hops after hop 7 in network 'PSINet, Inc.' respond particularly slowly. This slow speed could perhaps be accounted for by the fact that the remote network is located far away.
RTT avg,max 230.0ms / 1114ms
Packet Loss 0.0% / 100%
Traceroute to www.visualware.com
9. Paris
14. Washington
6. (Pakistan)
Traceroute to www.visualware.com
RTT ms
800
600
400
200
0
192.168.0.136
192.168.0.1
10.81.178.33
10.81.74.6
110.93.202.236
110.93.253.208
149.14.125.89
130.117.50.165
154.54.57.69
154.54.42.85
154.54.40.110
154.54.3.218
38.100.141.76
You are on day 1 of a 15 day trial. For purchase information click here or enter a license key.
Your database is out of date. Click here to install update.

Figure 2-43: Visual Route Application

Footprinting through Social Engineering

In footprinting, one of the easiest components to hack is human being itself. We can collect information from a human quite easily with social engineering. Some basic social engineering techniques are:

- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Impersonation

Social Engineering

Social Engineering is the art of extracting sensitive information from people. Social Engineers play with human psychology and trick people into sharing their valuable information. In Information Security, footprinting through social engineering is done for gathering information such as:

- Credit card information
- Usernames and passwords
- Security devices and technology information
- Operating System information
- Software information
- Network information
- IP address and name server's information

Eavesdropping

Eavesdropping is a type of Social Engineering footprinting in which the social engineer gathers information by covertly listening to conversations. This includes listening, reading, and accessing any source of information without being detected.

Phishing

In the process of Phishing, emails sent to a targeted group contain messages that look legitimate. The recipient clicks the link provided in the email assuming that it as a legitimate link. Once the reader clicks