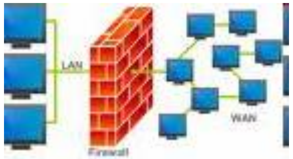
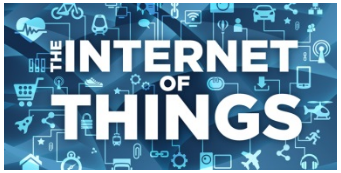
Hidden Universes of Cybersecurity Awareness

Norton from symantec





Find us on Facebook

DANGER

PHISHING SCAM

Anonymizer.com
Privacy is your right.

Free Wi Fi spot

FISSEA Conference 3/2018
Russ Haynal
Instructor & Speaker
Internet: Search, OSINT, Infrastructure, Cybersecurity Awareness
navigators.com

Give a person a Phish,
you feed them for a day
Teach a person how to Phish,
you feed them for a lifetime

Today's session shows how to quickly find the best resources for any topic, using several very clever and efficient search techniques

All example searches – and links to some great search results are posted online:

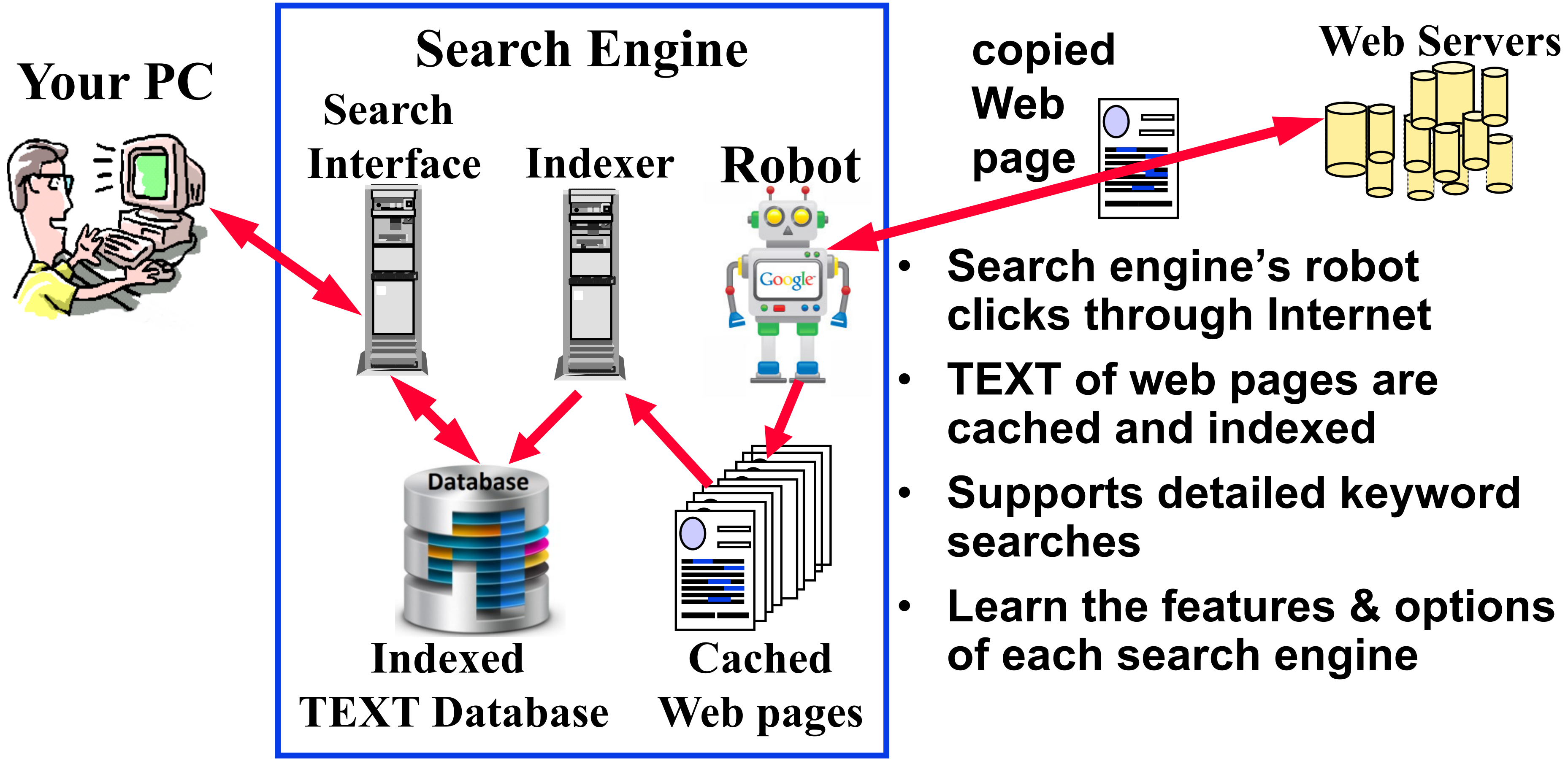
http://navigators.com/fissea.html

Disclaimer

- This session illustrates several clever search techniques and research methods
- Consult your organization’s policies to verify if these methods are approved for your type of Internet connections

Search Engines

(google.com , bing.com)



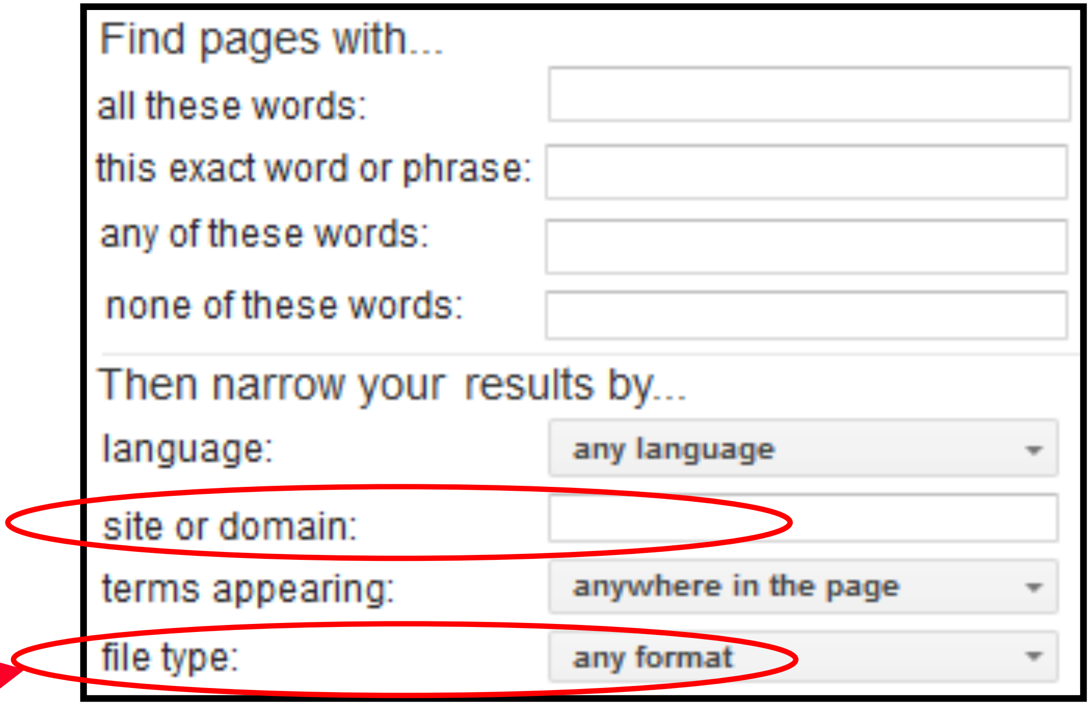
- Search engine’s robot clicks through Internet
- TEXT of web pages are cached and indexed
- Supports detailed keyword searches
- Learn the features & options of each search engine

You must envision the target page
“Use your imagination”

Advanced Search = Efficient Search !

basic search

advanced search



Find pages with...

all these words:

this exact word or phrase:

any of these words:

none of these words:

Then narrow your results by...

language: any language

site or domain:

terms appearing: anywhere in the page

file type: any format

Limit search to specific sites or domains

filetype:pdf = detailed content from great web sites

- **Bottom right of Google home page: Settings → Advanced Search**
- **Top right of Google search results: Settings → Advanced Search**

- **Also choose 100 results per page: Settings → Search Settings**

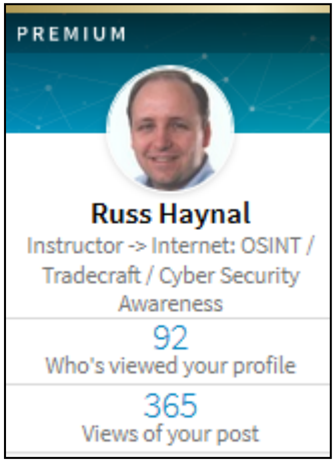
Search Examples

cybersecurity framework	51,000,000 - both words anywhere
“cybersecurity framework”	203,000 - words adjacent, correct order
“cybersecurity framework” filetype:pdf	126,000 - research papers / presentations
“cybersecurity framework” filetype:ppt	36 - Powerpoint presentations
“cybersecurity framework” site:slideshare.net	1,600 - presentations
“cybersecurity framework” site:nist.gov	4,750 – hits from just nist.gov
“cybersecurity framework” site:nist.gov filetype:pdf	1,310 – pdf’s hosted at nist.gov
“cybersecurity framework” site:edu filetype:pdf	19,000 – pdf’s hosted at U.S. universities
“cybersecurity framework” site:linkedin.com/in	7,430– linkedin profiles
site:linkedin.com/in cissp ts sci	20,200 – certified security professionals revealing they have Top Secret clearance
site:linkedin.com/in your_agency job-title eg. system administrator	= spear phishing targets at YOUR agency

- When using “site:” command, do not include “http://www”

Cautions about Social Media

- Confirm policies for viewing, joining, or interacting on social media
- Understand each site's different levels of interactions:
  - viewing, following, group member, connecting, friend, messaging
- What information is shared to the other end user?
- What information is shared with 3rd party advertisers / data brokers?
- ALL interactions are known to the owner of the social media site
  --> learn who owns the site
- Who has "jurisdiction" over the site? (VK --> Russia, QQ --> China)



PREMIUM

Russ Haynal

Instructor -> Internet: OSINT / Tradecraft / Cyber Security Awareness

92
Who's viewed your profile

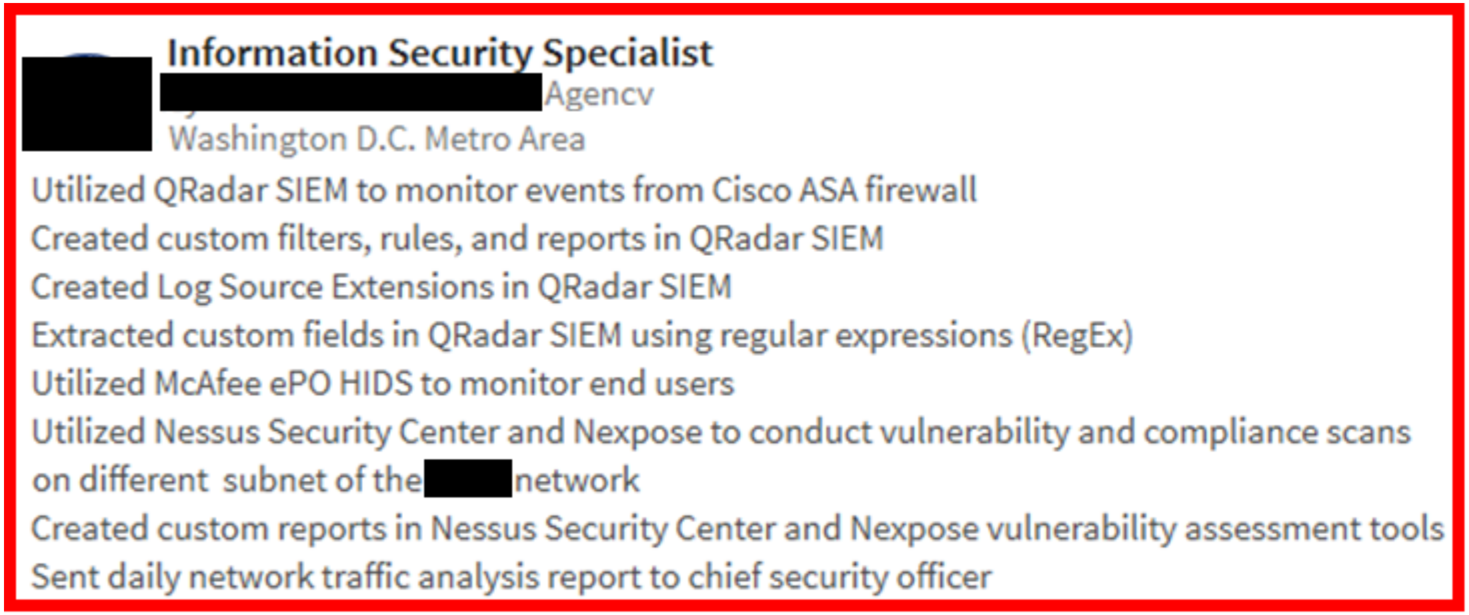
365
Views of your post

- Linkedin example:
- Different membership levels have various capabilities
- free ($0/month), premium, premium personal, premium career, sales navigator, recruiter lite, recruiter ($900/month)
- "recruiter" has unlimited access to everyone's full profiles, and leaves no "hits" on the people they view

Free account = YOU are the "product" being sold!

Compare level of detail in these two Linkedin profiles

Reveals security defenses and procedures, and recipe for spear phishing



[redacted]

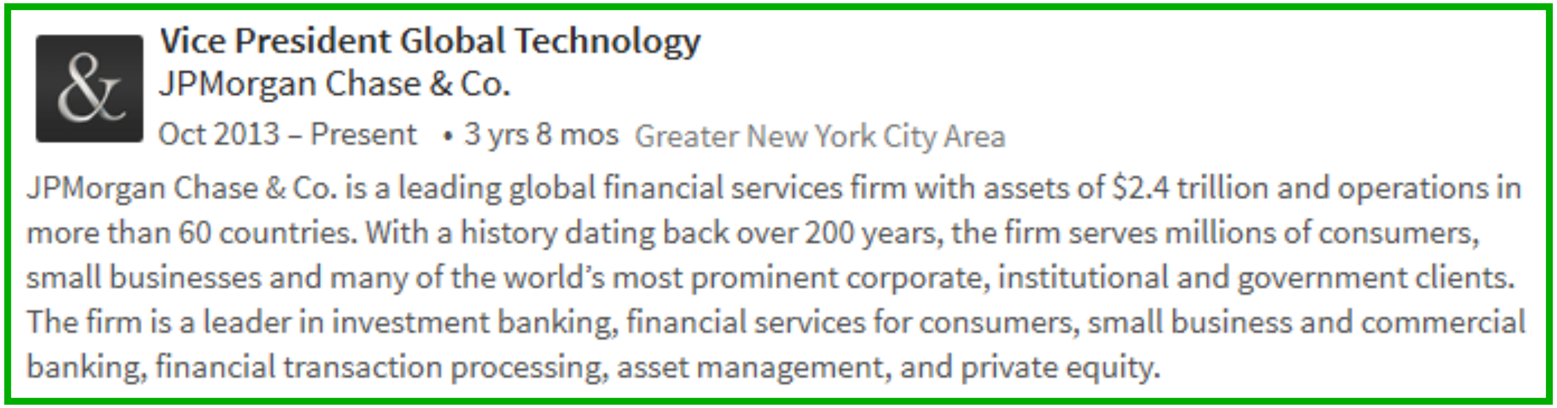
Information Security Specialist

[redacted] Agencv

Washington D.C. Metro Area

Utilized QRadar SIEM to monitor events from Cisco ASA firewall
Created custom filters, rules, and reports in QRadar SIEM
Created Log Source Extensions in QRadar SIEM
Extracted custom fields in QRadar SIEM using regular expressions (RegEx)
Utilized McAfee ePO HIDS to monitor end users
Utilized Nessus Security Center and Nexpose to conduct vulnerability and compliance scans on different subnet of the [redacted] network
Created custom reports in Nessus Security Center and Nexpose vulnerability assessment tools
Sent daily network traffic analysis report to chief security officer

Reveals JPMorgan is a bank (this is posted by MANY JPMorgan employees)



Vice President Global Technology

JPMorgan Chase & Co.

Oct 2013 – Present • 3 yrs 8 mos Greater New York City Area

JPMorgan Chase & Co. is a leading global financial services firm with assets of $2.4 trillion and operations in more than 60 countries. With a history dating back over 200 years, the firm serves millions of consumers, small businesses and many of the world's most prominent corporate, institutional and government clients. The firm is a leader in investment banking, financial services for consumers, small business and commercial banking, financial transaction processing, asset management, and private equity.

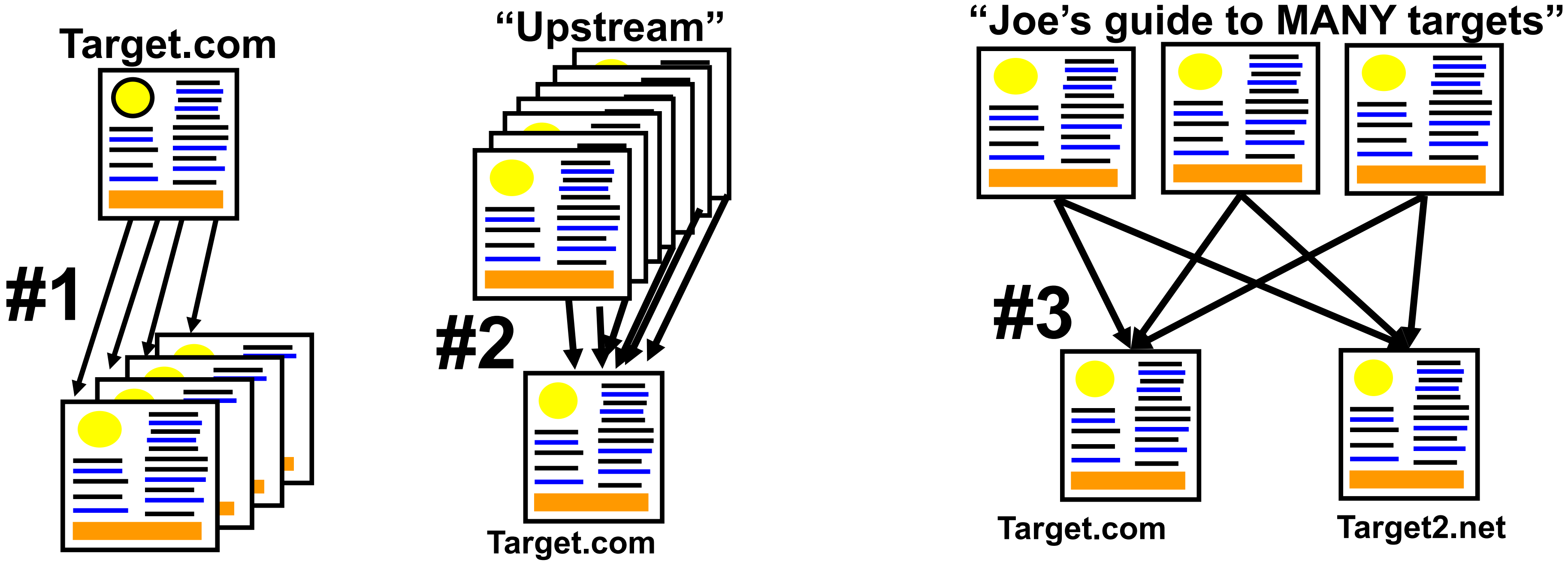
Forums of people who know your topic

- Forum – discussion focused on a particular topic
- Many users can participate by posting messages
- Moderators may "police" comments that are considered off-topic
- Try searching for:
- Your topic forum post replies = forum of users that discuss your topic
- Use search terms that would be used by people in that industry: acronyms, slang, jargon, etc

- "cybersecurity framework" forum post replies = 11,100
- specific publication numbers: "800 53" forum post replies
- name of a product/vendor and forum post replies
- etc

Surfing Upstream vs. Downstream

Russ Haynal
Internet Instructor & Speaker
http://navigators.com/
search_upstream.html



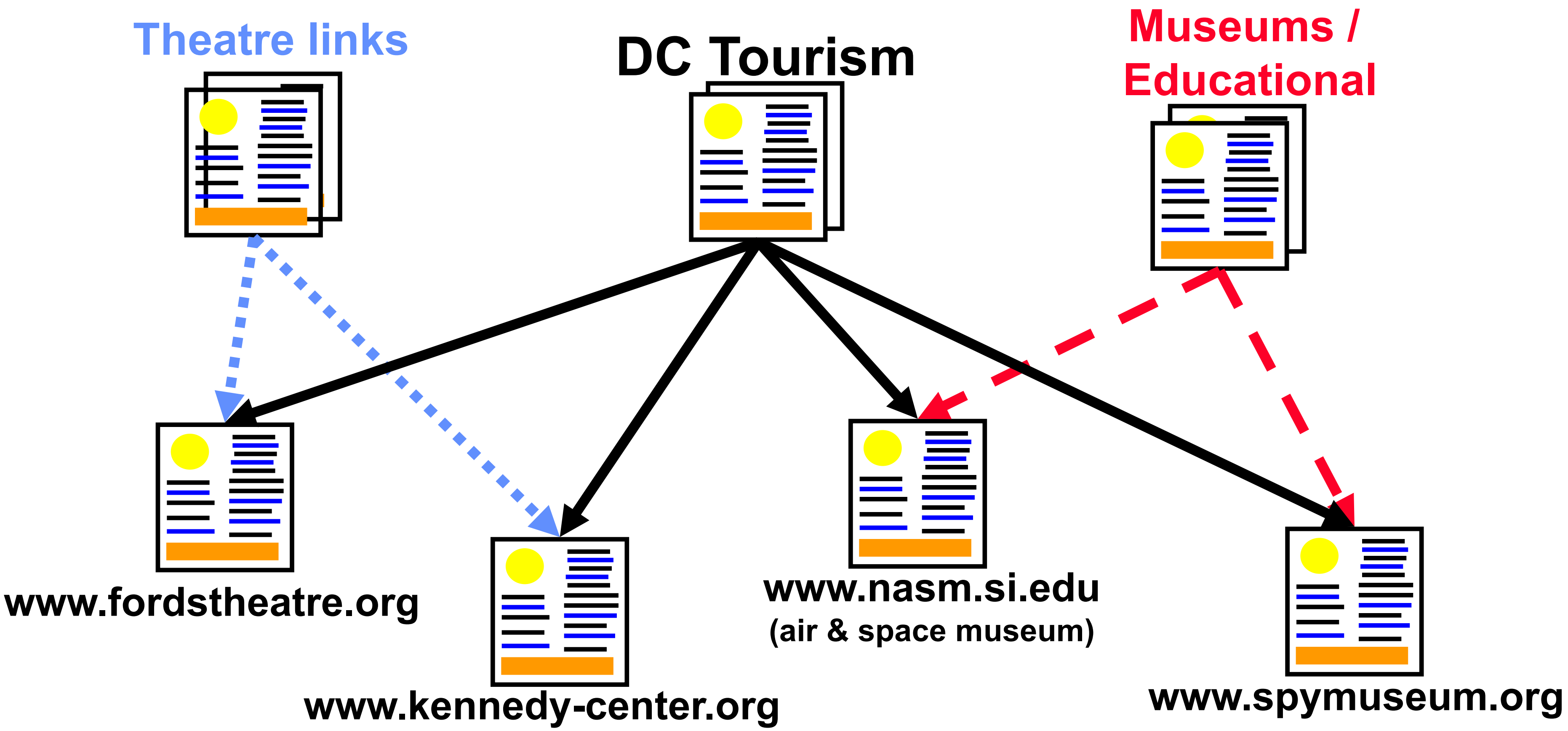
#1 Most researchers follow the links "downstream" from an interesting page

#2 Shows pages that link towards the target (=upstream)
This is an Indication of the page's "popularity"
= who knows about target.com

#3 Shows pages that link to both target sites …
= "user pages" for that topic

Be Creative When Surfing Upstream

Example: Washington DC Tourist Sites



- Any combination of these target pages will lead you to “DC Tourism” pages, but certain pairings may also lead you to subject-specific pages

Surfing Upstream Details

search format at google or bing	search results
“www.example.com”	contain text: www.example.com
“www.example.com/pageA.html”	contain text of the specific page address
+“www.example1.com” +“www.example2.com”	contain text of both example site addresses This is a great way to discover “user pages” (e.g. Joe's guide to many example-sites)

- You need to decide which scenario makes more sense; Row #1 or Row #2
  e.g. who links to the home page of the entire site vs,
  who links to a specific webpage within the site
- A 3rd and 4th site can be added if they are popular enough
- Note: do not include “http://”
- Who links to: 2 anti-phishing vendors, 2 animation products, 2 security conferences, etc.

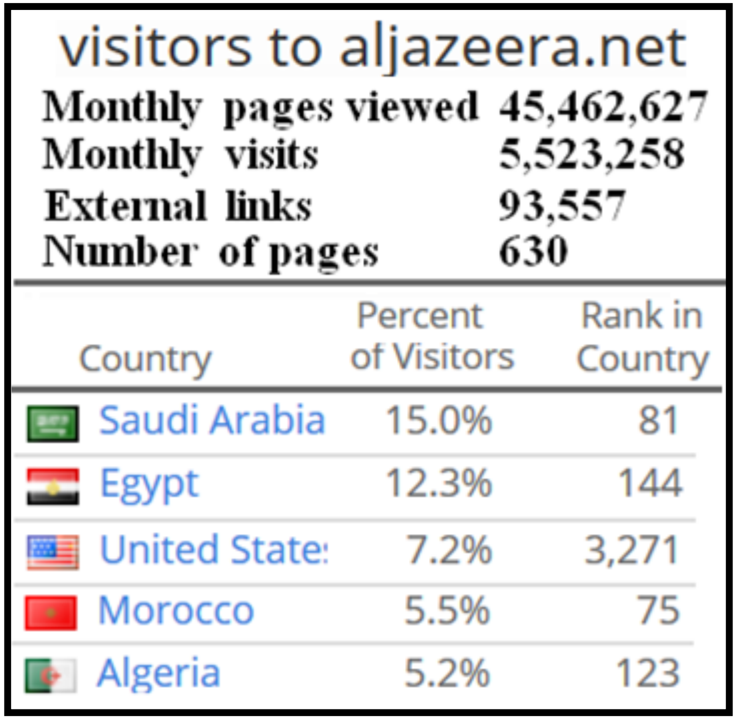
Web Analytics

alexa.com similarweb.com
urlm.com urlm.co.uk

Each of these tools offer a sampling of analytics for free:

- **Popularity of a web site**
- **Audience demographics**
- **Search terms used to find the site**
- **Visitor engagement levels**
- **Traffic history**
- **Related sites = more sites**

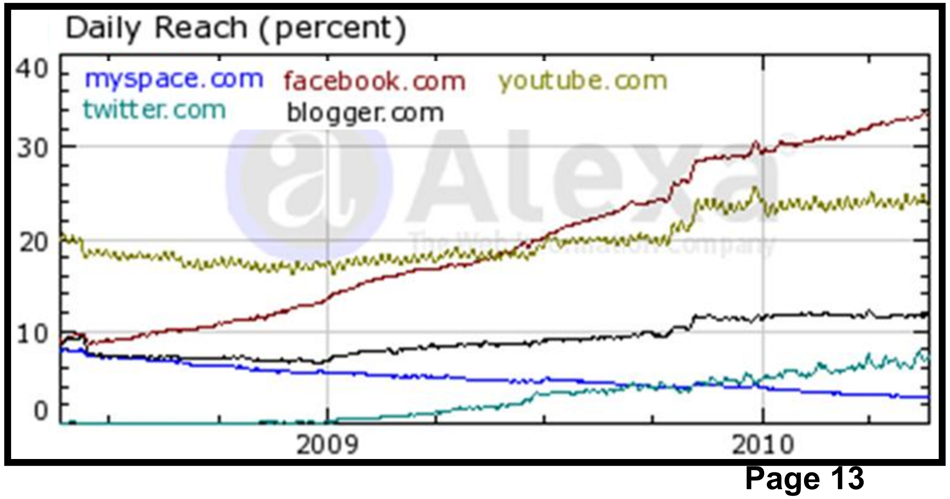
Enter a domain name (not search terms)



visitors to aljazeera.net

Monthly pages viewed	45,462,627
Monthly visits	5,523,258
External links	93,557
Number of pages	630

Country	Percent of Visitors	Rank in Country
Saudi Arabia	15.0%	81
Egypt	12.3%	144
United State:	7.2%	3,271
Morocco	5.5%	75
Algeria	5.2%	123



Your Homework Mission, Should You Decide To Accept It…

- Google settings –> 100 hits
- Use clever search techniques
- Find “people without a life” who have already done the research:
- They post PDFs and PPTs, participate in forums, share on linkedin, link to many resources

Contact Information

Russ Haynal   russ @ navigators.com   703-729-1757

www.linkedin.com/in/russhaynal

Note: If you send me an email, and it’s not from .gov or .mil, put “internet training” in the e-mail's subject