Using the Internet as an Investigative Tool
The Internet

- The web contains more than 8 billion pages
- There are more than 2.27 billion people online (doubled since 2007)
- Every minute of the day:
  - 100,000 tweets are sent
  - 684,478 pieces of content are shared on Facebook
  - 2 million search queries are made on google
  - 48 hours of video are uploaded to YouTube
  - 47,000 apps are downloaded from the App Store
  - 3,600 photos are shared on Instagram
  - 571 websites are created
  - $272,000 is spent by consumers online

Source: AllTwitter
General Search / Research Tips

• Start broad and narrow results
• Use Boolean string searches to narrow results
• Adjust “reading level”
• Diagram / Document your path
• Preserve relevant findings IMMEDIATELY
## Search Engines

### Popular Search Engines
- [www.google.com](http://www.google.com)
- [www.yahoo.com](http://www.yahoo.com)
- [www.bing.com](http://www.bing.com)
- [www.msn.com](http://www.msn.com)
- [www.ask.com](http://www.ask.com)
- [www.cuil.com](http://www.cuil.com)
- [www.lycos.com](http://www.lycos.com)
- [www.altavista.com](http://www.altavista.com)

### Meta-Search Engines
- [www.dogpile.com](http://www.dogpile.com)
- [www.metacrawler.com](http://www.metacrawler.com)
- [www.webcrawler.com](http://www.webcrawler.com)
- [www.hotbot.com](http://www.hotbot.com)
- [www.excite.com](http://www.excite.com)
- [www.mama.com](http://www.mama.com)
- [www.search.yippy.com](http://www.search.yippy.com)
Advanced Google Searches

• Use (*) to indicate any one word or symbol
• Use the plus sign (+) to force a search for an overly common word. Use the minus sign (-) to exclude a term from a search. No space follows these signs.
• To search for a phrase, supply the phrase surrounded by double quotes (" ")
• A period (.) serves as a single-character wildcard
• Synonyms of a word can be searched for with the (~) sign
• Use two periods between two numbers to search for items in a range (prices, dates, measurements, etc.)
Google Shortcuts

- **Plus sign (+)** to search for things like blood type [ AB+ ] or the programming language [ C++ ]
- "**At" sign (@)" for finding social tags like [ @google ] or [ @ladygaga ]
- **Ampersand (&)** for strongly connected ideas and phrases like [ A&E ] or [ Brothers & Sisters ]
- **Dollar sign ($)** to indicate prices, so [ nikon 400 ] and [ nikon $400 ] give different results
- **Hashtag/number sign (#)** to search for trending topics indicated by hashtags like [ #lifewithoutgoogle ]
- **Dash (-)** will sometimes be used as a sign that the words around it are very strongly connected, as in [ twelve-year-old dog ] and [ cross-reference ]
- **Underscore symbol (_)** is not ignored when it connects two words, like [ quick_sort ]
Google Operators

- “site:”
  - Iran site:cnn.com

- OR

- AND

- “-”
  - Charles Barkley –sixers

- “filetype:”
  - filetype:ppt

- “Intitle:”
  - Intitle:Gadhafi Doles Out Cash to the People

- “Insubject:”
  - Must be used in google.groups.com. Insubject: Football

- “related:”
  - related:www.google.com

- “link:”
  - Link:www.phillies.com

- “*”
  - The President voted * on the * bill

- “+”
Google Alerts

Search terms: [ ]

Type: [Everything]

How often: [once a day]

Volume: [Only the best results]

Your email: [ ]

Create Alert

Monitor the Web for interesting new content
Google Alerts are email updates of the latest relevant Google results (web, news, etc.) based on your choice of query or topic.

Enter the topic you wish to monitor, then click preview to see the type of results you'll receive. Some handy uses of Google Alerts include:

- monitoring a developing news story
- keeping current on a competitor or industry
- getting the latest on a celebrity or event
- keeping tabs on your favorite sports teams

You can also sign in to manage your alerts

Manage your alerts - Google Alerts Help - Terms of Use - Privacy Policy - Google Home

© 2011 Google
Google Cache

- Google takes a snapshot of each page it examines and stores that version
- Snapshot of a page
Pointing a Server
### Deep Web/People Searching

- [www.zabasearch.com](http://www.zabasearch.com)
- [www.pipl.com](http://www.pipl.com)
- [www.123people.com](http://www.123people.com)
- [www.zoominfo.com/search](http://www.zoominfo.com/search)
- [www.spoke.com](http://www.spoke.com)
- [www.411locate.com](http://www.411locate.com)
- [www.addresses.com](http://www.addresses.com)
- [www.bigfoot.com](http://www.bigfoot.com)
- [www.people.yahoo.com](http://www.people.yahoo.com)
- [www.whitepages.com](http://www.whitepages.com)
- [www.switchboard.com](http://www.switchboard.com)
Finding Company Information

- PA Corporation Search
  http://www.corporations.state.pa.us/corp/
- Dun and Bradstreet
  www.dnb.com
- UCC Filings
  www.corporations.state.pa.us/ucc/soskb/SearchStandardRA9.asp
Top Social Networking Sites (SNS)

Top 10 Social-Networking Websites & Forums
by US Market Share of Visits (%)
January 2011

Facebook: 63.58%
YouTube: 18.87%
MySpace: 2.18%
Yahoo! Answers: 1.10%
Twitter: 1.00%
Tagged: 0.91%
myYearbook: 0.48%
Mylife: 0.39%
LinkedIn: 0.36%
Club Penguin: 0.29%

Source: Experian Hitwise

*Other brands, names, or images are the property of their respective owners.
Social Media Security

• 1 in 4 users location tag their Facebook posts each month
• More than 20 million US users have their birthday and year included in their profile
• An average user has 229 Facebook friends
• 50% of Facebook users check their security settings every 2-3 months

Source: AllTwitter
Facebook

• 950 million active users and over 2 billion registered users
• 91% of online adults use social media regularly
• Internet users spend 22.5% of their online time social networking
• there are 152 million blogs on the internet
• 93% of US adult Internet users are on Facebook
• Facebook has 232 million users in Europe, 222 million in North America, and 219 million users Asia.

Source: AllTwitter
Information on Facebook

- Personal data
- Status updates
- Photographs
- Interests
- Activities
- Friends
Tips

• Emails
  – Don’t just search the email. Many times first part of email will be the handle
    • Example: Runningbunny@yahoo.com
    • Search: “Runningbunny”

• Screen Name/Handle
  – Real life nicknames and handles may be screen names

• Phone Numbers

• Verify Information
• Classmates Search
• Coworker Search
Facebook

- Search Facebook without logging in
  - www.facepinch.com
  - www.yourbook.org
  - www.openfacebooksearch.com
Twitter

- Over 500 million registered users, but just 140 million active users
- About 9% of the adult US internet users use Twitter
- Monitoring Tweets
  - Twitter
  - Twittorati
  - Monitter
SNS by country

- China
  - QQ (www.qq.com), Xiaonei (www.renren.com)
- Russia
  - V Kontakte (www.vkontakte.ru), Odnoklassniki (www.Odnoklassniki.ru)
- India, Brazil
  - Orkut (www.orkut.com)
- Peru, Columbia, Ecuador, Portugal, Mongolia, Romania
  - Hi5 (www.hi5.com)
- France
  - Skyrocket (www.skyrocket.com)
- United Kingdom
  - Bebo (www.bebo.com)
- Netherlands
  - (www.hyves.nl)
Blogs

• Platforms
  – Wordpress (www.wordpress.com)
  – Blogger (www.blogger.com)
  – Typepad (www.typepad.com)
  – Livejournal (www.livejournal.com)
  – Tumblr (www.tumblr.com)
  – Posterous (www.posterous.com)
  – Moveabletype (www.movabletype.org)
Maps and Satellites

Street View
Maps and Satellites

Bird’s Eye View
Translator

- www.babelfish.yahoo.com
In August of 2010, Adam Savage, of MythBusters, took a photo of his vehicle using his smartphone. He then posted the photo to his Twitter account including the phrase off to work.

The image contained metadata revealing the exact geographical location the photo was taken.

By taking and posting a photo, Savage revealed the exact location of his home, the vehicle he drives and the time he leaves for work.
Photo Sharing

- Flickr
  - www.flickr.com
- Photobucket
  - www.photobucket.com
- Picasa
  - www.picasaweb.google.com
- Smug Mug
  - www.smugmug.com
Metadata

• Usually defined as “data about data”
• Metadata can be created automatically (embedded by a camera) or manually (input from user)
• Much to the benefit of investigators, metadata tends to be disregarded or forgotten about by everyday users
<table>
<thead>
<tr>
<th>EXIF Tag</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make</td>
<td>NIKON CORPORATION</td>
</tr>
<tr>
<td>Model</td>
<td>NIKON D200</td>
</tr>
<tr>
<td>Orientation</td>
<td>Top left</td>
</tr>
<tr>
<td>XResolution</td>
<td>300</td>
</tr>
<tr>
<td>YResolution</td>
<td>300</td>
</tr>
<tr>
<td>ResolutionUnit</td>
<td>Inch</td>
</tr>
<tr>
<td>Software</td>
<td>Ver.2.00</td>
</tr>
<tr>
<td>DateTime</td>
<td>2007:01:06 18:24:26</td>
</tr>
<tr>
<td>YCbCrPositioning</td>
<td>Co-Sited</td>
</tr>
<tr>
<td>ExifOffset</td>
<td>228</td>
</tr>
<tr>
<td>ExposureTime</td>
<td>1/10 seconds</td>
</tr>
<tr>
<td>FNumber</td>
<td>4.00</td>
</tr>
<tr>
<td>ExposureProgram</td>
<td>Normal program</td>
</tr>
<tr>
<td>ISOSpeedRatings</td>
<td>800</td>
</tr>
<tr>
<td>ExifVersion</td>
<td>0221</td>
</tr>
<tr>
<td>DateTimeOriginal</td>
<td>2007:01:06 18:24:26</td>
</tr>
<tr>
<td>DateTimeDigitized</td>
<td>2007:01:06 18:24:26</td>
</tr>
<tr>
<td>ComponentsConfiguration</td>
<td>YCbCr</td>
</tr>
<tr>
<td>CompressedBitsPerPixel</td>
<td>4 (bits/pixel)</td>
</tr>
<tr>
<td>ExposureBiasValue</td>
<td>0.00</td>
</tr>
<tr>
<td>MaxApertureValue</td>
<td>F 4.00</td>
</tr>
<tr>
<td>MeteringMode</td>
<td>Center weighted average</td>
</tr>
<tr>
<td>LightSource</td>
<td>Auto</td>
</tr>
<tr>
<td>Flash</td>
<td>Not fired</td>
</tr>
<tr>
<td>FocalLength</td>
<td>26.00 mm</td>
</tr>
<tr>
<td>UserComment</td>
<td>copyright tamar weinberg</td>
</tr>
<tr>
<td>SubsecTime</td>
<td>7</td>
</tr>
</tbody>
</table>
Steganography

- Steganography involves hiding messages in such a way that no one other than the sender and recipient suspect the existence of the message.
- Differs from encryption in that instead of protecting data, “steg” will hide its existence.

Possible Uses for Steganography:

Corporate Espionage

Pornography

Secret communications

Terrorism
Steganography (cont.)

What can be hidden in a digital picture?

(other) Pictures Audio
Text Web pages
Many additional file formats

Other files can also host hidden information!

(i.e. – pictures within audio, audio within audio, etc.)
Video Sharing

- Youtube
  - www.youtube.com
- Metacafe
  - www.metacafe.com
- Vimeo
  - www.vimeo.com
- Live Leaks
  - www.liveleaks.com
- Dailymotion
  - www.dailymotion.com
Example

• 2006, Harrisburg, PA
• Rap video posted to Youtube.com
  – Allison Hill street corner
  – Half a dozen young men posing with handguns and what appeared to be crack cocaine
• Patriot News reported on story
  – Many on probation
  – One individual was out of prison on bail
Tracing IP Addresses

- Registered a website
- Technical contact
- Can be used to look up IP locations
- Can be used to determine if an individual has any other websites registered
- Address and phone number information can be determined
Tracing IP Addresses

- [www.whois.com](http://www.whois.com)
- [www.networksolutions.com](http://www.networksolutions.com)
Wayback Machine

- www.waybackmachine.org
Other Useful Websites

• Disgruntled Employees (www.jobvent.com)
• Yahoo Finance message boards (www.yahoo.com)
• Company Reviews (http:www.glassdoor.com)
Investigative Integrity

- Do you want to remain anonymous?
  - Dedicated computer with a normal system configuration
  - Dedicated undercover internet connection
  - Computer with IP hiding capability
- Be cautious about where you search!
Summary

• Knowing where to search is important
• Knowing how to search is more important
• Avoid information overload by narrowing your searches
• Know employment law limitations
• Verify all information!
Questions