

# Footprinting

## Chapter 4



# Losing Control of Information

- Business loss
- Information leakage
- Privacy loss
- Corporate espionage



# What Is Footprinting?

The process of researching and uncovering details about your target will take some time to complete, but the time will be well spent if it helps you refine your actions later to make them more effective.

Process of researching a target carefully and looking for useful information

Uncovering detailed information

Looking for information that may be useful during later steps

Using publically available resources to gain information

Looking for carelessly or thoughtlessly shared information in places such as social networking sites



# What Types of Information to Look For?

- Technical sources such as network information, applications, IP address ranges, and device information
- Administrative information such as organizational structure, policies, hiring procedures, employee information, phone directories, and more
- Physical details such as location data, facility data, people details, and social interactions



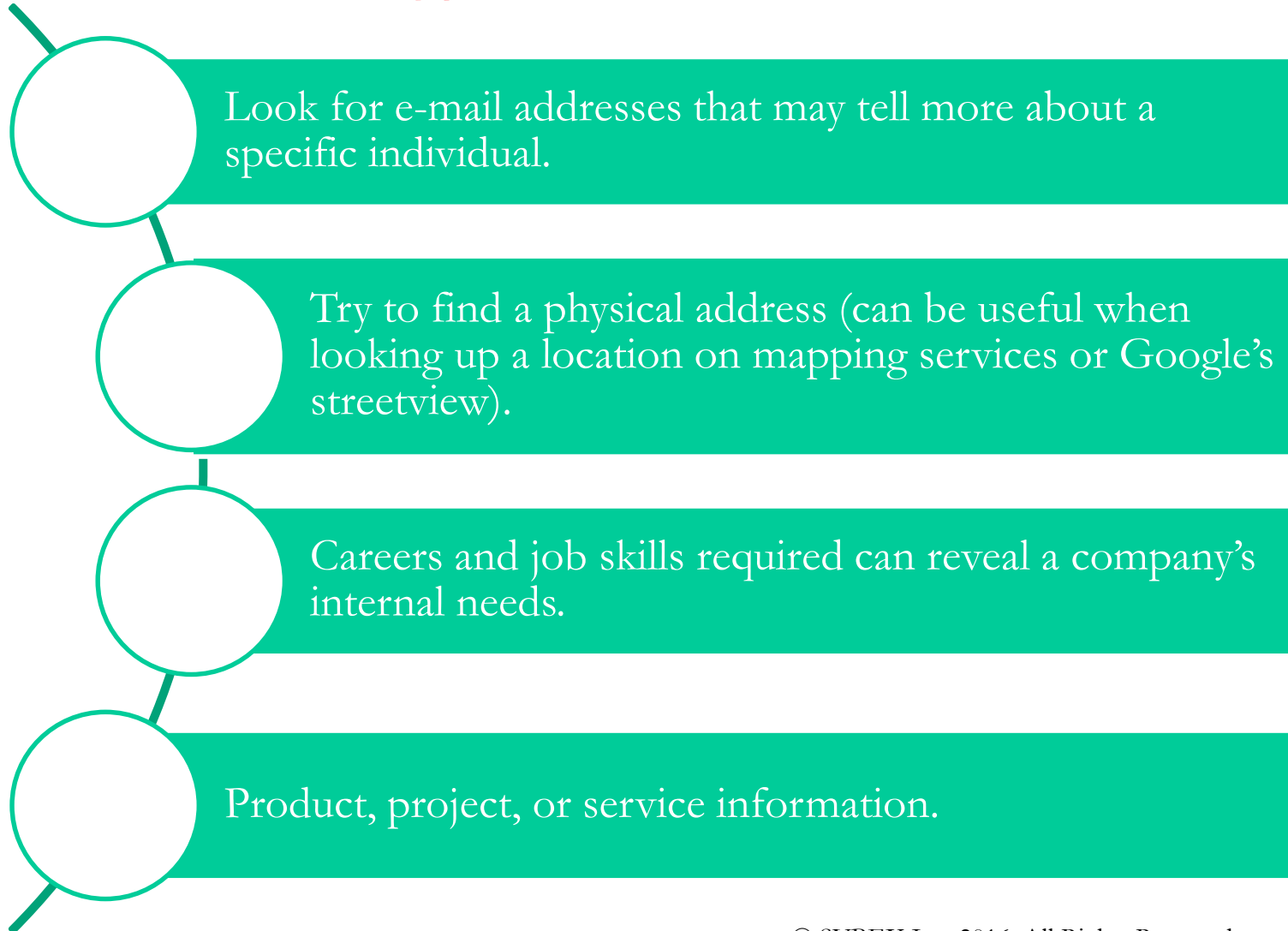
# How to Gather Information

Passive methods are those that do not interact with the target.

Active methods are those that directly engage the target such as using phone calls.

Open source intelligence (OSINT) consists of those sources such as newspapers, websites, press releases, and other sources.

# Examining a Company's Website



# Examining a Website Offline

Downloading content to a local drive allows for a much closer and detailed examination of website content than may be possible when viewing the website online through a browser.

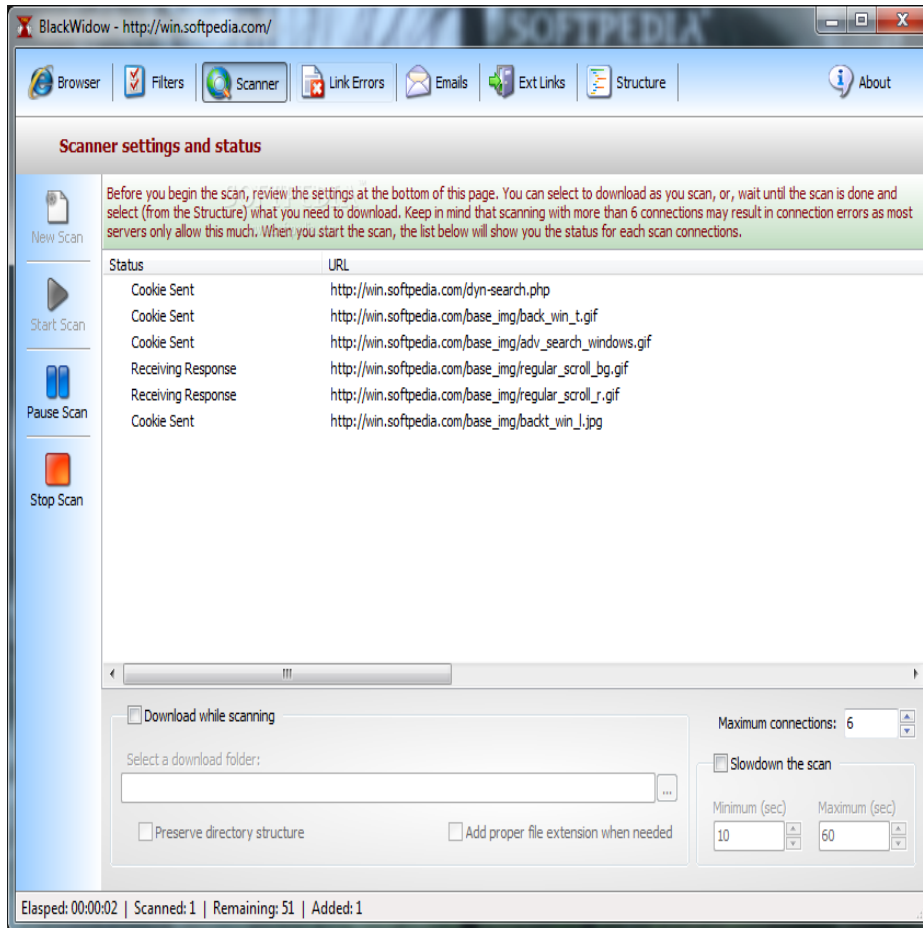
Examining a website can be made easier by copying it to a local drive.

Allows you to search the files and information within at your leisure.

Website downloaders are designed to perform this task.



# What Can BlackWidow Do?



- What can it download?
- Scriptable
- Network Spy
- Snapshot of web pages
- Scan filters
- Support for customizable scans



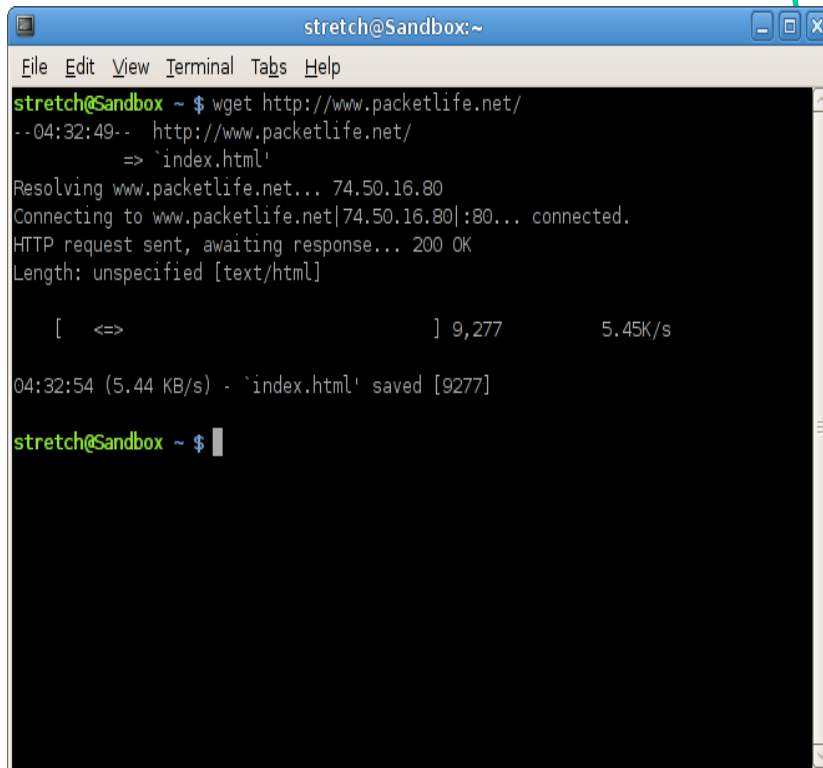
# Downloading Sites with Wget

Stands for Web Get

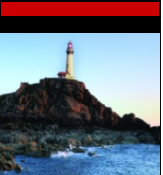
Is available on just about every major platform

Is noninteractive

Can work with slow or unreliable networks



```
stretch@Sandbox:~  
File Edit View Terminal Tabs Help  
stretch@Sandbox ~ $ wget http://www.packetlife.net/  
--04:32:49-- http://www.packetlife.net/  
=> 'index.html'  
Resolving www.packetlife.net... 74.50.16.80  
Connecting to www.packetlife.net[74.50.16.80]:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: unspecified [text/html]  
  
[ <=> ] 9,277 5.45K/s  
  
04:32:54 (5.44 KB/s) - 'index.html' saved [9277]  
stretch@Sandbox ~ $
```



# What Else to Learn from a Website

What about subdomains?

Try locating a child of a website such as `beta.microsoft.com`.

Subdomains are common but not always easily detectable

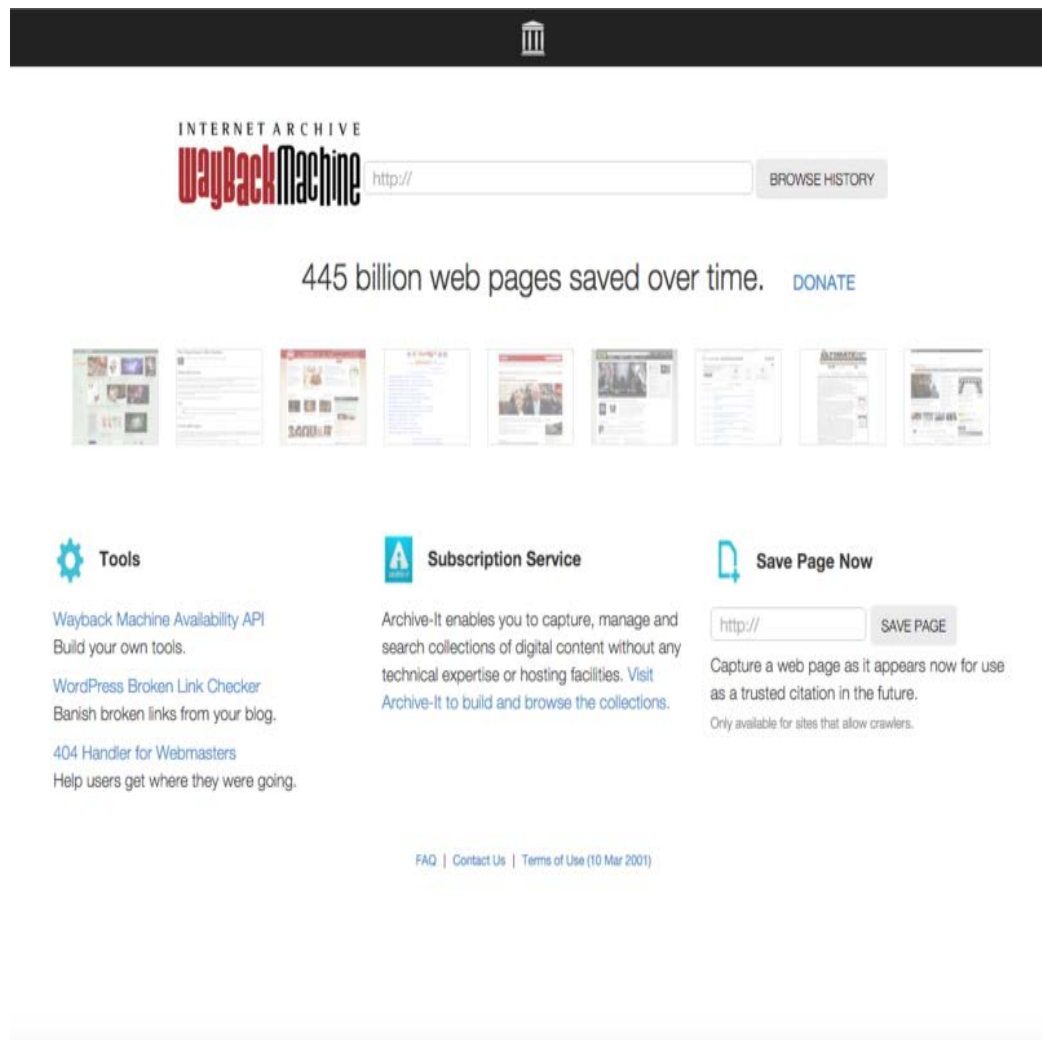
They can be used to hide content.

They can also be used to delegate control to parts of a company.

Subdomains are a division the main website name. For example, a subdomain of `Microsoft.com` would be `support.microsoft.com` or `beta.microsoft.com`.



# Finding Old Versions of Websites



- Sometimes an old and long since removed version of a website needs to be located.
- Using Archive.org these websites can be located.
- Archive.org features the Wayback Machine for viewing old sites.
- Can be useful in locating information that a company realized was a bad idea to publish and removed.

# What About Google?



Search engines provide quick access to information, but not all.

Search engines show only a small fraction of available information.

Additional information is available with extra effort.

Google hacking is used to retrieve this hidden information.



# Google Hacking Keywords

*cache* will display the version of a web page that Google contains in its cache.

- Usage: `cache:<website name>`

*link* is used to list any web pages that contain links to the page in the query.

- Usage: `link:<website name>`

*site* will restrict the search to the location specified.

- Usage: `<keyword> site:<website name>`

*allintitle* will return pages with specified keywords in their title.

- Usage: `allintitle:<keywords>`

*allinurl* will only return results with the specific query in the URL.

- Usage: `allinurl:<keywords>`



# Using Google Alerts

Alerts are a feature present in many search engines that notify you when something that fits your search criteria has been posted.

- **Google alerts are a customized automated search.**
- **They can be built to look for details that are useful.**
- **They can be used to keep an eye on a search while you work on other tasks.**
- **Up to 1,000 alerts can be assigned to an e-mail address.**



# Searching for People

Spokeo: [www.spokeo.com](http://www.spokeo.com)

Pipl: [www.pipl.com](http://www.pipl.com)

Yasni: [www.yasni.com](http://www.yasni.com)

Zabasearch: [www.zabasearch.com](http://www.zabasearch.com)

Intelius: [www.intelius.com](http://www.intelius.com)

ZoomInfo: [www.zoominfo.com](http://www.zoominfo.com)

Infospace: [www.infospace.com](http://www.infospace.com)

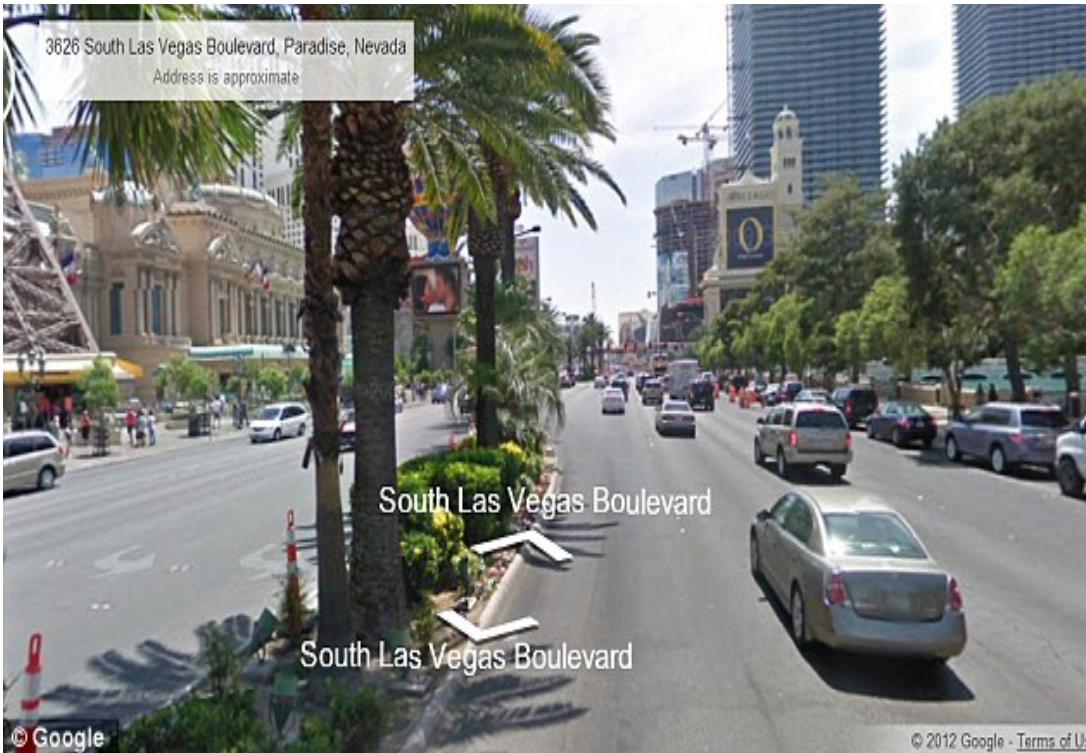
KGB: [www.kgbpeople.com](http://www.kgbpeople.com)

People: [www.peepdb.com](http://www.peepdb.com)

Radaris: [www.radaris.com](http://www.radaris.com)



# Determining Location



- **Google Earth**
- **Google Maps**
- **Google Streetview**
- **Webcams**





# Using Social Networking

Because of the nature of these services and their tendency to skew toward openness and ease of sharing information, an attacker does not have to put in a tremendous amount of work to learn useful details.

Useful tool for information gathering

Common to encounter over-sharing of information accidentally or deliberately

Easy to encounter information leakage

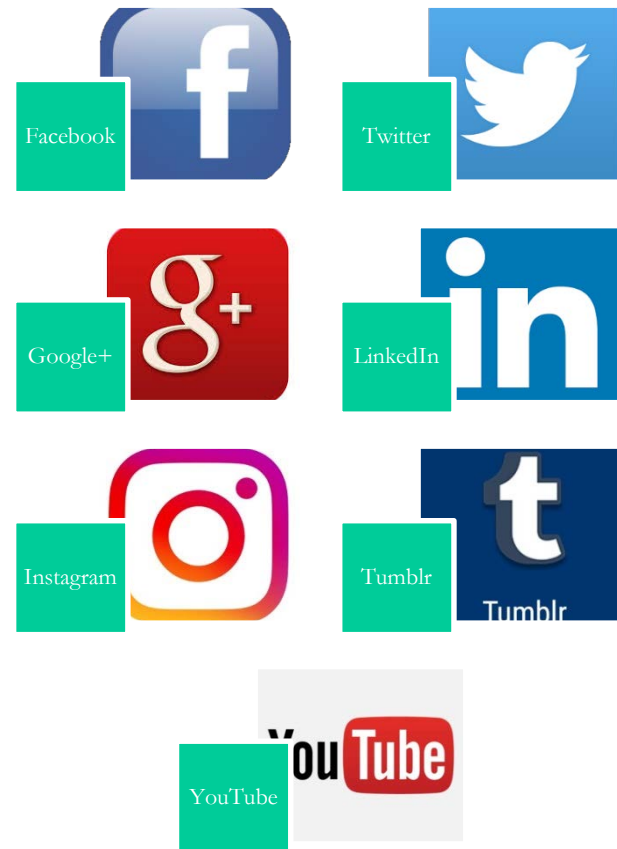
Drawback is openness of networks

Easy to collect information



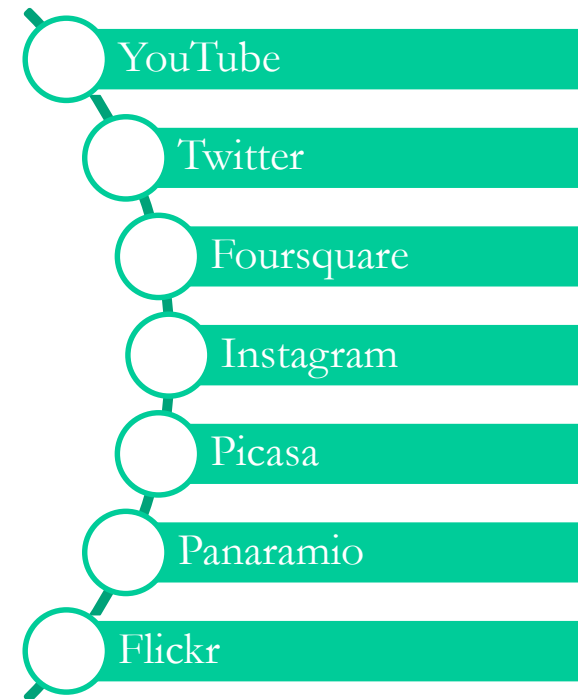
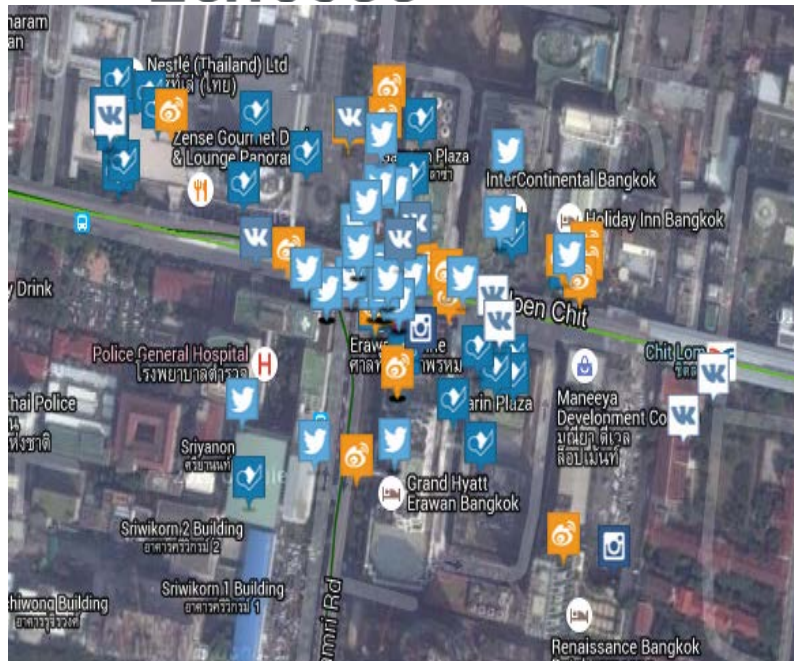
# Popular Social Networking Sites

There are several social networks you can use to search for information, each with its own built-in search function allowing you to read people's information. In addition, we also locate it based on geographic data.



# Using Echosec to Mine Social Networking

Services such as Facebook, Twitter, and Instagram can include information from the GPS included in your smartphone or use location services on your laptop or tablet to embed location data.



# Looking Up Financial Information

Services such as Yahoo, Google, CNBC, Usatoday, and countless others provide information about a company that may not be readily available through other means.



Financial data can reveal useful information about a company.

Public companies can be searched via stock symbol.

Competitors may also have useful information about the target.

Look for a company's partners.

Look up press releases.

Find office locations.



# Using Job Sites

If you have browsed job postings, you have undoubtedly noticed the myriad of forms these things take, but one of the common items is the skills and experience section.



Job requirements and experience

Employer profile

Employee profile

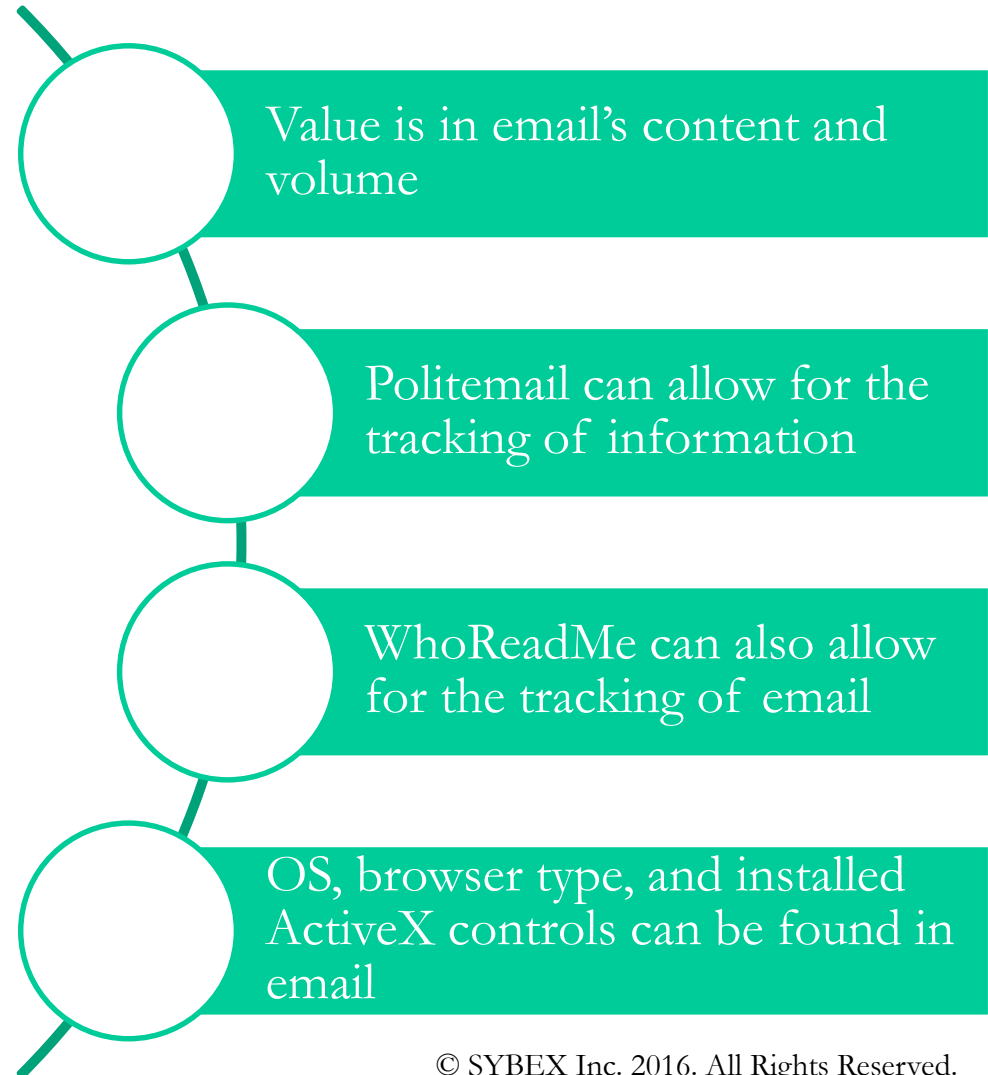
Hardware information

Software information



# Working with Email as an Information Source

For a malicious party and a pen tester, the information carried by this medium is staggering and is valuable to an attacker looking for information of all types.



# Using Whois

Whois is a utility designed to allow you to collect information about a domain name or web address.



```
Command Prompt
C:\temp>
C:\temp>whoiscl -r microsoft.com

WHOIS Server: whois.opensrs.net

Registrant:
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

Domain name: MICROSOFT.COM

Administrative Contact:
Administrator, Domain domains@microsoft.com
One Microsoft Way
Redmond, WA 98052
US
+1.4258828000

Technical Contact:
Hostmaster, MSN msnhst@microsoft.com
One Microsoft Way
Redmond, WA 98052
US
+1.4258828000
```

Whois

Cross-platform utility for looking up domain information

Can collect information that may not be located elsewhere

Includes address information, phone numbers, names, and nameserver information

Should be cross-checked as information may be anonymous



# Social Engineering

Inside every environment is the human being. This is in most cases the weakest and easiest component to target. Human beings tend to be one of the easiest places to extract information from.

- **Baiting**
- **Phishing**
- **Spear phishing**
- **Pretexting**
- **Tailgating**
- **Eavesdropping**
- **Shoulder surfing**
- **Dumpster diving**





# Summary

- Wealth of resources for gaining information.
- Most are easily accessible.
- Research should be meticulous.
- A healthy amount of time should be spent on footprinting.
- Thorough research will pay off later.
- Be mindful of documentation.

