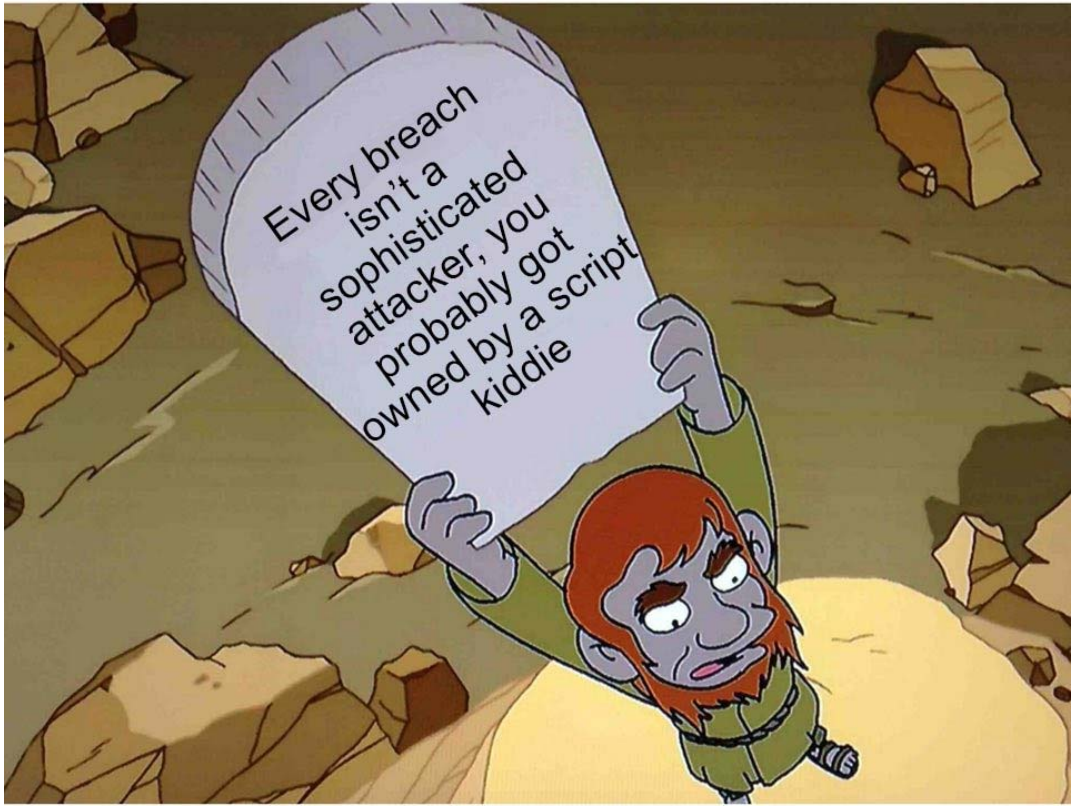
CSCE 629
Cyber Attack

Reconnaissance

Behold, the one commandment!



Dr. Barry Mullins
AFIT/ENG
Bldg 642
Room 209
255-3636 x7979

Computer and Network Hacker Exploits

- **Step 1: Reconnaissance**
  - Low Tech Recon
  - STFW
  - Whois Databases
  - DNS
  - Recon Tools
- Step 2: Scanning
- Step 3: Gaining Access
  - Application and Operating System Attacks
  - Network Attacks
  - Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Reconnaissance

- Must "do your homework" to learn the target
- Experienced attackers always perform recon
- Systematically and methodically gather all info available
  - Domain name (e.g., afit.edu)
  - Network Blocks / Reachable IP addresses / Network topology
  - Services running on systems (e.g., TCP and UDP)
  - System architecture (e.g., Sparc, x86, etc.)
  - Security appliances (firewalls, IDS)
- Also known as Open Source Intelligence
  - OSINT

Computer and Network Hacker Exploits

- **Step 1: Reconnaissance**
  - Low Tech Recon
  - STFW
  - Whois Databases
  - DNS
  - Recon Tools
- Step 2: Scanning
- Step 3: Gaining Access
  - Application and Operating System Attacks
  - Network Attacks
  - Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Low-tech Reconnaissance

- Physical break-in
  - Tailgate someone into building
  - "Borrow" a computer
  - Plug into an open Ethernet port using your computer
    - This bypasses firewalls
  - Install a keystroke logger
  - Could be arrested or shot!

Low-tech Reconnaissance

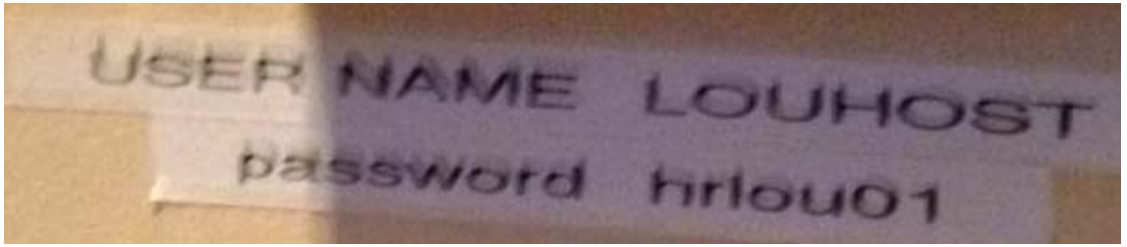
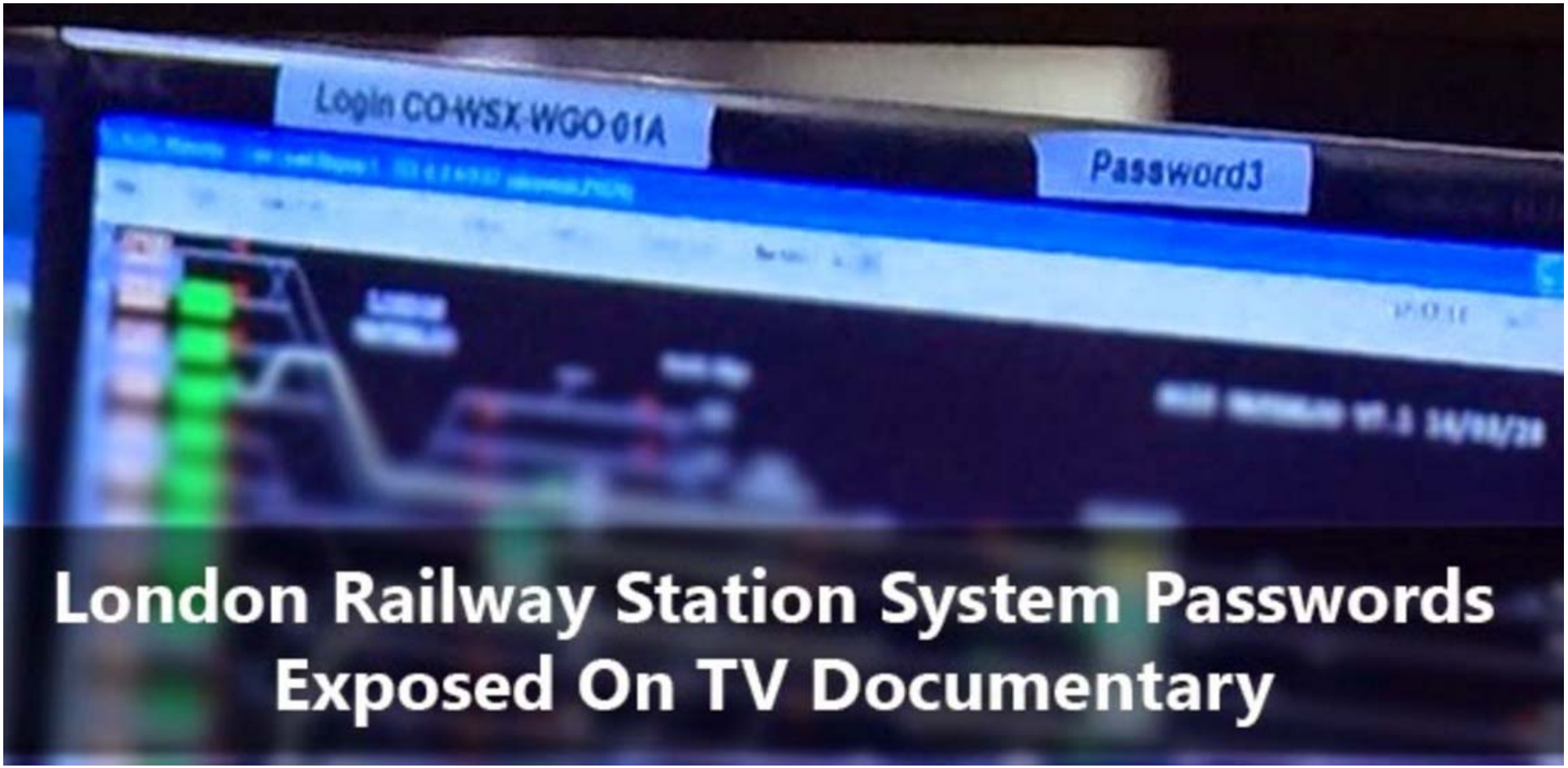


Photo taken outside a hotel window @ DerbyCon 2013!



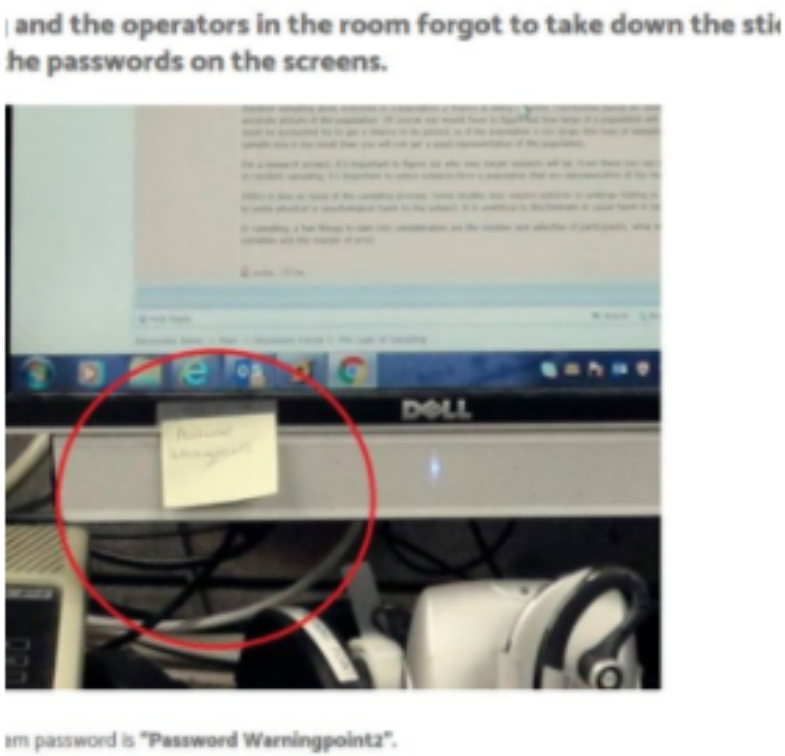
http://thehackernews.com/2015/05/railway-system-password.html

Low-tech Reconnaissance

Swamp Drainer
@FedupWithSwamp

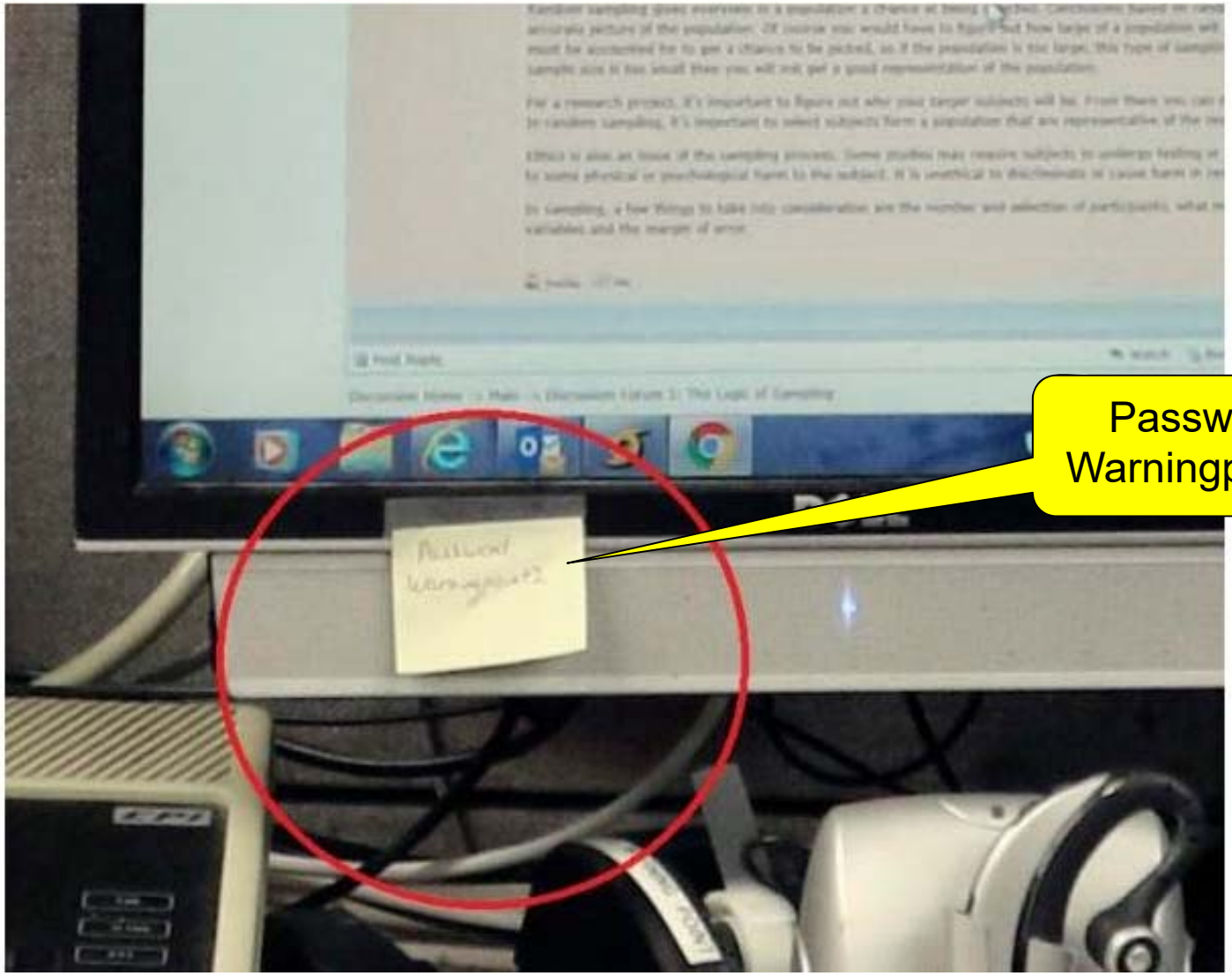
Follow

Did anyone catch this? An Anon did. Wong left the password is on the sticky note at the HI alert system. If he's working for us, he needs to tighten up.

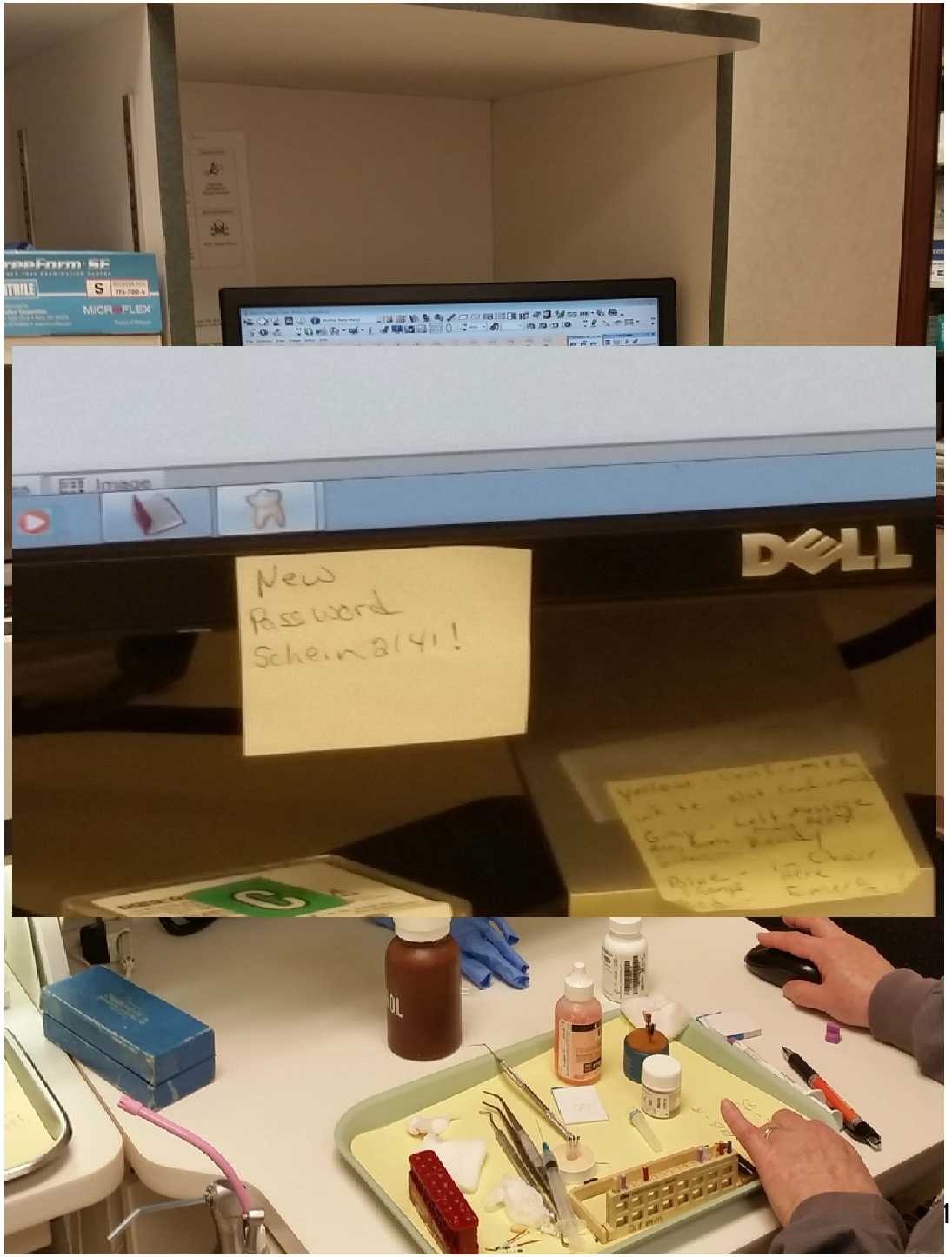


7:53 PM - 15 Jan 2018

Wong and the operators in the room forgot to take down the sticky notes with the passwords on the screens.



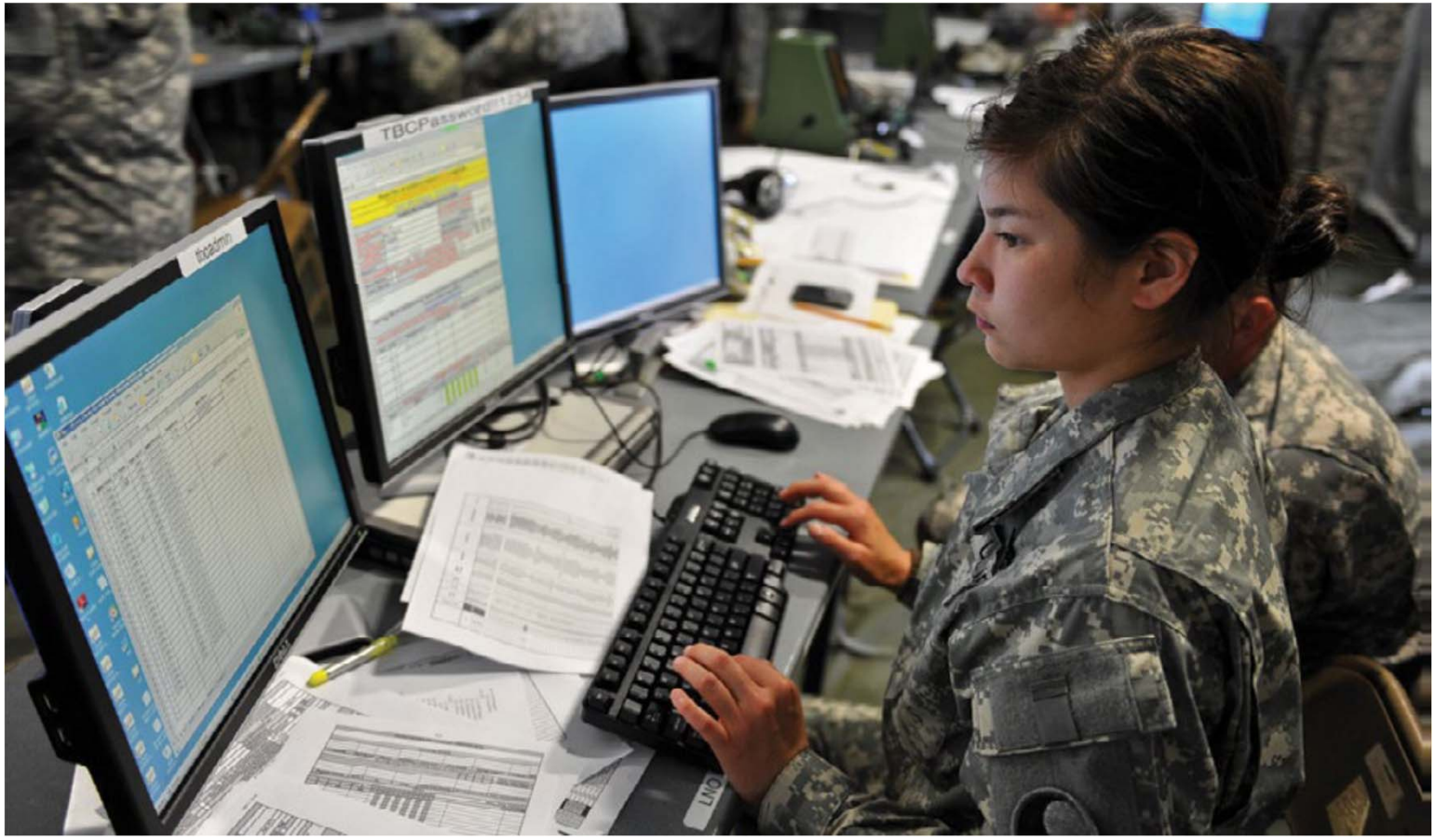
Low-tech Reconnaissance



Low-tech Reconnaissance
Military Review May-Jun 2014

Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy

Col. Harry D. Tunnell IV, U.S. Army, Retired



Low-tech Reconnaissance

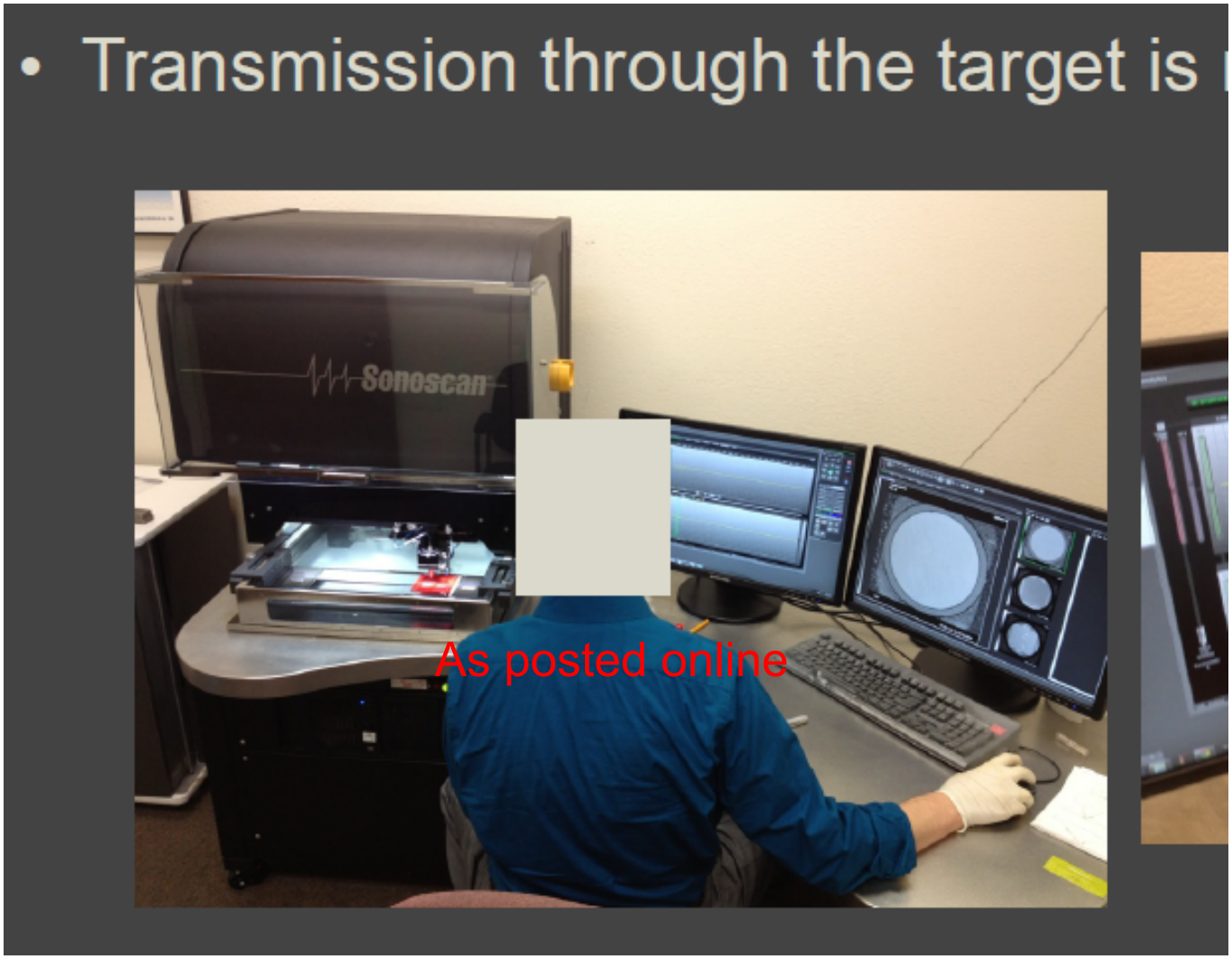
- Listen in on conversations near the target
- Dumpster diving
  - Rifling through trash for sensitive info
- Learn employee identities
  - Check out these "sanitized" published materials

As posted online

After a copy and paste of image

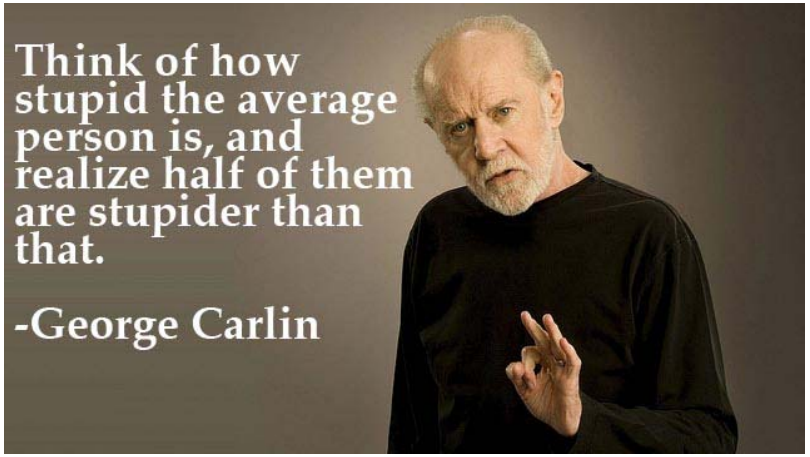
Low-tech Reconnaissance

30 Jul 15: https://www.blackhat.com/docs/webcast/04232014-tools-of-the-hardware-hacking-trade.pdf

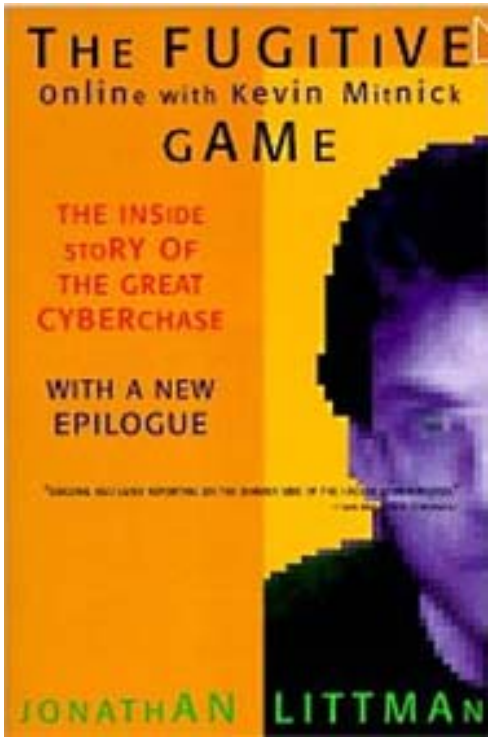


Low-tech Reconnaissance - Spy

Social Engineering (SE)



- Convincing someone to do something they shouldn't or wouldn't normally do
- Attempt to solicit information from a victim by calling someone masquerading as an authoritative person or someone seeking help
- A skilled social engineer will build trust before asking for sensitive information
  - Must know the lingo
- Notable social engineers
  - Jayson Street
  - Kevin Mitnick
  - Chris Hadnagy
- Top 5 SE Techniques
  - https://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html

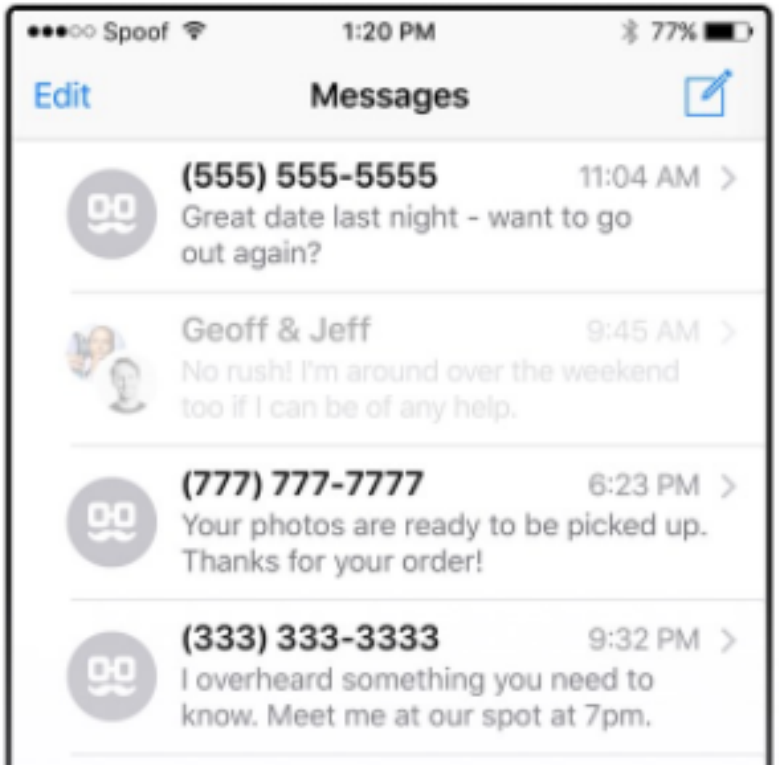


What is White Hat Hacking?

- Jayson Street

Spoofing Caller ID / Texts

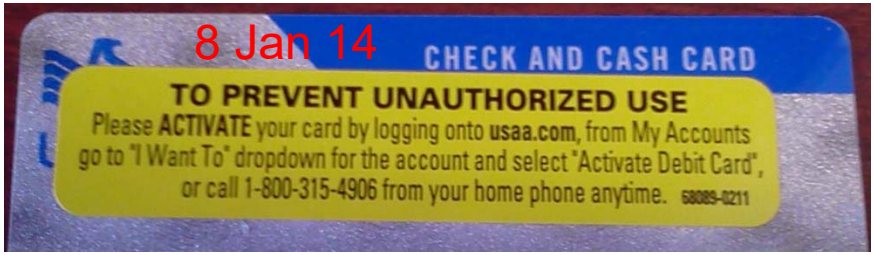
- Spoof your called ID number or texts to any number
- Employees are more likely to trust someone from "within" company
- www.spoofcard.com
  - Can set it to go directly to voicemail
  - Can also change your voice… including your gender!

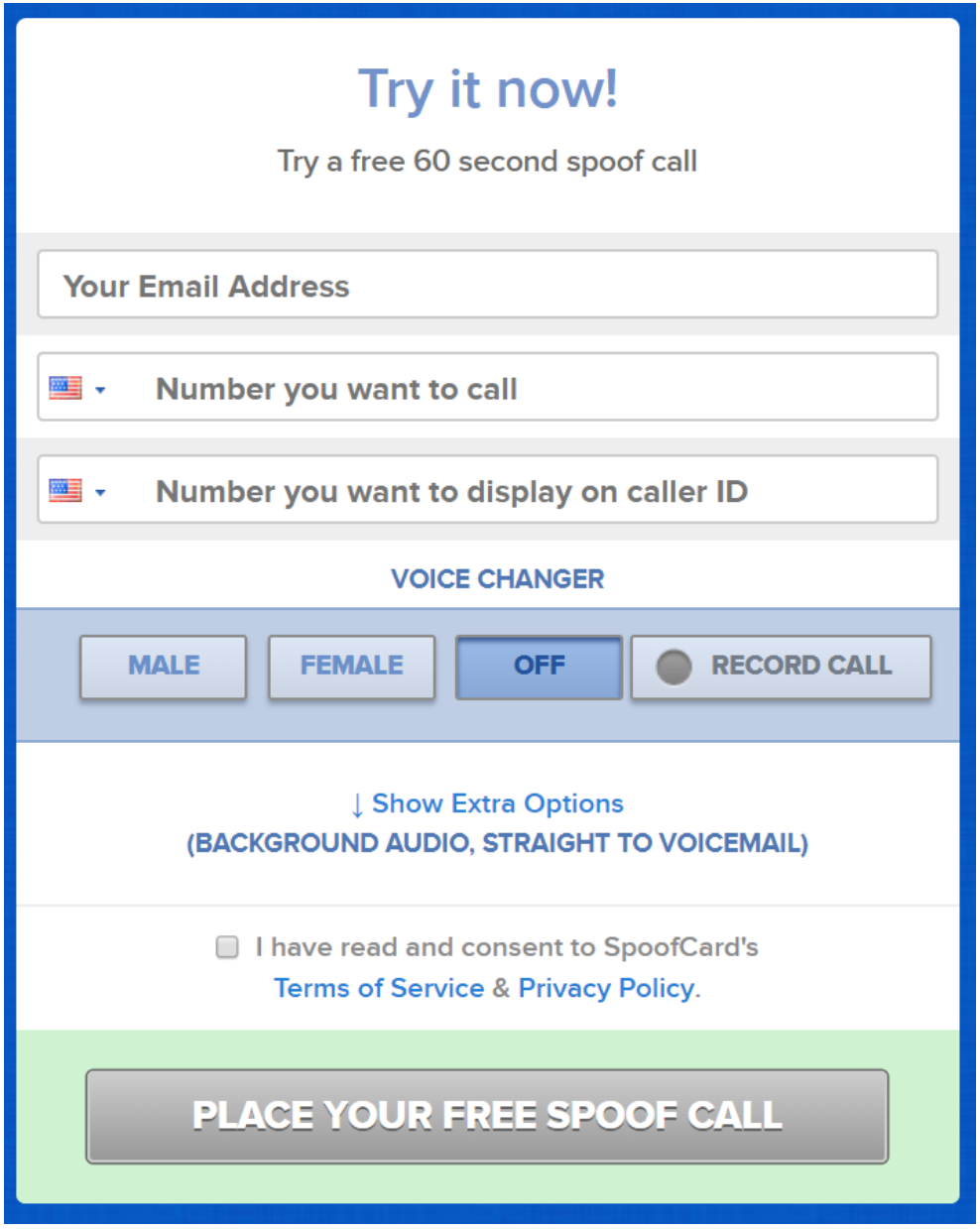


- Under the Truth in Caller ID Act of 2009, FCC rules:
  - Prohibit any person or entity from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value

https://consumercomplaints.fcc.gov/hc/en-us/articles/202654304-Caller-ID-and-Spoofing

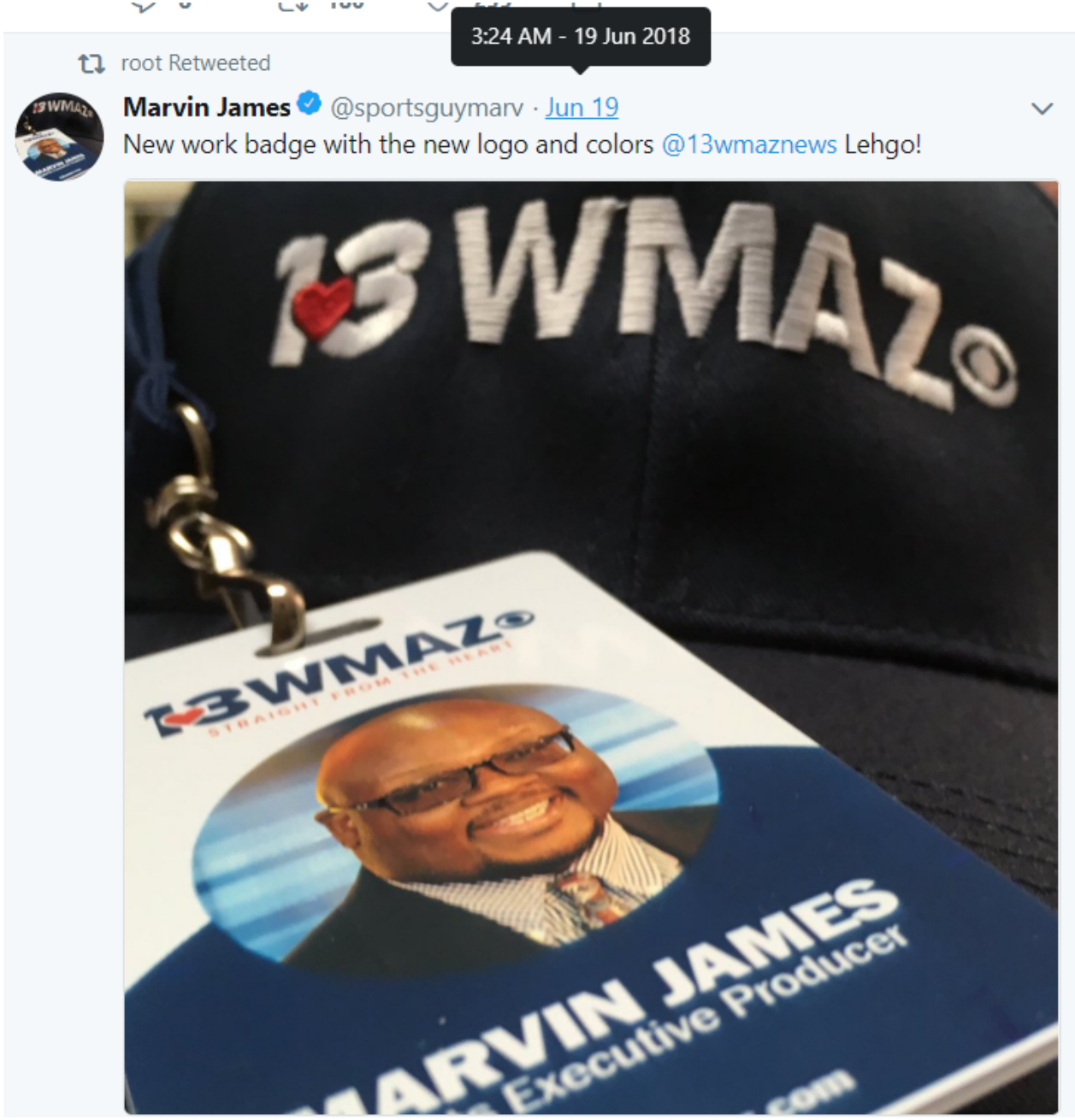
www.spoofcard.com





https://www.spoofcard.com/free-spoof-caller-id

Badges!!


3:24 AM - 19 Jun 2018
root Retweeted
Marvin James @sportsguymarv · Jun 19
New work badge with the new logo and colors @13wmaznews Lehgo!
13WMAZ
STRAIGHT FROM THE HEART
MARVIN JAMES
Executive Producer

Badges!!

Sam. 🕯️
@GreenEggsnSam_

Follow

Can we all just appreciate the fact that my new work badge is 900000% better then my first st. Joes one

12:29 AM - 20 Jul 2018

Debit Cards on Twitter

Mark
@Mark88933736

Follow

My new debit card 😍😍😍 #debitcards

6:18 AM - 25 Nov 2018

Computer and Network Hacker Exploits

- **Step 1: Reconnaissance**
  - Low Tech Recon
  - STFW
  - Whois Databases
  - DNS
  - Recon Tools
- Step 2: Scanning
- Step 3: Gaining Access
  - Application and Operating System Attacks
  - Network Attacks
  - Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Search the Fine Web

- Use public information readily available on the Internet
  - Perfectly legal since info is public
- What are you looking for?
  - Organizational function / structure / mission
  - Manning information
  - Location(s)
  - Contact names and phone numbers

- Acquire information from target or third party sources
- Be prepared for possibly large amounts of data
  - Sifting through the data can be time-consuming

Start Search at the Target's Web Site

- Robots.txt
  - Nike?

- Personal information on employees
- Learn the company's lingo
- Technology announcements
  - White papers / Press releases / Design docs / Patent apps
- Business partners
- Corporate people / star employees
- What technologies are they using? Windows IIS? Oracle?
- Job listings
  - On target website, monster.com, Linkedin, …
  - "Seeking sys admin with experience in Apache administration"

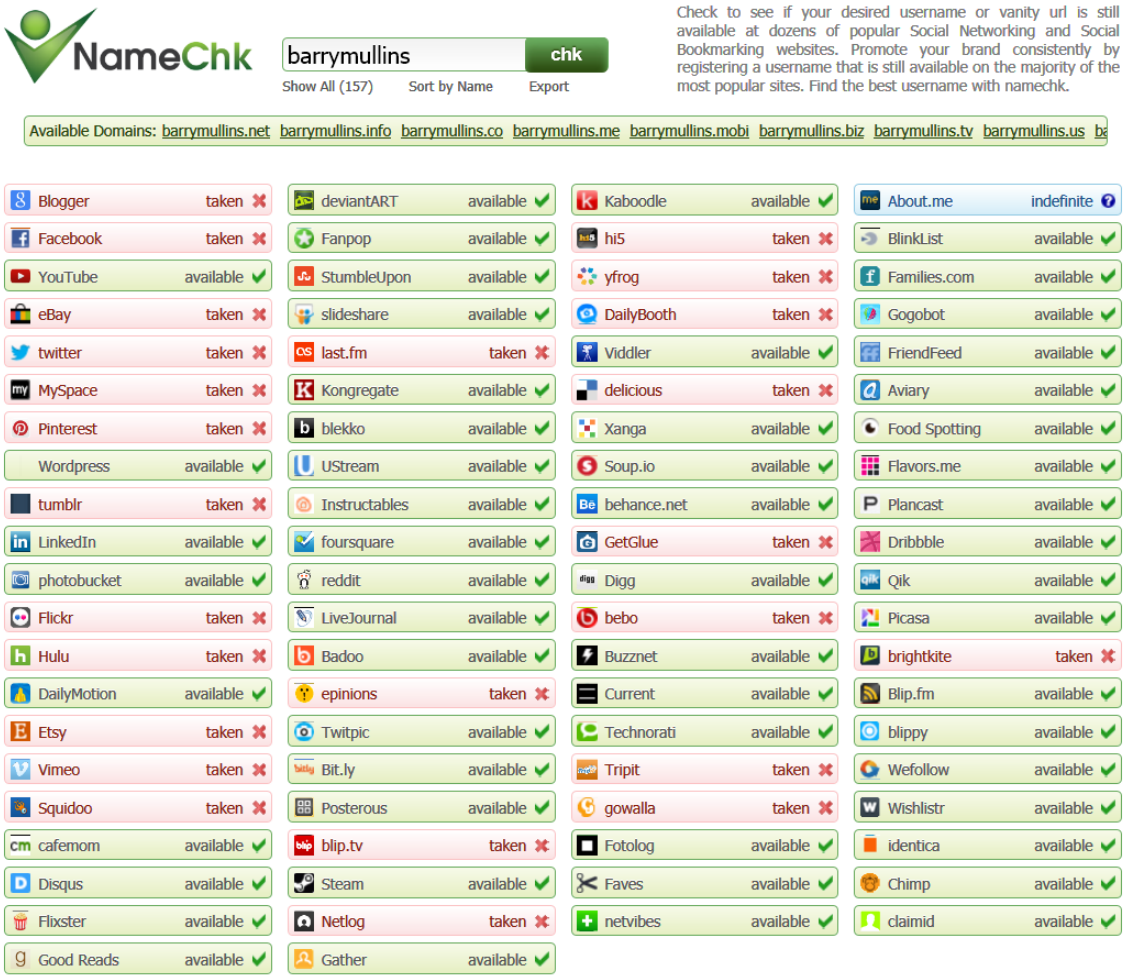
Also Look at Other Sources

- Now expand your search to sites with ties to target
  - ISP, business partners, courier services, providers of phone, electric, gas, …

- Also use publically-accessible databases
  - Companies publicly traded in the US are required to file registration statements, periodic reports, and other forms with the Electronic Data Gathering, Analysis and Retrieval (EDGAR) database
    - Who signed the docs?
    - www.sec.gov/edgar/quickedgar.htm

Social Networking Sites

- Facebook, Twitter, LinkedIn…
- Does the target use social media?
  - namechk.com



Got Photos?

- Extract EXIF data (if available)
  - Right click on image in Windows → Properties
  - Upload photo to exif.regex.info/exif.cgi

Basic Image Information

Camera:	Lg Electronics VS910 4G
Lens:	4.3 mm
Date:	**December 5, 2012** 1:35:28PM (timezone not specified) (9 minutes, 14 seconds ago, assuming image timezone of 5 hours behind GMT)
Location:	Latitude/longitude: **39**° 46' 57.4" North, **84**° 4' 57.3" West (39.782600, -84.082584) Photos on Jeffrey's blog that are near this location. Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 0 m Timezone guess from earthtools.org: 5 hours behind GMT
File:	**2,592** × **1,944** JPEG (**5.0** megapixels) 1,170,567 bytes (1.1 megabytes) Image compression: 92%

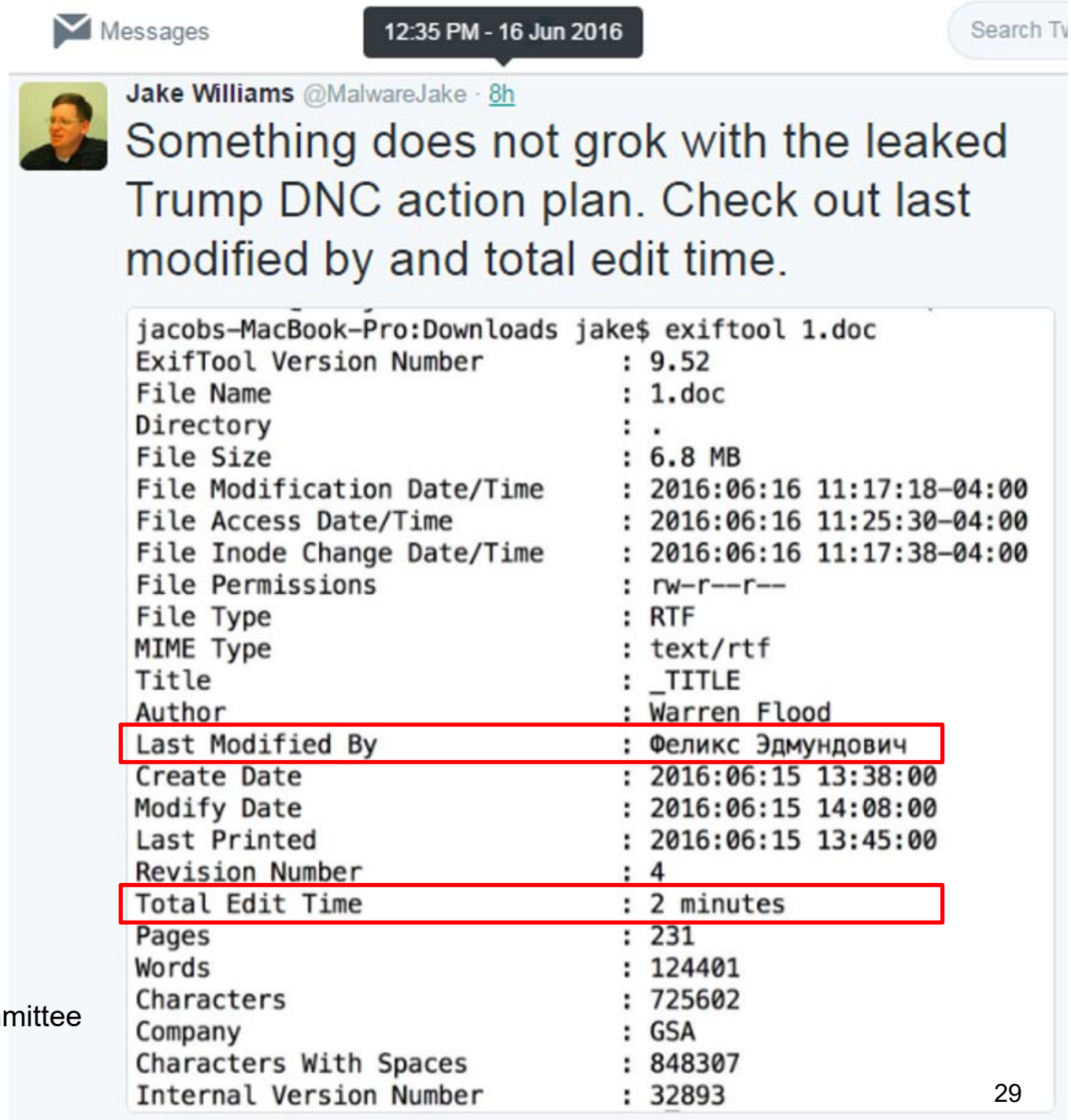
EXIF - Exchangeable Image File Format

Got Photos?

GPS-encoded location: 39° 46' 57"N, 84° 4' 57"W
Map center: 39° 46' 57"N, 84° 4' 57"W
Display area: 1.19 km × 413 m
Distance between: 0 m

Click on map to measure distance from GPS-encoded location

Works On Most Files



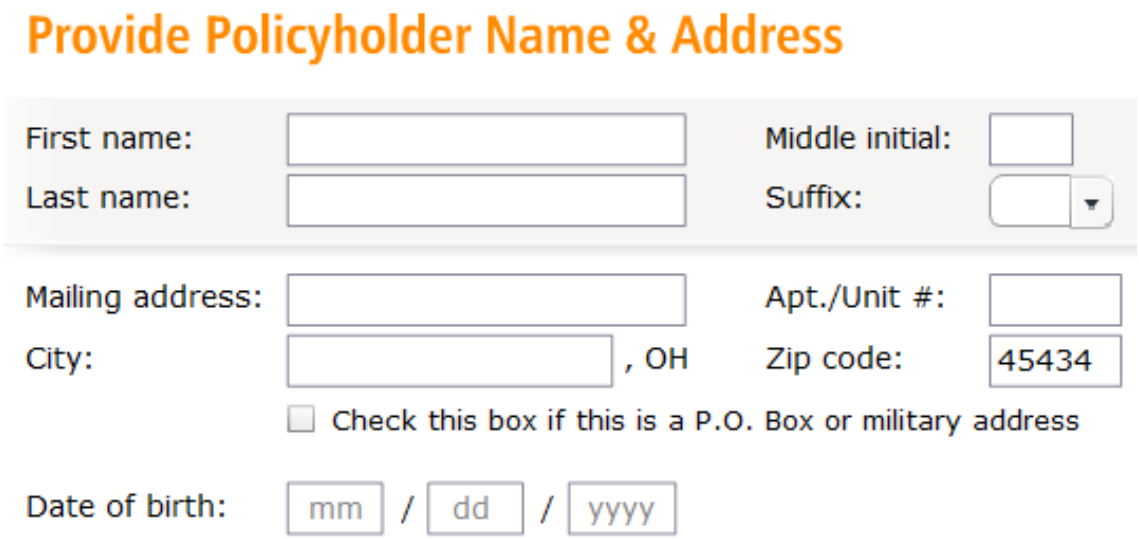
DNC: Democratic National Committee

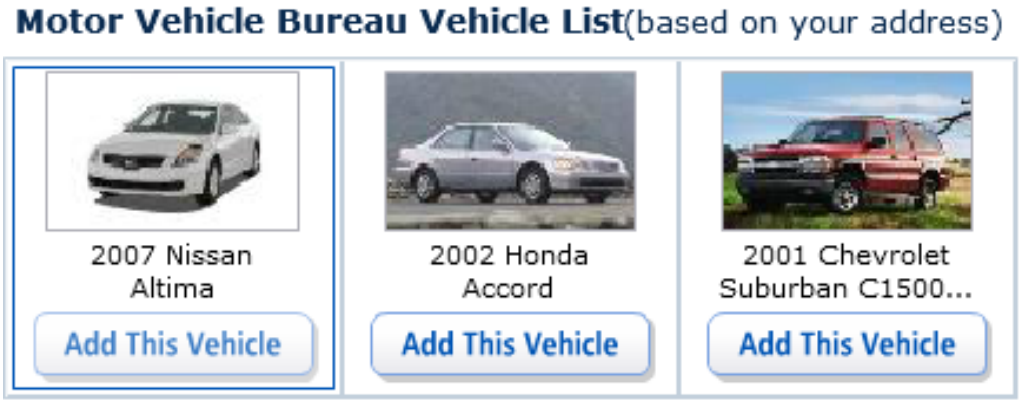
More Sources

- Now you have employee names…
  - Where do they live?
  - What are their spouse's name?
  - Where do they vote?
  - How much did they pay for their property?
  - What does their property look like?
- County Assessor's / Auditor's Office
  - apps.co.greene.oh.us/auditor/ureca/default.aspx
  - Real estate records with current estimated value
  - www.zillow.com – just property values
- Search for a person including previous addresses and relatives
  - www.peoplefinders.com
  - www.zabasearch.com
  - www.intellus.com

Vehicles

- We now have an address …
- What vehicles do the targets own?
- www.progressive.com / www.nationwide.com
  - Enter any Name
  - Enter any Date of Birth



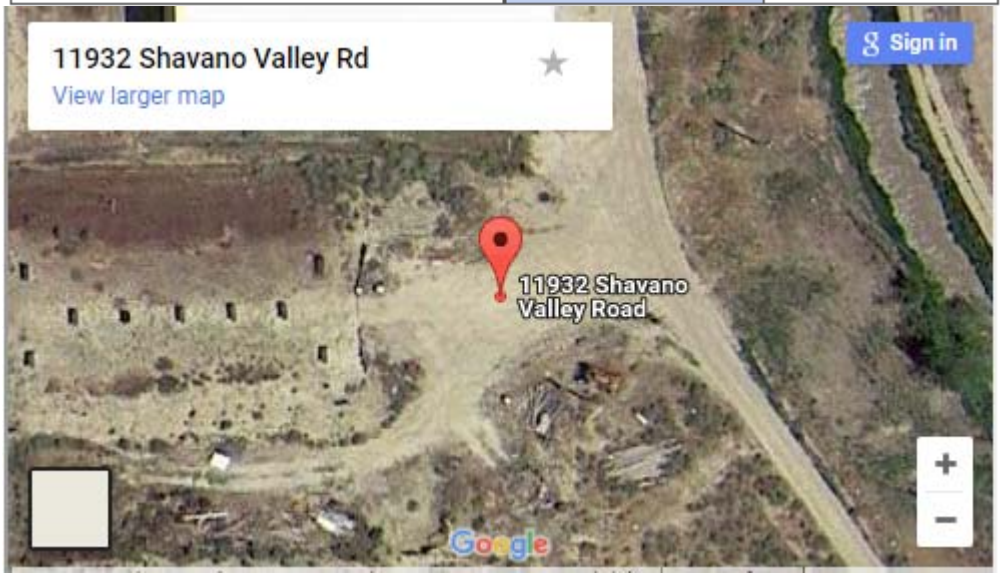


License Plates Reveal Data

- HAM radio vanity plates
  - www.radioqth.net/lookup

Operator Information for AA0CW

License Holder:	Call Data:	
Adams, James M 11932 Shavano Valley Road Montrose, CO 81403	Call Sign:	AA0CW
	Call Status:	Active
	Prev. Call Sign:	K0BAM
	FRN:	0019379361



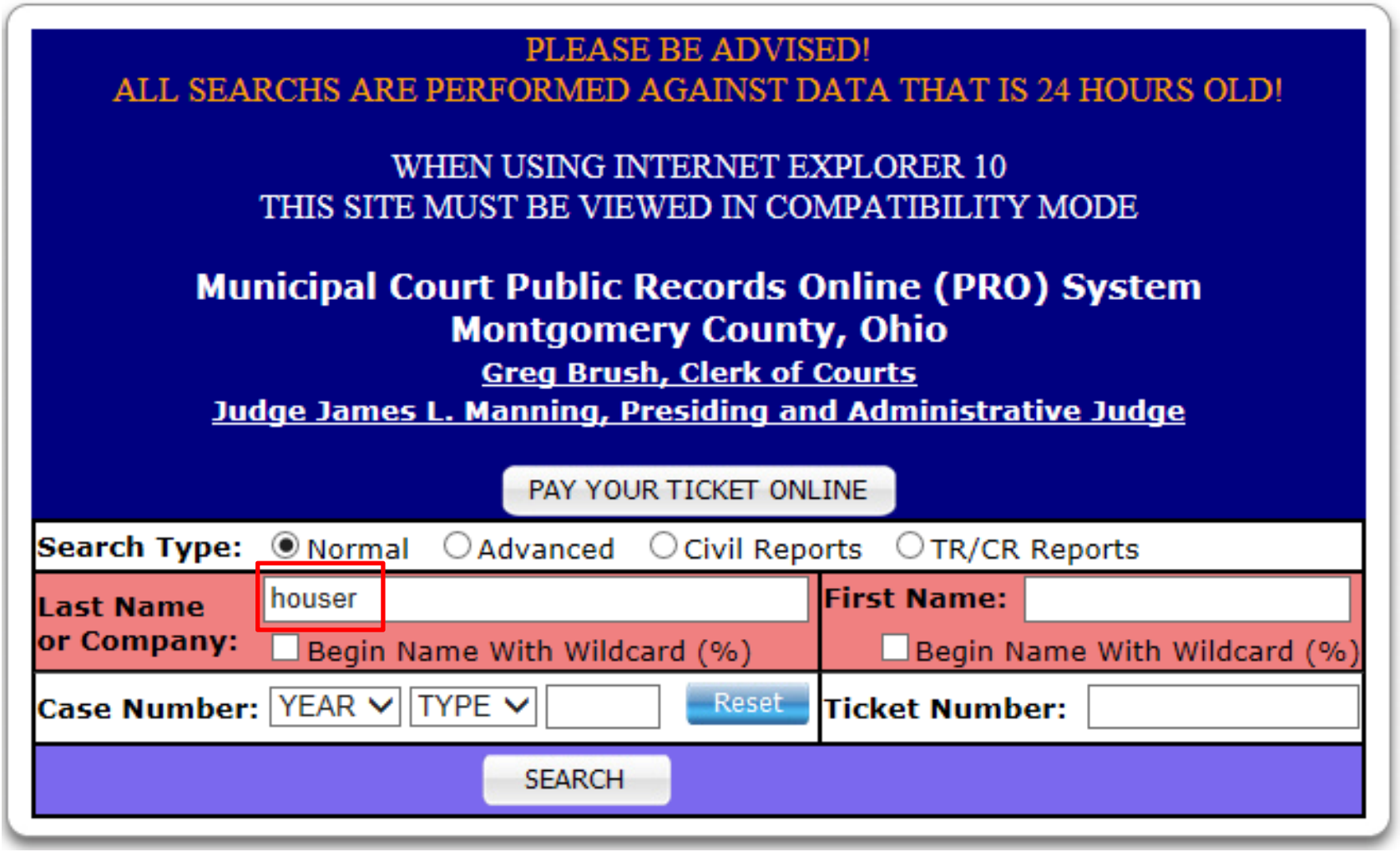
Please enter callsign:

Enter Callsign:

aa0cw Search

Court Records

- Google: Montgomery county municipal court public records
- www.clerk.co.montgomery.oh.us/pro/



Court Records

THE MUNICIPAL COURT OF MONTGOMERY COUNTY, OH
EASTERN DIVISION
CASE NUMBER 2005TRD05666

VIOLATOR INFORMATION

Name:	HOUSER [redacted]	Driver's License Held:	
DOB:	24 Nov 1955	DL Returned:	
Address:	6186 CHARLESGATE RD		
City/State/Zip:	HUBER HEIGHTS, OH 45424		

TICKET/COMPLAINANT INFORMATION

File Date:	21 Dec 2005	Officer:	Reckner, Michael
Ticket No:	64291	Agency:	Huber Heights
Violation Date:	20 Dec 2005	Arrest Date:	
Incident No:		Insurance:	Yes

VIOLATION INFORMATION

VIOLATION 1 **SPEED** **Degree: MM**

Code:	333.03	Bond Information:	
Speed:	42 IN A 25 ZONE	Plea:	Waiver 30 Dec 2005
Initial Court Date:	29 Dec 2005 01:12 PM		

DISPOSITION

Court Records

Fairborn Municipal Court

Information on traffic case number TRC 0900021A

Click for Docket Entries

Party Involved

Defendants Name: SMITH, [redacted]
A.K.A.:
Address: 1113 Pursell Ave
City/State/ZIP: Dayton, Oh 45420
Telephone #: Confidential
Social Security #: Confidential
# of Priors:
Warrant(s): None

Date of Birth: 05-20-1986
Race: White\Caucasian
Sex: Male
Eye Color: Blue
Height: 5'09"
Weight: 135 Pounds
Hair Color: Black

Complainant/Officer

Name: B Wisecup
Agency Code: State Of Ohio (Bpd)
Unit Number:

Violation Information

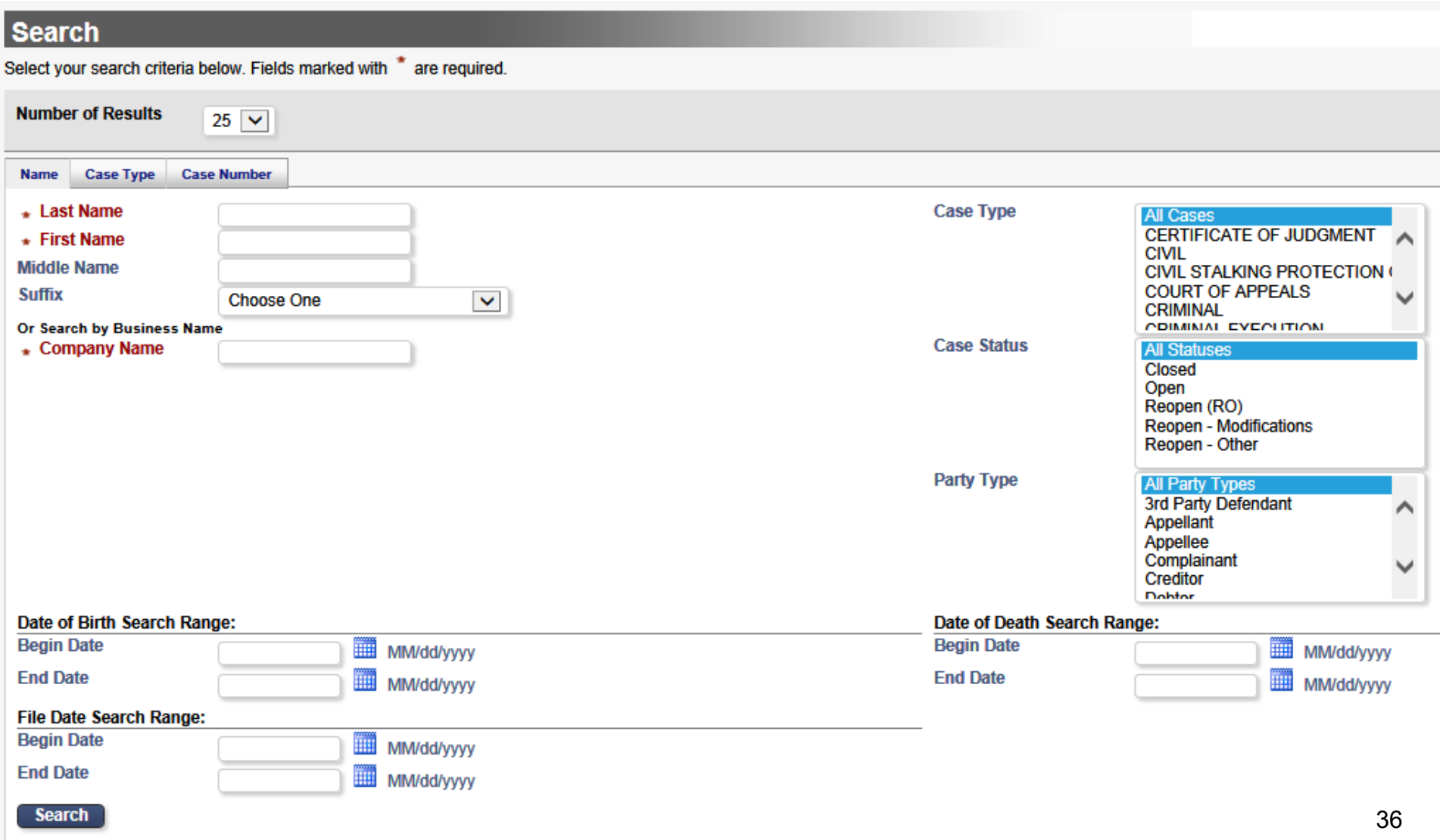
File Date: 01-02-2009
Ticket Number: A135531
Violation Date: 01-01-2009
Violation Time:
Violation Description: O.V.I/Under Inf

Section #: 4511.19A1H
Degree: 1st Degree Misdemeanor
Points:
BMV Offense Code: 02
Waive Amount:

http://www.fairbornmunicipalcourt.us/search.php

Court Records

- courts.co.greene.oh.us/eservices/home.page.2



Got info?

- If not, then just ask someone who has a lot!!!!

Google™

"I can't explain it – it's just a funny feeling that I'm being Googled."

Some of Google's Search Directives

- How can we restrict / refine Google's output?
- "site:"
  - Searches only a given domain
  - site:afit.edu ← restrict the search to only afit.edu
  - site:*.com:8088 ← which .com sites are listing on port 8088
- "link:"
  - Shows all sites linked to a given web page but exclude that site
  - link:www.afit.edu -site:afit.edu
- "intitle:"
  - Shows pages with titles that contain the search text
  - intitle:"index of" "parent directory"

- Can combine directives
  - site:usafa.edu intitle:index.of

Some of Google's Search Directives

- "cache:www.afit.edu"
  - Returns latest cached version
  - First 101 KB of HTML is loaded from Google
  - Images come from original web site (NOT Google's cache)
    - Your IP may show up in their logs
  - Clicking on a link will take you to the actual site
    - Your IP may show up in their logs
- To prevent Google from loading external references and display text only
  - Click Text-only version or
  - Take resulting Google URL and change: **`&strip=1`**
- Google also caches several file types such as
  - .doc, .xls, .ppt, .pdf, …

Wayback Machine

- www.archive.org → billions of cached webpages since 1996
- If you click on a link, you get the archived page, not the current page
  - More clandestine
  - One catch…

    Images still come from the original site

- Blocked on EDU and CDN networks
  - Try on another net
    - Home, Einstein's, etc.

Peabody & Sherman Set the WABAC Machine

Google Search Tips

- "**filetype:pdf**" or "**ext:**"
  - Searches only for files of a given type
  - Could search for active or vulnerable pages
    - asp, jsp, php or cgi extensions
  - Available remote desktop systems: **ext:rdp**
- "Test Page for the Apache Web Server"
- Add minus (-) to a search term to exclude pages with a given word
  - **site:edu "cyber attack tool list" -ppt**
- Combining directives together can yield very targeted results

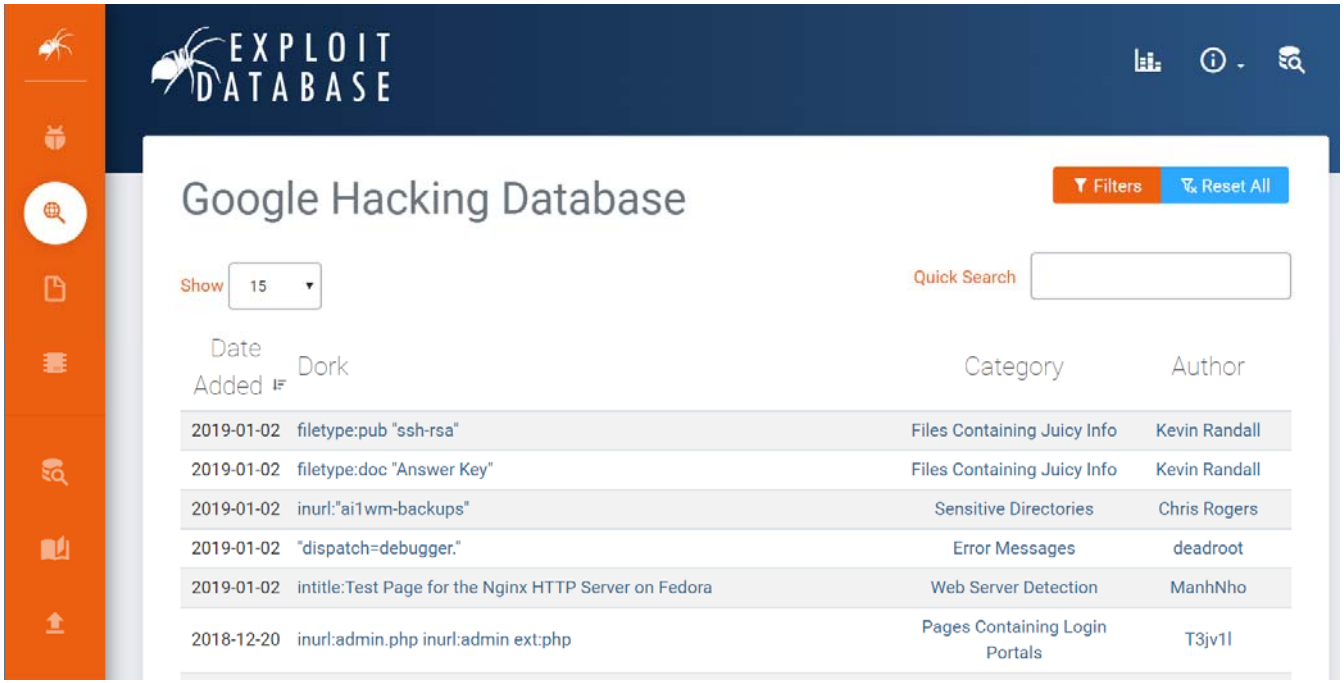
  site:www.bigbank.com filetype:xls ssn
- How about admin passwords?

"# -FrontPage-" filetype:pwd inurl:(service | authors| administrators | users)

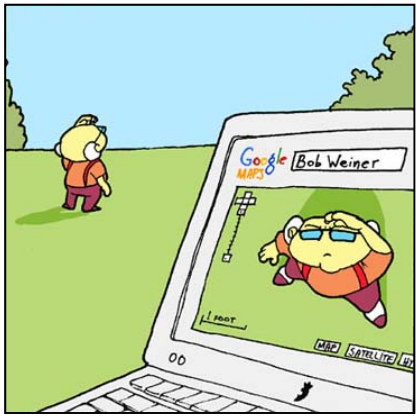
Google Resources

- Johnny "Ihackstuff" Long
  - http://www.hackersforcharity.org/
  - Created the Google Hacking DB

- www.exploit-db.com/google-hacking-database/
  - New home of the Google Hacking Database (GHDB)
    - A vast archive of Google searches to find vulnerable systems



Google Maps/Earth



www.kulfoto.com/interesting/660/the-top-15-most-extraordinary-google-street-views/9784/copenhagen-denmark

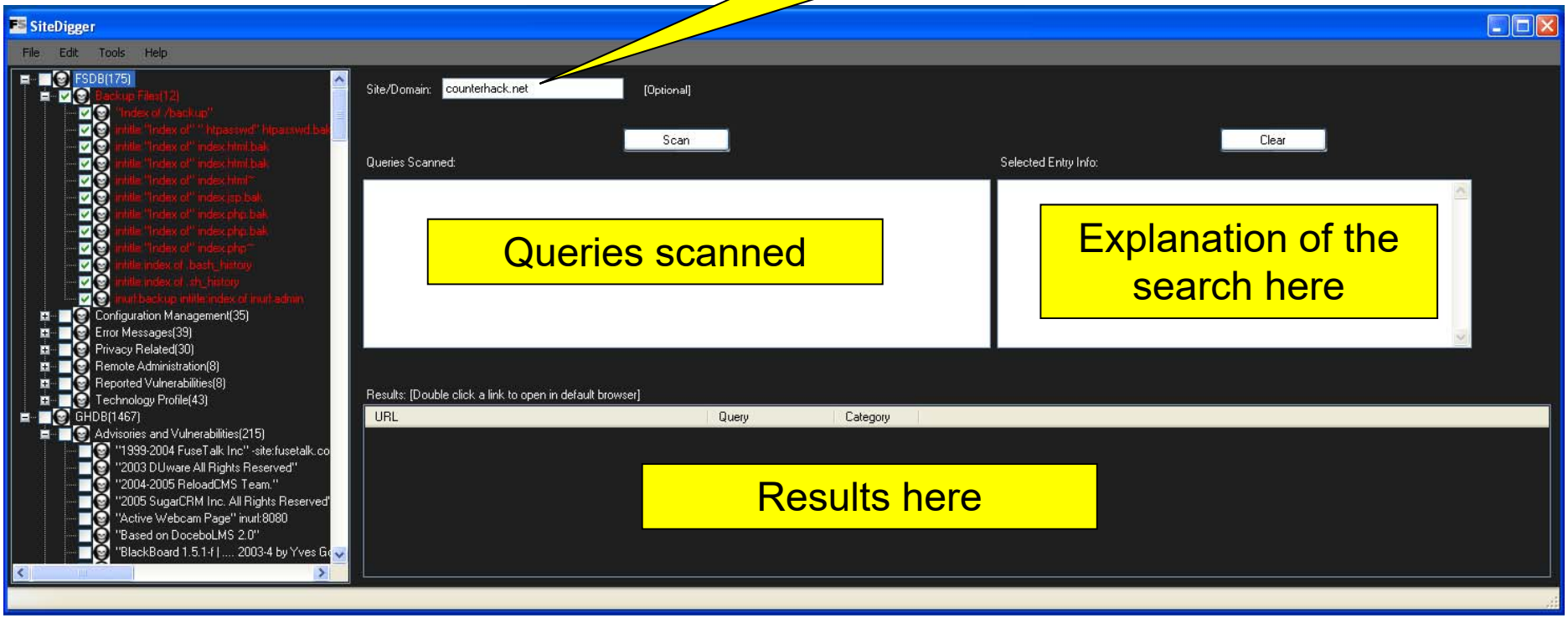
Automating Google Queries

- Typing all of these strings into Google is very labor-intensive
  - **`filetype:php inurl:wiki (inurl:"SystemInfo" | inurl:FindPage| inurl:HelpContents| inurl:RecentChanges)`**
  - Tools automate the process by searching through each vulnerability listed in the GHDB as well as other databases maintained by companies

- SiteDigger by Foundstone
  - https://sitedigger.apponic.com/

- Wikto (Nikto for Windows)
  - github.com/sensepost/wikto

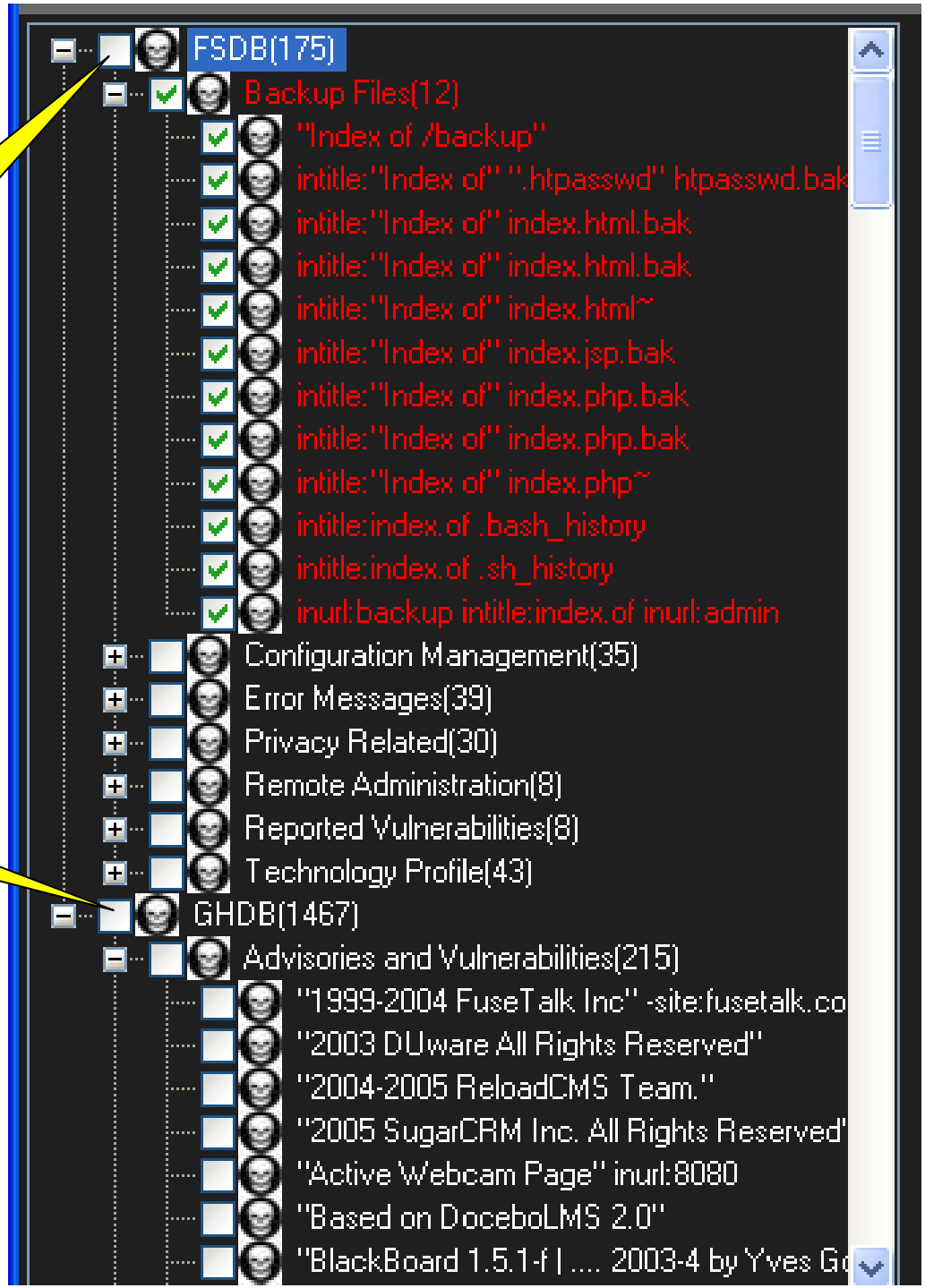
SiteDigger™ Example



SiteDigger™ Example

Foundstone DB

Google hacking DB



Google Query Example – 8 Apr 15

- **db.inc filetype:inc -backup_migrate -github.com**
  - There is a hit: **ninthwave.co.uk/p/flashdev/db.inc**

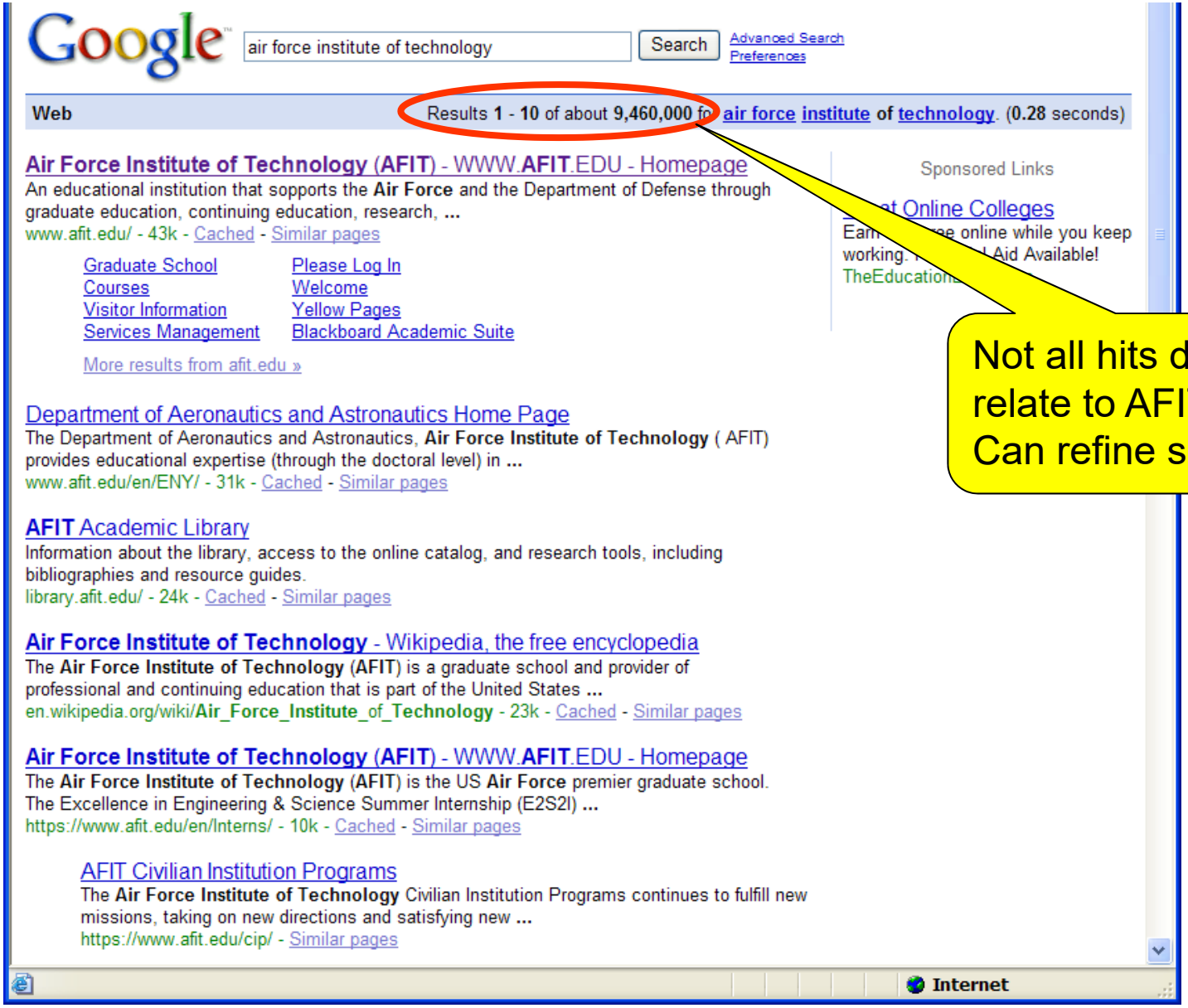
- Inspect the code

```
function dbcnx1() {
 include("../cfg.inc");
 $dbcnx1=@mysql_connect($serverName, $userName, $userPassword);
 if (!$dbcnx1) {
  exit("Can't connect to database");
```

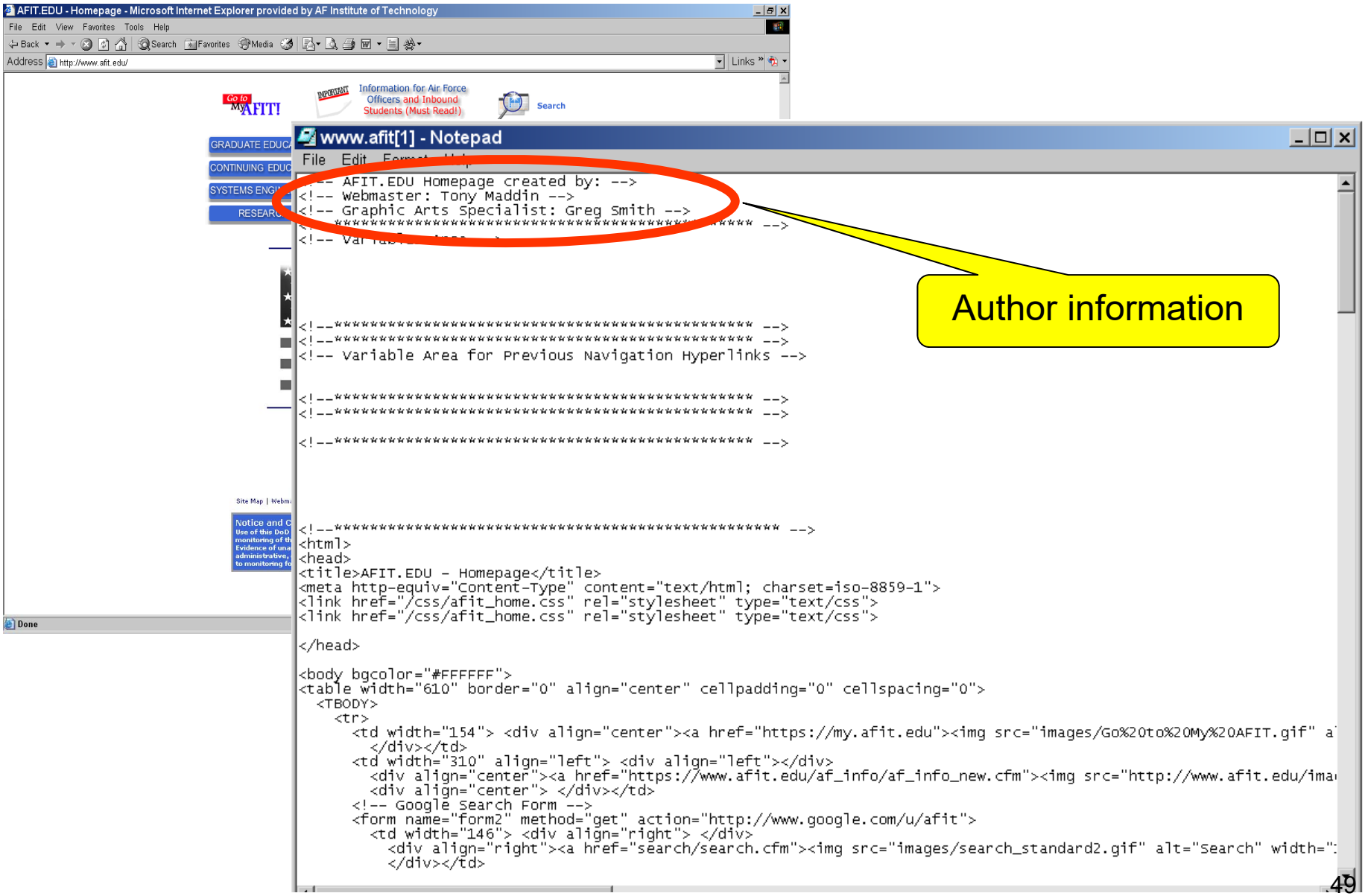
- Now grab **ninthwave.co.uk/p/flashdev/cfg.inc**

```
<?php
 $serverName = "chriscurddesign.co.uk";
 $userName = "ninthwave";
 $userPassword = "ninthwave1";
 $dbName = "ninthwavedb";
?>
```

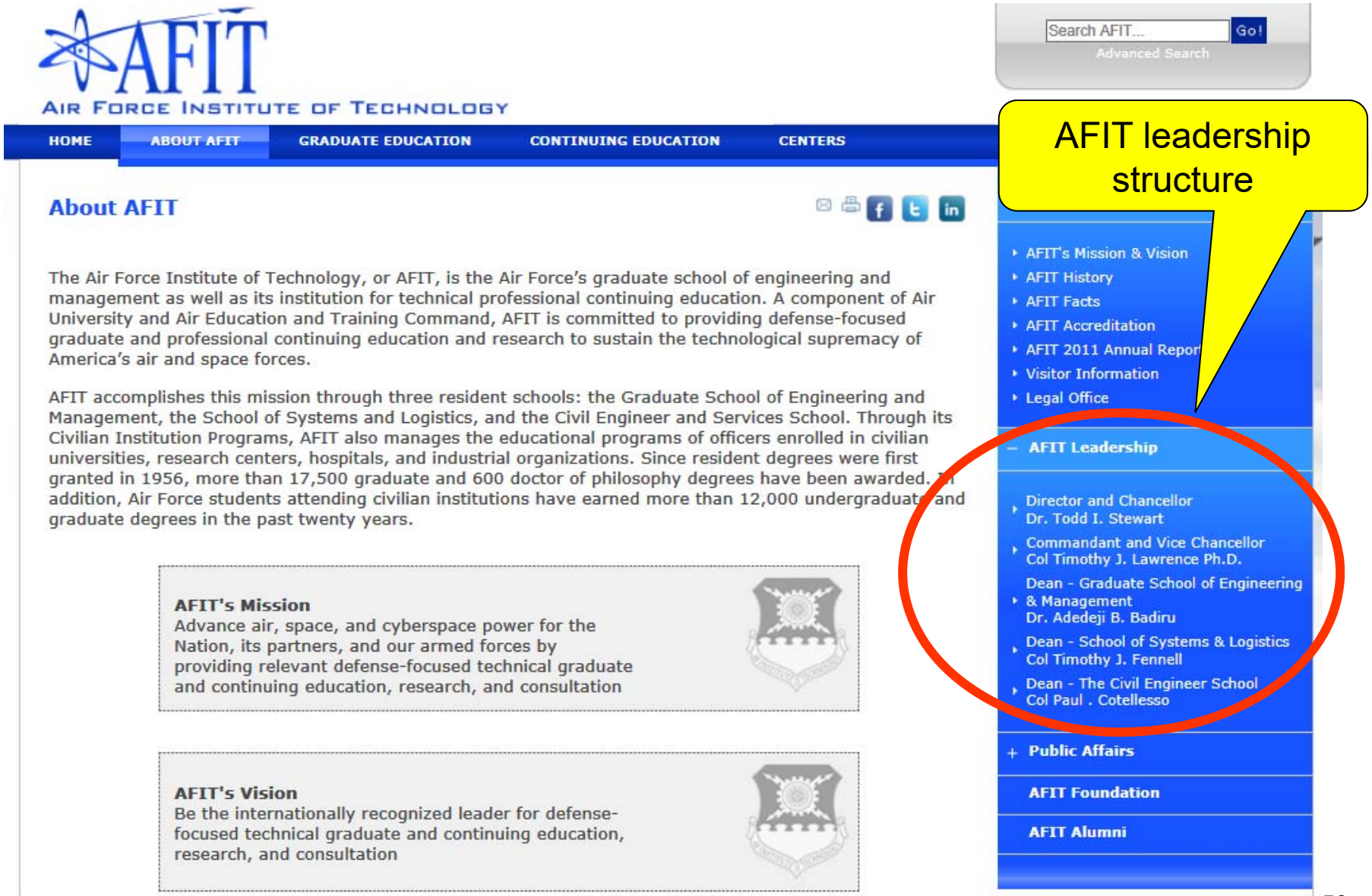
Reconnaissance Example



Reconnaissance Example



Reconnaissance Example



Shodan – www.shodan.io

John Matherly

- Search engine for specific types of devices
  - Routers, traffic controller systems, security cameras, home heating systems
  - Control systems for water parks, gas stations, water plants, power grids, nuclear power plants, …
  - Most have little to no security
  - www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools
    - Shodan Hacking Database – SHDB and many more!

Computer and Network Hacker Exploits

- **Step 1: Reconnaissance**
  - Low Tech Recon
  - STFW
  - Whois Databases
  - DNS
  - Recon Tools
- Step 2: Scanning
- Step 3: Gaining Access
  - Application and Operating System Attacks
  - Network Attacks
  - Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Whois Databases

- Network Enumeration
  - Identify domain names and networks related to target
- Internet Corporation for Assigned Names and Numbers (ICANN)
  - Controls IP address and domain name distribution
  - Domain names registered through hundreds of private companies (www.internic.net/alpha.html) accredited by ICANN
- Whois databases contain all of this information… and is accessible
  - Registrar
  - POCs for admin & technical
  - E-mail addresses
  - Registration dates
  - Name and address of company
  - Telephone numbers
  - Postal addresses
  - Name servers with IP addresses

How to Use Whois

- Many websites provide whois information
  - https://who.is has worked well for me

- Linux **whois** command

```
root@kali:~# whois mit.edu

Domain Name: MIT.EDU

Registrant:
   Massachusetts Institute of Technology
   77 Massachusetts Ave
   Cambridge, MA 02139
   UNITED STATES

Administrative Contact:
   Mark Silis
   Massachusetts Institute of Technology
```

Sample Whois (as of 7 Jan 15)

Domain Name: AFIT.EDU

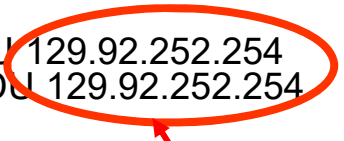
Registrant:
Air Force Institute of Technology
Bldg 642, Room 221
2950 Hobson Way
WPAFB, OH 45433-7765
UNITED STATES

Administrative Contact:
Lori L Gilbert
AFIT Administrative Group
Air Force Institute of Technology
AFIT/SCOS
2950 Hobson Way, Bldg 642, Room 221
Wright-Patterson AFB, OH 45433-7765
UNITED STATES
(937) 255-6565 x4252
afit.domainregadmin@afit.edu

Technical Contact:
Paul A Bergeron
AFIT Technical Group
Air Force Insitutue of Technology
AFIT/SCOI
2950 Hobson Way, Bldg 642, Room 223
Wright-Patterson AFB, OH 45433-7765
UNITED STATES
(937) 255-6565 x4231
afit.domainregtech@afit.edu

Name Servers:
GOLDILOCKS.AFIT.EDU 129.92.252.254
GOLDILOCKS1.AFIT.EDU 129.92.252.254

Domain record activated: 02-Mar-1999
Domain record last updated: 05-Jul-2012
Domain expires: 31-Jul-2015



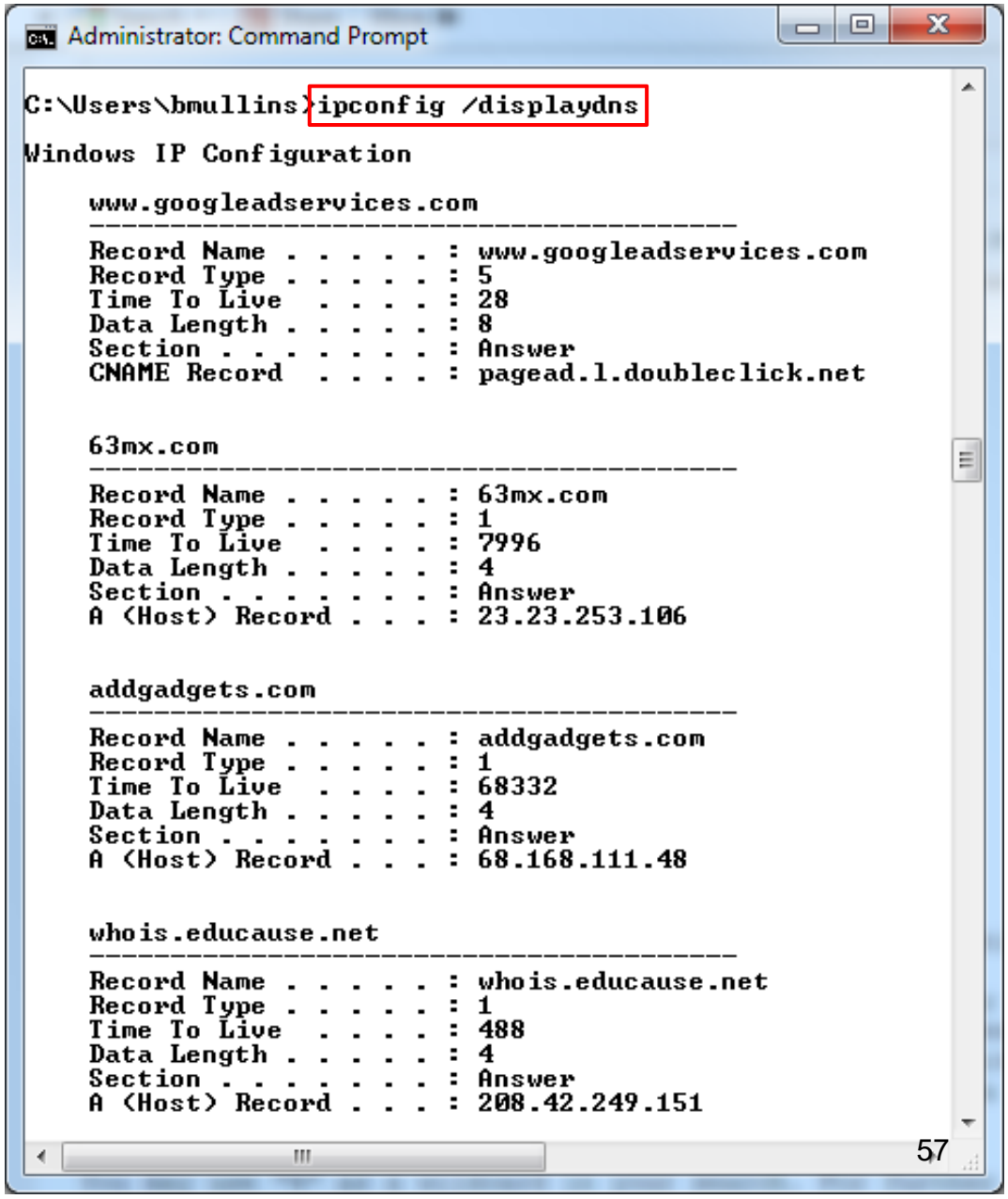
Attacker will now query those DNS servers to get more target info

Computer and Network Hacker Exploits

- **Step 1: Reconnaissance**
  - Low Tech Recon
  - STFW
  - Whois Databases
  - DNS
  - Recon Tools
- Step 2: Scanning
- Step 3: Gaining Access
  - Application and Operating System Attacks
  - Network Attacks
  - Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

DNS Lookup

- Domain Name System (DNS)
- We use a cache at the client and the local name server
- **`ipconfig /displaydns`**



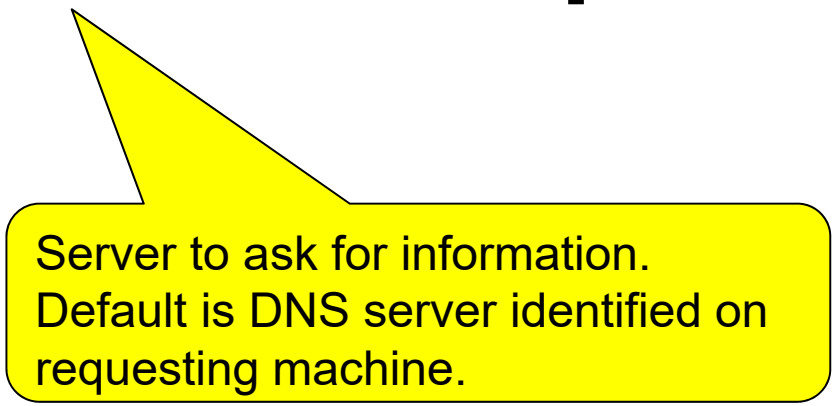
DNS Lookup

- DNS is also full of useful info including numerous IP addresses
- Linux:
  - **# dig @[DNS_server_IP] [target_domain] type**

```
root@kali:~# dig afit.edu any

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> afit.edu any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40811
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 4

;; QUESTION SECTION:
;afit.edu.                      IN      ANY

;; ANSWER SECTION:
afit.edu.               2994    IN      A       129.92.252.254
afit.edu.               3135    IN      NS      goldilocks1.afit.edu.
afit.edu.               3135    IN      NS      goldilocks.afit.edu.
afit.edu.               2994    IN      SOA     swa-afit-02.afit.edu. hostmaster.swa-afit-02.afit.edu.
afit.edu.               2994    IN      MX      10 mr-afit-03.afit.edu.
afit.edu.               2994    IN      MX      10 mr-afit-02.afit.edu.
afit.edu.               2994    IN      TXT     "v=spf1 mx ip4:129.92.253.248 ip4:129.92.253.249 -all"

;; ADDITIONAL SECTION:
goldilocks1.afit.edu.   2615    IN      A       129.92.252.254
goldilocks.afit.edu.    2615    IN      A       129.92.252.254
mr-afit-03.afit.edu.    2994    IN      A       129.92.253.249
mr-afit-02.afit.edu.    2994    IN      A       129.92.253.248
```

DNS Zone Transfer in Windows

- Ask a name server to send all information about a domain
  - Legit purpose is to replicate the database across DNS servers
- Try it:
  - **C:\> nslookup**
  - **> server [authoritative_server IP or name]**
  - **> set type=any**
  - **> [target_domain]**

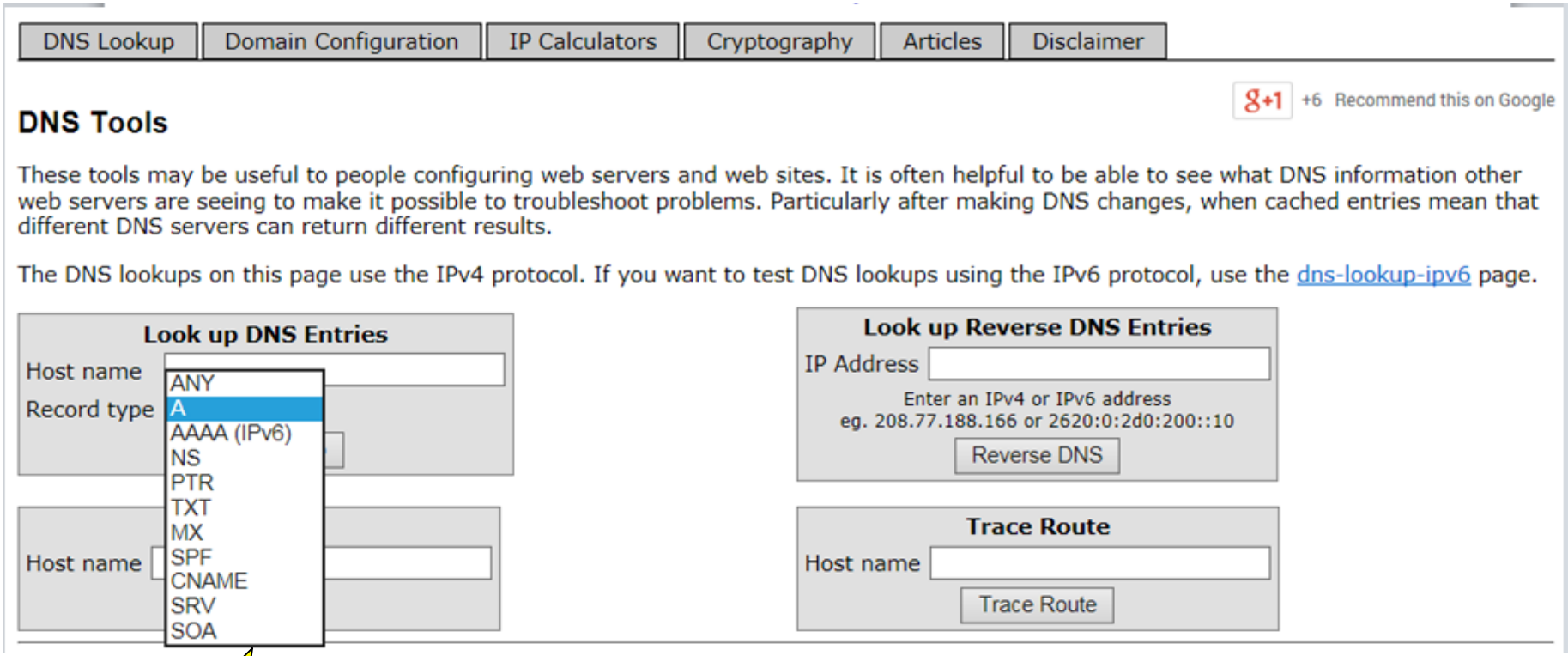


DNS Interrogation

```
C:\Users\Barry>nslookup
Default Server:  dns-cac-lb-01.rr.com
Address:  209.18.47.61

> google.com
Server:  dns-cac-lb-01.rr.com
Address:  209.18.47.61

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:4009:803::1006
          173.194.46.104
          173.194.46.105
          173.194.46.110
          173.194.46.96
          173.194.46.97
          173.194.46.98
          173.194.46.99
          173.194.46.100
          173.194.46.101
          173.194.46.102
          173.194.46.103

> set type=any
> google.com
Server:  dns-cac-lb-01.rr.com
Address:  209.18.47.61

Non-authoritative answer:
google.com      MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
google.com      MX preference = 30, mail exchanger = alt2.aspmx.l.google.com
google.com      MX preference = 40, mail exchanger = alt3.aspmx.l.google.com
google.com      MX preference = 50, mail exchanger = alt4.aspmx.l.google.com
google.com      MX preference = 10, mail exchanger = aspmx.l.google.com
google.com      AAAA IPv6 address = 2607:f8b0:4009:800::1001
google.com      internet address = 74.125.225.35
google.com      internet address = 74.125.225.36
google.com      internet address = 74.125.225.37
google.com      internet address = 74.125.225.38
google.com      internet address = 74.125.225.39
google.com      internet address = 74.125.225.40
google.com      internet address = 74.125.225.41
google.com      internet address = 74.125.225.46
google.com      internet address = 74.125.225.32
google.com      internet address = 74.125.225.33
google.com      internet address = 74.125.225.34
google.com      nameserver = ns4.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns3.google.com
>
```

Web-based DNS Lookups

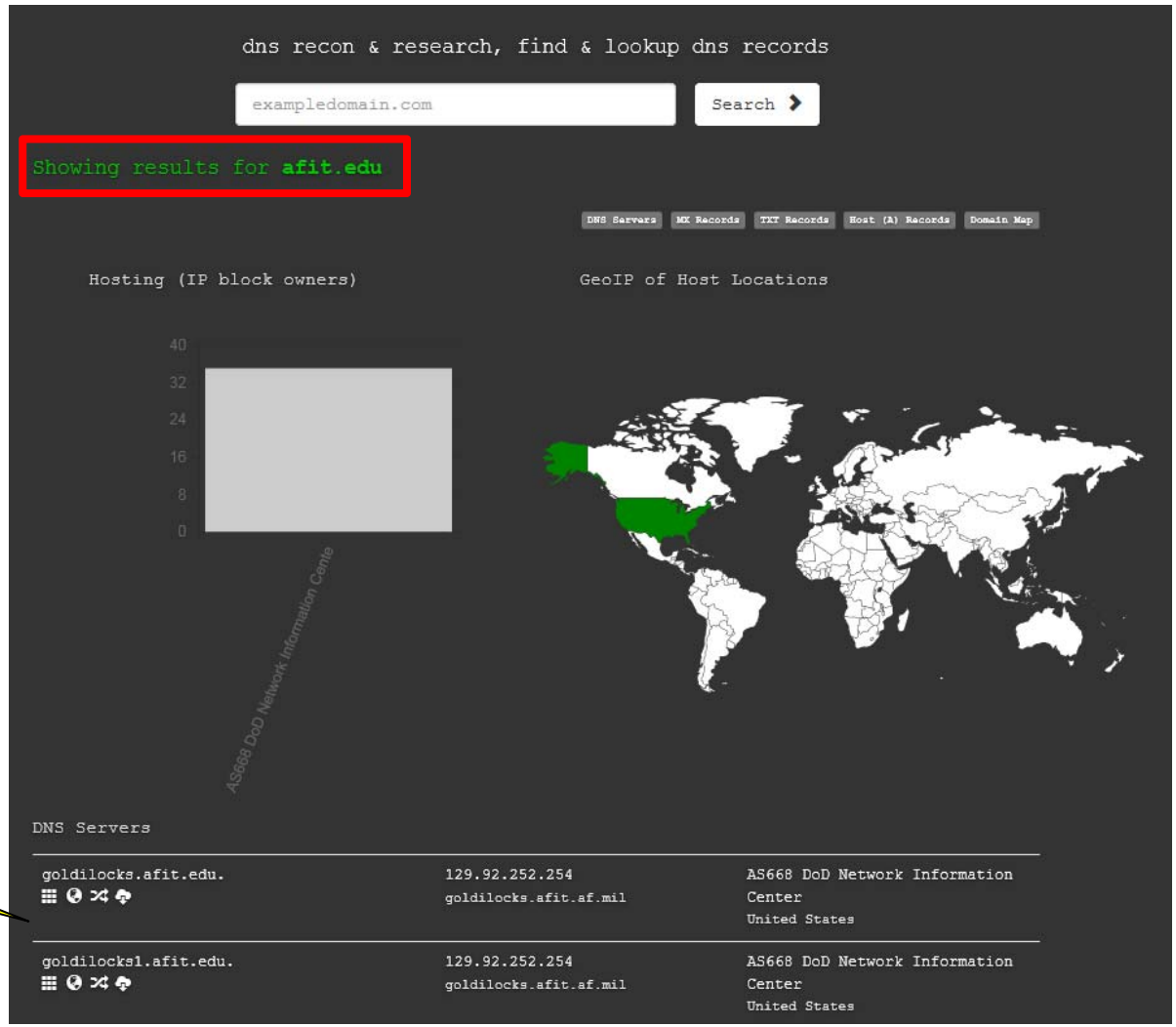
- Can use a website to do DNS lookup
  - www.webdnstools.com/dnstools/dns-lookup



Look at all those options!

Web-based DNS Lookups

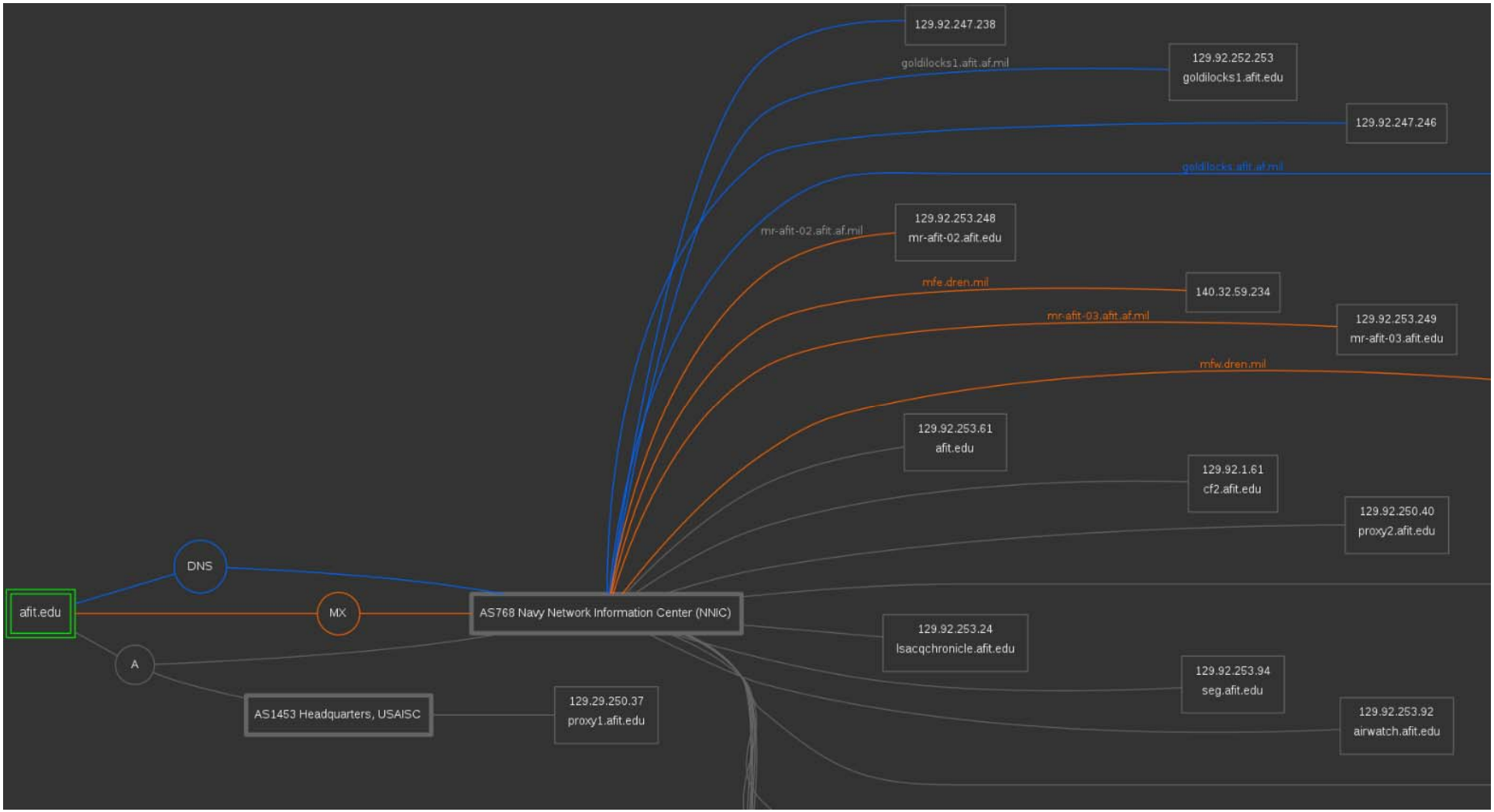
- dnsdumpster.com
  - Powered by data collected by scans.io (Internet-Wide Scan Data Repository)
  - Provides much more than just DNS records



2 DNS servers
2 MX records
31 host records

Web-based DNS Lookups

- dnsdumpster.com



Web-based DNS Lookups

- dnsdumpster.com
  - Traceroute from website to target


```
Start: Thu May  7 06:16:49 2015
HOST: htapi                                    Loss%   Snt   Last
  1.|-- router2-nac.linode.com                   0.0%     4    0.5
  2.|-- 207.99.53.45                             0.0%     4    0.3
  3.|-- 0.e1-2.tbr2.ewr.nac.net                  0.0%     4    1.1
  4.|-- nyk-b2-link.telia.net                    0.0%     4   30.2
  5.|-- nyk-bb1-link.telia.net                   0.0%     4    1.4
  6.|-- nyk-b5-link.telia.net                    0.0%     4    1.7
  7.|-- qwest-ic-152399-nyk-b5.c.telia.net       0.0%     4    1.5
  8.|-- ???                                     100.0     4    0.0
  9.|-- 63.148.64.222                           75.0%     4    8.0
 10.|-- int-0-0-2-xe.equinix-iad.core.dren.net   0.0%     4    7.6
 11.|-- int-1-1-5-nd.equinix-iad.core.dren.net  25.0%     4    7.9
 12.|-- np-5-1-1-nd.wpafb.core.dren.net          0.0%     4   31.6
 13.|-- 140.6.9.66                              0.0%     4   31.5
 14.|-- ???                                     100.0     4    0.0
```

Network Reconnaissance

- Network Reconnaissance
  - Try to determine the network topology
  - Try to determine potential access paths into the network

- Traceroute
  - Windows command → **`tracert`**
  - Diagnostic tool to view the route an IP packet follows from one host to the next moving from source to destination
  - Uses IP time-to-live (TTL) field as a hop counter

Tracert in use

```
C:\Users\Barry>tracert google.com

Tracing route to google.com [74.125.225.67]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3    17 ms     9 ms    16 ms  be21-1058.dytnoh5501r.midwest.rr.com [184.59.244
.228]
  4    26 ms    42 ms    20 ms  cpe-65-29-34-70.wi.res.rr.com [65.29.34.70]
  5    32 ms    55 ms    18 ms  be28.clevohek01r.midwest.rr.com [65.29.1.46]
  6    27 ms    33 ms    38 ms  107.14.19.58
  7    71 ms    62 ms    37 ms  ae-1-0.pr0.dca10.tbone.rr.com [66.109.6.165]
  8     *        *        *     Request timed out.
  9    67 ms    64 ms    52 ms  209.85.252.46
 10    49 ms    55 ms    56 ms  72.14.236.98
 11    42 ms    39 ms    96 ms  72.14.232.73
 12    54 ms    59 ms    58 ms  72.14.237.131
 13    44 ms    67 ms    48 ms  209.85.250.30
 14    46 ms    47 ms    57 ms  ord08s07-in-f3.1e100.net [74.125.225.67]

Trace complete.
```

Computer and Network Hacker Exploits

- **Step 1: Reconnaissance**
  - Low Tech Recon
  - STFW
  - Whois Databases
  - DNS
  - Recon Tools
- Step 2: Scanning
- Step 3: Gaining Access
  - Application and Operating System Attacks
  - Network Attacks
  - Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Wget

- Command line tool to retrieve files using HTTP, HTTPS and FTP
  - Website scanner and site mirroring tool
- Crawl website
  - **`C:\tools\wget\wget -m www.afit.edu`**
  - Create a local mirror of the website called www.afit.edu
  - Search mirrored website at your leisure for keywords and information that may not be exposed to the Internet
    - Hidden form elements, e-mail addresses, passwords
  - Create a dictionary of unique words found on the website
    - Use the dictionary for password cracking
- **Often** used in malware to download malicious code/scripts
- Built into Kali or download at: **`ftp.gnu.org/gnu/wget/`**

Create a mirror of the site

Wget

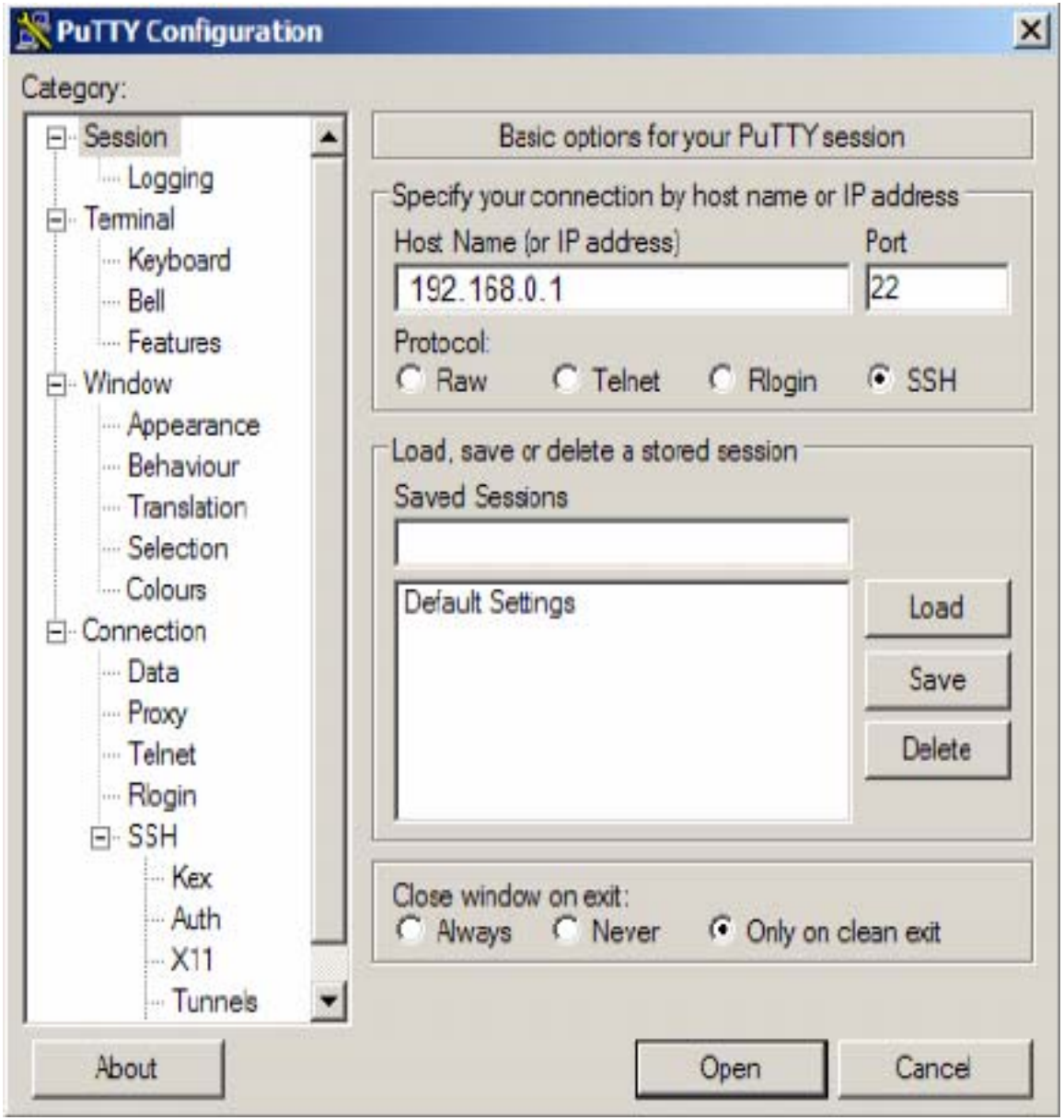
```
root@kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@kali:~# pwd
/root
root@kali:~# wget -m www.mit.edu
--2017-01-05 16:22:50--  http://www.mit.edu/
Resolving www.mit.edu (www.mit.edu)... 184.85.255.170, 2600:1408:10:197::2
Connecting to www.mit.edu (www.mit.edu)|184.85.255.170|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19318 (19K) [text/html]
Saving to: 'www.mit.edu/index.html'
```

<<snip>>

```
FINISHED --2017-01-05 16:22:54--
Total wall clock time: 3.6s
Downloaded: 32 files, 1.4M in 1.6s (919 KB/s)
root@kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  www.mit.edu
root@kali:~# cd www.mit.edu
root@kali:~/www.mit.edu# ls
files  index.html  robots.txt
root@kali:~/www.mit.edu# cat index.html
<!DOCTYPE html>
```

Establishing SSH Sessions

- Use SSH (Putty) to log into an SSH (Secure Shell) Server
- Enter the server's IP address
- Click on "Open" button
- Select "Yes" if you get a PuTTY Security Alert
- Putty will open a DOS window
- You will be asked for a username (root) and password
  - Guess root's password
  - Unless you know it



http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Web-based Recon Tools and Attack Portals

- Enormous number of web-based recon tools available
- Insert target name or IP, click and recon is done for you from the website (not your machine!)
  - Website's IP shows up in logs
- Some sites can even attack your target for you
  - www.network-tools.com
  - www.dnsstuff.com
  - www.traceroute.org
  - www.securityspace.com (commercial—free trial available)
  - www.all-nettools.com/toolbox
  - privacy.net/analyze/

Assignment

- Watch the slide show "Killing with Keyboards" on the shared drive

- Watch the short clip at
  - www.aclu.org/sites/default/files/pizza/images/screen.swf

Assignment

- Watch the video "Watch hackers break into the US power grid"

Your Targets' Skills Vary