Footprinting and Reconnaissance

Module 02

Security News

ABOUT US | PRODUCTS | NEWS | SERVICES | SOLUTION | CONTACT

Facebook a 'treasure trove' of Personally Identifiable Information

April 10, 2012

Facebook contains a "treasure trove" of personally identifiable information that hackers manage to get their hands on.

A report by Imperva revealed that users' "general personal information" can often include a date of birth, home address and sometimes mother's maiden name, allowing hackers to access this and other websites and applications and create targeted spearphishing campaigns.

It detailed a concept I call "friend-mapping", where an attacker can get further knowledge of a user's circle of friends; having accessed their account and posing as a trusted friend, they can cause mayhem. This can include requesting the transfer of funds and extortion.

Asked why Facebook is so important to hackers, Imperva senior security strategist Noa Bar-Yosef said: "People also add work friends on Facebook so a team leader can be identified and this can lead to corporate data being accessed, project work being discussed openly, while geo-location data can be detailed for military intelligence."

"Hacktivism made up 58 per cent of attacks in the Verizon Data Breach Intelligence Report, and they are going after information on Facebook that can be used to humiliate a person. All types of attackers have their own techniques."

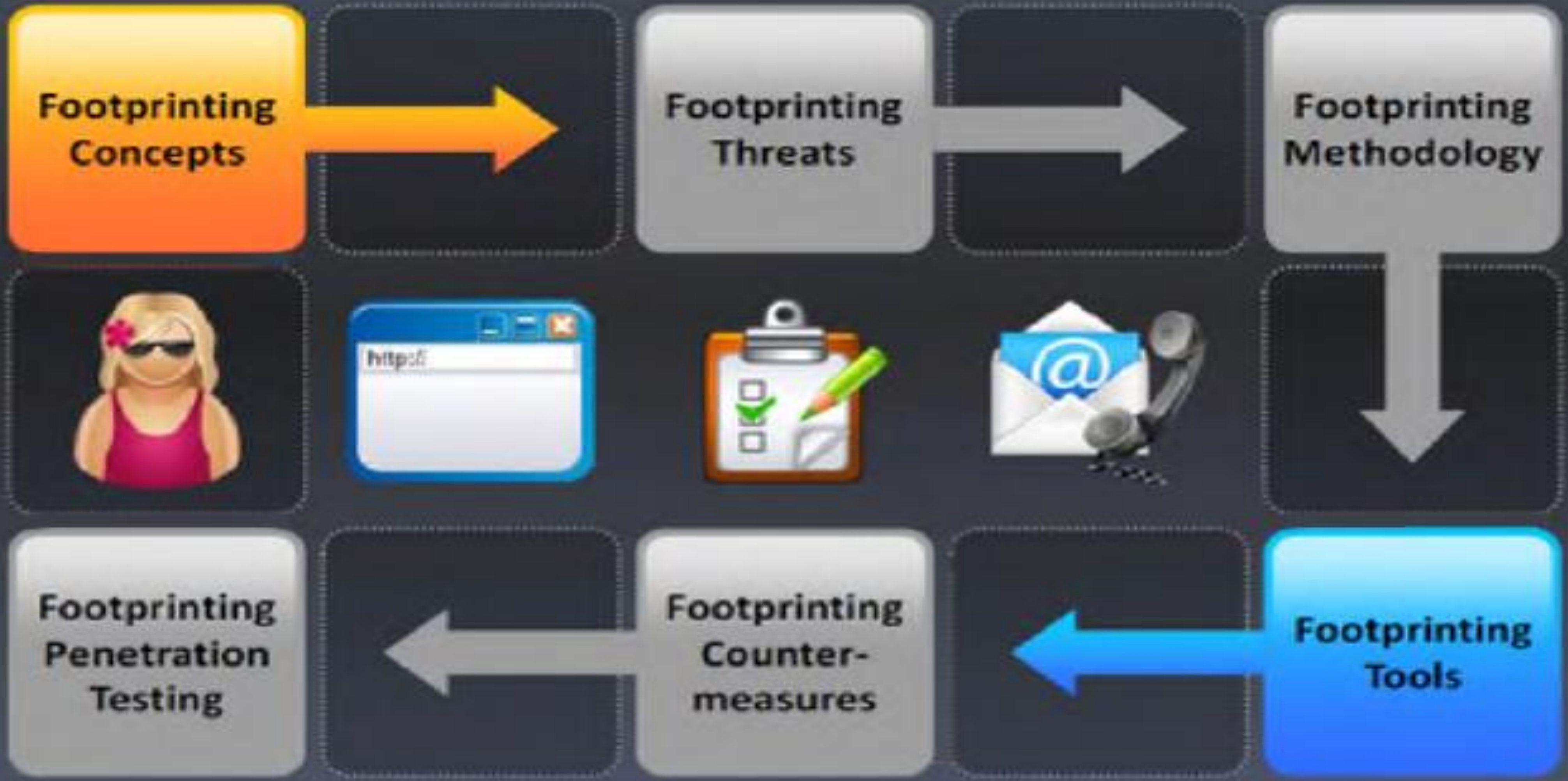
http://www.scmagazineuk.com

Module Objectives

- Footprinting Terminology
- What Is Footprinting?
- Objectives of Footprinting
- Footprinting Threats
- Footprinting through Search Engines
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting Using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Pen Testing

Module Flow



Footprinting Concepts

Footprinting Threats

Footprinting Methodology

Footprinting Tools

Footprinting Counter-measures

Footprinting Penetration Testing

Footprinting Terminology

Open Source or Passive Information Gathering

Collect information about a target from the publicly accessible sources

Active Information Gathering

Gather information through social engineering on-site visits, interviews, and questionnaires

Anonymous Footprinting

Gather information from sources where the author of the information cannot be identified or traced

Pseudonymous Footprinting

Collect information that might be published under a different name in an attempt to preserve privacy

Organizational or Private Footprinting

Collect information from an organization's web-based calendar and email services

Internet Footprinting

Collect information about a target from the Internet

What Is Footprinting?

Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system

Process involved in Footprinting a Target

1 Collect basic information about the target and its network

2 Determine the operating system used, platforms running, web server versions, etc.

3 Perform techniques such as Whois, DNS, network and organizational queries

4 Find vulnerabilities and exploits for launching attacks

Why Footprinting?

Know Security Posture

Footprinting allows attacker to know about the complete **security posture of an organization**

Reduce Attack Area

It reduces attacker's **attack area to specific range** of IP address, networks, domain names, remote access, etc.

Build Information Database

It allows attacker to **build their own information database** about target organization's security weakness to take appropriate actions

Draw Network Map

It allows attacker to **draw a map or outline the target organization's network infrastructure** to know about the actual environment that they are going to break

Objectives of Footprinting

Collect Network Information

- Domain name
- Internal domain names
- Network blocks
- IP addresses of the reachable systems
- Rogue websites/private websites
- TCP and UDP services running
- Access control Mechanisms and ACL's
- Networking protocols
- VPN Points
- ACLs
- IDSes running
- Analog/digital telephone numbers
- Authentication mechanisms
- System Enumeration

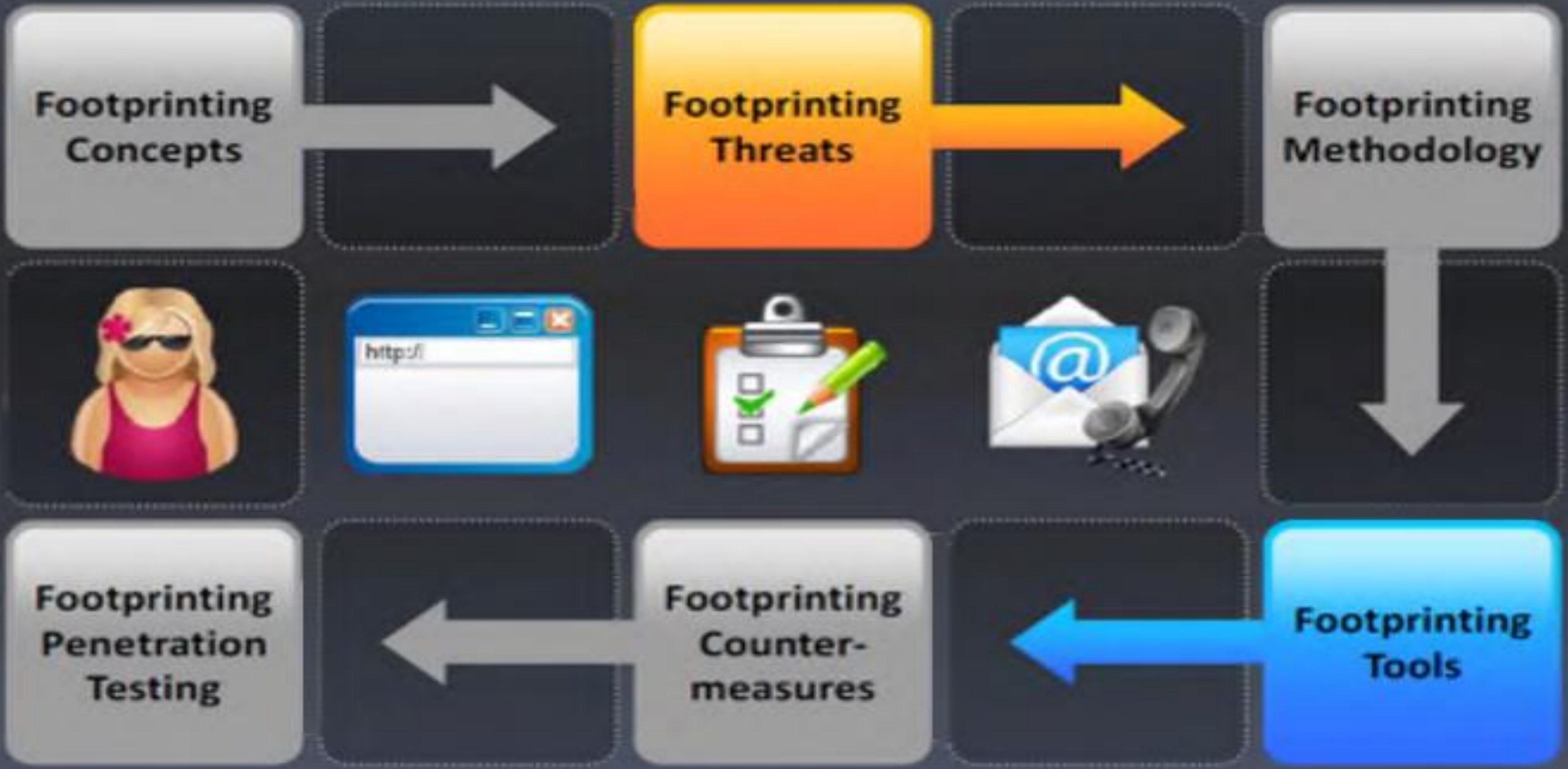
Collect System Information

- User and group names
- System banners
- Routing tables
- SNMP information
- System architecture
- Remote system type
- System names
- Passwords

Collect Organization's Information

- Employee details
- Organization's website
- Company directory
- Location details
- Address and phone numbers
- Comments in HTML source code
- Security policies implemented
- Web server links relevant to the organization
- Background of the organization
- News articles/press releases

Module Flow



Footprinting Concepts

Footprinting Threats

Footprinting Methodology

Footprinting Tools

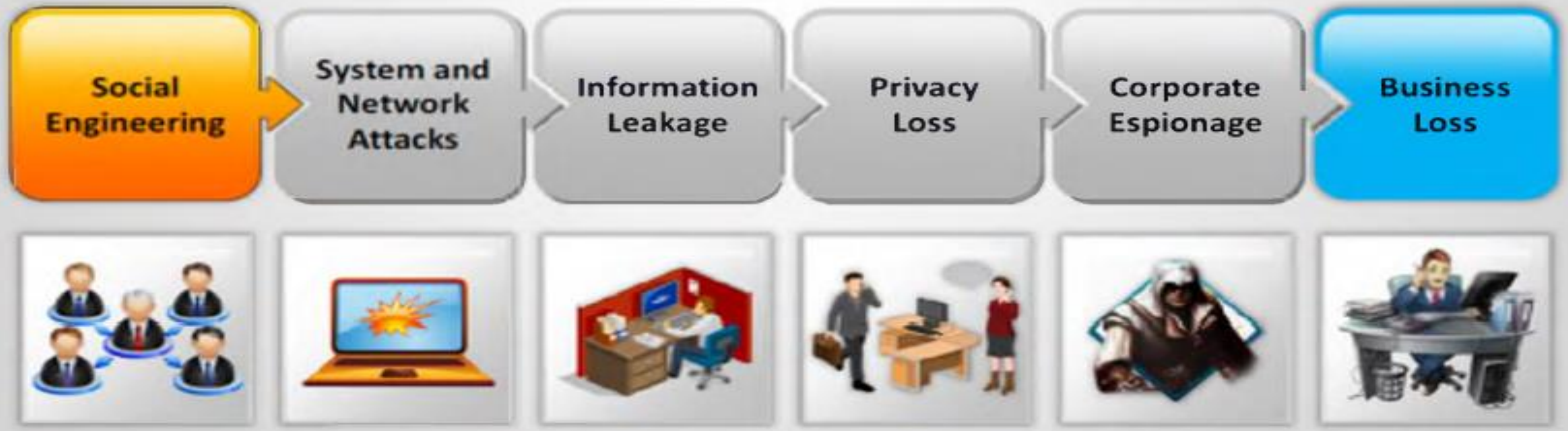
Footprinting Counter-measures

Footprinting Penetration Testing

Footprinting Threats

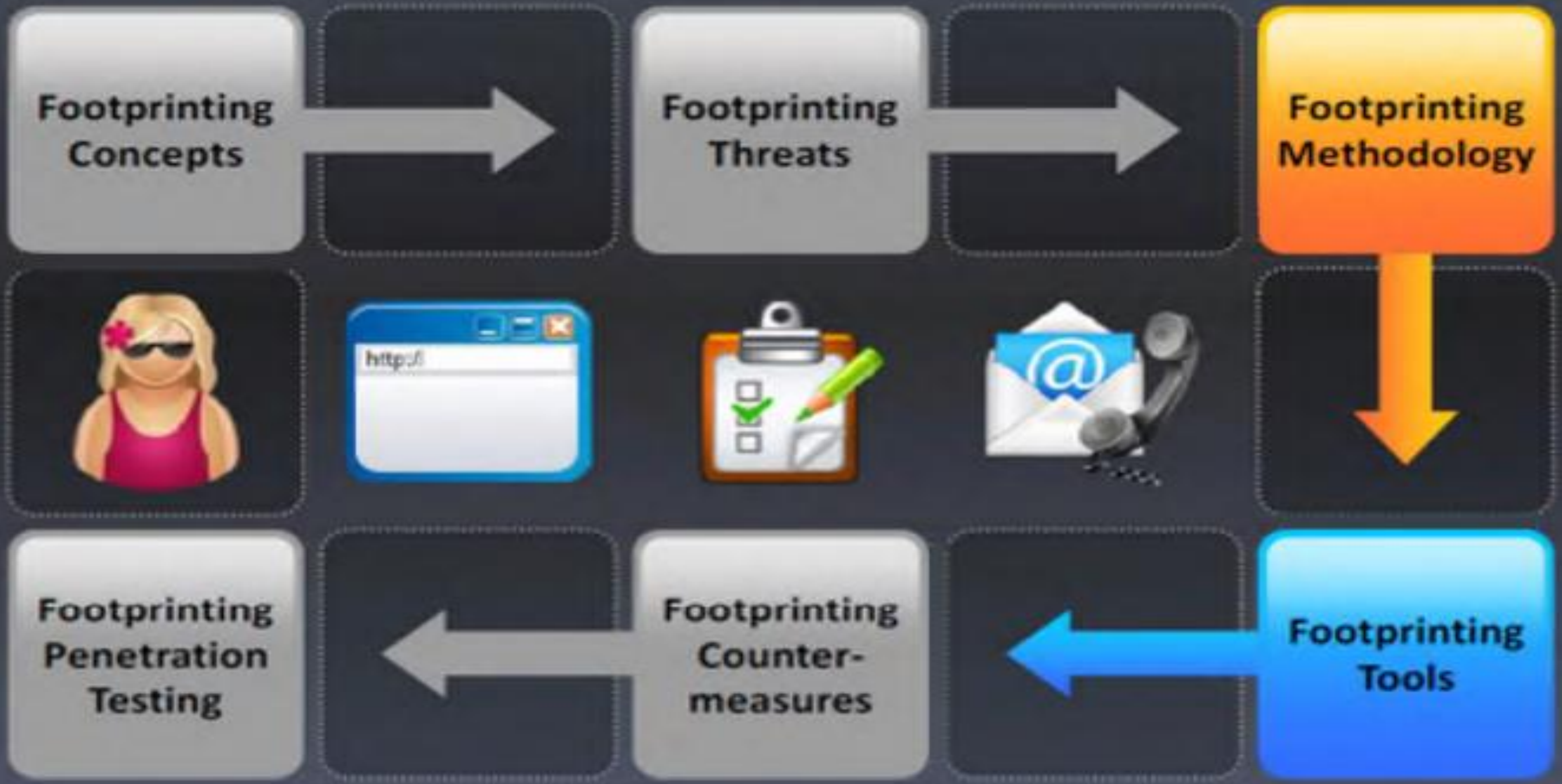
- Attackers gather valuable system and network information such as account details, operating system and installed applications, network components, server names, database schema details, etc. from footprinting techniques

Types of Threats



Social Engineering → System and Network Attacks → Information Leakage → Privacy Loss → Corporate Espionage → Business Loss

Module Flow



Footprinting Concepts

Footprinting Threats

Footprinting Methodology

Footprinting Tools

Footprinting Counter-measures

Footprinting Penetration Testing

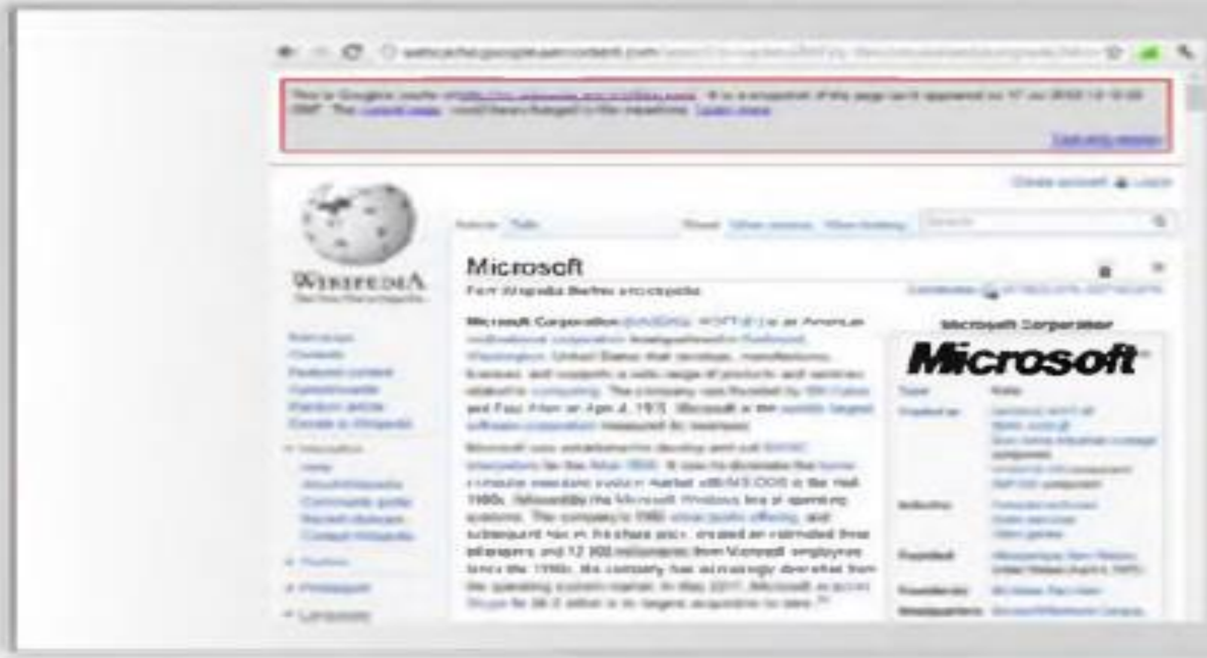
Footprinting Methodology

- Footprinting through Search Engines
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting through Search Engines

- Attackers use search engines to **extract information about a target** such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks
- Search engine **cache may provide sensitive information** that has been removed from the World Wide Web (WWW)



Finding Company's External and Internal URLs

- Search for the target company's external URL in a search engine such as Google or Bing
- Internal URLs provide an insight into different departments and business units in an organization
- You may find an internal company's URL by trial and error method

Tools to Search Internal URLs

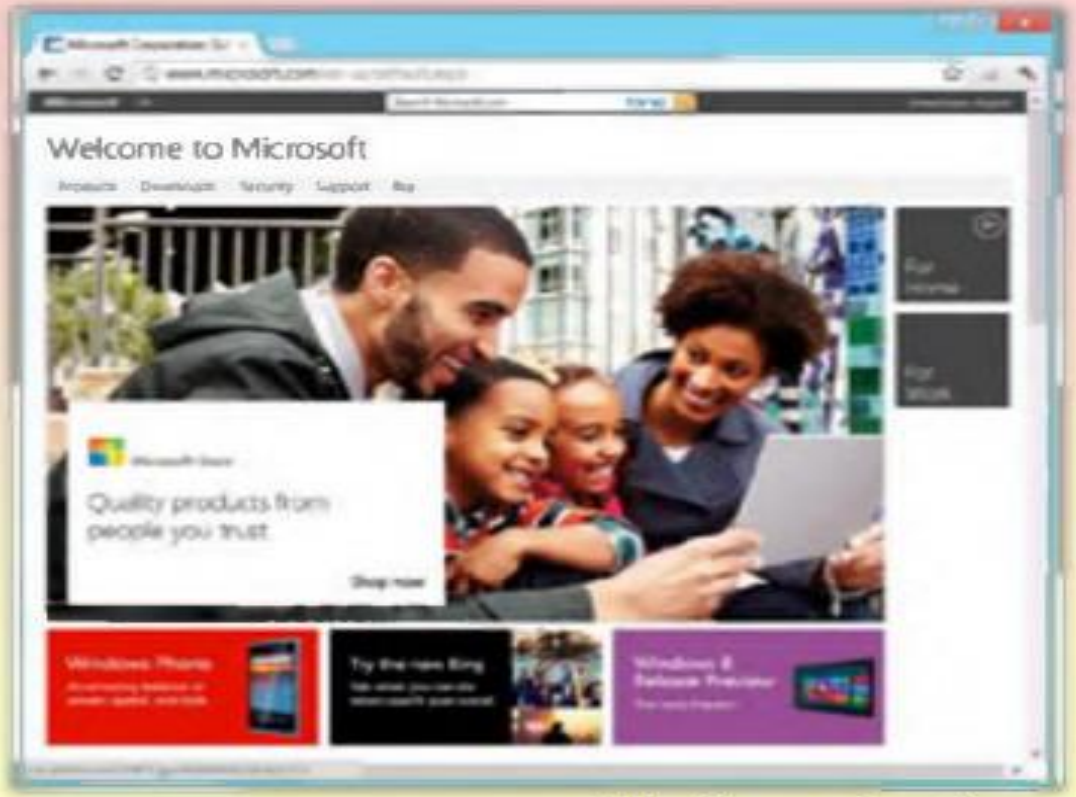
- http://news.netcraft.com
- http://www.webmaster-a.com/link-extractor-internal.php

Internal URL's of microsoft.com

- support.microsoft.com
- office.microsoft.com
- search.microsoft.com
- msdn.microsoft.com
- update.microsoft.com
- technet.microsoft.com
- windows.microsoft.com

Public and Restricted Websites

Identify a company's **private and public websites**


Welcome to Microsoft
Products Downloads Security Support Buy
Quality products from people you trust
Shop now
For home
For work
Windows Phone
Try the new Bing
Windows 8 Release Preview

http://www.microsoft.com

Public Website

http://technet.microsoft.com

http://windows.microsoft.com

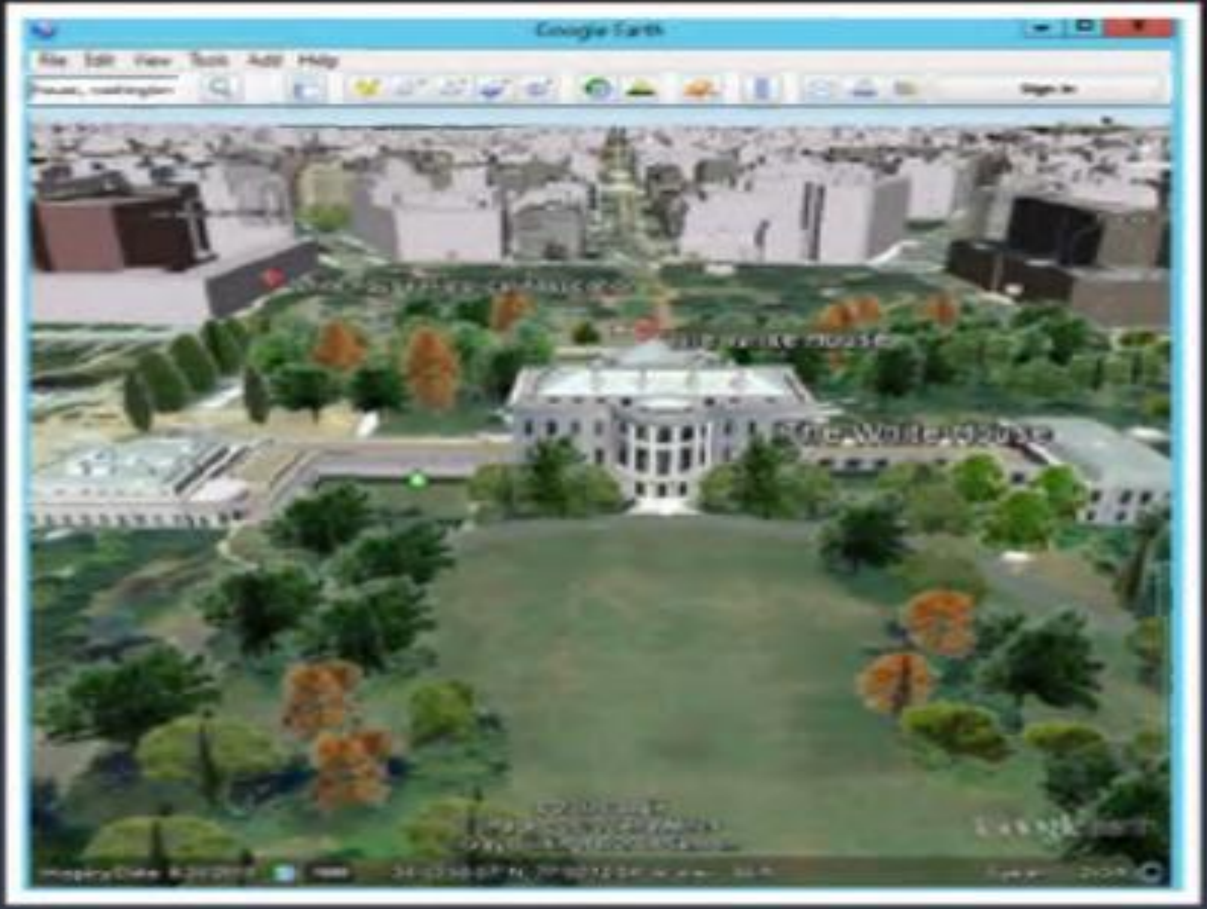
http://office.microsoft.com

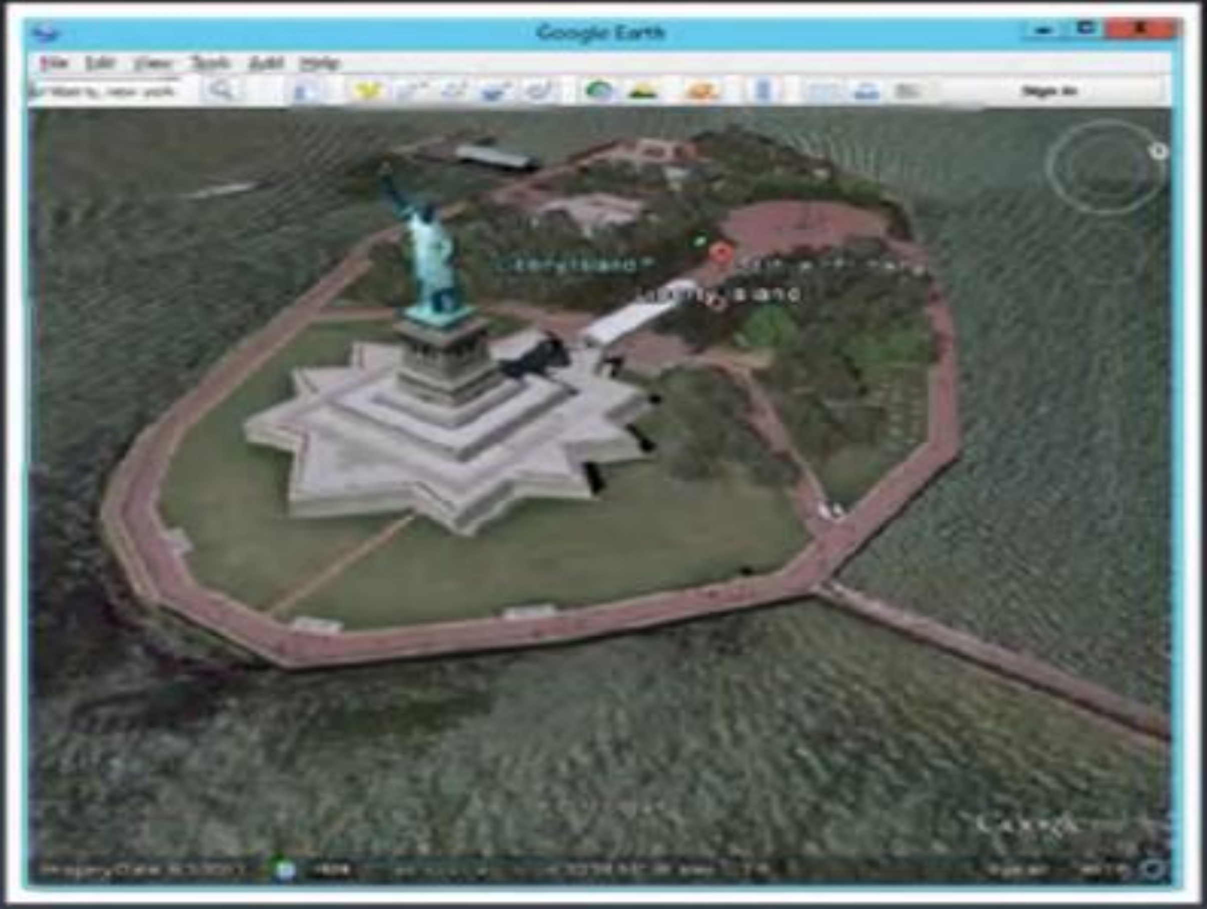
http://answers.microsoft.com

Restricted Website

Collect Location Information

Use **Google Earth** tool to get the location of the place





http://earth.google.com

People Search

Information about an individual can be found at various **people search websites**

The people search returns the following **information about a person**:

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of private residencies

http://pipl.com

http://www.spokeo.com

People Search Online Services

Zaba Search
http://www.zabasearch.com

ZoomInfo
http://www.zoominfo.com

Wink People Search
http://wink.com

AnyWho
http://www.anywho.com

People Lookup
https://www.peoplelookup.com

123 People Search
http://www.123people.com

PeekYou
http://www.peekyou.com

Intelius
http://www.intelius.com

PeopleSmart
http://www.peoplesmart.com

WhitePages
http://www.whitepages.com

People Search on Social Networking Services

http://www.facebook.com

http://www.linkedin.com

http://twitter.com

https://plus.google.com

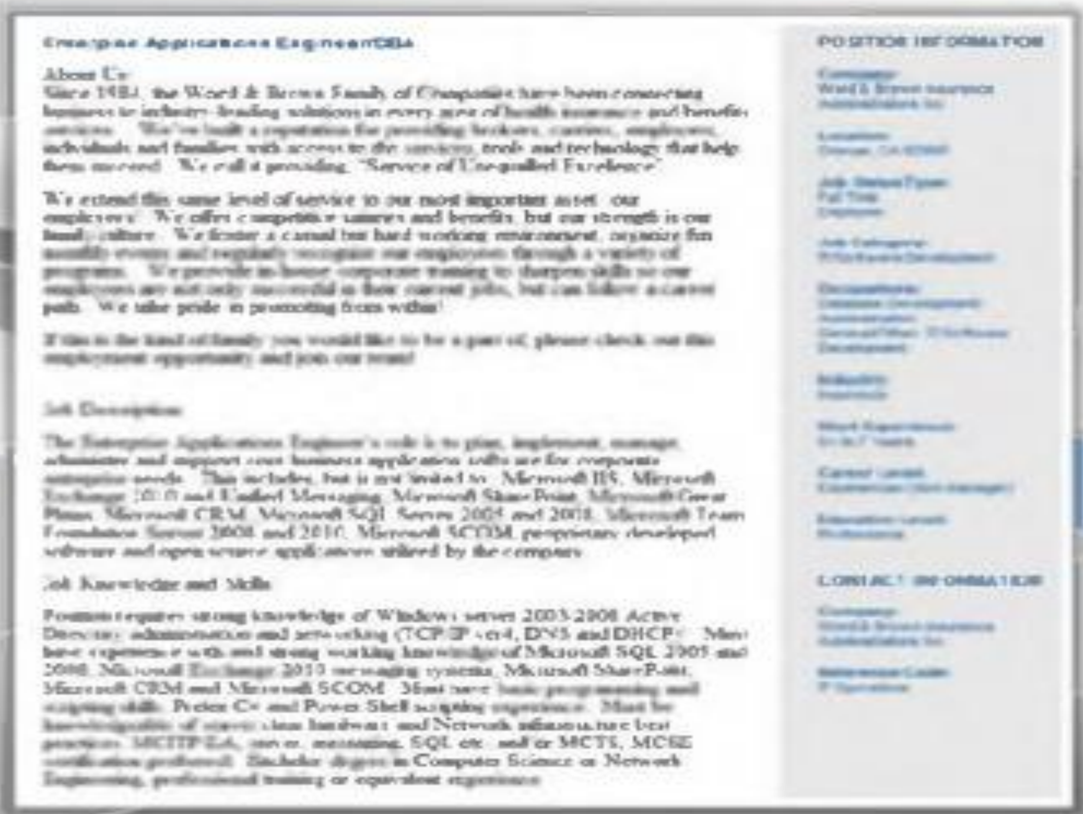
Gather Information from Financial Services

Google Finance
(http://finance.google.com/finance)

Yahoo Finance
(http://finance.yahoo.com)

Footprinting through **Job Sites**

You can gather **company's infrastructure details** from job postings



Enterprise Applications Engineer/DBA

About Us
Since 1984, the Word & Brown Family of Companies have been connecting [illegible] to industry-leading solutions in every area of health insurance and benefits services. We've built a reputation for providing brokers, carriers, employers, individuals and families with access to the services, tools and technology that help them succeed. We call it providing "Service of Une-qualled Excellence".

We extend this same level of service to our most important asset: our employees! We offer competitive salaries and benefits, but our strength is our family culture. We foster a casual but hard working environment, organize fun monthly events and regularly recognize our employees through a variety of programs. We provide in-house corporate training to sharpen skills so our employees are not only successful in their current jobs, but can follow a career path. We take pride in promoting from within!

If this is the kind of family you would like to be a part of, please check out this employment opportunity and join our team!

Job Description

The Enterprise Applications Engineer's role is to plan, implement, manage, administer and support core business applications utilized for corporate enterprise needs. This includes, but is not limited to: Microsoft IIS, Microsoft Exchange 2010 and Unified Messaging, Microsoft SharePoint, Microsoft Great Plains, Microsoft CRM, Microsoft SQL Server 2005 and 2008, Microsoft Team Foundation Server 2008 and 2010, Microsoft SCOM, proprietary developed software and open source applications utilized by the company.

Job Knowledge and Skills

Position requires strong knowledge of Windows server 2003-2008 Active Directory administration and networking (TCP/IP v4, DNS and DHCP). Must have experience with and strong working knowledge of Microsoft SQL 2005 and 2008, Microsoft Exchange 2010 messaging systems, Microsoft SharePoint, Microsoft CRM and Microsoft SCOM. Must have basic programming and scripting skills. Prefer C# and Power Shell scripting experience. Must be knowledgeable of server class hardware and Network infrastructure best practices. MCITP:EA, server, messaging, SQL etc. and/or MCTS, MCSE certification preferred. Bachelor degree in Computer Science or Network Engineering, professional training or equivalent experience.

POSITION INFORMATION

Company:
Word & Brown Insurance Administrators Inc.

Location:
Orange, CA [illegible]

Job Status/Type:
Full Time
Employee

Job Category:
IT/Software Development

Occupations:
Database Development/Administration
General/Other: IT/Software Development

Industry:
Insurance

Work Experience:
5 to 7 Years

Career Level:
Experienced (Non-Manager)

Education Level:
Professional

CONTACT INFORMATION

Company:
Word & Brown Insurance Administrators Inc.

Reference Code:
IT Operations

Look for these:

- Job requirements
- Employee's profile
- Hardware information
- Software information

Examples of Job Websites

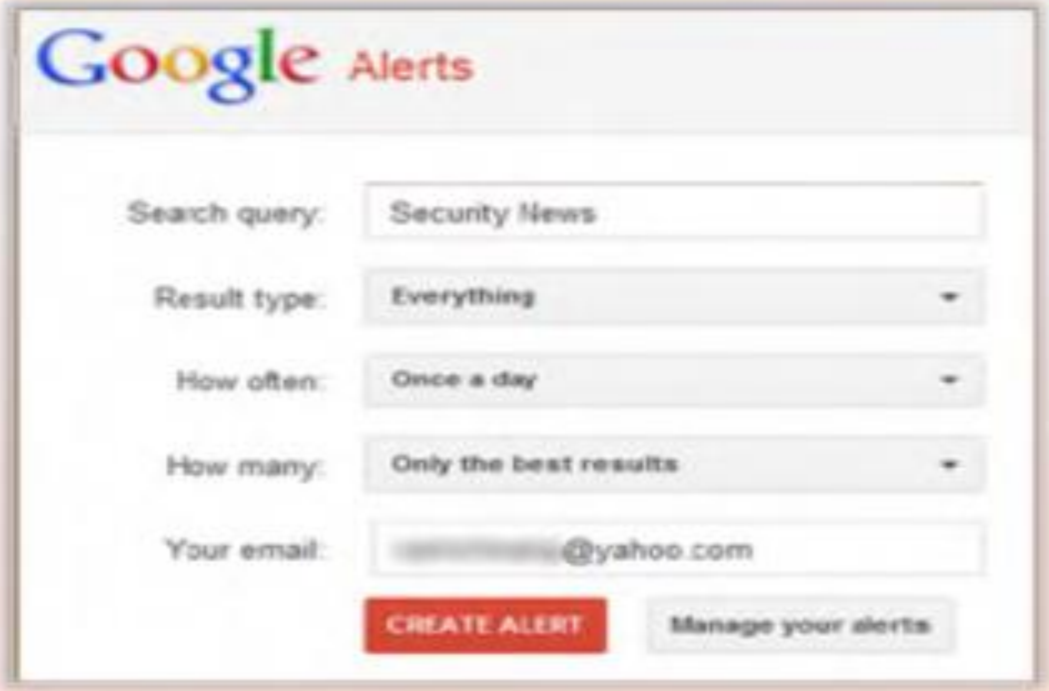
- http://www.monster.com
- http://www.careerbuilder.com
- http://www.dice.com
- http://www.simplyhired.com
- http://www.indeed.com
- http://www.usajobs.gov

Monitoring Target Using Alerts

Alerts are the content monitoring services that provide up-to-date information based on your preference usually via email or SMS in an automated manner

Examples of Alert Services

- Google Alerts - http://www.google.com/alerts
- Yahoo! Alerts - http://alerts.yahoo.com
- Giga Alert - http://www.gigaalert.com



Google Alerts

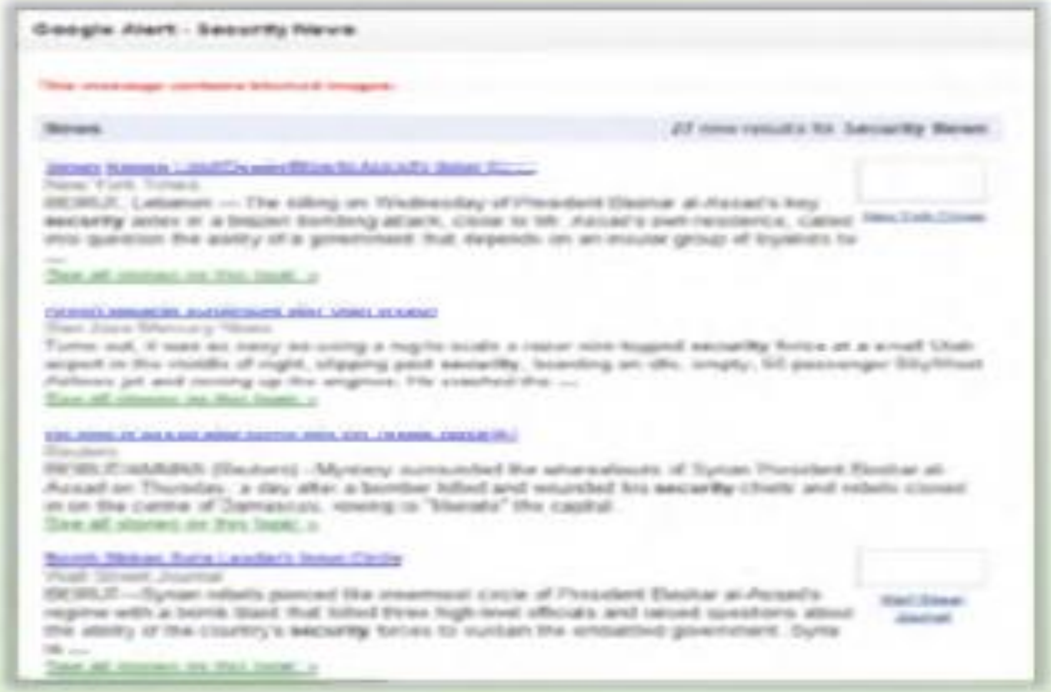
Search query: Security News

Result type: Everything

How often: Once a day

How many: Only the best results

Your email: [redacted]@yahoo.com



Google Alert - Security News

This message contains blocked images.

News — 27 new results for Security News

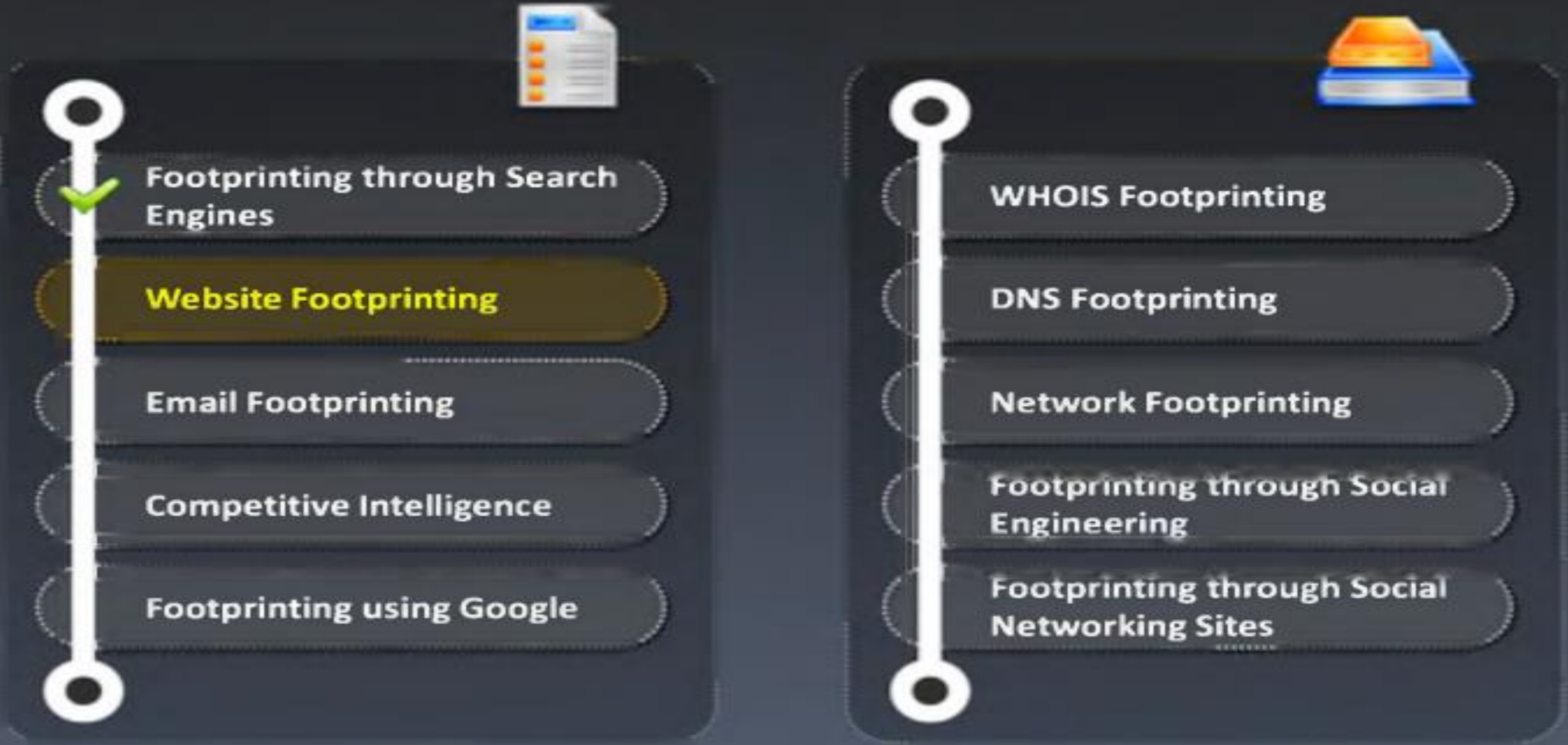
[illegible]
New York Times
BEIRUT, Lebanon — The killing on Wednesday of President Bashar al-Assad's key security aides in a brazen bombing attack, close to Mr. Assad's own residence, called into question the ability of a government that depends on an insular group of loyalists to ...
See all stories on this topic »

[illegible]
Salt Lake Deseret News
Turns out, it was as easy as using a [illegible] to scale a razor wire-topped security fence at a small Utah airport in the middle of night, slipping past security, boarding an idle, empty, 50-passenger SkyWest Airlines jet and revving up the engines. He crashed the ...
See all stories on this topic »

[illegible]
Reuters
BEIRUT/AMMAN (Reuters) - Mystery surrounded the whereabouts of Syrian President Bashar al-Assad on Thursday, a day after a bomber killed and wounded his security chiefs and rebels closed in on the centre of Damascus, vowing to "liberate" the capital.
See all stories on this topic »

Bomb Strikes Syria Leader's Inner Circle
Wall Street Journal
BEIRUT—Syrian rebels pierced the innermost circle of President Bashar al-Assad's regime with a bomb blast that killed three high-level officials and raised questions about the ability of the country's security forces to sustain the embattled government. Syria is ...
See all stories on this topic »

Footprinting Methodology



- ✓ Footprinting through Search Engines
- **Website Footprinting**
- Email Footprinting
- Competitive Intelligence
- Footprinting using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Website Footprinting

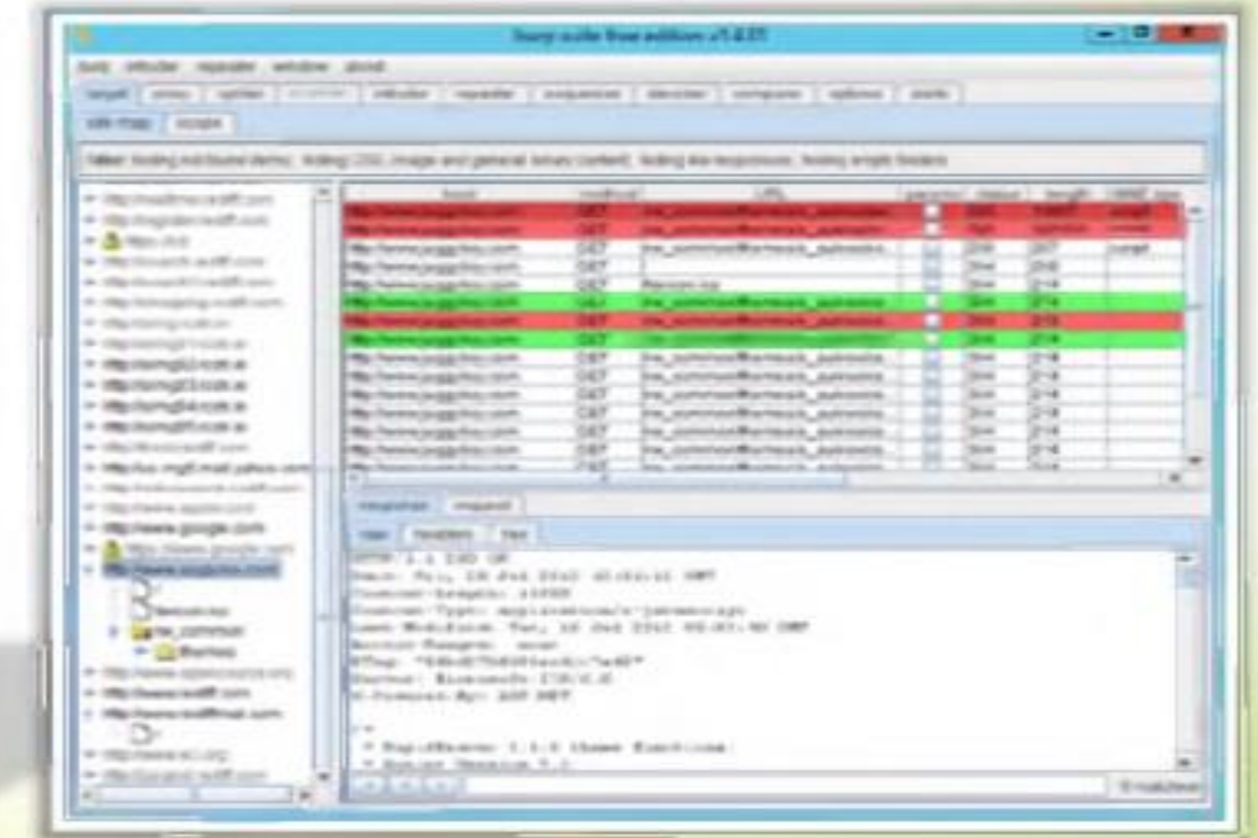
Information obtained from target's website enables an attacker to build a detailed **map of website's structure and architecture**

Browsing the target website may provide:

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

Use Zaproxy, Burp Suite, Firebug, etc. to view headers that provide:

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



http://portswigger.net

Website Footprinting (Cont'd)

Examining HTML source provides:

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

```
Microsoft Corporation: Software, Smartphones, Online, Games, Cloud
Computing, IT Business Technology, Downloads
```

Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used

Mirroring Entire Website

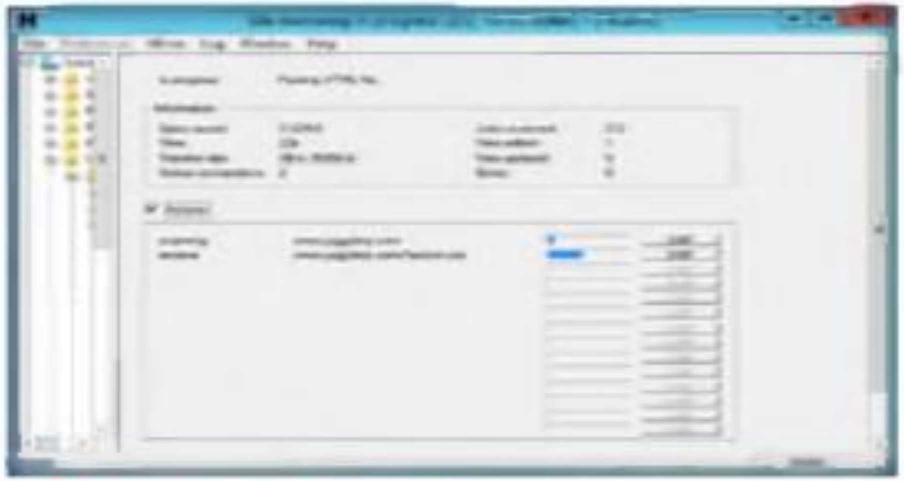
- Mirroring an entire website onto the local system enables an attacker to dissect and identify vulnerabilities; it also assists in finding directory structure and other valuable information without multiple requests to web server
- Web mirroring tools allow you to download a website to a local directory, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer

http://www.juggyboy.com
C:\juggyboy.com

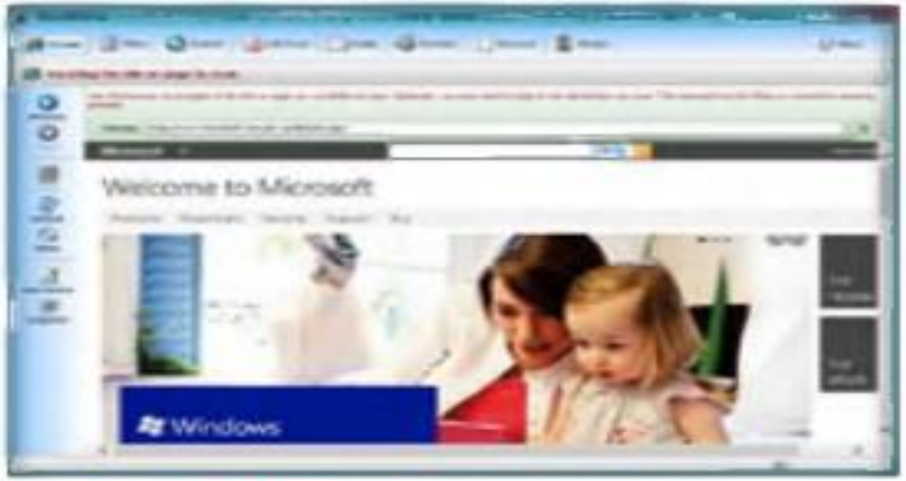
Original Website

Mirrored Website

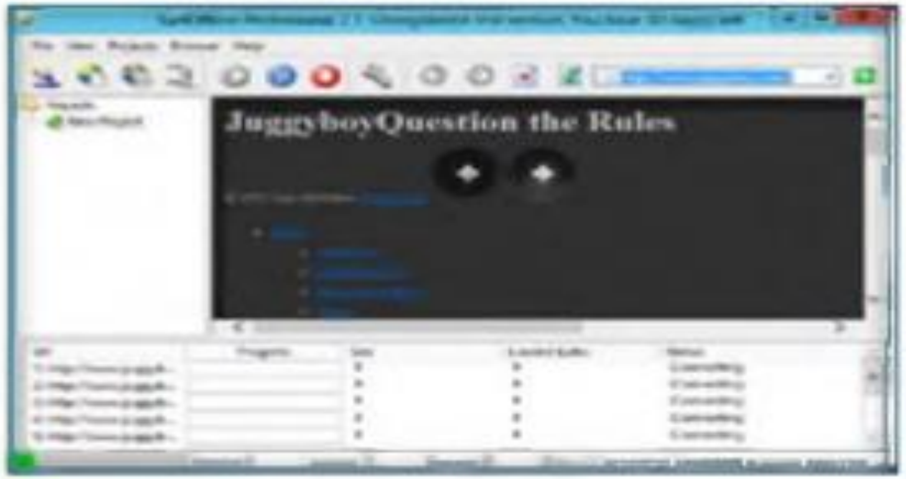
Website Mirroring Tools



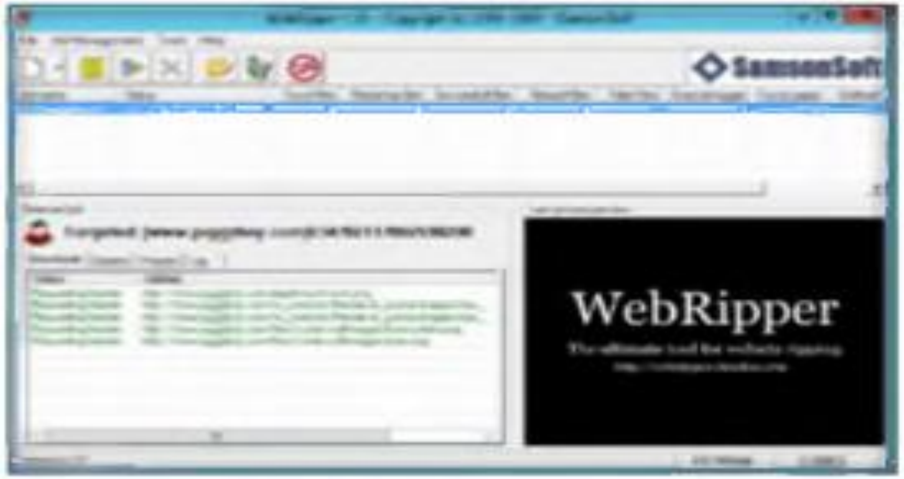
HTTrack Web Site Copier (*http://www.httrack.com*)



BlackWidow (*http://softbytelabs.com*)



SurfOffline (*http://www.surfoffline.com*)



WebRipper (*http://www.calluna-software.com*)

Website Mirroring Tools (Cont'd)

Website Ripper Copier
http://www.tensons.com

Teleport Pro
http://www.tenmax.com

Portable Offline Browser
http://www.metaproducts.com

Proxy Offline Browser
http://www.proxy-offline-browser.com

iMiser
http://internetresearchtool.com

PageNest
http://www.pagenest.com

Backstreet Browser
http://www.spadixbd.com

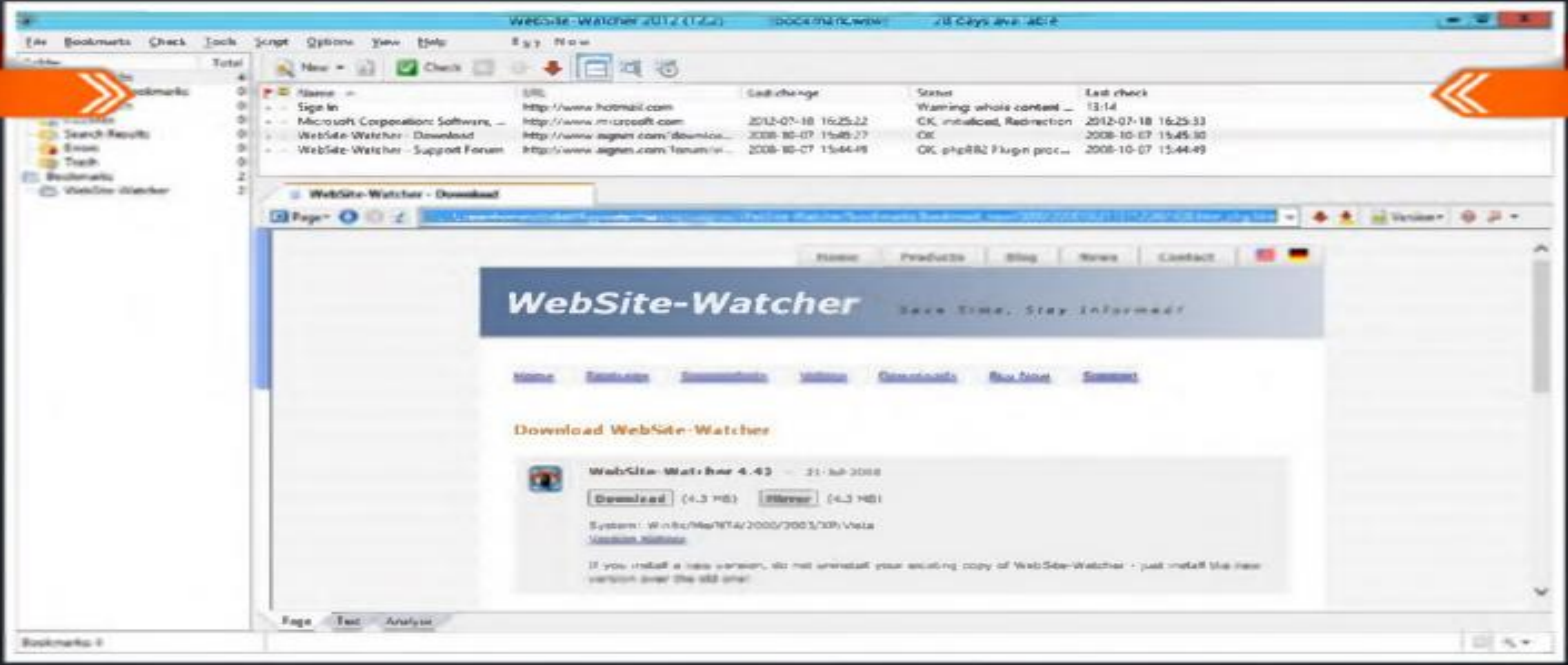
Offline Explorer Enterprise
http://www.metaproducts.com

GNU Wget
http://www.gnu.org

Hooeey Webprint
http://www.hooeeywebprint.com

Monitoring Web Updates Using **Website Watcher**

Website Watcher **automatically checks web pages** for updates and changes



Name	URL	Last change	Status	Last check
Sign In	http://www.hotmail.com		Warning: whole content ...	13:14
Microsoft Corporation: Software, ...	http://www.microsoft.com	2012-07-18 16:25:22	OK, initialized, Redirection	2012-07-18 16:25:33
WebSite-Watcher - Download	http://www.aignes.com/downloa...	2008-10-07 15:45:27	OK	2008-10-07 15:45:30
WebSite-Watcher - Support Forum	http://www.aignes.com/forum/vi...	2008-10-07 15:44:49	OK, phpBB2 Plugin proc...	2008-10-07 15:44:49

WebSite-Watcher

Save time, stay informed!

Download WebSite-Watcher

WebSite-Watcher 4.43 - 21-Jul-2008

Download (4.3 MB) Mirror (4.3 MB)

System: Win9x/Me/NT4/2000/2003/XP/Vista

If you install a new version, do not uninstall your existing copy of WebSite-Watcher - just install the new version over the old one!

http://aignes.com

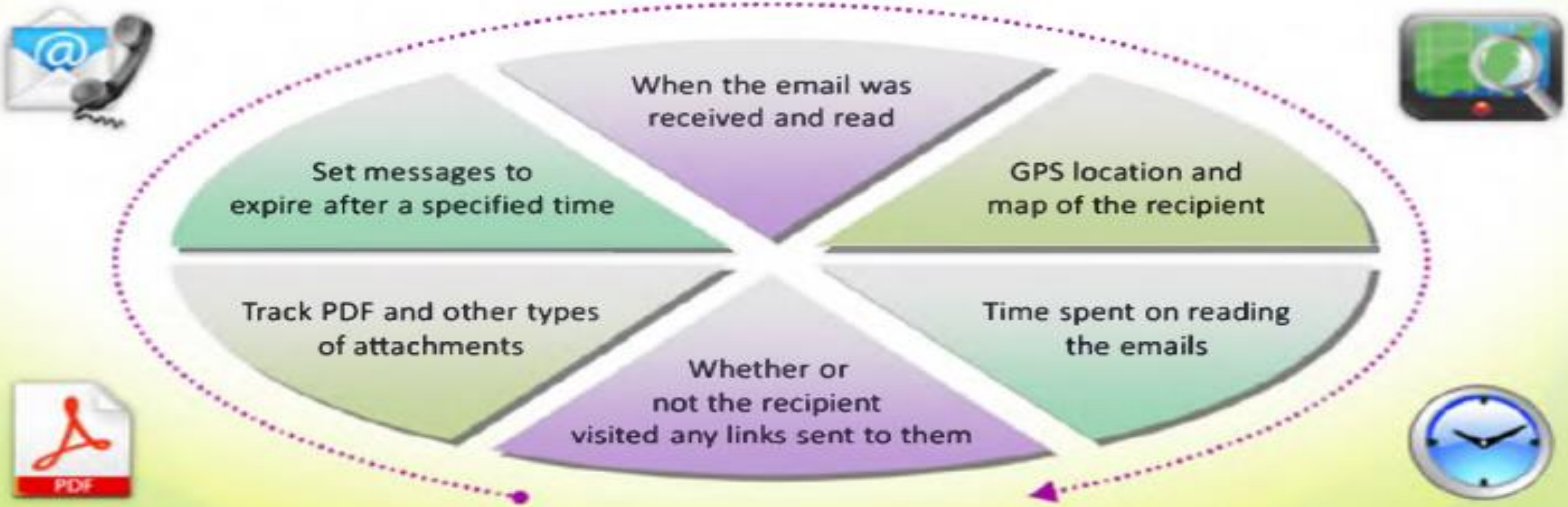
Footprinting Methodology

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- **Email Footprinting**
- Competitive Intelligence
- Footprinting using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Tracking Email Communications

- Attacker tracks email to gather information about the **physical location of an individual** to perform social engineering that in turn may help in **mapping target organization's network**
- Email tracking is a method to **monitor and spy on the delivered emails** to the intended recipient



When the email was received and read

GPS location and map of the recipient

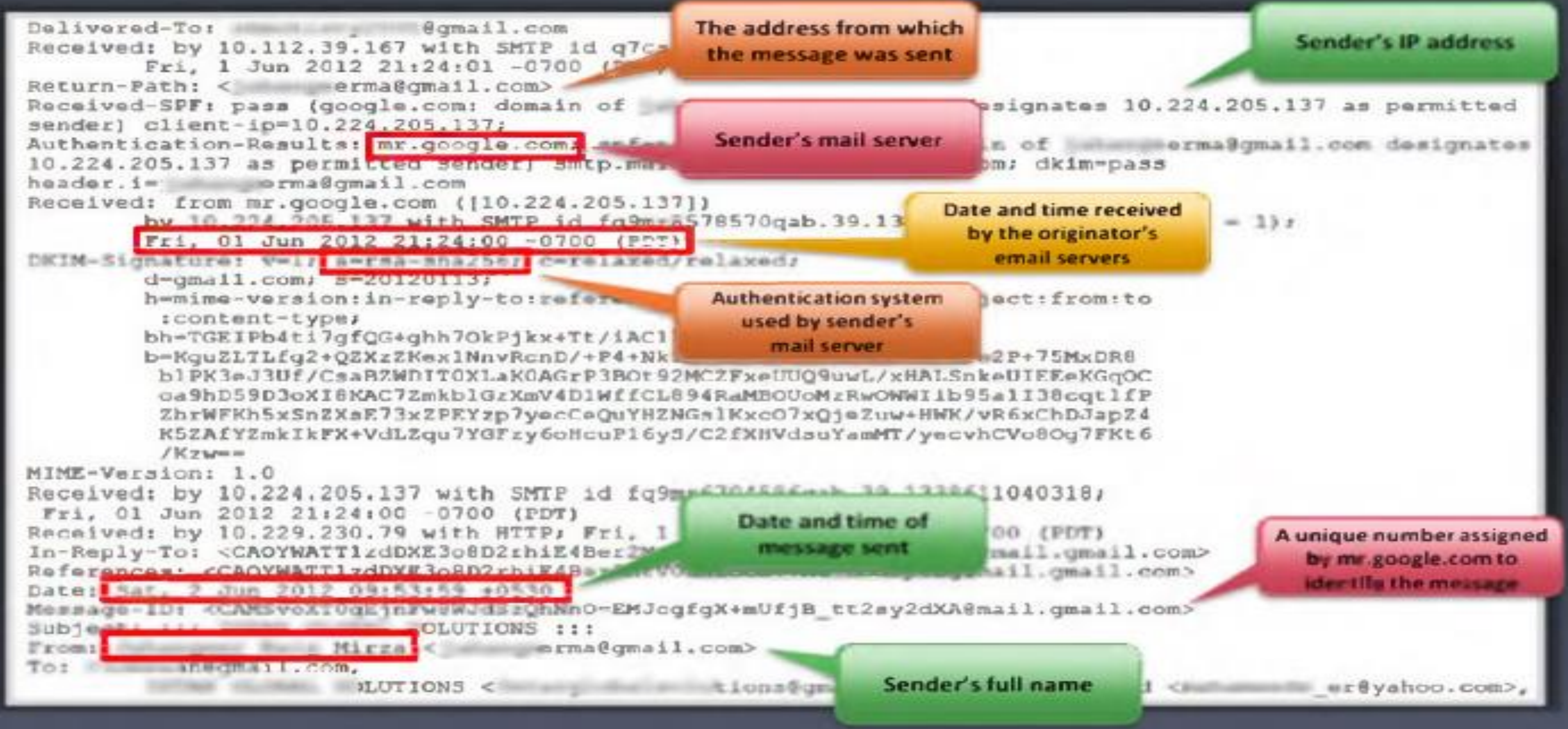
Time spent on reading the emails

Whether or not the recipient visited any links sent to them

Track PDF and other types of attachments

Set messages to expire after a specified time

Collecting Information from Email Header



```
Delivered-To: [redacted]@gmail.com
Received: by 10.112.39.167 with SMTP id q7c
        Fri, 1 Jun 2012 21:24:01 -0700 (
Return-Path: <[redacted]erma@gmail.com>
Received-SPF: pass (google.com: domain of [redacted]          esignates 10.224.205.137 as permitted
sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; spf                  n of [redacted]erma@gmail.com designates
10.224.205.137 as permitted sender) smtp.ma                 om; dkim=pass
header.i=[redacted]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
        by 10.224.205.137 with SMTP id fq9mr6578570qab.39.13                    = 1);
        Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:in-reply-to:refere                   ject:from:to
         :content-type;
        bh=TGEIPb4ti7gfQG+ghh7OkPjkx+Tt/iAC1
        b=KguZLTLfg2+QZXzZKex1NnvRcnD/+P4+Nk                2P+75MxDR8
         b1PK3eJ3Uf/CsaBZWDITOXLaK0AGrP3BOt92MCZFxeUUQ9uwL/xHALSnkeUIEFeKGqOC
         oa9hD59D3oXI8KAC7Zmkb1GzXmV4D1WffCL894RaMBOUoMzRwOWWIib95a1I38cqt1fP
         ZhrWFKh5xSnZXaE73xZPEYzp7yecCeQuYHZNGs1KxcO7xQjeZuw+HWK/vR6xChDJapZ4
         K5ZAfYZmkIkFX+VdLZqu7YGFzy6oHcuP16y5/C2fXHVdsuYamMT/yecvhCVo8Og7FKt6
         /Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9m                1040318;
 Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Fri, 1                 00 (PDT)
In-Reply-To: <CAOYWATT1zdDXE3o8D2zhiE4Ber2M                  mail.gmail.com>
References: <CAOYWATT1zdDXE3o8D2rhiE4B                        ail.gmail.com>
Date: Sat, 2 Jun 2012 09:53:59 +0530
Message-ID: <CAMSvoXT0gEjnFwsWJdszQhNnO-EMJcgfgX+mUfjB_tt2sy2dXA@mail.gmail.com>
Subject: ::: [redacted] OLUTIONS :::
From: [redacted] Mirza <[redacted]erma@gmail.com>
To: [redacted]ne@gmail.com,
        [redacted] OLUTIONS <[redacted]tions@gm                d <[redacted]_er@yahoo.com>,
```

The address from which the message was sent

Sender's IP address

Sender's mail server

Date and time received by the originator's email servers

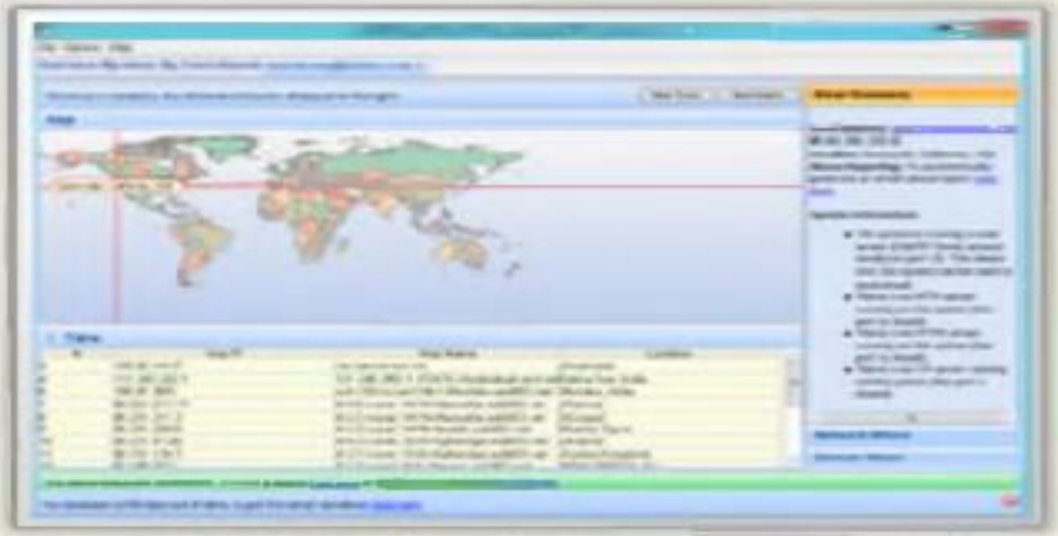
Authentication system used by sender's mail server

Date and time of message sent

A unique number assigned by mr.google.com to identify the message

Sender's full name

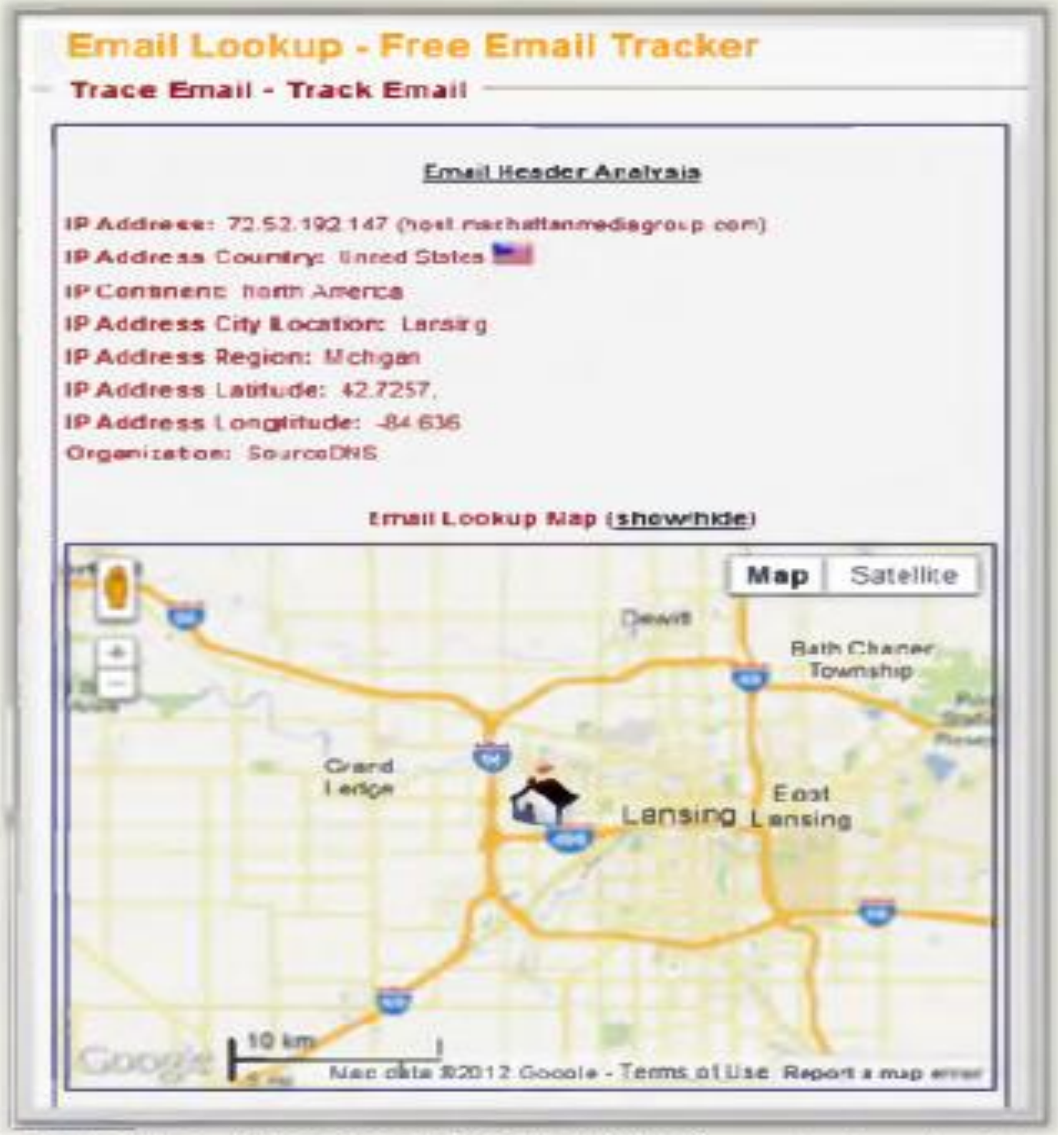
Email Tracking Tools



eMailTrackerPro (*http://www.emailtrackerpro.com*)

Email Metrics

PoliteMail (*http://www.politemail.com*)



Email Lookup - Free Email Tracker

Trace Email - Track Email

Email Header Analysis

IP Address: 72.52.192.147 (host.manhattanmediagroup.com)

IP Address Country: United States

IP Continent: North America

IP Address City Location: Lansing

IP Address Region: Michigan

IP Address Latitude: 42.7257,

IP Address Longitude: -84.636

Organization: SourceDNS

Email Lookup Map (show/hide)

Email Lookup – Free Email Tracker (*http://www.ipaddresslocation.org*)

Email Tracking Tools (Cont'd)

Read Notify
http://www.readnotify.com

DidTheyReadIt
http://www.didtheyreadit.com

Trace Email
http://whatismyipaddress.com

MSGTAG
http://www.msgtag.com

Zendio
http://www.zendio.com

Pointofmail
http://www.pointofmail.com

Super Email Marketing Software
http://www.bulk-email-marketing-software.net

WhoReadMe
http://whoreadme.com

GetNotify
http://www.getnotify.com

G-Lock Analytics
http://glockanalytics.com

Footprinting **Methodology**

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- **Competitive Intelligence**
- Footprinting using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

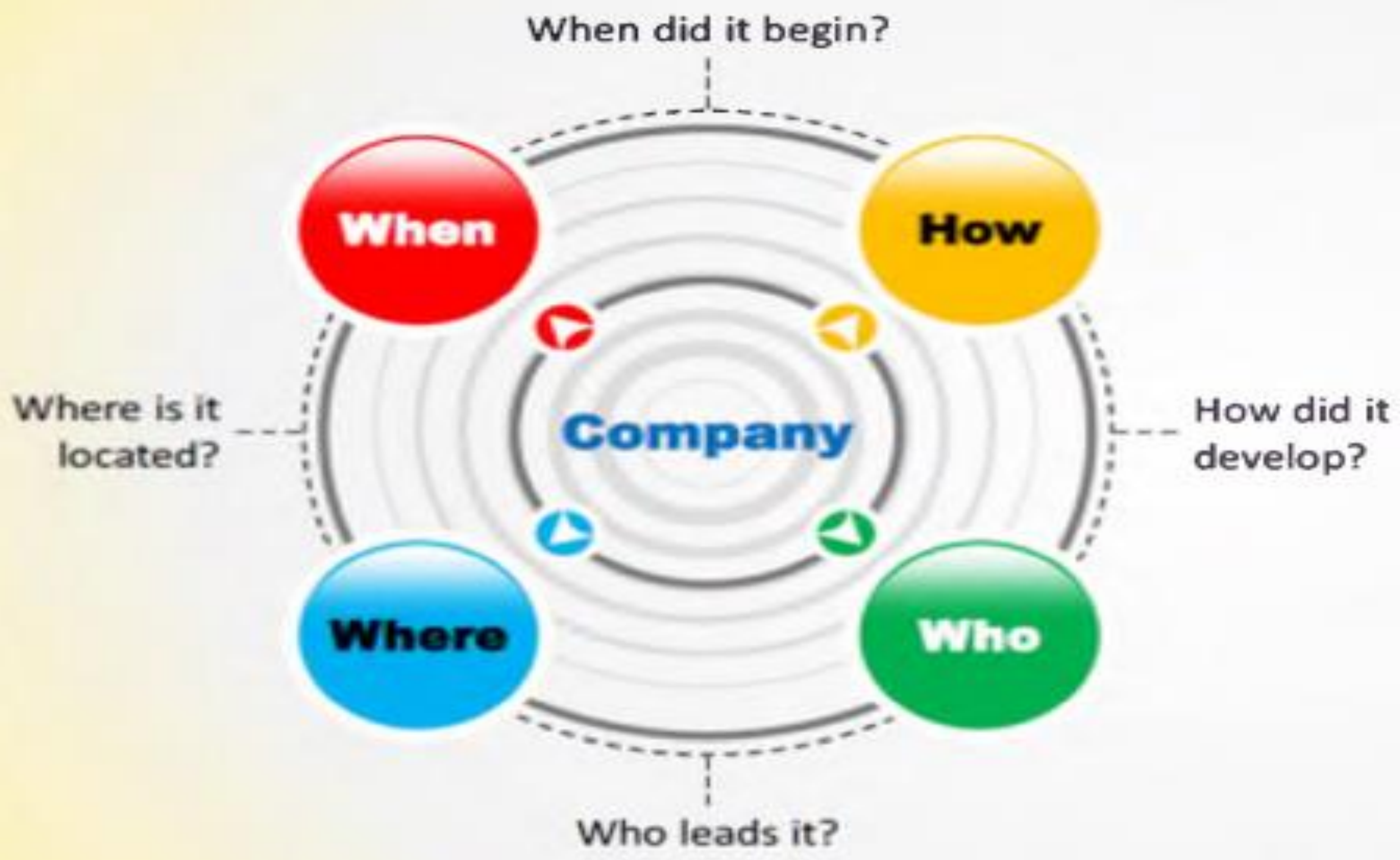
Competitive Intelligence Gathering

- Competitive intelligence 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 databases
3. Press releases and annual reports
4. Trade journals, conferences, and newspaper
5. Patent and trademarks
6. Social engineering employees
7. Product catalogues and retail outlets
8. Analyst and regulatory reports
9. Customer and vendor interviews
10. Agents, distributors, and suppliers

Competitive Intelligence - When Did this Company Begin? How Did it Develop?



Visit These Sites

01. EDGAR Database

http://www.sec.gov/edgar.shtml

02. Hoovers

http://www.hoovers.com

03. LexisNexis

http://www.lexisnexis.com

04. Business Wire

http://www.businesswire.com

Competitive Intelligence - What Are the Company's Plans?

Competitive Intelligence Sites

- ✓ Market Watch (*http://www.marketwatch.com*)
- ✓ The Wall Street Transcript (*http://www.twst.com*)
- ✓ Lipper Marketplace (*http://www.lippermarketplace.com*)
- ✓ Euromonitor (*http://www.euromonitor.com*)
- ✓ Fagan Finder (*http://www.faganfinder.com*)
- ✓ SEC Info (*http://www.secinfo.com*)
- ✓ The Search Monitor (*http://www.thesearchmonitor.com*)

Competitive Intelligence - What Expert Opinions Say About the Company

Compete PRO™
http://www.compete.com

Copernic Tracker
http://www.copernic.com

ABI/INFORM Global
http://www.proquest.com

SEMRush
http://www.semrush.com

AttentionMeter
http://www.attentionmeter.com

Jobitorial
http://www.jobitorial.com

Footprinting Methodology

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- Footprinting using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprint Using Google Hacking Techniques

101010
010101
101
http://

Query String

Google hacking refers to creating search queries to extract sensitive or hidden information

Vulnerable Targets

It helps attackers to find vulnerable targets

Google Operators

It uses Google operators to locate specific strings of text within the search results

What a Hacker can do with Google Hacking?

Attacker gathers:

- Advisories and server vulnerabilities
- Error messages that contain sensitive information
- Pages containing network or vulnerability data
- Files containing passwords
- Pages containing logon portals
- Sensitive directories

Google Advance Search Operators

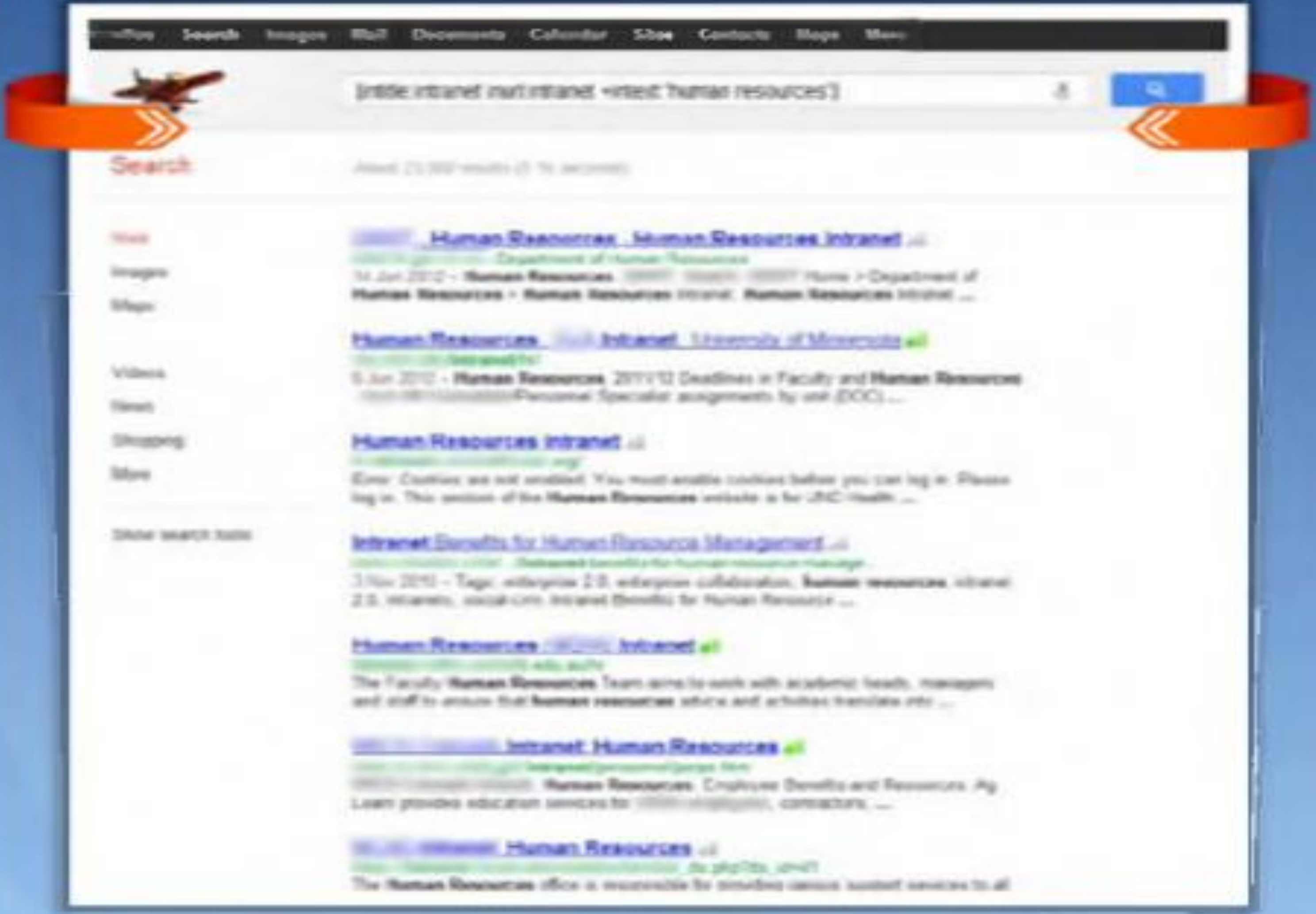
Google supports several advanced operators that help in modifying the search

[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 a 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
[allintitle:]	Restricts the results to those websites with all of 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 with all of the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL

Finding Resources Using Google Advance Operator

[intitle:intranet inurl:intranet +intext:"human resources"]:

The above combination of the Google advanced search operators allows you to access a target company's private network and collect **sensitive information** such as **employee listings**, **key contact details**, etc. that can be incredibly useful for any social engineering endeavor



[intitle:intranet inurl:intranet +intext:"human resources"]

About 21,300 results (0.15 seconds)

Human Resources - Human Resources Intranet
Department of Human Resources
14 Jun 2012 – Human Resources ... Home > Department of Human Resources > Human Resources Intranet. Human Resources Intranet ...

Human Resources ... Intranet - University of Minnesota
... intranet/hr/
5 Jun 2012 – Human Resources. 2011/12 Deadlines in Faculty and Human Resources ... Personnel Specialist assignments by unit (DOC) ...

Human Resources Intranet
... .org/
Error: Cookies are not enabled. You must enable cookies before you can log in. Please log in. This section of the Human Resources website is for UNC Health ...

Intranet Benefits for Human Resource Management
... Intranet-benefits-for-human-resource-manage...
3 Nov 2010 – Tags: enterprise 2.0, enterprise collaboration, human resources, intranet 2.0, intranets, social crm. Intranet Benefits for Human Resource ...

Human Resources ... Intranet
... edu.au/hr/
The Faculty Human Resources Team aims to work with academic heads, managers and staff to ensure that human resources advice and activities translate into ...

... Intranet: Human Resources
... intranet/personnel/pages.htm
... Human Resources. Employee Benefits and Resources. Ag Learn provides education services for ... employees, contractors, ...

... Human Resources
... /lo.php?ds_id=0
The Human Resources office is responsible for providing various support services to all

Google Hacking Tool: Google Hacking Database (GHDB)

Advisories and Vulnerabilities

GHDB - Hackers For Charity
www.hackersforcharity.org
GHDB » Hackers For Charity
GHDB

Pages Containing Login Portals

http://www.hackersforcharity.org

Google Hacking Tools

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

Goolink Scanner
http://www.ghacks.net

SiteDigger
http://www.mcafee.com

Google Hacks
http://code.google.com

BiLE Suite
http://www.sensepost.com

Google Hack Honeypot
http://ghh.sourceforge.net

GMapCatcher
http://code.google.com

SearchDiggity
http://www.stachliu.com

Google HACK DB
http://www.secpoint.com

Gooscan
http://www.darknet.org.uk

Footprinting Methodology

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- ✓ Footprinting using Google

- **WHOIS Footprinting**
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

WHOIS Lookup

WHOIS databases are maintained by **Regional Internet Registries** and contain the **personal information of domain owners**

WHOIS query returns:

- Domain name details
- Contact details of domain owner
- Domain name servers
- NetRange
- When a domain has been created
- Expiry records
- Records last updated

Information obtained from WHOIS database assists an attacker to:

- Create detailed map of organizational network
- Gather personal information that assists to perform social engineering
- Gather other internal network details, etc.

Regional Internet Registries (RIRs)

AFRINIC

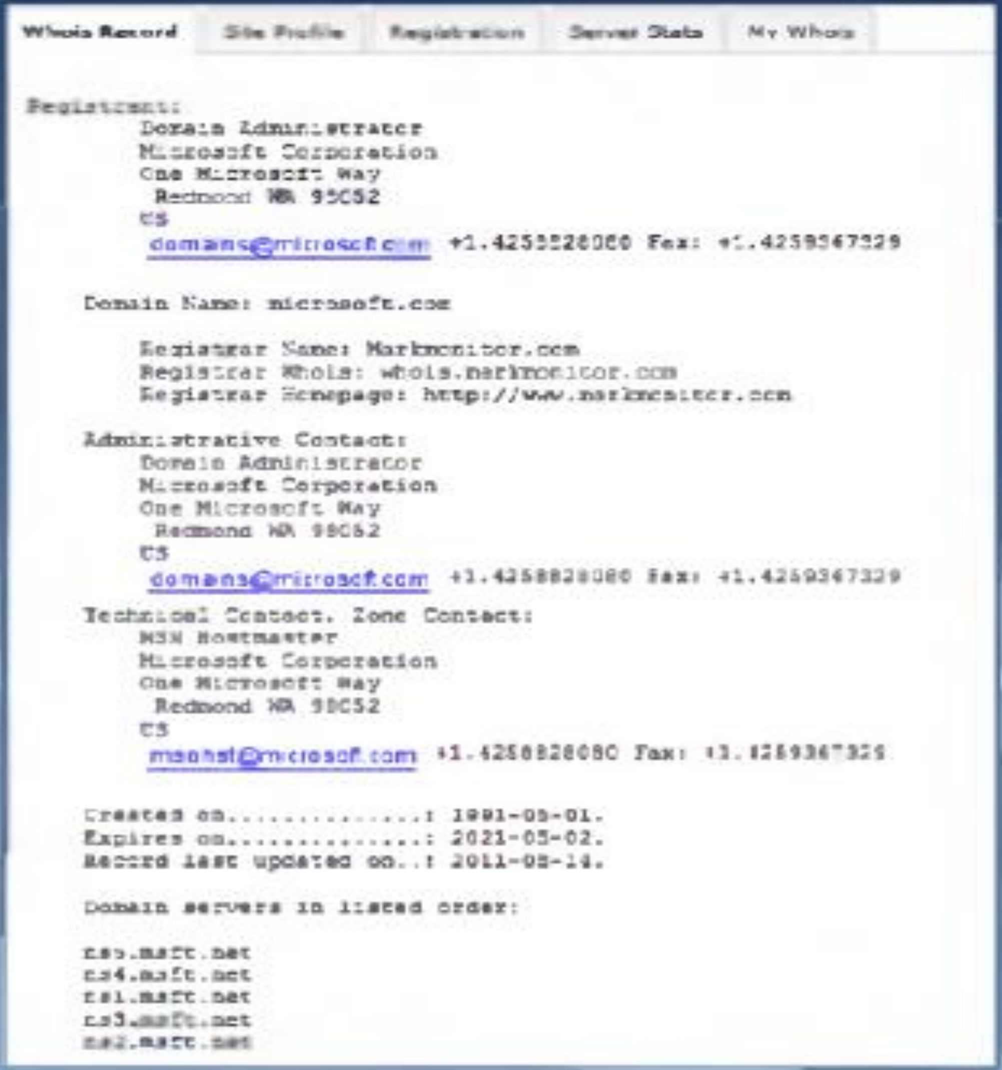
ARIN

APNIC

RIPE NCC

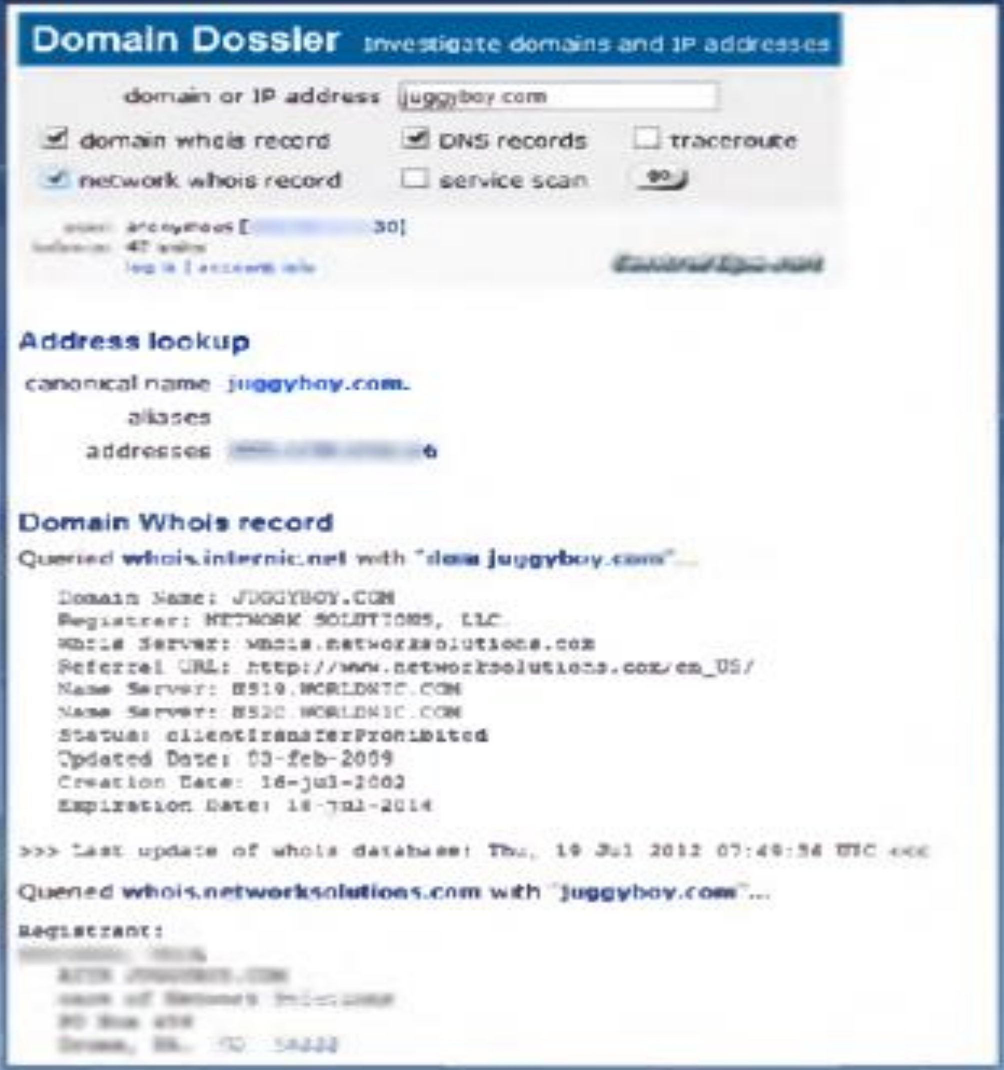
LACNIC

WHOIS Lookup Result Analysis



```
Registrant:
        Domain Administrator
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         domains@microsoft.com +1.4258828080 Fax: +1.4259367329

    Domain Name: microsoft.com

        Registrar Name: Markmonitor.com
        Registrar Whois: whois.markmonitor.com
        Registrar Homepage: http://www.markmonitor.com

    Administrative Contact:
        Domain Administrator
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         domains@microsoft.com +1.4258828080 Fax: +1.4259367329
    Technical Contact, Zone Contact:
        MSN Hostmaster
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         msnhst@microsoft.com +1.4258828080 Fax: +1.4259367329

    Created on..............: 1991-05-01.
    Expires on..............: 2021-05-02.
    Record last updated on..: 2011-08-14.

    Domain servers in listed order:

    ns5.msft.net
    ns4.msft.net
    ns1.msft.net
    ns3.msft.net
    ns2.msft.net
```

http://whois.domaintools.com



domain or IP address: juggyboy.com

☑ domain whois record ☑ DNS records □ traceroute
☑ network whois record □ service scan

user: anonymous [[redacted]30]
balance: 47 units
log in | account info

Address lookup

canonical name juggyboy.com.
aliases
addresses [redacted]6

Domain Whois record

Queried whois.internic.net with "dom juggyboy.com"...

```
Domain Name: JUGGYBOY.COM
Registrar: NETWORK SOLUTIONS, LLC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com/en_US/
Name Server: NS19.WORLDNIC.COM
Name Server: NS20.WORLDNIC.COM
Status: clientTransferProhibited
Updated Date: 03-feb-2009
Creation Date: 16-jul-2002
Expiration Date: 16-jul-2014
```

```
>>> Last update of whois database: Thu, 19 Jul 2012 07:49:56 UTC <<<
```

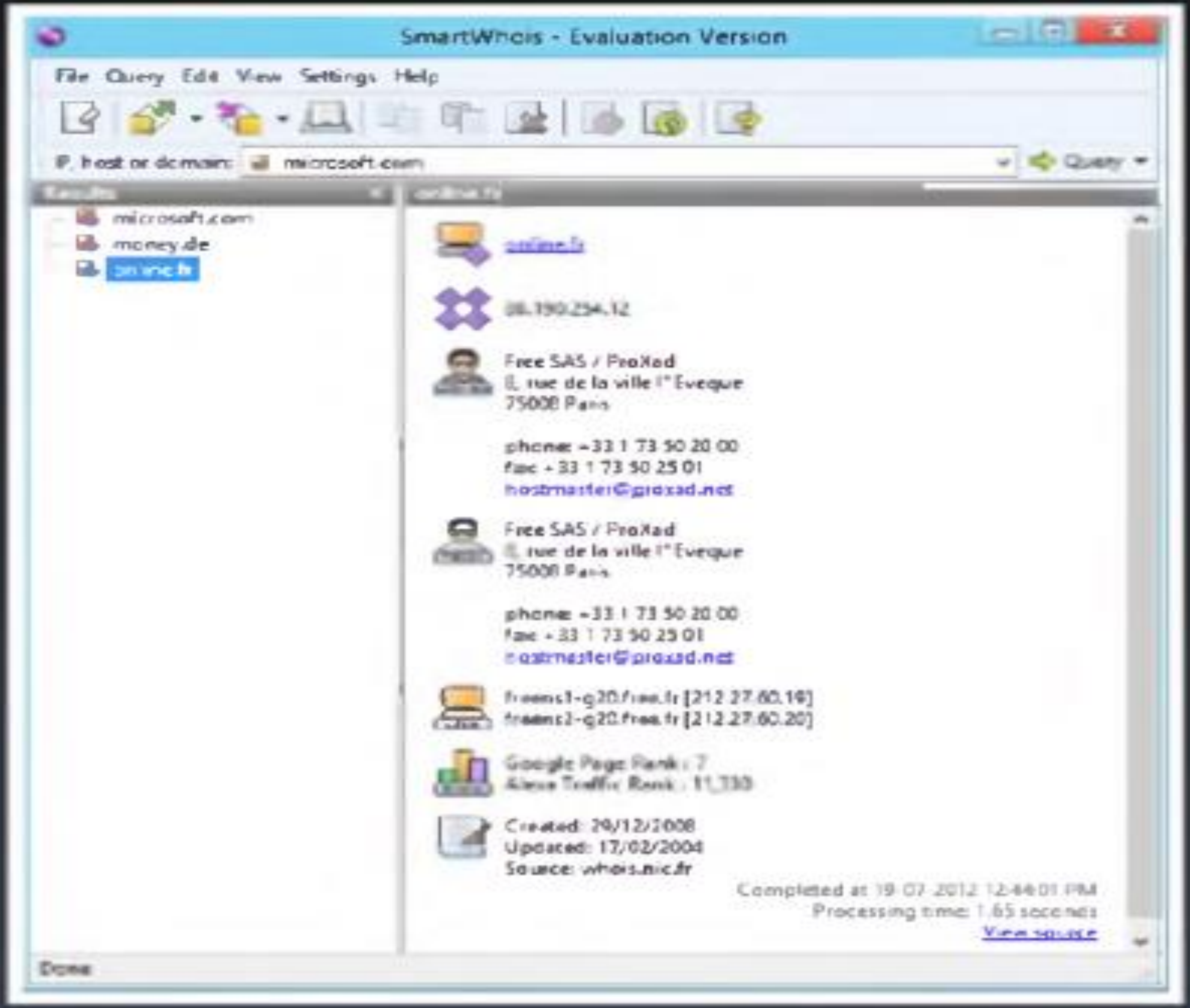
Queried whois.networksolutions.com with "juggyboy.com"...

```
Registrant:
[redacted]
```

http://centralops.net/co

WHOIS Lookup Tool: SmartWhois

- SmartWhois is a useful network information utility that allows you to look up all the available information about an **IP address**, **hostname**, or **domain**
- It also provides information about **country, state or province**, **city**, name of the network provider, administrator, and technical support contact information



IP, host or domain: microsoft.com

online.fr

88.190.254.12

Free SAS / ProXad
8, rue de la ville l'Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

Free SAS / ProXad
8, rue de la ville l'Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

freens1-g20.free.fr [212.27.60.19]
freens2-g20.free.fr [212.27.60.20]

Google Page Rank : 7
Alexa Traffic Rank : 11,330

Created: 29/12/2008
Updated: 17/02/2004
Source: whois.nic.fr

Completed at 19.07.2012 12:44:01 PM
Processing time: 1.65 seconds
View source

http://www.tamos.com

WHOIS Lookup Online Tools

SmartWhois
http://smartwhois.com

Better Whois
http://www.betterwhois.com

Whois Source
http://www.whois.sc

Web Wiz
http://www.webwiz.co.uk/domain-tools/whois-lookup.htm

Network-Tools.com
http://network-tools.com

Whois
http://tools.whois.net

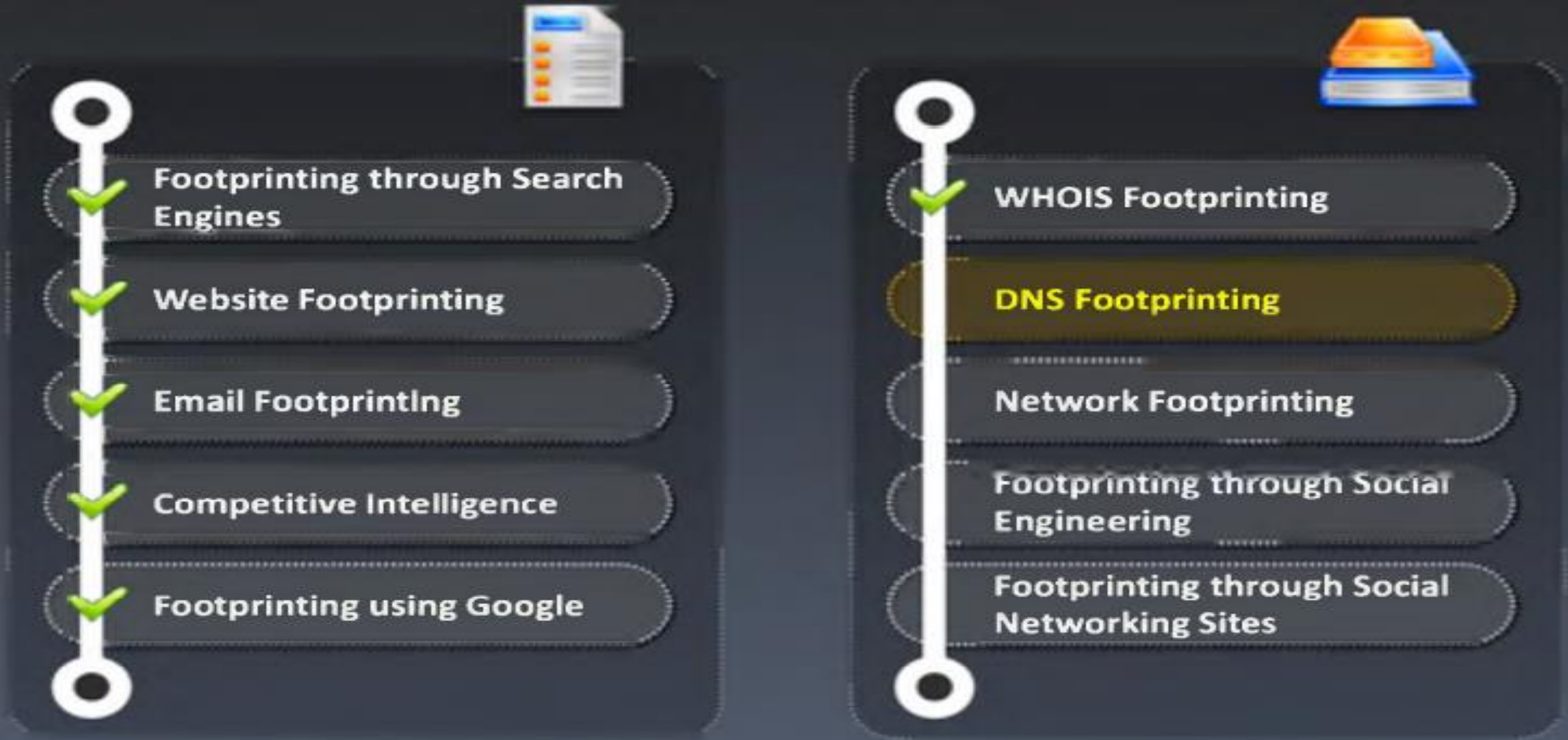
DNSstuff
http://www.dnsstuff.com

Network Solutions Whois
http://www.networksolutions.com

WebToolHub
http://www.webtoolhub.com/tn561381-whois-lookup.aspx

Ultra Tools
https://www.ultratools.com/whois/home

Footprinting Methodology



- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- ✓ Footprinting using Google

- ✓ WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Extracting DNS Information

Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks

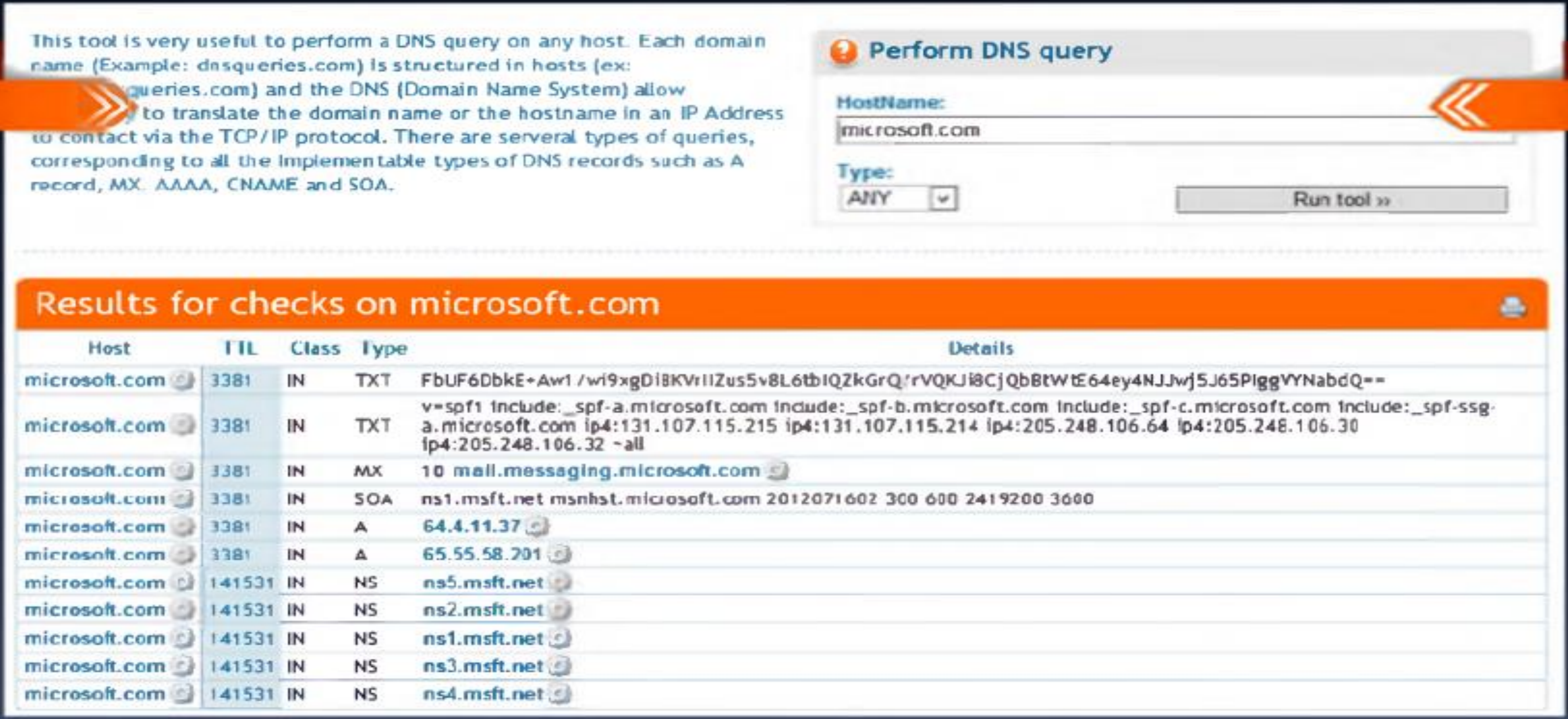
DNS records provide important information about location and type of servers

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 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

DNS Interrogation Tools

- http://www.dnsstuff.com
- http://network-tools.com

Extracting DNS Information
(Cont'd)



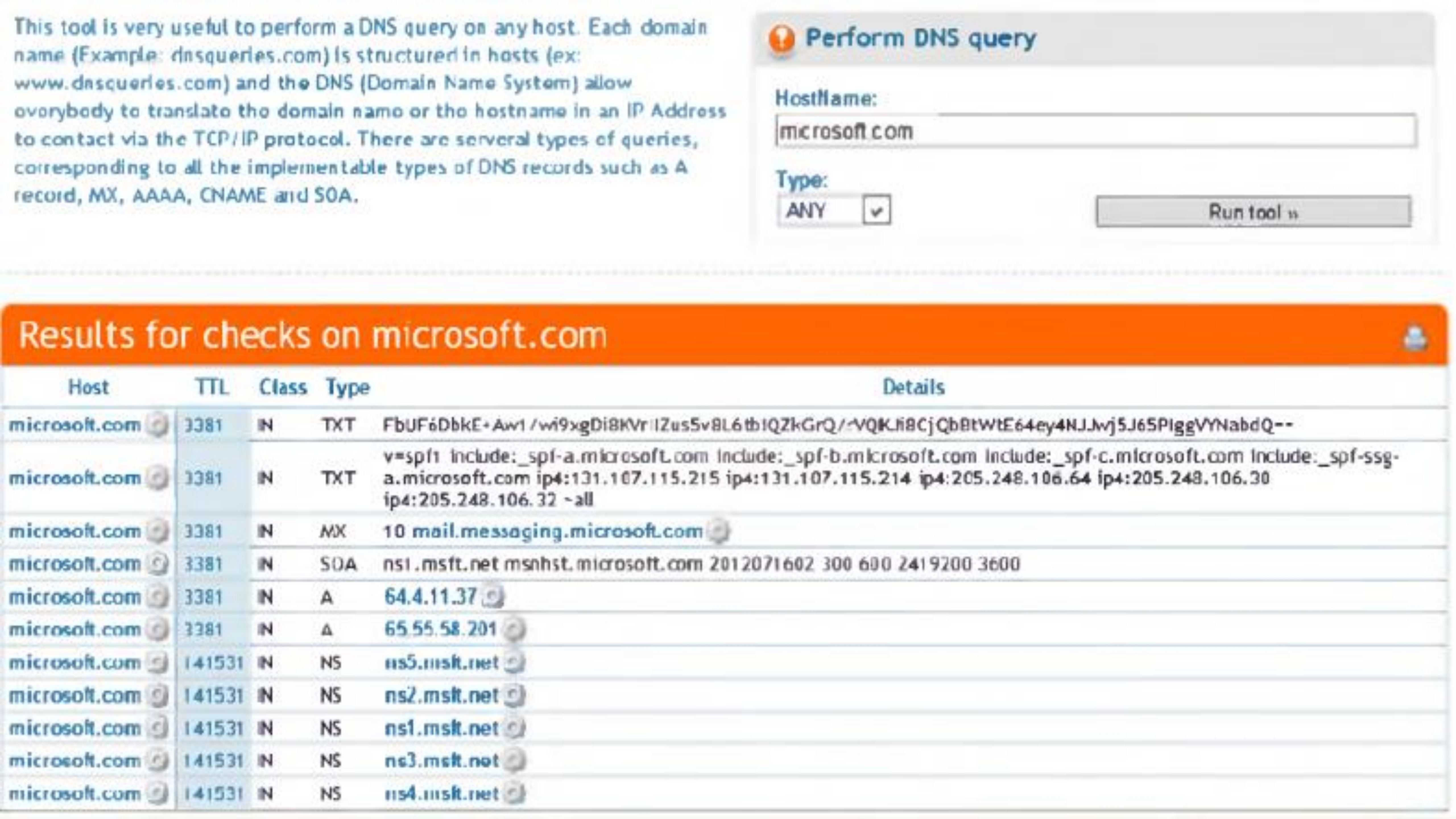
This tool is very useful to perform a DNS query on any host. Each domain name (Example: dnsqueries.com) is structured in hosts (ex: [illegible]queries.com) and the DNS (Domain Name System) allow [illegible] to translate the domain name or the hostname in an IP Address to contact via the TCP/IP protocol. There are serveral types of queries, corresponding to all the implementable types of DNS records such as A record, MX. AAAA, CNAME and SOA.

HostName: microsoft.com

Type: ANY

Results for checks on microsoft.com

Host	TTL	Class	Type	Details
microsoft.com	3381	IN	TXT	FbUF6DbkE+Aw1/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/rVQKJi8CjQbBtWtE64ey4NJJwj5J65PlggVYNabdQ==
microsoft.com	3381	IN	TXT	v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com ip4:131.107.115.215 ip4:131.107.115.214 ip4:205.248.106.64 ip4:205.248.106.30 ip4:205.248.106.32 ~all
microsoft.com	3381	IN	MX	10 mail.messaging.microsoft.com
microsoft.com	3381	IN	SOA	ns1.msft.net msnhst.microsoft.com 2012071602 300 600 2419200 3600
microsoft.com	3381	IN	A	64.4.11.37
microsoft.com	3381	IN	A	65.55.58.201
microsoft.com	141531	IN	NS	ns5.msft.net
microsoft.com	141531	IN	NS	ns2.msft.net
microsoft.com	141531	IN	NS	ns1.msft.net
microsoft.com	141531	IN	NS	ns3.msft.net
microsoft.com	141531	IN	NS	ns4.msft.net



This tool is very useful to perform a DNS query on any host. Each domain name (Example: dnsqueries.com) is structured in hosts (ex: www.dnsqueries.com) and the DNS (Domain Name System) allow everybody to translate the domain name or the hostname in an IP Address to contact via the TCP/IP protocol. There are serveral types of queries, corresponding to all the implementable types of DNS records such as A record, MX, AAAA, CNAME and SOA.

Perform DNS query

HostName: microsoft.com

Type: ANY

Results for checks on microsoft.com

Host	TTL	Class	Type	Details
microsoft.com	3381	IN	TXT	FbUF6DbkE+Aw1/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/+VQKJi8CjQbBtWtE64ey4NJJwj5J65PIggVYNabdQ--
microsoft.com	3381	IN	TXT	v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com ip4:131.107.115.215 ip4:131.107.115.214 ip4:205.248.106.64 ip4:205.248.106.30 ip4:205.248.106.32 ~all
microsoft.com	3381	IN	MX	10 mail.messaging.microsoft.com
microsoft.com	3381	IN	SOA	ns1.msft.net msnhst.microsoft.com 2012071602 300 600 2419200 3600
microsoft.com	3381	IN	A	64.4.11.37
microsoft.com	3381	IN	A	65.55.58.201
microsoft.com	141531	IN	NS	ns5.msft.net
microsoft.com	141531	IN	NS	ns2.msft.net
microsoft.com	141531	IN	NS	ns1.msft.net
microsoft.com	141531	IN	NS	ns3.msft.net
microsoft.com	141531	IN	NS	ns4.msft.net

DNS Interrogation Tools

DIG
http://www.kloth.net

myDNSTools
http://www.mydnstools.info

Professional Toolset
http://www.dnsstuff.com

DNS Records
http://network-tools.com

DNSData View
http://www.nirsoft.net

DNSWatch
http://www.dnswatch.info

DomainTools
http://www.domaintools.com

DNS
http://e-dns.org

DNS Lookup Tool
http://www.webwiz.co.uk

DNS Query Utility
http://www.webmaster-toolkit.com

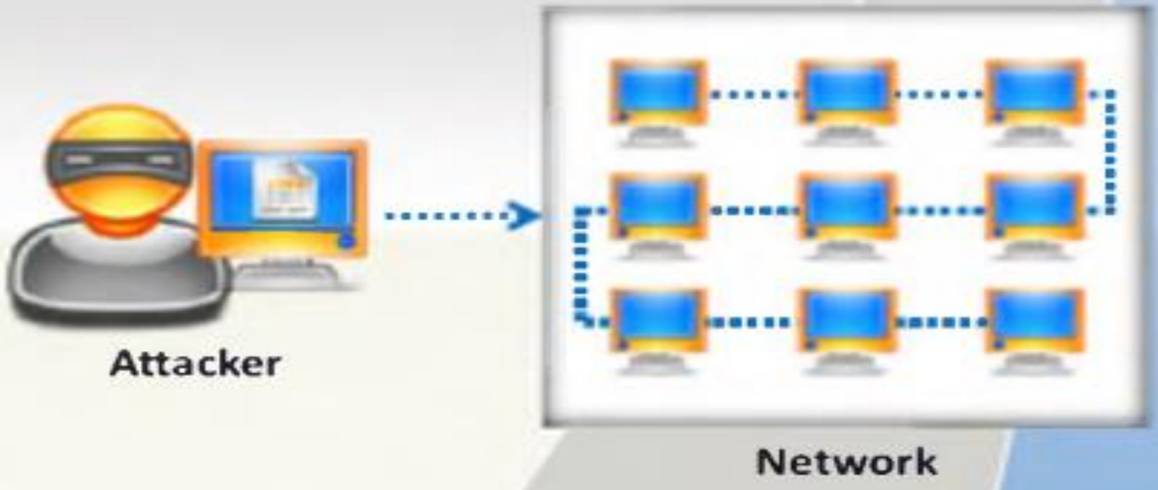
Footprinting Methodology

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- ✓ Footprinting using Google

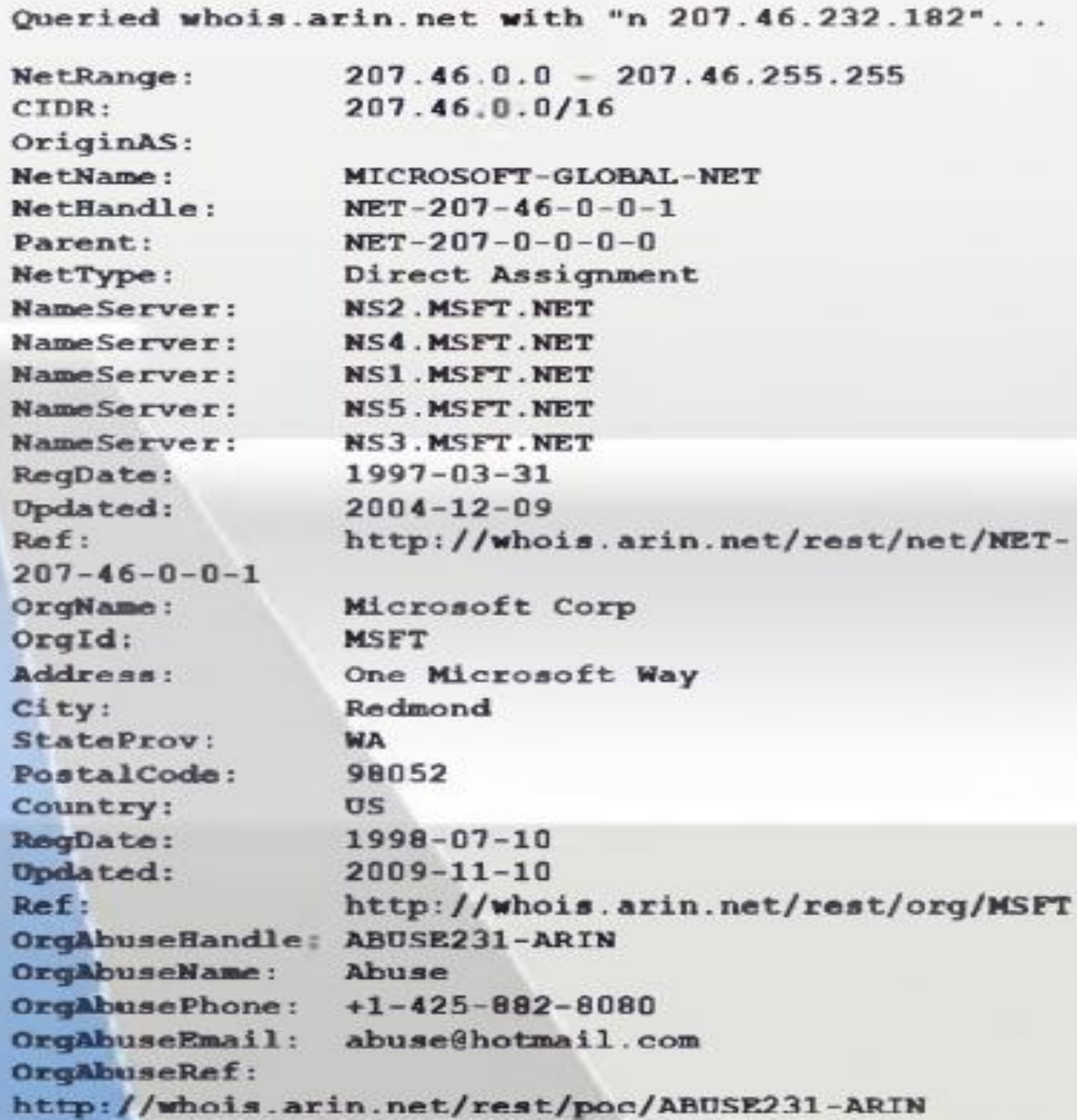
- ✓ WHOIS Footprinting
- ✓ DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Locate the Network Range

- Network range information obtained assists an attacker to create a **map of the target's network**
- Find the **range of IP addresses** using **ARIN whois database search** tool
- You can find the range of IP addresses and the subnet mask used by the target organization from **Regional Internet Registry (RIR)**



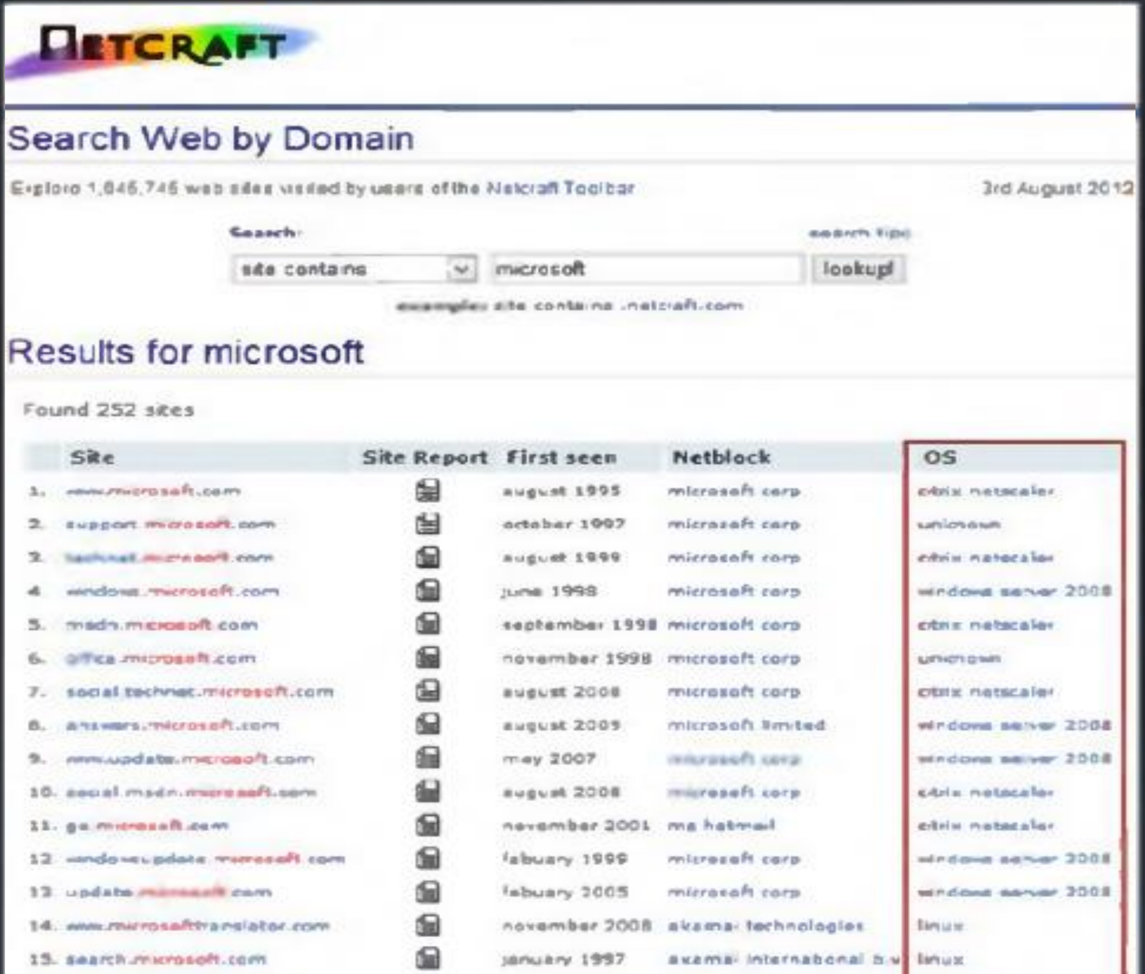
Network Whois Record



```
Queried whois.arin.net with "n 207.46.232.182"...

NetRange:          207.46.0.0 - 207.46.255.255
CIDR:              207.46.0.0/16
OriginAS:
NetName:           MICROSOFT-GLOBAL-NET
NetHandle:         NET-207-46-0-0-1
Parent:            NET-207-0-0-0-0
NetType:           Direct Assignment
NameServer:        NS2.MSFT.NET
NameServer:        NS4.MSFT.NET
NameServer:        NS1.MSFT.NET
NameServer:        NS5.MSFT.NET
NameServer:        NS3.MSFT.NET
RegDate:           1997-03-31
Updated:           2004-12-09
Ref:               http://whois.arin.net/rest/net/NET-
207-46-0-0-1
OrgName:           Microsoft Corp
OrgId:             MSFT
Address:           One Microsoft Way
City:              Redmond
StateProv:         WA
PostalCode:        98052
Country:           US
RegDate:           1998-07-10
Updated:           2009-11-10
Ref:               http://whois.arin.net/rest/org/MSFT
OrgAbuseHandle:    ABUSE231-ARIN
OrgAbuseName:      Abuse
OrgAbusePhone:     +1-425-882-8080
OrgAbuseEmail:     abuse@hotmail.com
OrgAbuseRef:
http://whois.arin.net/rest/poc/ABUSE231-ARIN
```

Determine the Operating System

Use the Netcraft tool to determine the OSes in use by the target organization



Search Web by Domain

Explore 1,645,745 web sites visited by users of the Netcraft Toolbar 3rd August 2012

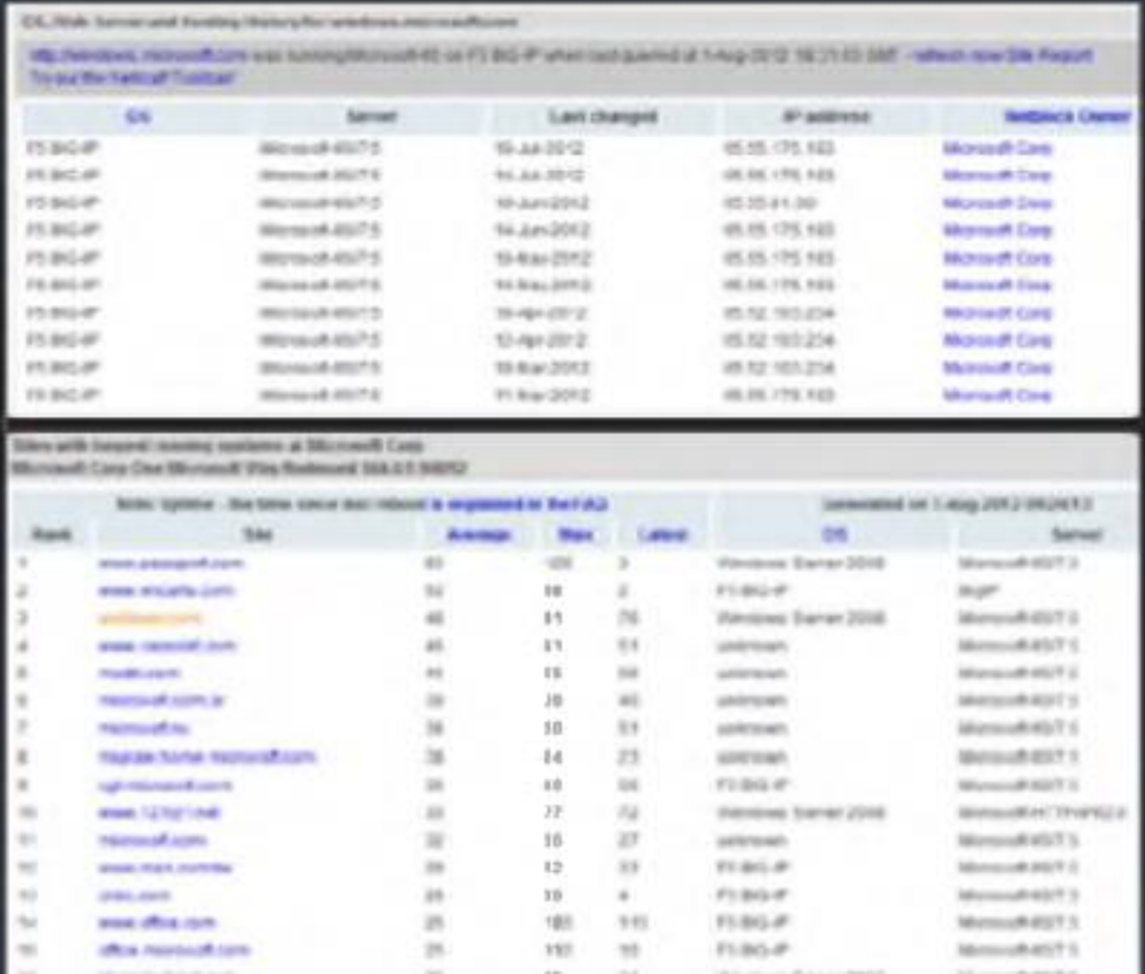
Search: site contains microsoft lookup! search tips

example: site contains .netcraft.com

Results for microsoft

Found 252 sites

	Site	Site Report	First seen	Netblock	OS
1.	www.microsoft.com		august 1995	microsoft corp	citrix netscaler
2.	support.microsoft.com		october 1997	microsoft corp	unknown
3.	technet.microsoft.com		august 1999	microsoft corp	citrix netscaler
4.	windows.microsoft.com		june 1998	microsoft corp	windows server 2008
5.	msdn.microsoft.com		september 1998	microsoft corp	citrix netscaler
6.	office.microsoft.com		november 1998	microsoft corp	unknown
7.	social.technet.microsoft.com		august 2008	microsoft corp	citrix netscaler
8.	answers.microsoft.com		august 2009	microsoft limited	windows server 2008
9.	www.update.microsoft.com		may 2007	microsoft corp	windows server 2008
10.	social.msdn.microsoft.com		august 2008	microsoft corp	citrix netscaler
11.	go.microsoft.com		november 2001	ms hotmail	citrix netscaler
12.	windowsupdate.microsoft.com		febuary 1999	microsoft corp	windows server 2008
13.	update.microsoft.com		febuary 2005	microsoft corp	windows server 2008
14.	www.microsofttranslator.com		november 2008	akamai technologies	linux
15.	search.microsoft.com		january 1997	akamai international b.v.	linux



OS, Web Server and Hosting History for windows.microsoft.com

http://windows.microsoft.com was running Microsoft-IIS on F5 BIG-IP when last queried at 1-Aug-2012 [illegible] GMT - refresh now Site Report

Try out the Netcraft Toolbar!

OS	Server	Last changed	IP address	Netblock Owner
F5 BIG-IP	Microsoft-IIS/7.5	19-Jul-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	14-Jul-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	19-Jun-2012	65.55.41.30	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	14-Jun-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	19-May-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	14-May-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	19-Apr-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	12-Apr-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	19-Mar-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	11-Mar-2012	65.55.175.183	Microsoft Corp

Sites with longest running systems at Microsoft Corp

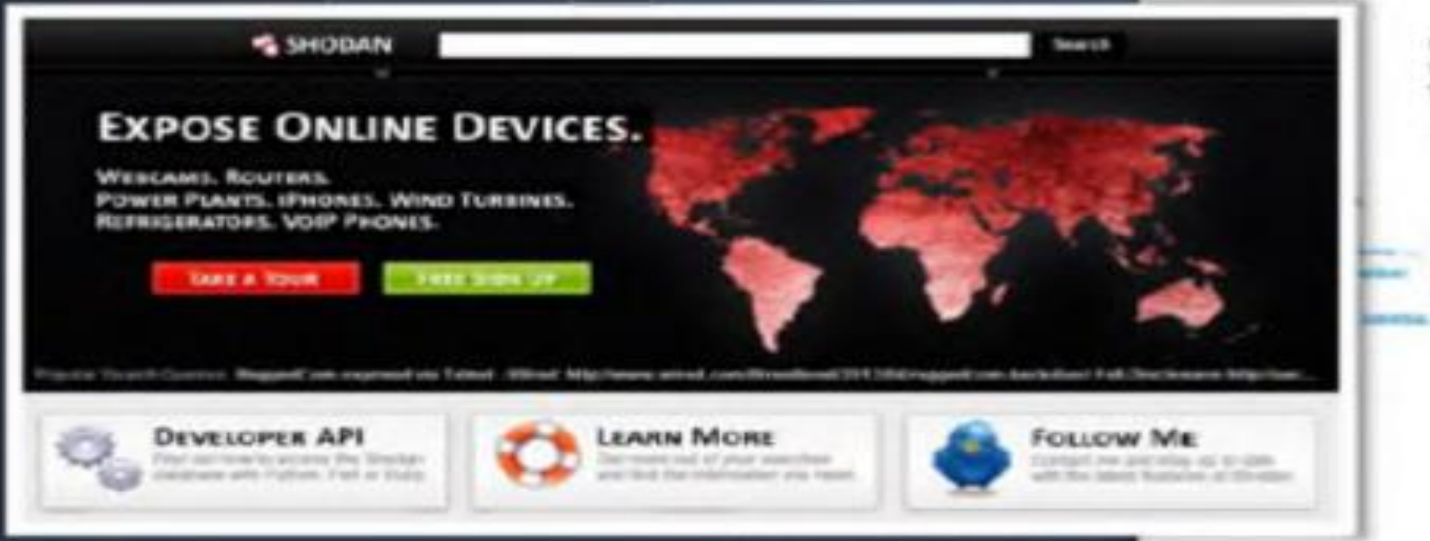
Microsoft Corp One Microsoft Way Redmond WA US 98052

Note: Uptime - the time since last reboot is explained in the FAQ generated on 1-Aug-2012 [illegible]

Rank	Site	Average	Max	Latest	OS	Server
1	www.passport.com	63	109	3	Windows Server 2008	Microsoft-IIS/7.5
2	www.encarta.com	52	18	2	F5 BIG-IP	BigIP
3	[illegible]	46	81	76	Windows Server 2008	Microsoft-IIS/7.5
4	www.[illegible].com	45	81	51	unknown	Microsoft-IIS/7.5
5	msdn.com	41	15	59	unknown	Microsoft-IIS/7.5
6	microsoft.com.[illegible]	39	18	40	unknown	Microsoft-IIS/7.5
7	microsoft.ru	38	10	51	unknown	Microsoft-IIS/7.5
8	[illegible].microsoft.com	38	14	23	unknown	Microsoft-IIS/7.5
9	[illegible].microsoft.com	35	10	56	F5 BIG-IP	Microsoft-IIS/7.5
10	www.[illegible]	33	77	72	Windows Server 2008	Microsoft-HTTPAPI/2.0
11	microsoft.com	32	16	27	unknown	Microsoft-IIS/7.5
12	www.msn.com.[illegible]	30	12	33	F5 BIG-IP	Microsoft-IIS/7.5
13	[illegible].com	29	10	4	F5 BIG-IP	Microsoft-IIS/7.5
14	www.office.com	25	185	115	F5 BIG-IP	Microsoft-IIS/7.5
15	office.microsoft.com	25	110	55	F5 BIG-IP	Microsoft-IIS/7.5

Determine the Operating System (Cont'd)

Use SHODAN search engine that lets you **find specific computers** (routers, servers, etc.) using a variety of filters



SHODAN [illegible] Search

EXPOSE ONLINE DEVICES.

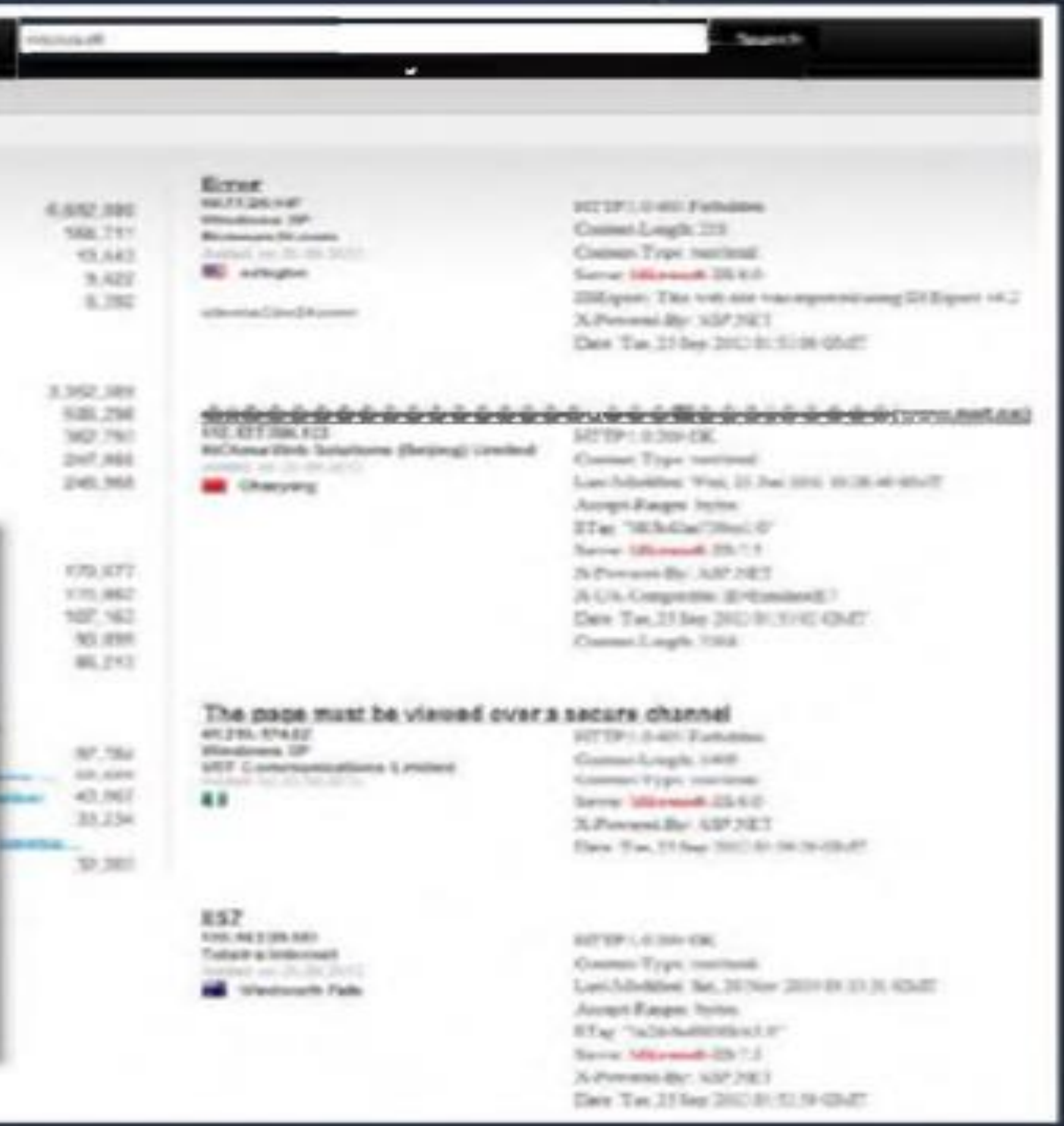
WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

TAKE A TOUR FREE SIGN UP

DEVELOPER API

LEARN MORE

FOLLOW ME



SHODAN microsoft Search

Services

HTTP
HTTP Alternate
FTP
SNMP
UPnP

Top Countries

United States
China
United Kingdom
Germany
Canada

Error

Windows XP

HTTP/1.0 403 Forbidden
Content-Length: [illegible]
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 [illegible] GMT

HTTP/1.0 200 OK
Content-Type: text/html
Last-Modified: [illegible]
Accept-Ranges: bytes
ETag: [illegible]
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 [illegible] GMT
Content-Length: [illegible]

The page must be viewed over a secure channel

Windows XP

HTTP/1.0 403 Forbidden
Content-Length: [illegible]
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 [illegible] GMT

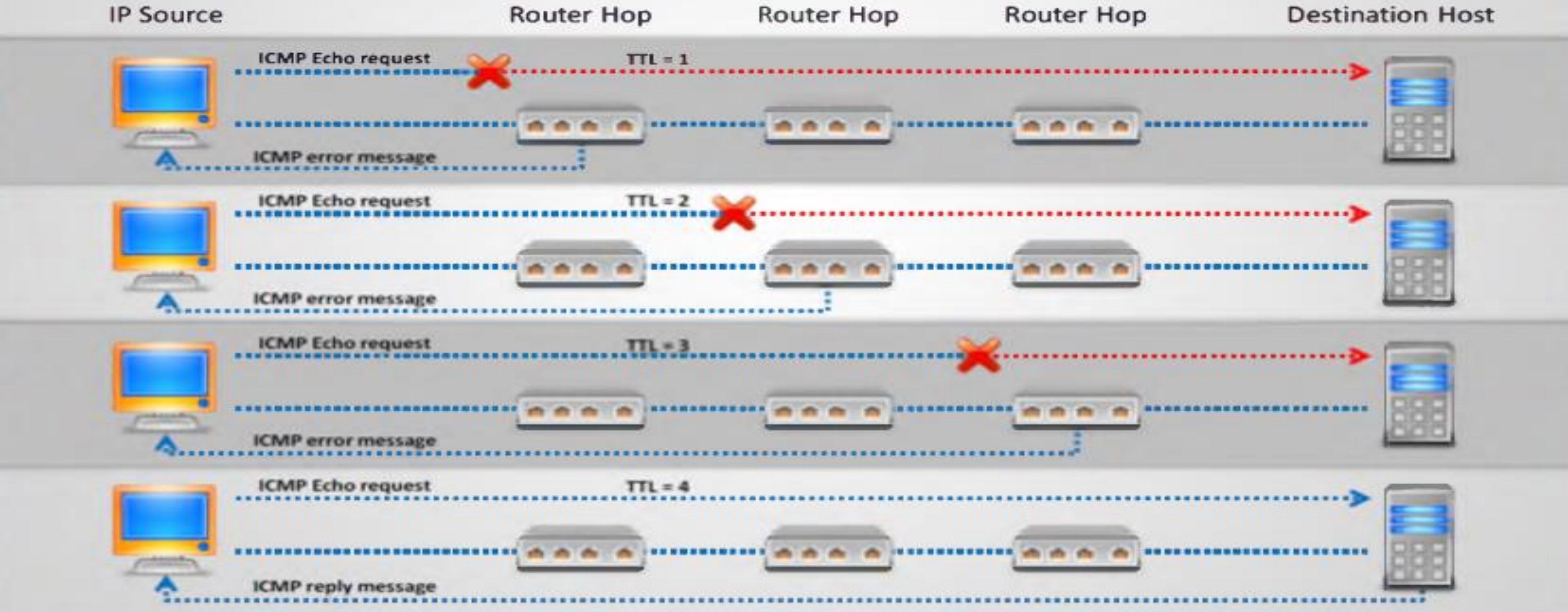
IIS7

HTTP/1.0 200 OK
Content-Type: text/html
Last-Modified: [illegible]
Accept-Ranges: bytes
ETag: [illegible]
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 [illegible] GMT

http://www.shodanhq.com

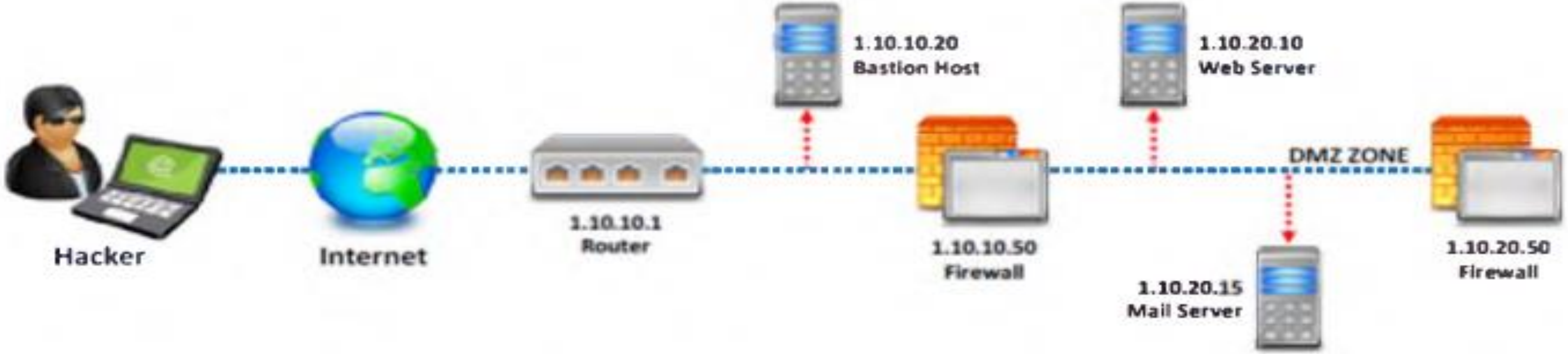
Traceroute

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



Traceroute Analysis

- Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations
- 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 putting this information together, attackers can draw the network diagram



Traceroute Tools

Path Analyzer Pro

http://www.pathanalyzer.com

VisualRoute 2010

http://www.visualroute.com

Traceroute Tools
(Cont'd)

Network Pinger
http://www.networkpinger.com

GEOSpider
http://www.oreware.com

vTrace
http://vtrace.pl

Trout
http://www.mcafee.com

Roadkil's Trace Route
http://www.roadkil.net

Magic NetTrace
http://www.tialsoft.com

3D Traceroute
http://www.d3tr.de

AnalogX HyperTrace
http://www.analogx.com

Network Systems Traceroute
http://www.net.princeton.edu

Ping Plotter
http://www.pingplotter.com

Footprinting Methodology

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- ✓ Footprinting using Google

- ✓ WHOIS Footprinting
- ✓ DNS Footprinting
- ✓ Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting through Social Engineering

- Social engineering is the art of **convincing people to reveal 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
- User names and passwords
- Other personal information
- Security products in use
- Operating systems and software versions
- Network layout information
- IP addresses and names of servers

Social engineers use these techniques:

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation on social networking sites

Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

Eavesdropping

- Eavesdropping is unauthorized listening of conversations or reading of messages
- It is interception of any form of communication such as audio, video, or written

1

Shoulder Surfing

- Shoulder surfing is the procedure where the attackers look over the user's shoulder to gain critical information
- Attackers gather information such as passwords, personal identification number, account numbers, credit card information, etc.

2

Dumpster Diving

- Dumpster diving is looking for treasure in someone else's trash
- It involves 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.

3

Footprinting Methodology

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- ✓ Footprinting using Google

- ✓ WHOIS Footprinting
- ✓ DNS Footprinting
- ✓ Network Footprinting
- ✓ Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Collect Information through Social Engineering on Social Networking Sites

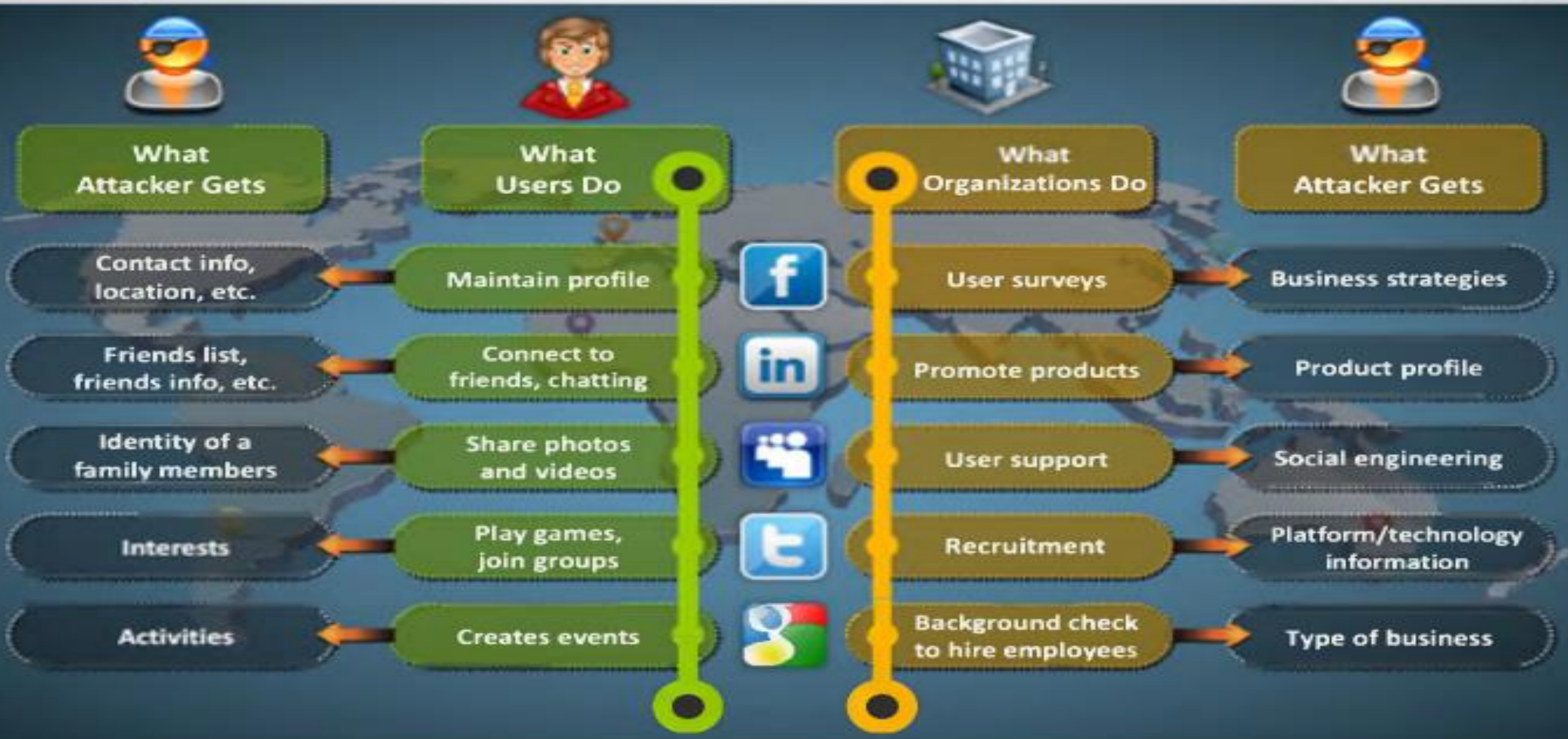
Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

Attackers create a fake profile on social networking sites and then use the false identity to lure the employees to give up their sensitive information

Employees may post personal information such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.

Using the details of an employee of the target organization, an attacker can compromise a secured facility

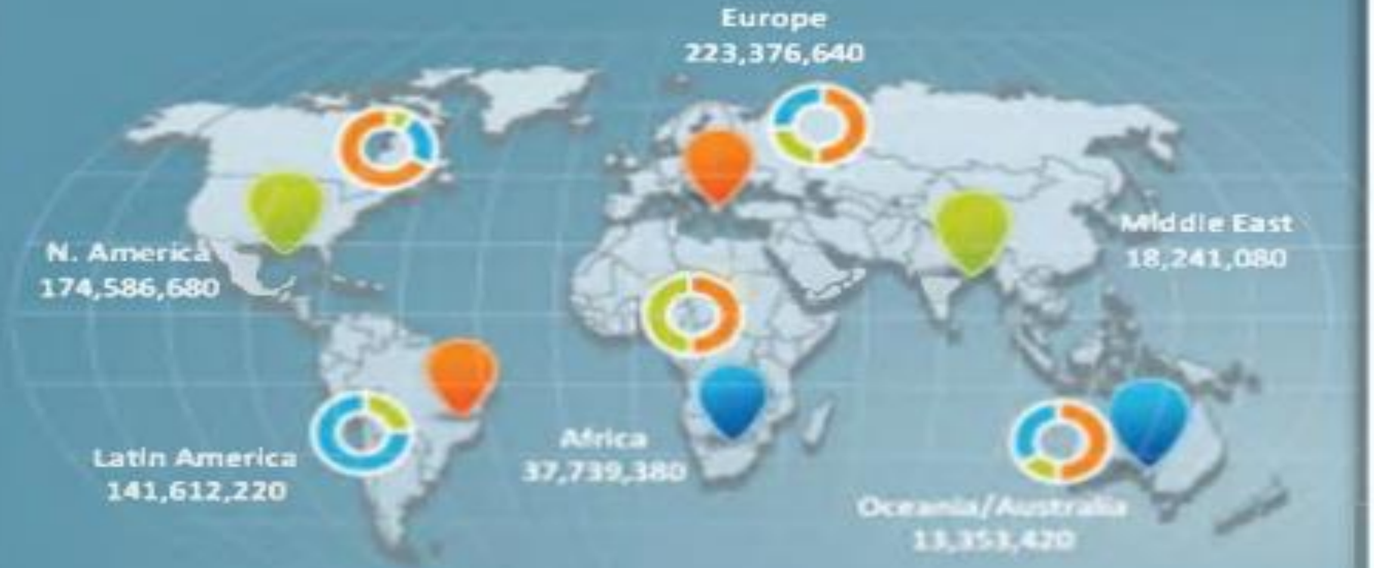
Information Available on Social Networking Sites



What Attacker Gets	What Users Do	What Organizations Do	What Attacker Gets
Contact info, location, etc.	Maintain profile	User surveys	Business strategies
Friends list, friends info, etc.	Connect to friends, chatting	Promote products	Product profile
Identity of a family members	Share photos and videos	User support	Social engineering
Interests	Play games, join groups	Recruitment	Platform/technology information
Activities	Creates events	Background check to hire employees	Type of business

Collecting Facebook Information

Facebook is a Treasure-trove for Attackers



Number of users using Facebook all over the world

About

Basic Info

Contact Info

845 million monthly active users

100 billion connections

250 million photos uploaded daily

1/5 1 of every 5 of all page views

20 minutes time spent per visit

Collecting Twitter Information

U.K.
23.8 million
Japan
29.9 million
United States
107.7 million
Indonesia
19.5 million
Brazil
33.3 million

Top 5 Countries with largest Twitter users

465 million accounts

350 million tweets a day

76% Twitter users now post status updates

55% Twitter users access the platform via their mobile

Wayne Rooney
@WayneRooney
[illegible]

Tweet to Wayne Rooney

Tweets
Following
Followers
Favorites
Lists
Recent images

Tweets [illegible]

Paul McCartney [illegible]
Nearly time ... [illegible]
Retweeted by Wayne Rooney

Piers Morgan [illegible]
I still don't quite understand why the hell we have to hear everything in FRENCH first? Utterly ridiculous. [illegible]
Retweeted by Wayne Rooney

[illegible]
cant believe @TheRealMC3 is not part of this ceremony #NoRespect he done so much 4 the country [illegible] #Olympics
Retweeted by Wayne Rooney

Wayne Rooney @WayneRooney
Becks smile on the boat was so funny.

Karl Hyde™ [illegible]
[illegible]
Retweeted by Wayne Rooney

Ian Nicholls [illegible]
[illegible]
Retweeted by Wayne Rooney

Wayne Rooney [illegible]
[illegible] best band ever

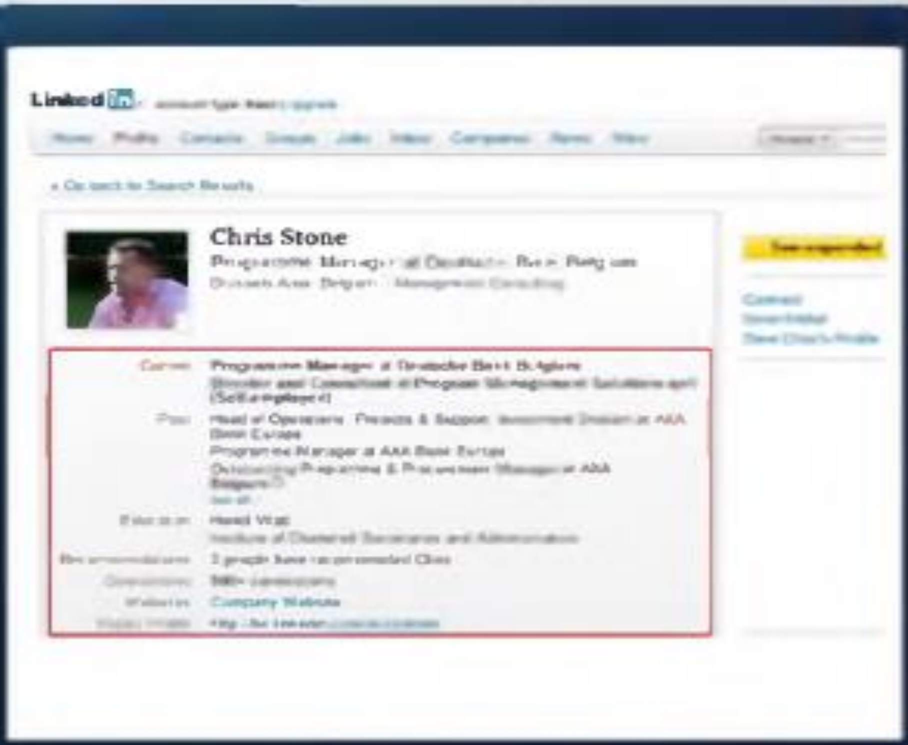
Wayne Rooney [illegible]
[illegible]

Wayne Rooney [illegible]
Great history of Britain already. [illegible] to any other ceremony I have seen before

Collecting Linkedin Information

161 million members in over 200 countries

2 million
6 million
4 million
4 million
57 million
4 million
2 million
in



Linked in
Home Profile Contacts Groups Jobs Inbox Companies News More
« Go back to Search Results

Chris Stone
Programme Manager at Deutsche Bank Belgium
Brussels Area, Belgium · Management Consulting

Current: Programme Manager at Deutsche Bank Belgium
Director and Consultant at Program Management Solutions sprl (Self-employed)

Past: Head of Operations, Projects & Support, Investment Division at AXA Bank Europe
Programme Manager at AXA Bank Europe
Outsourcing Programme & Procurement Manager at AXA Belgium
see all

Education: [illegible]
Institute of Chartered Secretaries and Administrators

Recommendations: 3 people have recommended Chris

Connections: 500+ connections

Websites: Company Website

Public Profile: http://be.linkedin.com/[illegible]

Connect
Send InMail
Save Chris's Profile

2 new members join every second

2,447 employees located around the world

$522 million revenue for 2011

2 million companies have LinkedIn company pages

Collecting Youtube Information

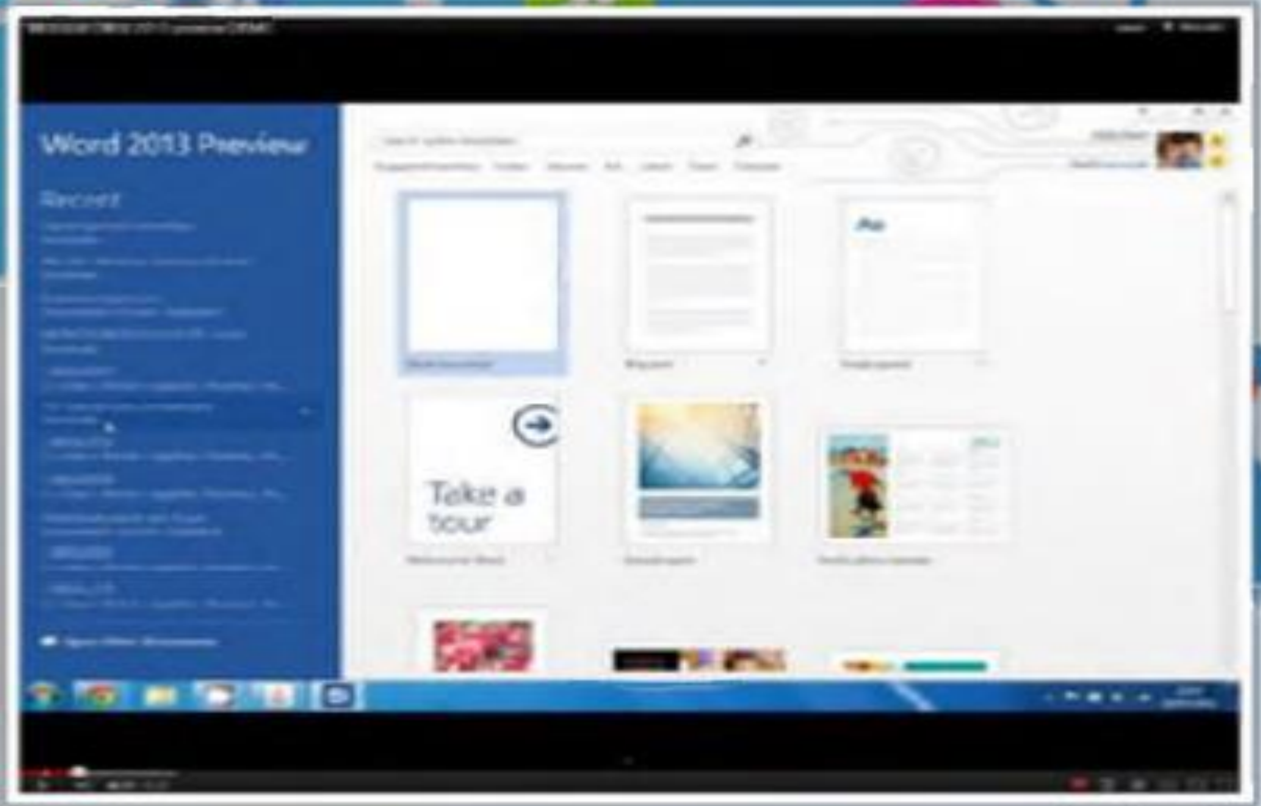
3rd | Most visited website according to Alexa

900 Sec | Average time users spend on YouTube every day

2 billion | Views per day

1/10 | One of every 10 Internet users opens YouTube

829,440 | Videos uploaded every day



Tracking Users on Social Networking Sites

- Users may use **fake identities** on social networking sites. Attackers use tools such as **Get Someones IP** or **IP-GRABBER** to track users' real identity
- Steps to get someone's IP address through chat on Facebook using **Get Someones IP** tool:
  - Go to ***http://www.myiptest.com/staticpages/index.php/how-about-you***
  - Three fields exist:

Link for Person

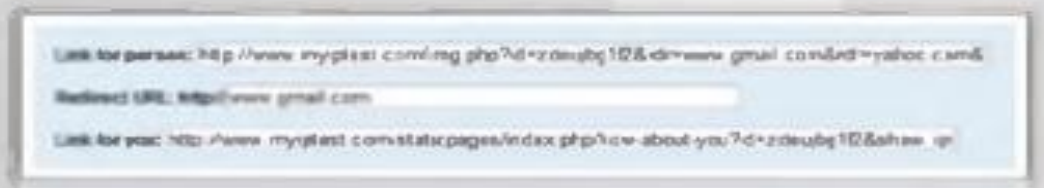
Copy the **generated link** of this field and send it to the target via **chat** to get IP address

Redirect URL

Enter any **URL** you want the target to redirect to

Link for you

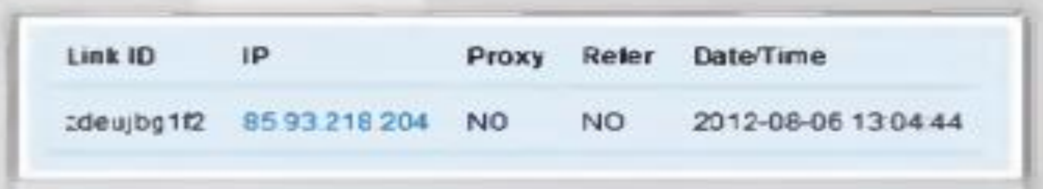
Open the URL in this field and keep checking for **target's IP**



Link for person: http://www.myiptest.com/img.php?id=zdeujbg1f2&dr=www.gmail.com&rd=yahoo.com&

Redirect URL: http://www.gmail.com

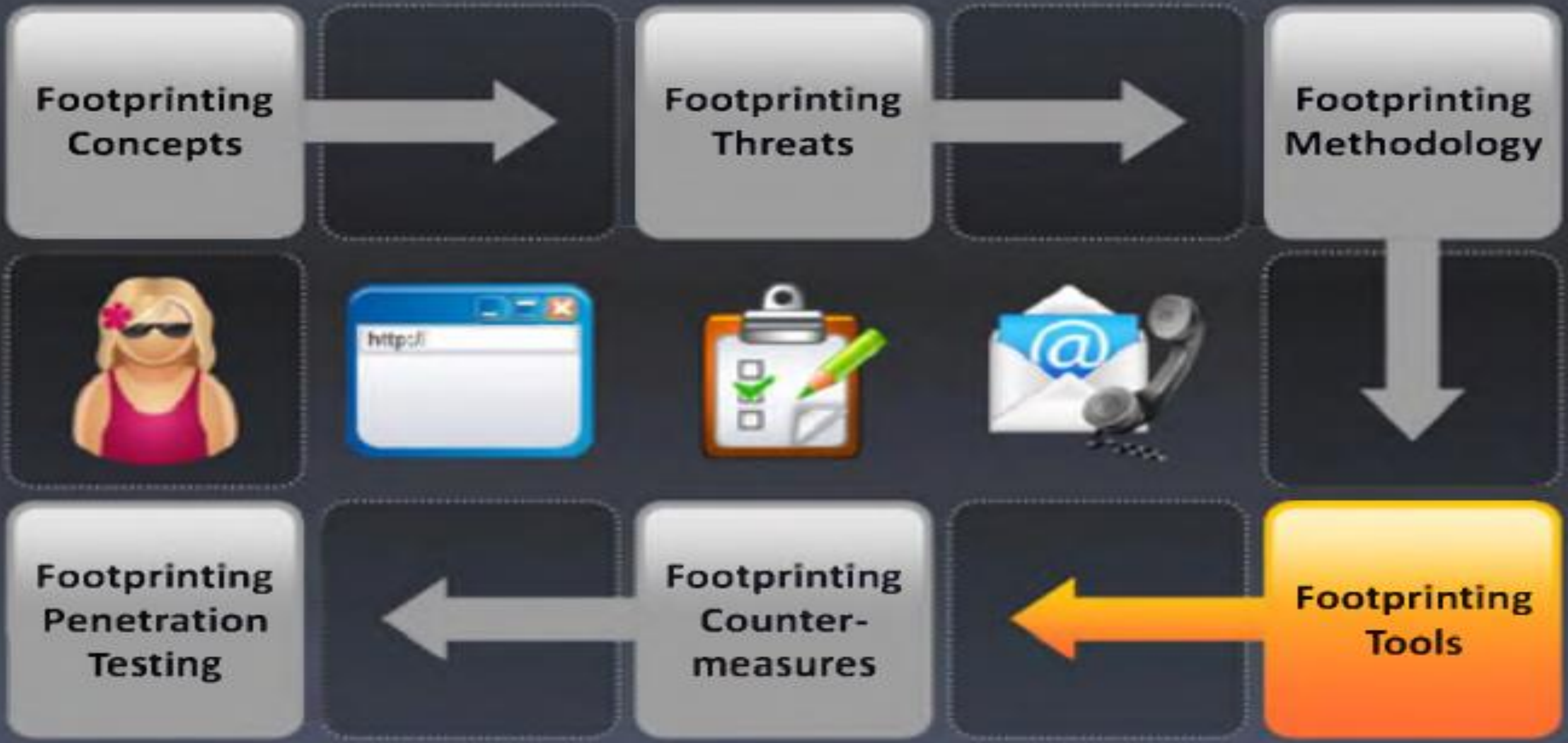
Link for you: http://www.myiptest.com/staticpages/index.php/how-about-you?id=zdeujbg1f2&show_ip



Link ID	IP	Proxy	Refer	Date/Time
zdeujbg1f2	85.93.218.204	NO	NO	2012-08-06 13:04:44

http://www.myiptest.com

Module Flow



Footprinting Concepts

Footprinting Threats

Footprinting Methodology

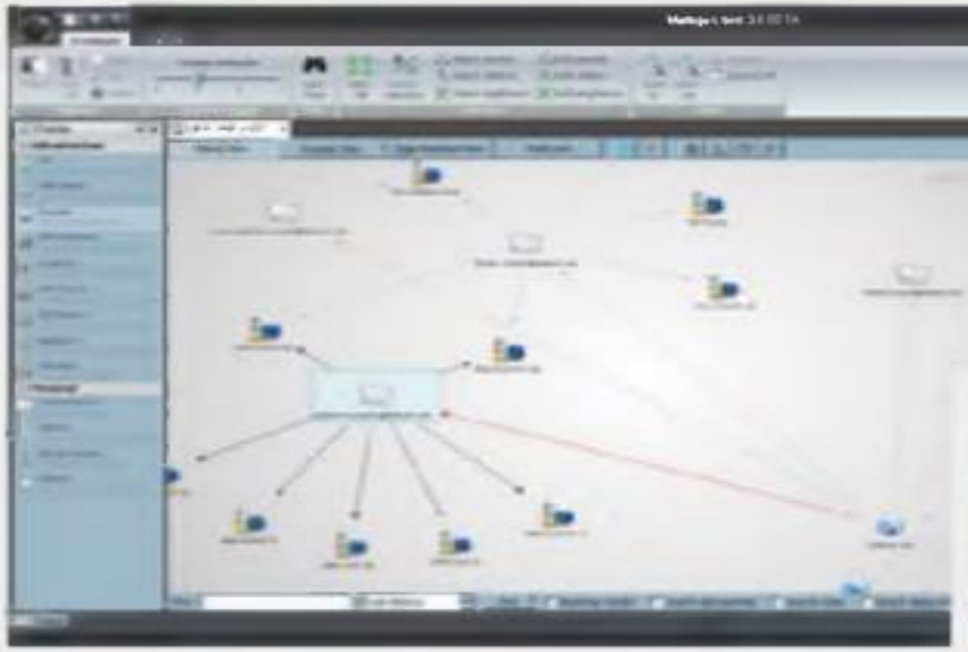
Footprinting Tools

Footprinting Counter-measures

Footprinting Penetration Testing

Footprinting Tool: Maltego

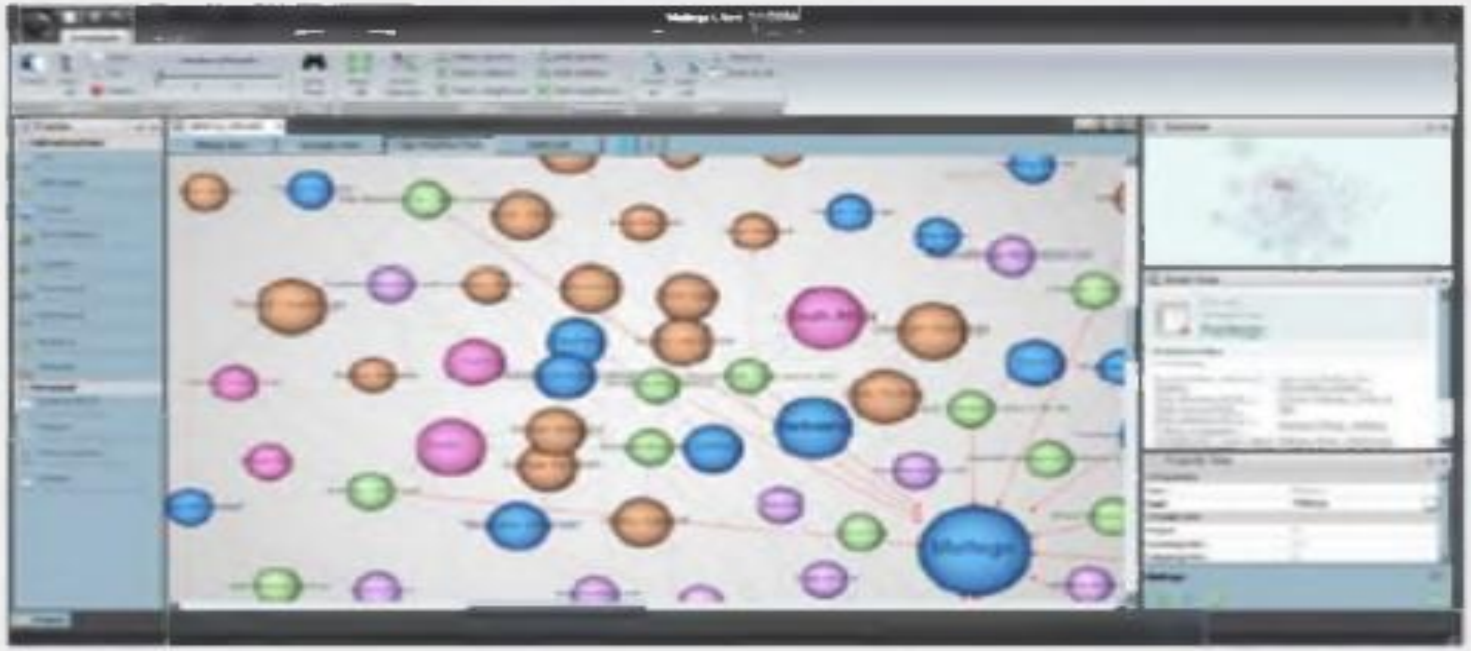
Maltego is a program that can be used to determine the **relationships and real world links** between people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files



Internet Domain

http://www.paterva.com

MALTEGO



Personal Information

Additional Footprinting Tools

Prefix WhoIs
http://pwhois.org

NetScanTools Pro
http://www.netscantools.com

Tctrace
http://www.phenoelit-us.org

Autonomous System Scanner (ASS)
http://www.phenoelit-us.org

DNS DIGGER
http://www.dnsdigger.com

Netmask
http://www.phenoelit-us.org

BingIng
http://www.blueinfy.com

Spiderzilla
http://spiderzilla.mozdev.org

Sam Spade
http://www.majorgeeks.com

Robtex
http://www.robtex.com

Additional Footprinting Tools (Cont'd)

Dig Web Interface
http://www.digwebinterface.com

Domain Research Tool
http://www.domainresearchtool.com

ActiveWhois
http://www.johnru.com

yoName
http://yoname.com

Ping-Probe
http://www.ping-probe.com

SpiderFoot
http://www.binarypool.com

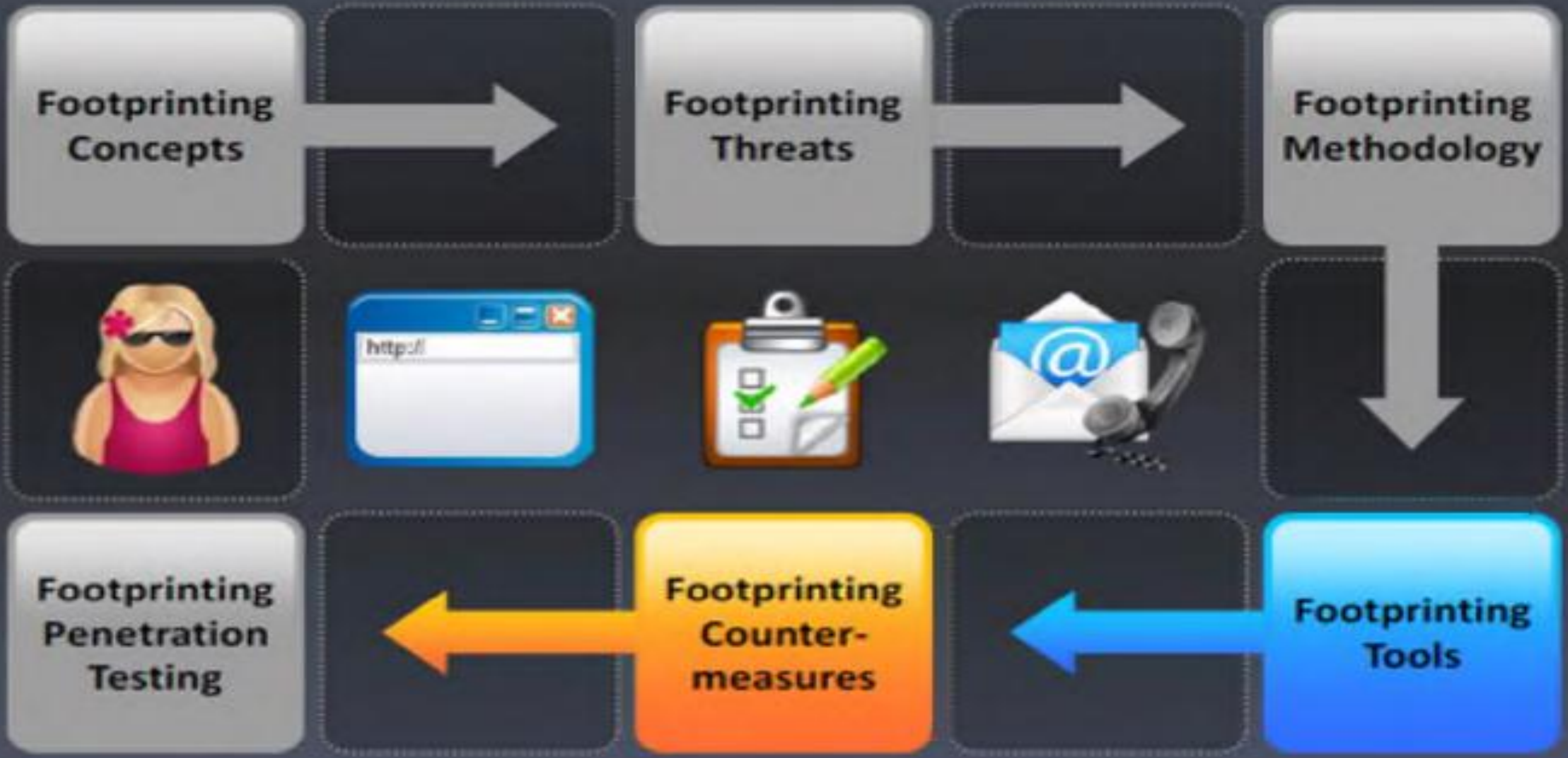
CallerIP
http://www.callerippro.com

Zaba Search
http://www.zabasearch.com

GeoTrace
http://www.nabber.org

DomainHostingView
http://www.nirsoft.net

Module Flow



Footprinting Concepts

Footprinting Threats

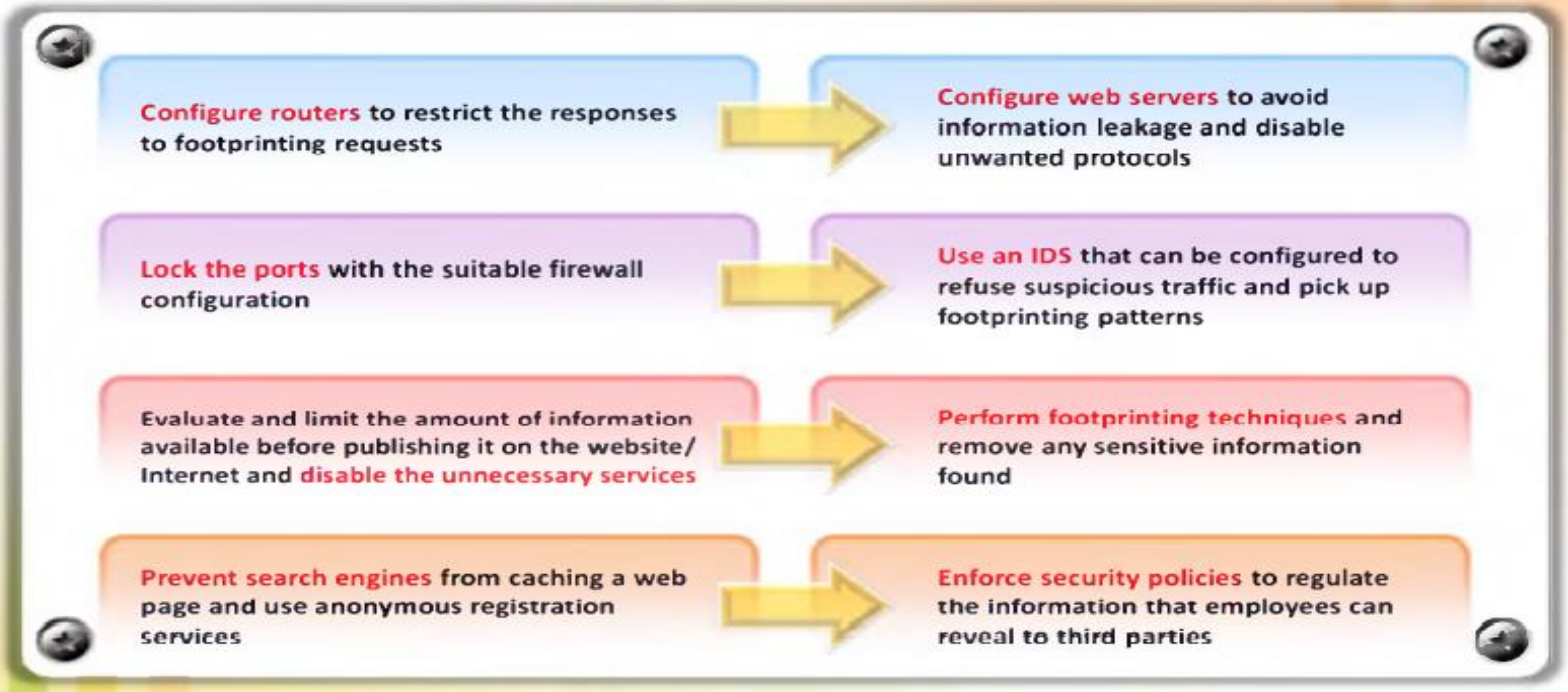
Footprinting Methodology

Footprinting Tools

Footprinting Counter-measures

Footprinting Penetration Testing

Footprinting Countermeasures



Configure routers to restrict the responses to footprinting requests

Configure web servers to avoid information leakage and disable unwanted protocols

Lock the ports with the suitable firewall configuration

Use an IDS that can be configured to refuse suspicious traffic and pick up footprinting patterns

Evaluate and limit the amount of information available before publishing it on the website/ Internet and disable the unnecessary services

Perform footprinting techniques and remove any sensitive information found

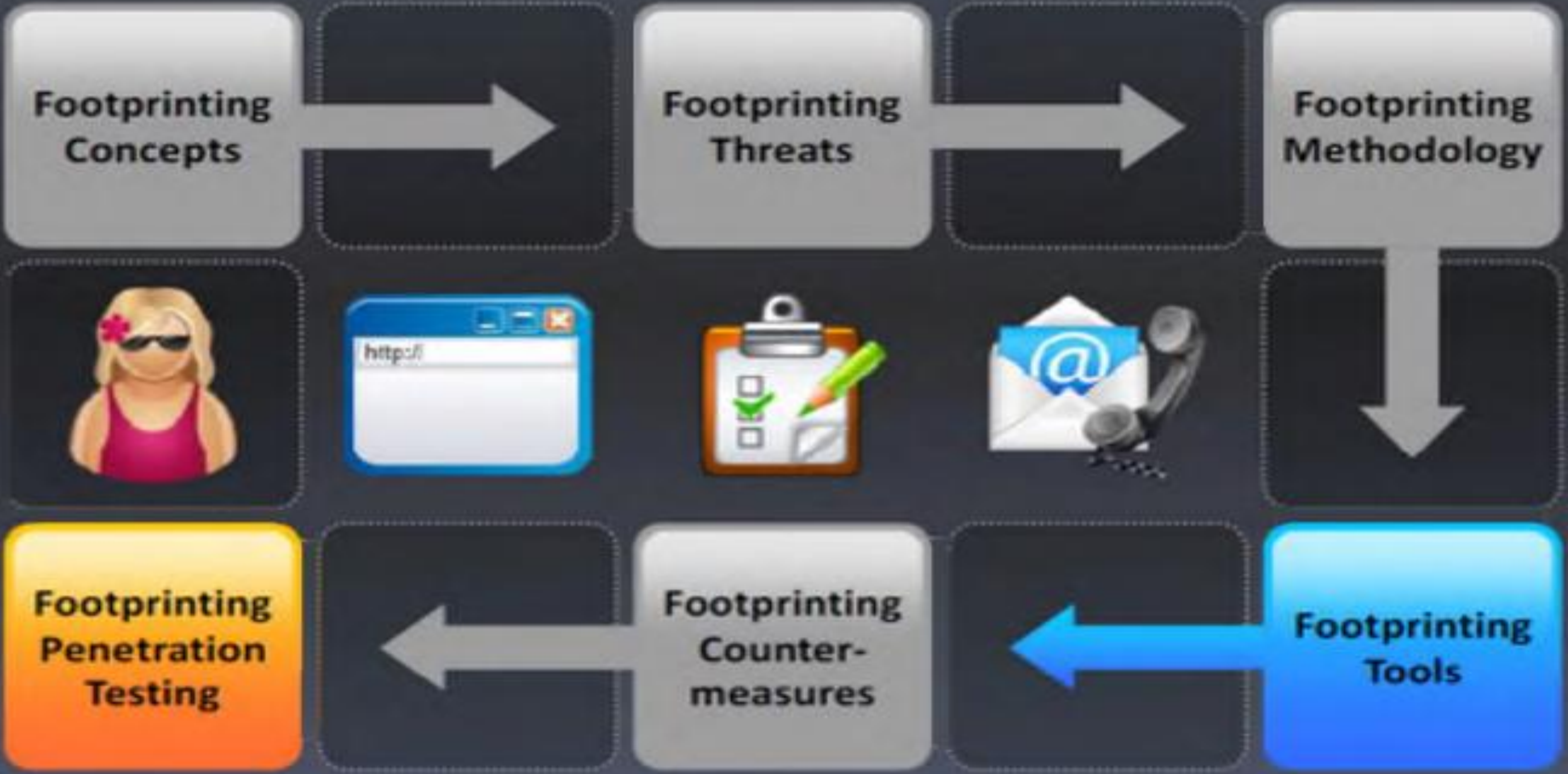
Prevent search engines from caching a web page and use anonymous registration services

Enforce security policies to regulate the information that employees can reveal to third parties

Footprinting Countermeasures (Cont'd)

- ✓ Set apart internal DNS and external DNS
- ✓ Disable directory listings and use split-DNS
- ✓ Educate employees about various social engineering tricks and risks
- ✓ Restrict unexpected input such as |; < >
- ✓ Avoid domain-level cross-linking for the critical assets
- ✓ Encrypt and password protect the sensitive information

Module Flow



Footprinting Concepts

Footprinting Threats

Footprinting Methodology

Footprinting Tools

Footprinting Counter-measures

Footprinting Penetration Testing

Footprinting Pen Testing

- Footprinting pen test is used to determine **organization's publicly available information on the Internet** such as network architecture, operating systems, applications, and users
- The tester attempts to gather as much information as possible about the target organization from the **Internet and other publicly accessible sources**

Footprinting pen testing helps administrator to:

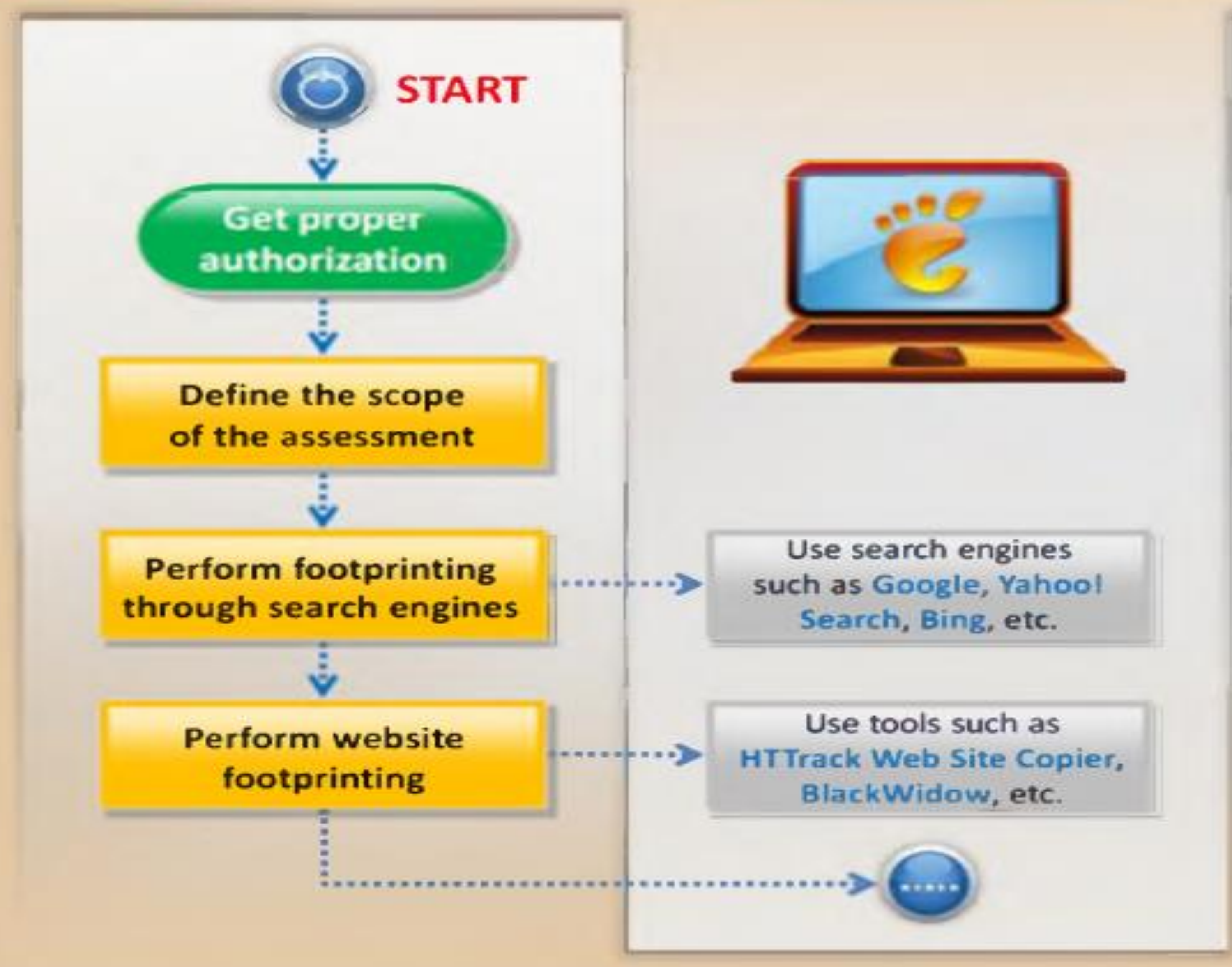
Prevent **information leakage**

Prevent **social engineering attempts**

Prevent **DNS record retrieval** from publically available servers

Footprinting Pen Testing

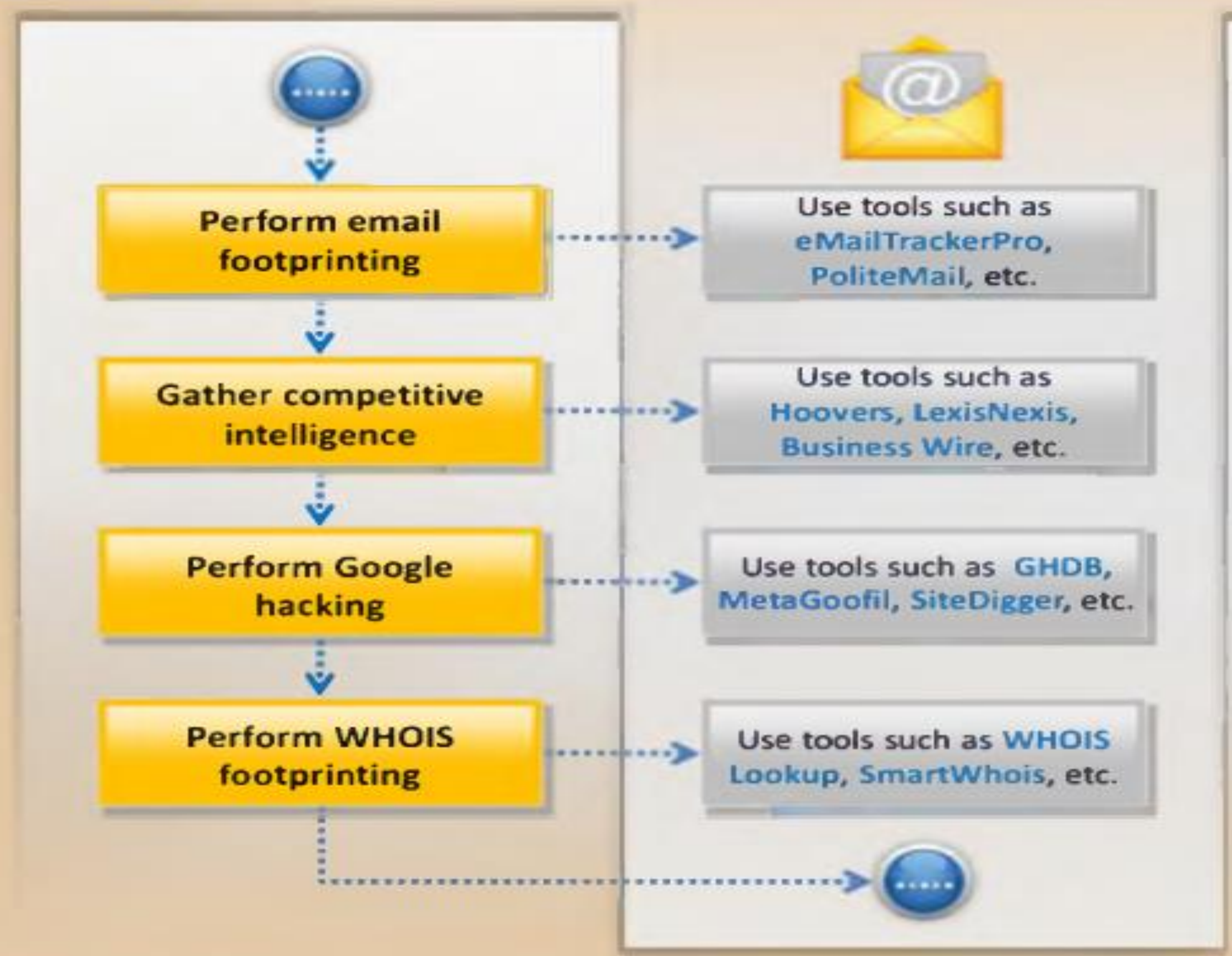
(Cont'd)


START
Get proper authorization
Define the scope of the assessment
Perform footprinting through search engines
Use search engines such as Google, Yahoo! Search, Bing, etc.
Perform website footprinting
Use tools such as HTTrack Web Site Copier, BlackWidow, etc.

- Get proper authorization and define the scope of the assessment
- Footprint search engines such as Google, Yahoo! Search, Ask, Bing, Dogpile, etc. to gather target organization's information such as employee details, login pages, intranet portals, etc. that helps in performing social engineering and other types of advanced system attacks
- Perform website footprinting using tools such as HTTrack Web Site Copier, BlackWidow, Webripper, etc. to build a detailed map of website's structure and architecture

Footprinting Pen Testing

(Cont'd)



Perform email footprinting

Use tools such as eMailTrackerPro, PoliteMail, etc.

Gather competitive intelligence

Use tools such as Hoovers, LexisNexis, Business Wire, etc.

Perform Google hacking

Use tools such as GHDB, MetaGoofil, SiteDigger, etc.

Perform WHOIS footprinting

Use tools such as WHOIS Lookup, SmartWhois, etc.

- Perform email footprinting using tools such as eMailTrackerPro, PoliteMail, Email Lookup – Free Email Tracker, etc. to gather information about the physical location of an individual to perform social engineering that in turn may help in mapping target organization's network
- Gather competitive intelligence using tools such as Hoovers, LexisNexis, Business Wire, etc.
- Perform Google hacking using tools such as GHDB, MetaGoofil, SiteDigger, etc.
- Perform WHOIS footprinting using tools such as WHOIS Lookup, SmartWhois, etc. to create detailed map of organizational network, to gather personal information that assists to perform social engineering, and to gather other internal network details, etc.

Module Summary

- □ Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system
- □ It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.
- □ Attackers use search engines to extract information about a target
- □ Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture
- □ Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet
- □ DNS records provide important information about location and type of servers
- □ Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations
- □ Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.