2.1 FOOTPRINTING CONCEPTS

- Footprinting
- Types of Information
- Information Sources
- Passive Footprinting/OSINT
- Active Footprinting

WHAT IS FOOTPRINTING?

- Footprinting is the first step in reconnaissance
  - The attacker looks for tracks and traces the target leaves about itself on the Internet
  - Collect as much information as possible
- Value of footprinting:
  - Gain knowledge of the target's overall security posture
  - Create a "bird's eye" view of the target
    - Physical/facility vulnerabilities
    - High-level network map
    - Potential target areas to attack
    - Potential human targets to engage
  - Information that may not seem immediately useful may gain relevance later

TYPES OF INFORMATION TO GATHER

Search for anything that might help you gain access to the target's network:

- General company information
  - Company mission, products, services, activities, location, contact information
- Employee information
  - Email addresses, contact information, job roles
- Internet presence
  - Domain names, website content, online services offered, IP addresses, network reachability
  - Leaked documents and login information
- Overall security posture
- Technologies used
- Industry and market information
  - Company profile, assets, financial information, competitors

FOOTPRINTING INFORMATION SOURCES

- Company website(s)
- Whois
- Search engines
- People searches
- Job boards
- Social networking / social media
- News articles and press releases
- Specialized OSINT tools

PASSIVE FOOTPRINTING / OSINT

- Open Source Intelligence
- Use the Internet/publicly available sources to gather information on a target
- Do not directly engage target

ACTIVE FOOTPRINTING

- Engage the target in seemingly innocuous ways
  - Use "normal" expected actions
  - Avoid arousing suspicion
- Interact with the target's public-facing servers
  - Query the organization's DNS server
  - Traceroute to the target network
  - Spider / mirror the target's website
  - Extract published document metadata
- Limited social engineering
  - Gather business cards
  - Chat with company representatives at trade shows and public events

FOOTPRINTING PROCESS

- If your target has a website, visit it for initial information
- Use search engines to obtain additional information about the target including news and press releases
  - Google, Yahoo, Bing, Ask, Baidu, DuckDuckGo, AOL Search
- Use search engine cached pages or Archive.org to see information no longer available
- Use OSINT tools to automate information gathering and find hidden information

FOOTPRINTING THROUGH SOCIAL ENGINEERING

- Collect names, job titles, personal information, contact information, email addresses, etc.
- Remember: at this stage you want to be subtle and go unnoticed
- Techniques include:
  - Casual face-to-face contact
    - Trade show or public event
  - Eavesdropping
  - Shoulder surfing
  - Dumpster diving
  - Impersonation on social networking sites

ALERTS AND UPDATE MONITORING

- Monitor website content for changes
- Set alerts to notify you of updates
- Alerts are usually sent via email or SMS
- To receive alerts, register on the website
  - Google Alerts
  - Yahoo Alerts
  - Twitter Alerts
  - Giga Alerts
- Some OSINT tools also offer monitoring and alerts

USING FOOTPRINTING RESULTS

- Analyze gathered information to determine your next moves
- Get a sense of the target's overall security posture
- Look for information that can be used in your next steps
- Devices that can get you into the network:
  - IP addresses to scan
  - Servers and services to vulnerability scan
  - Internet-attached IoT devices to compromise
- People to social engineer
    - Email addresses to phish
    - Phone numbers to call for impersonation
    - Names and job roles to target
- Locations for physical reconnaissance
  - Parking areas to scatter malicious USB sticks
  - Easily accessible areas to plant sniffing/snooping devices
  - Detect Wi-Fi signals

2.2 OSINT TOOLS

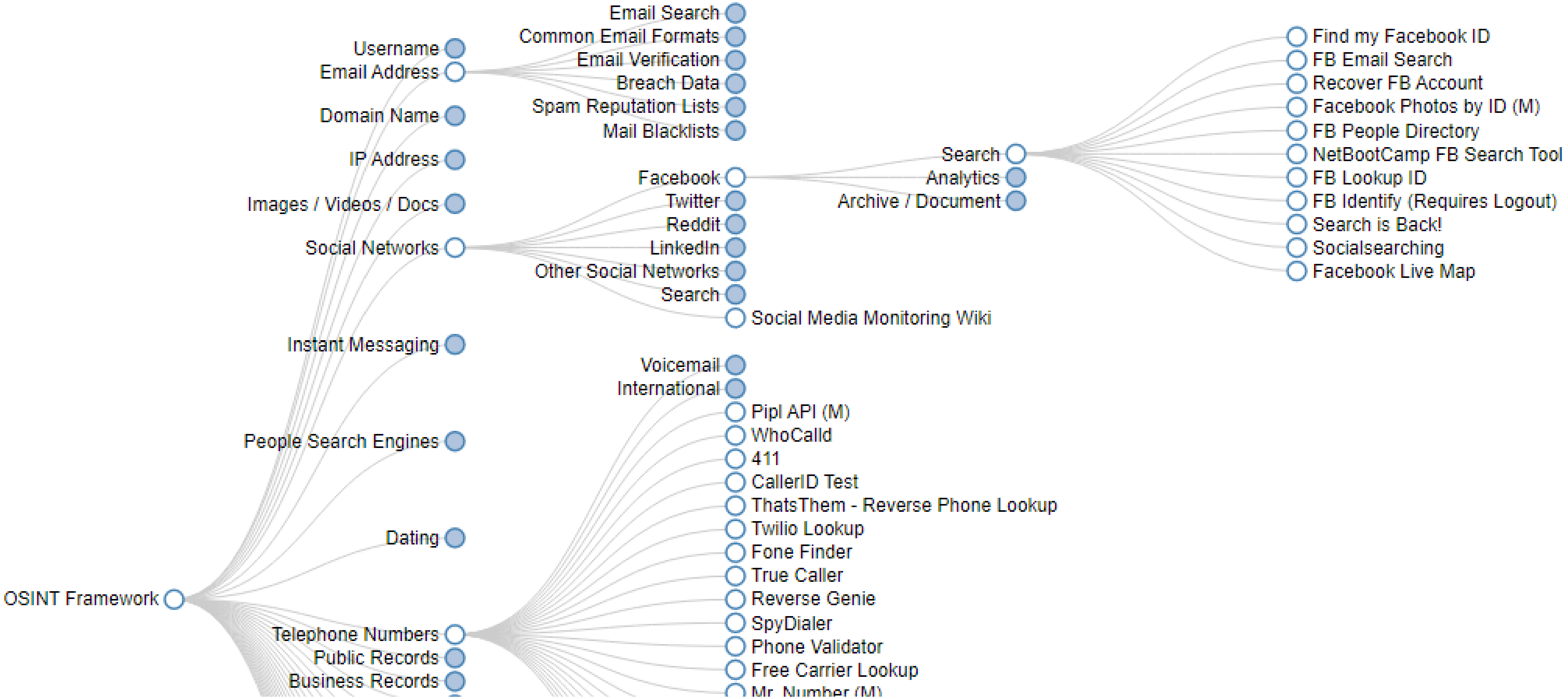
- Common Tools

OSINT FRAMEWORK

- A search engine that is also a cybersecurity framework
- Assembles information from publicly available sources
- Includes:
  - username, email address, contact information, language transition
  - public records, domain name, IP address, malicious file analysis,
  - threat intelligence and more

https://osintframework.com/

OSINT FRAMEWORK EXAMPLE

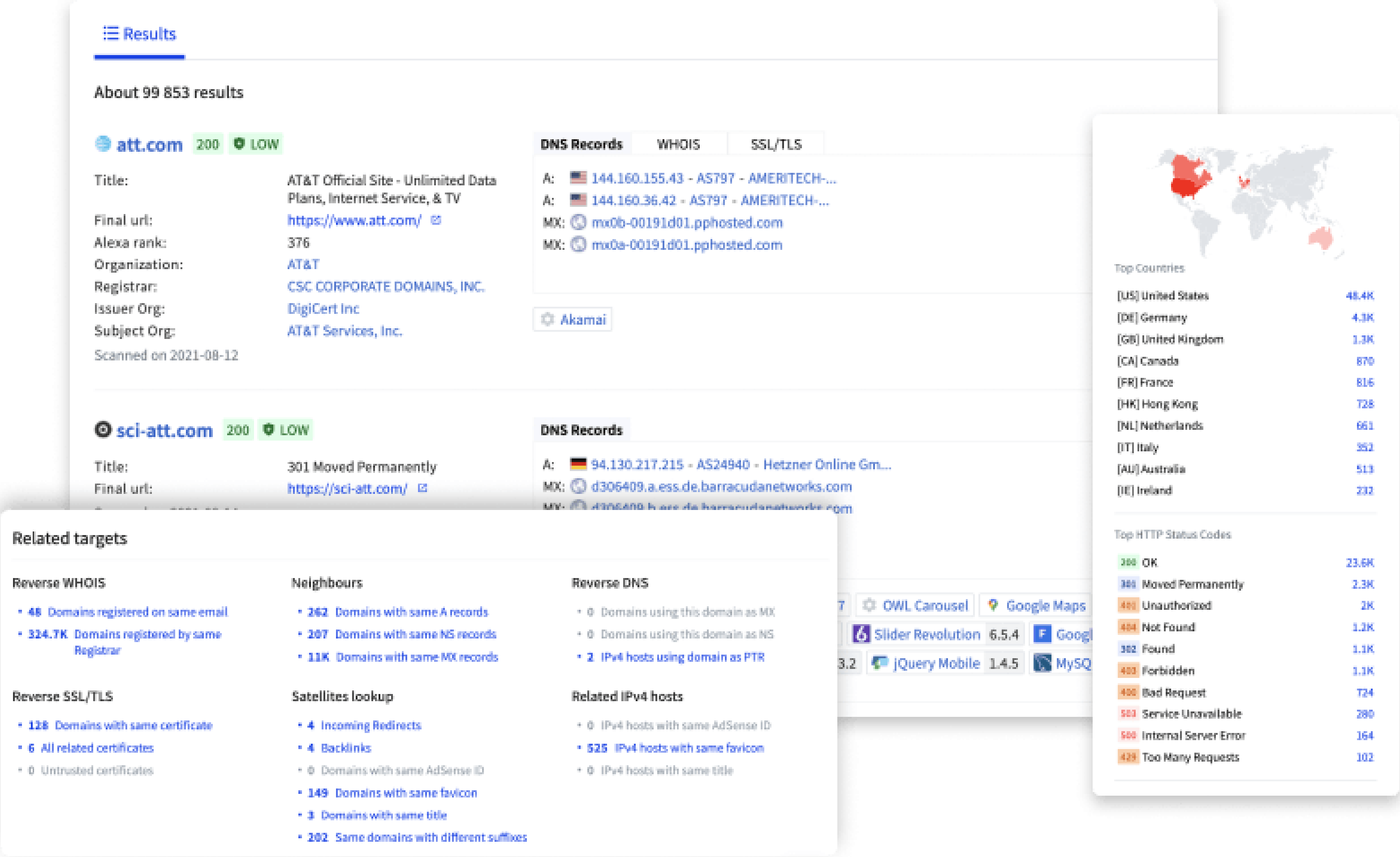


- OSINT Framework
  - Username
  - Email Address
    - Email Search
    - Common Email Formats
    - Email Verification
    - Breach Data
    - Spam Reputation Lists
    - Mail Blacklists
  - Domain Name
  - IP Address
  - Images / Videos / Docs
  - Social Networks
    - Facebook
      - Search
        - Find my Facebook ID
        - FB Email Search
        - Recover FB Account
        - Facebook Photos by ID (M)
        - FB People Directory
        - NetBootCamp FB Search Tool
        - FB Lookup ID
        - FB Identify (Requires Logout)
        - Search is Back!
        - Socialsearching
        - Facebook Live Map
      - Analytics
      - Archive / Document
    - Twitter
    - Reddit
    - LinkedIn
    - Other Social Networks
    - Search
    - Social Media Monitoring Wiki
  - Instant Messaging
  - People Search Engines
  - Dating
  - Telephone Numbers
    - Voicemail
    - International
    - Pipl API (M)
    - WhoCalld
    - 411
    - CallerID Test
    - ThatsThem - Reverse Phone Lookup
    - Twilio Lookup
    - Fone Finder
    - True Caller
    - Reverse Genie
    - SpyDialer
    - Phone Validator
    - Free Carrier Lookup
    - Mr. Number (M)
  - Public Records
  - Business Records

SPYSE

- Cyberspace search engine
- Combines several data gathering tools into a full-service online platform
- Users can get data directly from Spyse's web interface or their API
- Has free and paid features

SPYSE EXAMPLE



Results

About 99 853 results

att.com 200 LOW

Title:	AT&T Official Site - Unlimited Data Plans, Internet Service, & TV
Final url:	https://www.att.com/
Alexa rank:	376
Organization:	AT&T
Registrar:	CSC CORPORATE DOMAINS, INC.
Issuer Org:	DigiCert Inc
Subject Org:	AT&T Services, Inc.

Scanned on 2021-08-12

DNS Records | WHOIS | SSL/TLS

A: 144.160.155.43 - AS797 - AMERITECH-...
A: 144.160.36.42 - AS797 - AMERITECH-...
MX: mx0b-00191d01.pphosted.com
MX: mx0a-00191d01.pphosted.com

Akamai

sci-att.com 200 LOW

Title:	301 Moved Permanently
Final url:	https://sci-att.com/

DNS Records

A: 94.130.217.215 - AS24940 - Hetzner Online Gm...
MX: d306409.a.ess.de.barracudanetworks.com
MX: d306409.b.ess.de.barracudanetworks.com

OWL Carousel | Google Maps
Slider Revolution 6.5.4 | Googl
jQuery Mobile 1.4.5 | MySQ

Related targets

Reverse WHOIS

- 48 Domains registered on same email
- 324.7K Domains registered by same Registrar

Reverse SSL/TLS

- 128 Domains with same certificate
- 6 All related certificates
- 0 Untrusted certificates

Neighbours

- 262 Domains with same A records
- 207 Domains with same NS records
- 11K Domains with same MX records

Satellites lookup

- 4 Incoming Redirects
- 4 Backlinks
- 0 Domains with same AdSense ID
- 149 Domains with same favicon
- 3 Domains with same title
- 202 Same domains with different suffixes

Reverse DNS

- 0 Domains using this domain as MX
- 0 Domains using this domain as NS
- 2 IPv4 hosts using domain as PTR

Related IPv4 hosts

- 0 IPv4 hosts with same AdSense ID
- 525 IPv4 hosts with same favicon
- 0 IPv4 hosts with same title

Top Countries

[US] United States	48.4K
[DE] Germany	4.3K
[GB] United Kingdom	1.3K
[CA] Canada	870
[FR] France	816
[HK] Hong Kong	728
[NL] Netherlands	661
[IT] Italy	352
[AU] Australia	513
[IE] Ireland	232

Top HTTP Status Codes

200 OK	23.6K
301 Moved Permanently	2.3K
401 Unauthorized	2K
404 Not Found	1.2K
302 Found	1.1K
403 Forbidden	1.1K
400 Bad Request	724
503 Service Unavailable	280
500 Internal Server Error	164
429 Too Many Requests	102

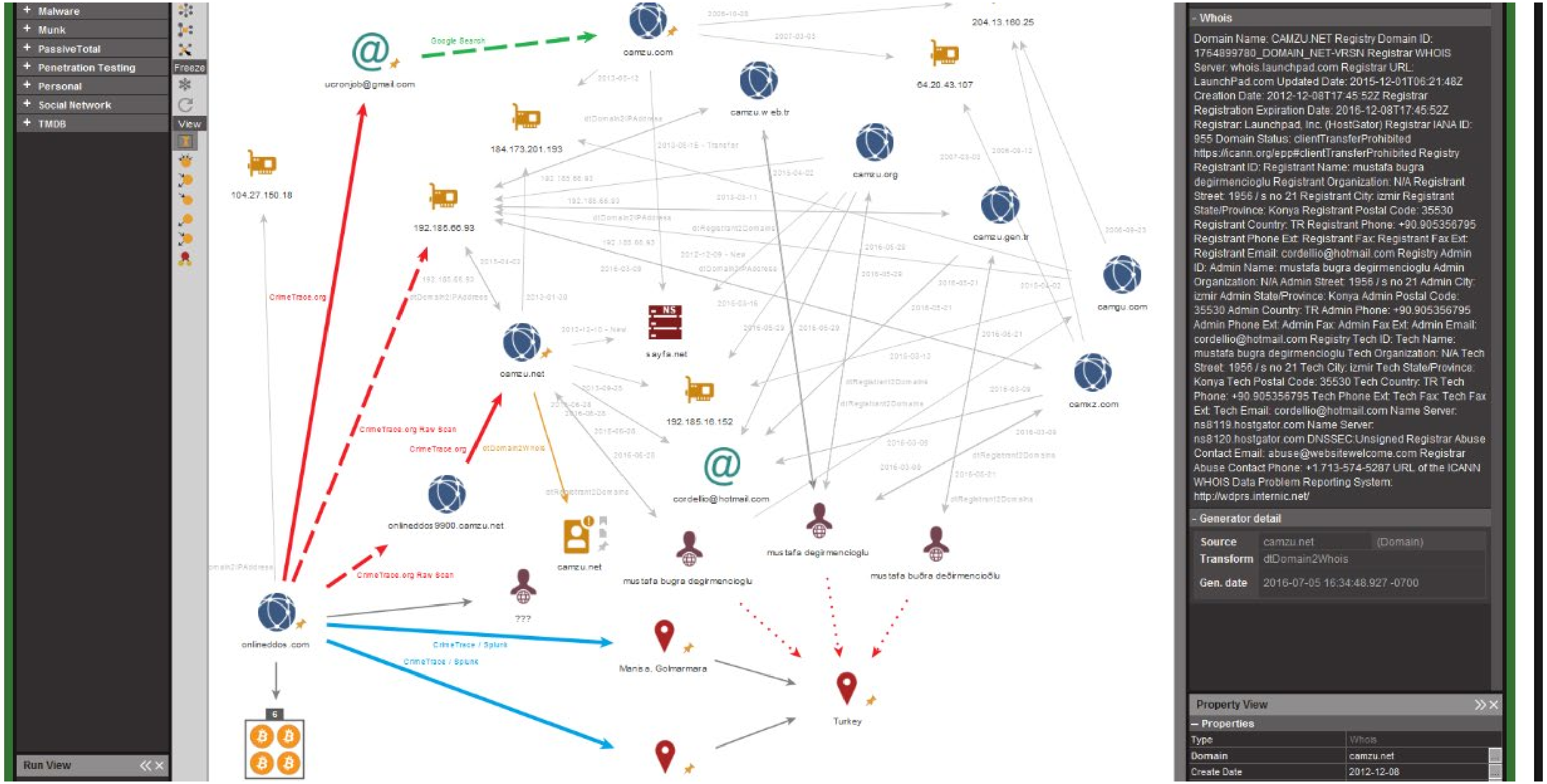
MALTEGO

- An open source intelligence and forensics application
- Use to mine, gather and visualize data and relationships in an easy-to-understand format
- Find relationships and links between people, groups, companies, organizations, websites, Internet infrastructure, phrases, documents, files, etc.
- Used by law enforcement to analyze social media accounts
  - Track profiles, understand social networks of influence, interests and groups

During the COVID-19 crisis Maltego was used to aid virus containment efforts:

- Scientific study of the virus spread
- Trace tourist/visitor movement from coronavirus hotspots to other locations

MALTEGO EXAMPLES



- Whois

Domain Name: CAMZU.NET Registry Domain ID: 1764899780_DOMAIN_NET-VRSN Registrar WHOIS Server: whois.launchpad.com Registrar URL: LaunchPad.com Updated Date: 2015-12-01T06:21:48Z Creation Date: 2012-12-08T17:45:52Z Registrar Registration Expiration Date: 2016-12-08T17:45:52Z Registrar: Launchpad, Inc. (HostGator) Registrar IANA ID: 955 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registry Registrant ID: Registrant Name: mustafa bugra degirmencioglu Registrant Organization: N/A Registrant Street: 1956 / s no 21 Registrant City: izmir Registrant State/Province: Konya Registrant Postal Code: 35530 Registrant Country: TR Registrant Phone: +90.905356795 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: cordellio@hotmail.com Registry Admin ID: Admin Name: mustafa bugra degirmencioglu Admin Organization: N/A Admin Street: 1956 / s no 21 Admin City: izmir Admin State/Province: Konya Admin Postal Code: 35530 Admin Country: TR Admin Phone: +90.905356795 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: cordellio@hotmail.com Registry Tech ID: Tech Name: mustafa bugra degirmencioglu Tech Organization: N/A Tech Street: 1956 / s no 21 Tech City: izmir Tech State/Province: Konya Tech Postal Code: 35530 Tech Country: TR Tech Phone: +90.905356795 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: cordellio@hotmail.com Name Server: ns8119.hostgator.com Name Server: ns8120.hostgator.com DNSSEC:Unsigned Registrar Abuse Contact Email: abuse@websitewelcome.com Registrar Abuse Contact Phone: +1.713-574-5287 URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

- Generator detail

Source camzu.net (Domain)
Transform dtDomain2Whois
Gen. date 2016-07-05 16:34:48.927 -0700

Property View

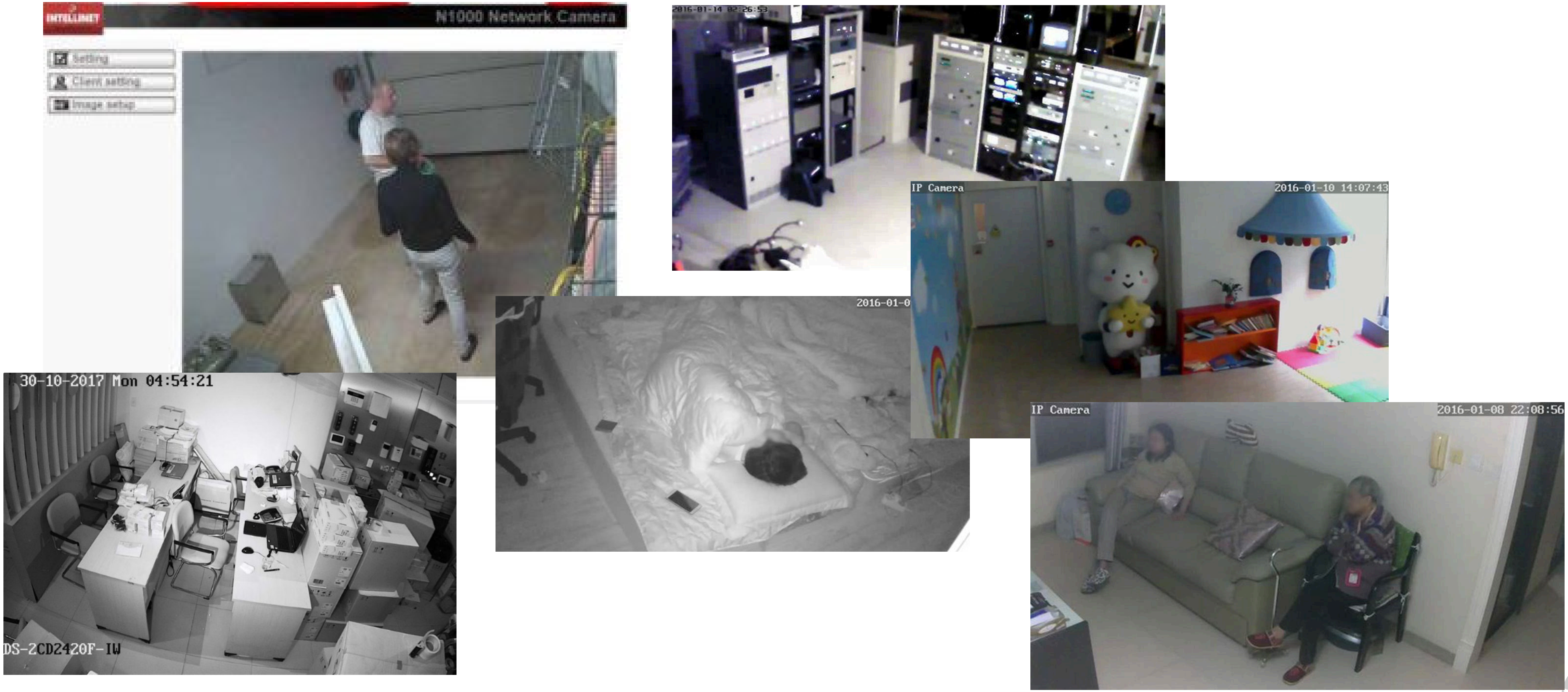
- Properties

Type Whois
Domain camzu.net
Create Date 2012-12-08

SHODAN

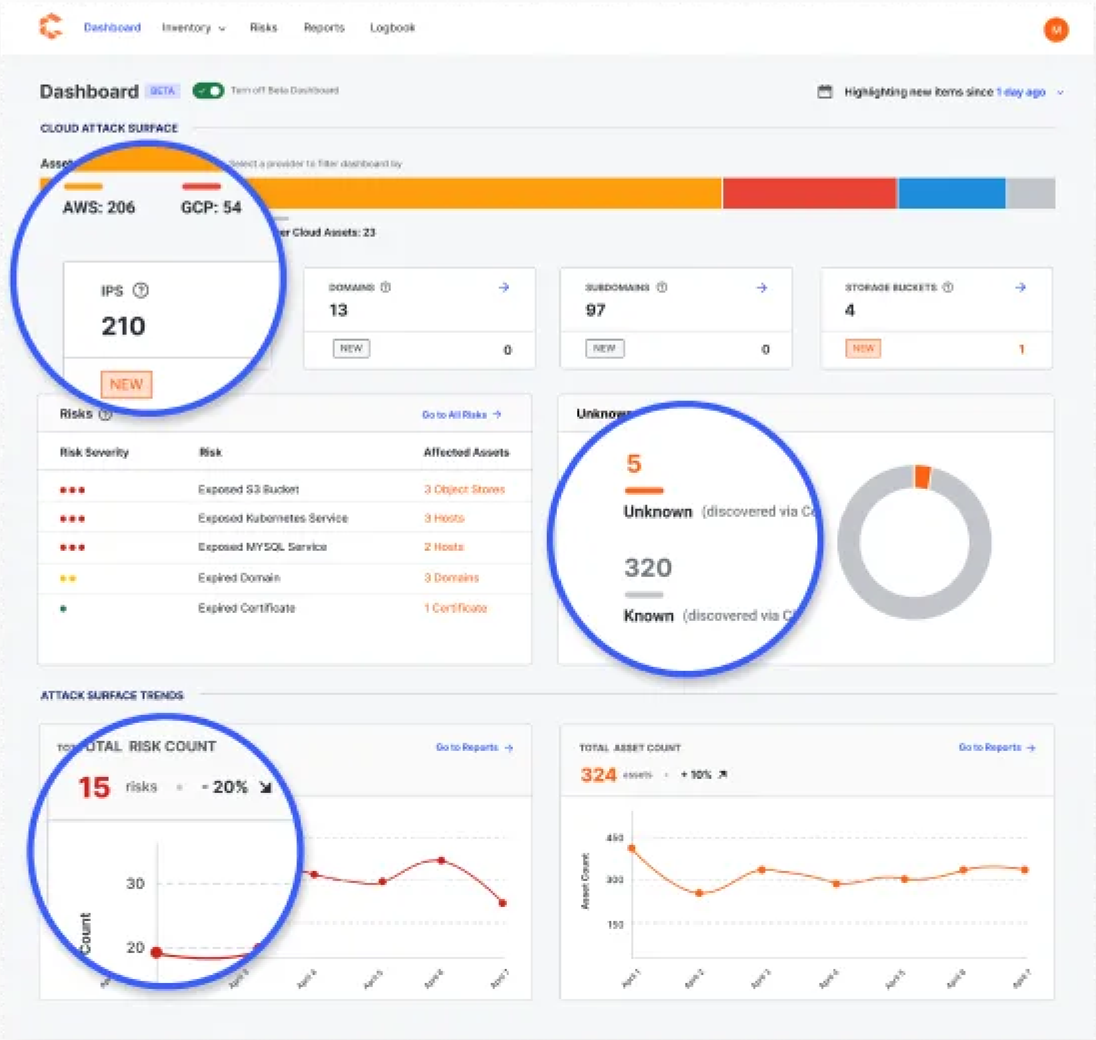
- Shodan.io
- Search engine for Internet-connected devices
- Most commonly used to help users identify potential security issues with their devices
- Can find anything that connects directly to the internet:
  - Routers and servers
  - Baby monitors
  - Security cameras
  - Maritime satellites
  - Water treatment facilities
  - Traffic light systems
  - Prison pay phones
  - Nuclear power plants

SHODAN.IO EXAMPLES



CENSYS.IO

- Similar to Shodan
- Continually discovers Internet-facing assets including IoT devices
- Offers cloud-based dashboard



Risk Severity	Risk	Affected Assets
●●●	Exposed S3 Bucket	3 Object Stores
●●●	Exposed Kubernetes Service	3 Hosts
●●●	Exposed MYSQL Service	2 Hosts
●●	Expired Domain	3 Domains
●	Expired Certificate	1 Certificate

THEHARVESTER

- OSINT tool for gathering:
  - emails, sub-domains, hosts, employee names, open ports, and banners from different public sources like search engines, PGP key servers, and SHODAN computer database
- Written in Python
- Many of its functions require an API key to effectively query the source

THEHARVESTER EXAMPLE

```
theHarvester -d www.hackthissite.org -n -b  google
```

```
[*] Emails found: 2
---------------------
ab790c1315@www.hackthissite.org
staff@hackthissite.org

[*] Hosts found: 7
--------------------
0.loadbalancer.www.hackthissite.org:
22www.hackthissite.org:
2522www.hackthissite.org:
253dwww.hackthissite.org:
www.hackthissite.org:137.74.187.104, 137.74.187.100, 137.74.187.101, 137.74.187.103, 137.74.187.102
x22www.hackthissite.org:
```

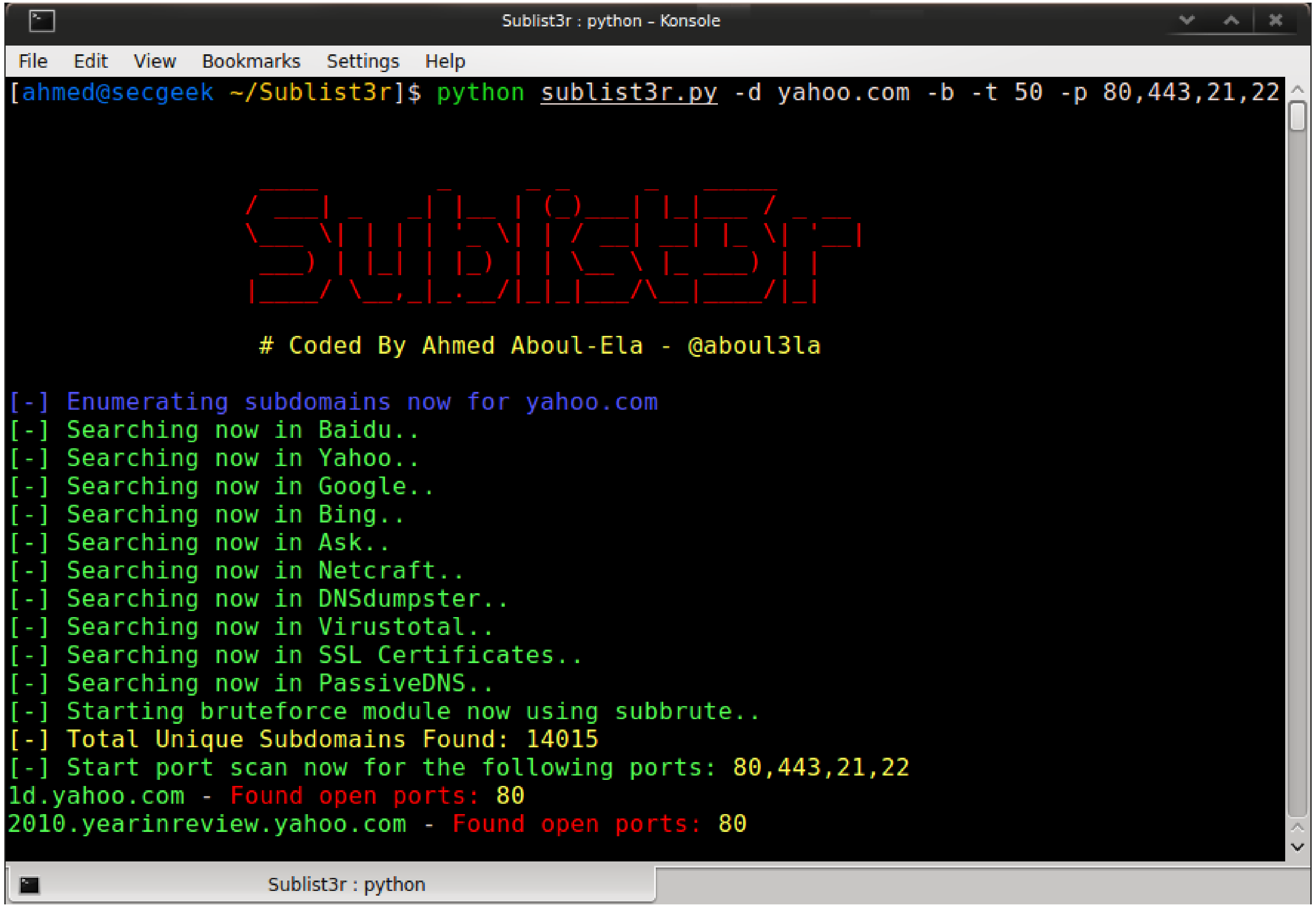
SUBLIST3R

- Uses OSINT and a variety of search engines to enumerate website subdomains
- Can conduct port scans against discovered websites

Subdomains are sometimes preferred targets for attackers:

- Often separately managed by the smaller child organization
- Frequently less secure than the parent domain
- Child organizations are typically smaller with fewer resources than the parent

SUBLIST3R EXAMPLE

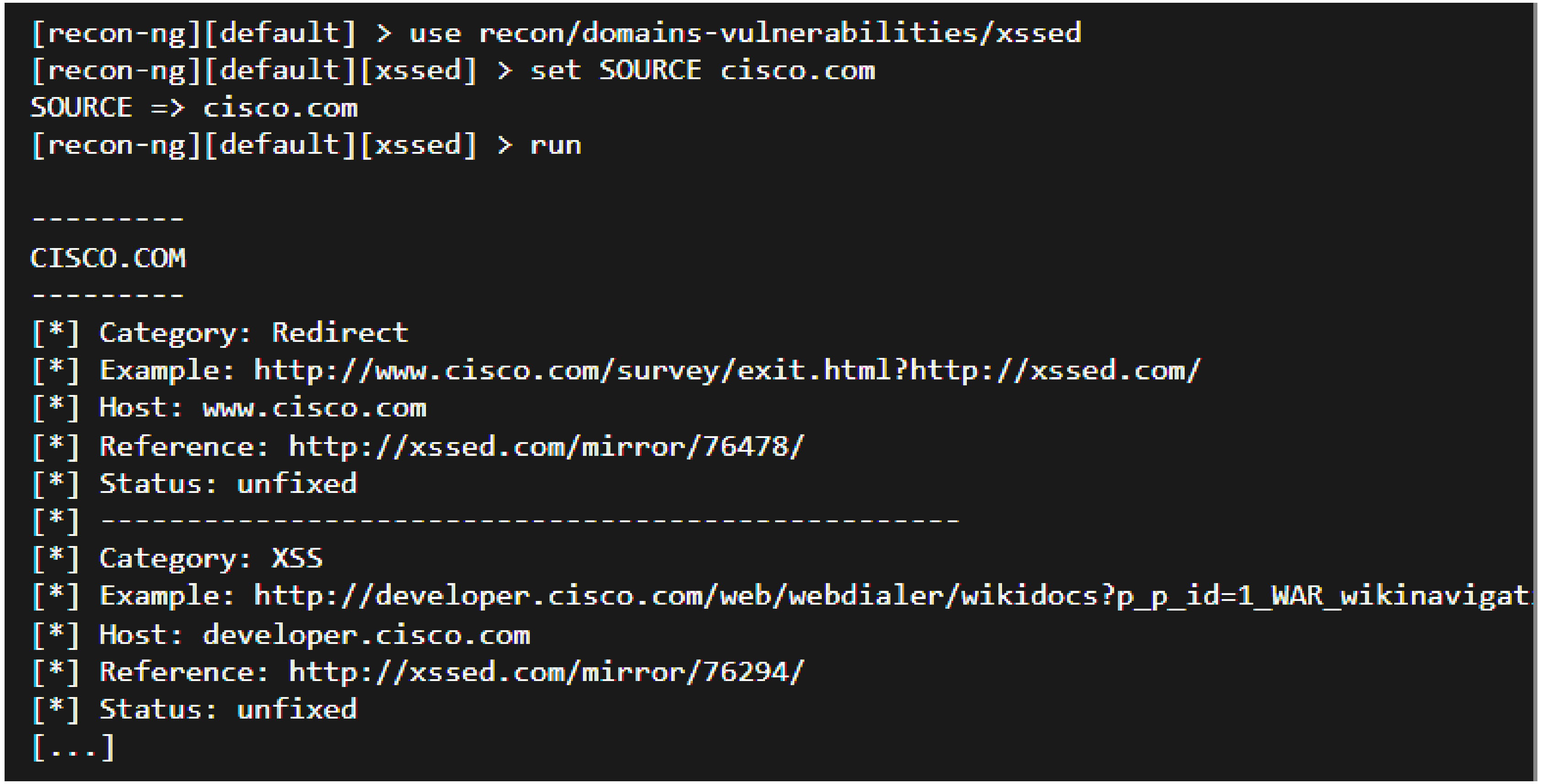


```
[ahmed@secgeek ~/Sublist3r]$ python sublist3r.py -d yahoo.com -b -t 50 -p 80,443,21,22

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for yahoo.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Starting bruteforce module now using subbrute..
[-] Total Unique Subdomains Found: 14015
[-] Start port scan now for the following ports: 80,443,21,22
1d.yahoo.com - Found open ports: 80
2010.yearinreview.yahoo.com - Found open ports: 80
```

RECON-NG

- Full-featured web reconnaissance framework
- Has many modules with specific functions for conducting OSINT
- Written in Python
- Requires API keys from targets to be effective

RECON-NG EXAMPLE



```
[recon-ng][default] > use recon/domains-vulnerabilities/xssed
[recon-ng][default][xssed] > set SOURCE cisco.com
SOURCE => cisco.com
[recon-ng][default][xssed] > run

---------
CISCO.COM
---------
[*] Category: Redirect
[*] Example: http://www.cisco.com/survey/exit.html?http://xssed.com/
[*] Host: www.cisco.com
[*] Reference: http://xssed.com/mirror/76478/
[*] Status: unfixed
[*] --------------------------------------------------
[*] Category: XSS
[*] Example: http://developer.cisco.com/web/webdialer/wikidocs?p_p_id=1_WAR_wikinavigat
[*] Host: developer.cisco.com
[*] Reference: http://xssed.com/mirror/76294/
[*] Status: unfixed
[...]
```

INSPY

- Gathers information from LinkedIn
- Install in Kali Linux:

```
apt install inspy
```

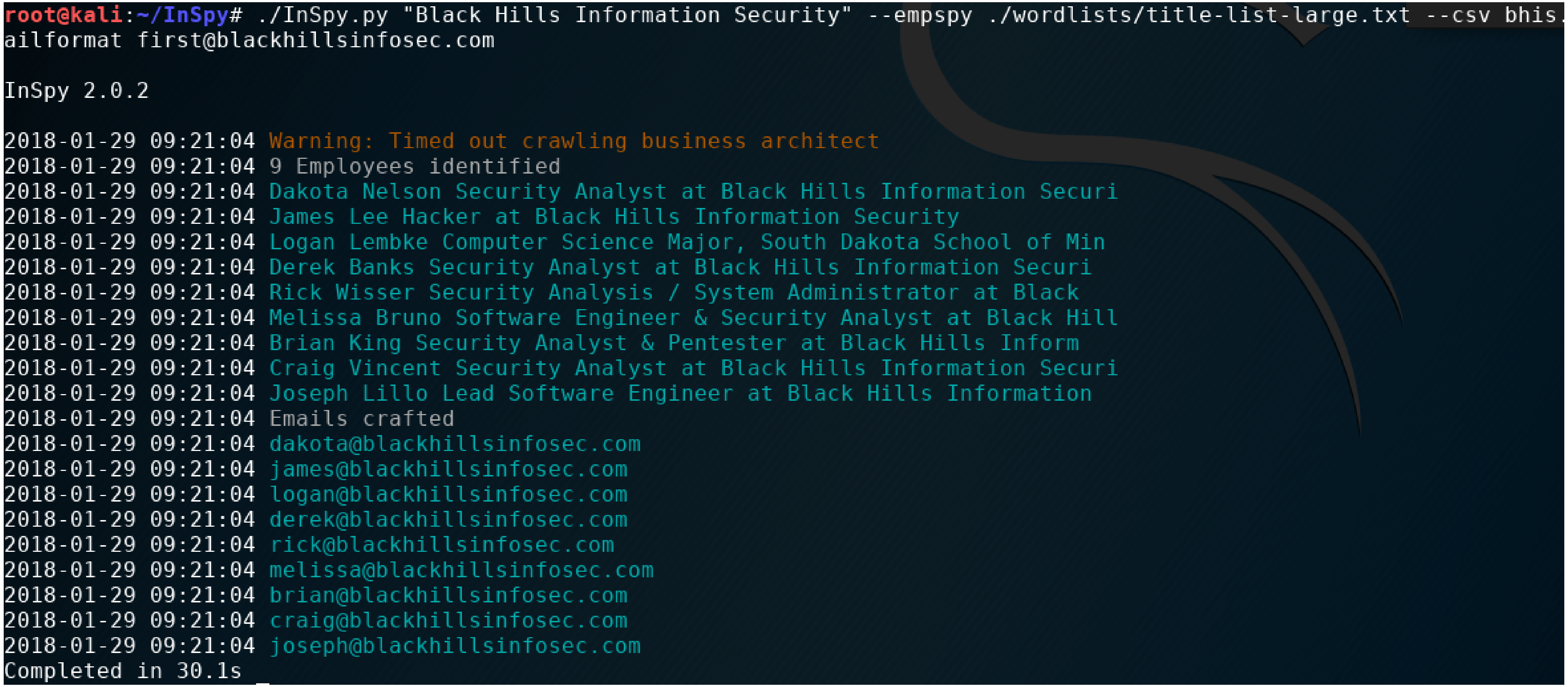
Search LinkedIn for ***Google*** employees using the provided wordlist of possible job titles:

```
inspy --empspy /usr/share/inspy/wordlists/title-list-
large.txt Google
```

Search for technologies (***–techspy***) in use at the target company (***cisco***) using the provided list of terms:

```
inspy --techspy /usr/share/inspy/wordlists/tech-list-
small.txt cisco
```

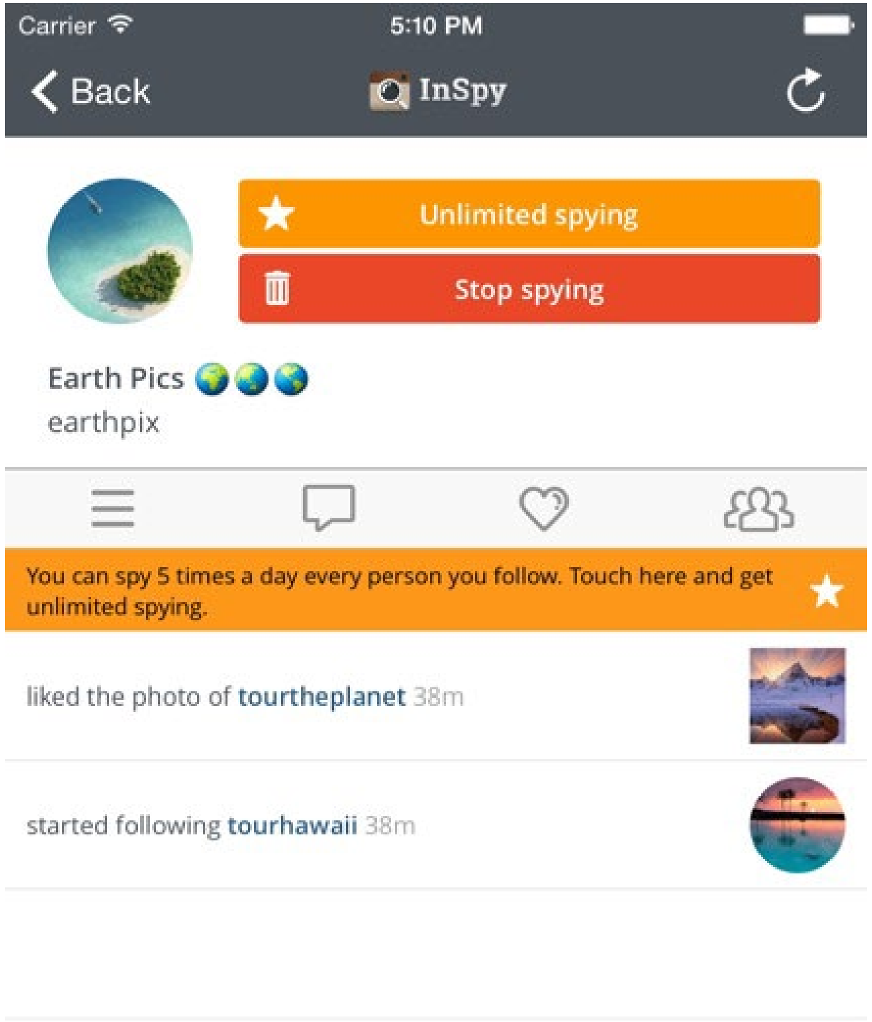
INSPY EXAMPLE



```
root@kali:~/InSpy# ./InSpy.py "Black Hills Information Security" --empspy ./wordlists/title-list-large.txt --csv bhis.
ailformat first@blackhillsinfosec.com

InSpy 2.0.2

2018-01-29 09:21:04 Warning: Timed out crawling business architect
2018-01-29 09:21:04 9 Employees identified
2018-01-29 09:21:04 Dakota Nelson Security Analyst at Black Hills Information Securi
2018-01-29 09:21:04 James Lee Hacker at Black Hills Information Security
2018-01-29 09:21:04 Logan Lembke Computer Science Major, South Dakota School of Min
2018-01-29 09:21:04 Derek Banks Security Analyst at Black Hills Information Securi
2018-01-29 09:21:04 Rick Wisser Security Analysis / System Administrator at Black
2018-01-29 09:21:04 Melissa Bruno Software Engineer & Security Analyst at Black Hill
2018-01-29 09:21:04 Brian King Security Analyst & Pentester at Black Hills Inform
2018-01-29 09:21:04 Craig Vincent Security Analyst at Black Hills Information Securi
2018-01-29 09:21:04 Joseph Lillo Lead Software Engineer at Black Hills Information
2018-01-29 09:21:04 Emails crafted
2018-01-29 09:21:04 dakota@blackhillsinfosec.com
2018-01-29 09:21:04 james@blackhillsinfosec.com
2018-01-29 09:21:04 logan@blackhillsinfosec.com
2018-01-29 09:21:04 derek@blackhillsinfosec.com
2018-01-29 09:21:04 rick@blackhillsinfosec.com
2018-01-29 09:21:04 melissa@blackhillsinfosec.com
2018-01-29 09:21:04 brian@blackhillsinfosec.com
2018-01-29 09:21:04 craig@blackhillsinfosec.com
2018-01-29 09:21:04 joseph@blackhillsinfosec.com
Completed in 30.1s _
```

ANDROID INSPY

- Follow a target's Instagram likes and comments



Earth Pics 🌍🌏🌎
earthpix

You can spy 5 times a day every person you follow. Touch here and get unlimited spying.

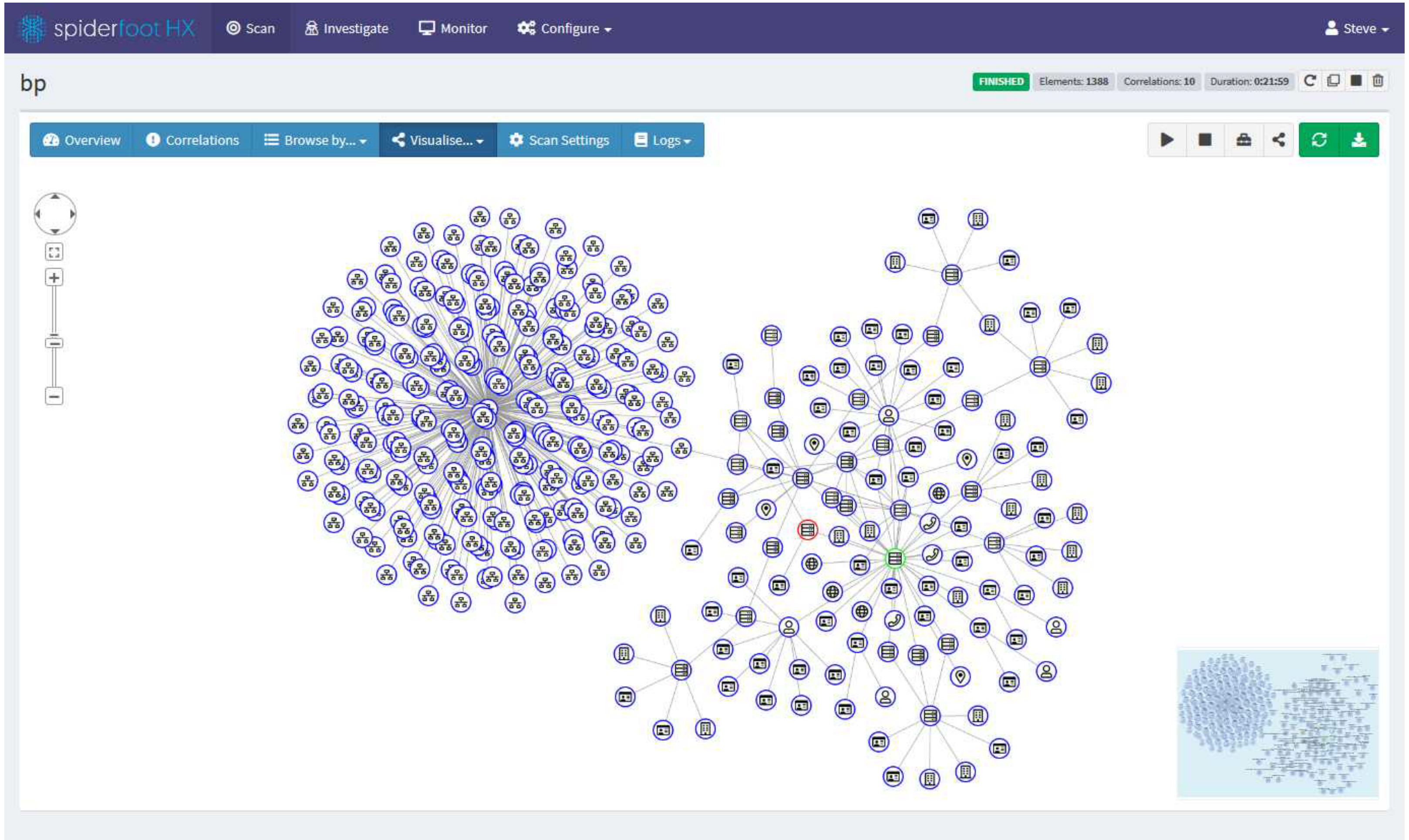
liked the photo of tourtheplanet 38m

started following tourhawaii 38m

SPIDERFOOT

- OSINT automation tool
  - Including target monitoring
- Written in Python
- Alternatively has a cloud-hosted version
  - Different subscription levels

SPIDERFOOT EXAMPLE

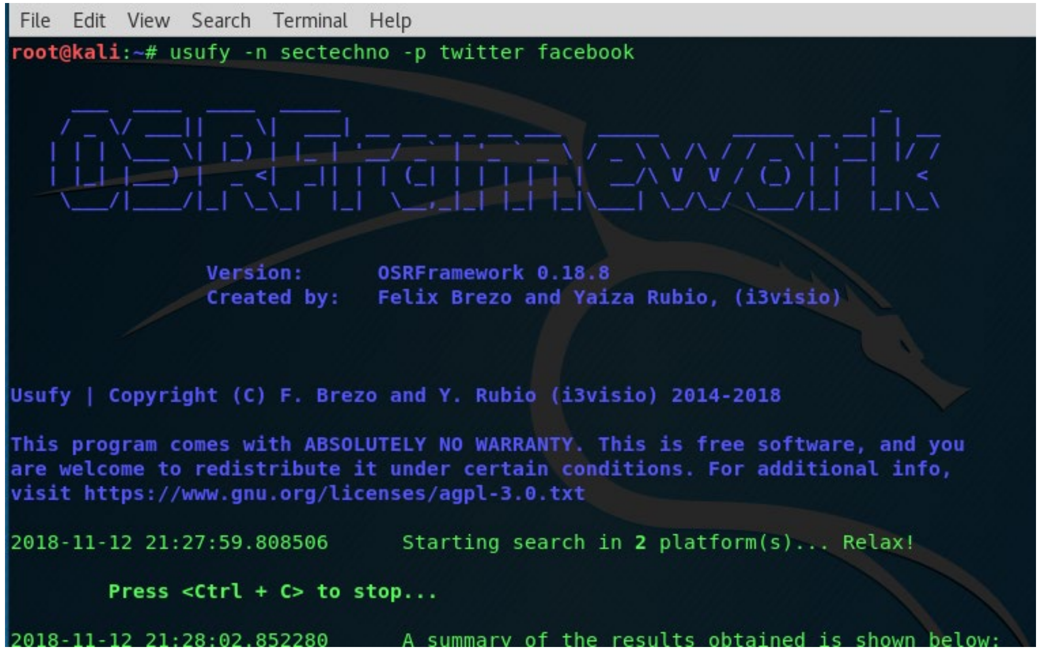


bp

FINISHED Elements: 1388 Correlations: 10 Duration: 0:21:59

OSR FRAMEWORK

- A set of libraries for performing Open Source Intelligence tasks
- Has various scripts and applications for:
  - Username checking
  - DNS lookups
  - Information leaks research
  - Deep web search
  - Regular expressions extraction
  - etc.

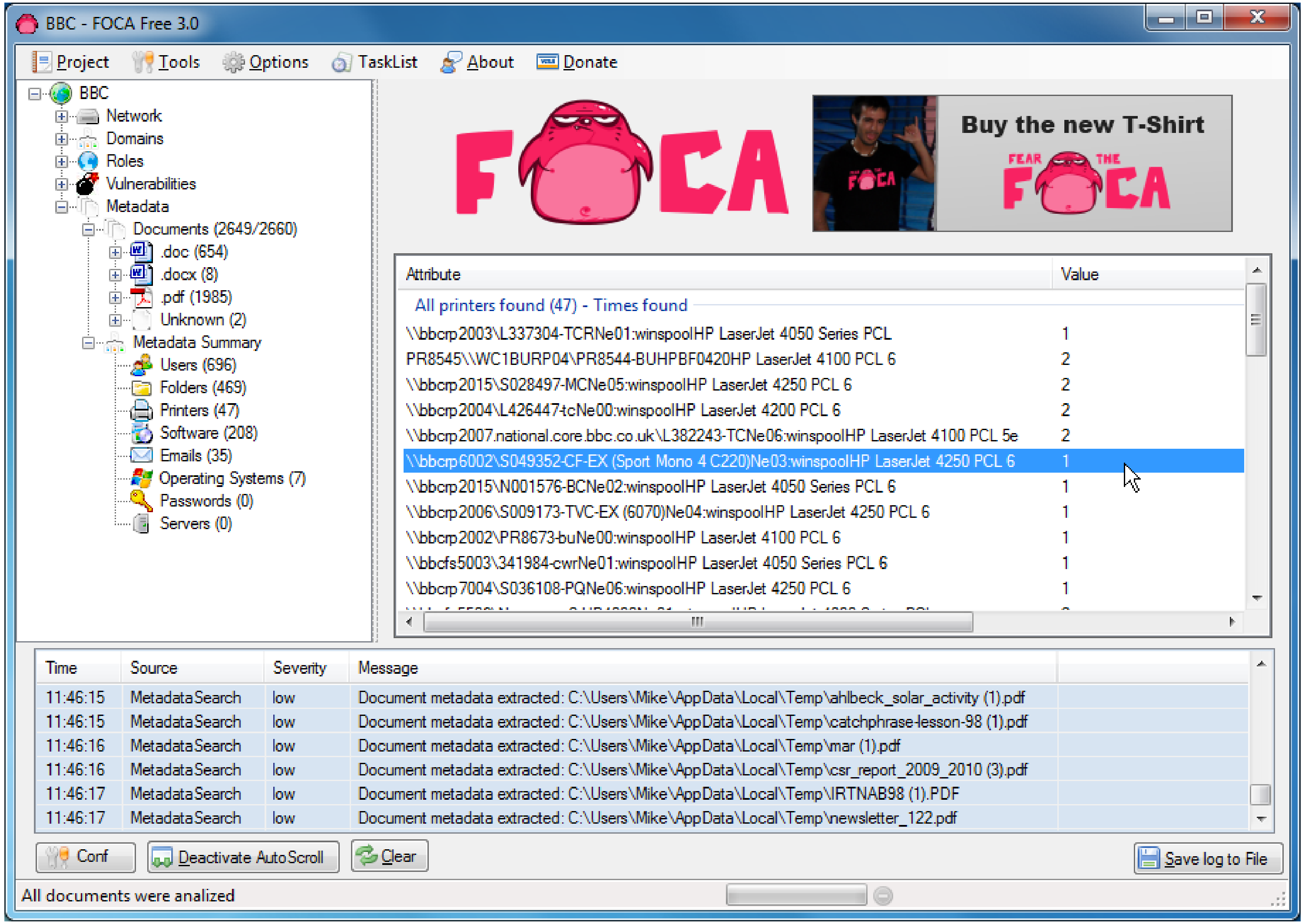


```
root@kali:~# usufy -n sectechno -p twitter facebook

                Version:      OSRFramework 0.18.8
                Created by:   Felix Brezo and Yaiza Rubio, (i3visio)


Usufy | Copyright (C) F. Brezo and Y. Rubio (i3visio) 2014-2018

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit https://www.gnu.org/licenses/agpl-3.0.txt

2018-11-12 21:27:59.808506      Starting search in 2 platform(s)... Relax!

        Press <Ctrl + C> to stop...

2018-11-12 21:28:02.852280      A summary of the results obtained is shown below:
```

METADATA EXTRACTION

- Useful information might reside in PDF or Office files
- Use this hidden metadata to perform social engineering
- Tools:
  - Metagoofil
  - ExtractMetadata
  - FOCA
  - Meta Tag Analyzer
  - BuzzStream
  - Analyze Metadata
  - Exiftool

FOCA EXAMPLE



Attribute	Value
All printers found (47) - Times found	
\\bbcrp2003\L337304-TCRNe01:winspoolHP LaserJet 4050 Series PCL	1
PR8545\\WC1BURP04\PR8544-BUHPBF0420HP LaserJet 4100 PCL 6	2
\\bbcrp2015\S028497-MCNe05:winspoolHP LaserJet 4250 PCL 6	2
\\bbcrp2004\L426447-tcNe00:winspoolHP LaserJet 4200 PCL 6	2
\\bbcrp2007.national.core.bbc.co.uk\L382243-TCNe06:winspoolHP LaserJet 4100 PCL 5e	2
\\bbcrp6002\S049352-CF-EX (Sport Mono 4 C220)Ne03:winspoolHP LaserJet 4250 PCL 6	1
\\bbcrp2015\N001576-BCNe02:winspoolHP LaserJet 4050 Series PCL 6	1
\\bbcrp2006\S009173-TVC-EX (6070)Ne04:winspoolHP LaserJet 4250 PCL 6	1
\\bbcrp2002\PR8673-buNe00:winspoolHP LaserJet 4100 PCL 6	1
\\bbcfs5003\341984-cwrNe01:winspoolHP LaserJet 4050 Series PCL 6	1
\\bbcrp7004\S036108-PQNe06:winspoolHP LaserJet 4250 PCL 6	1

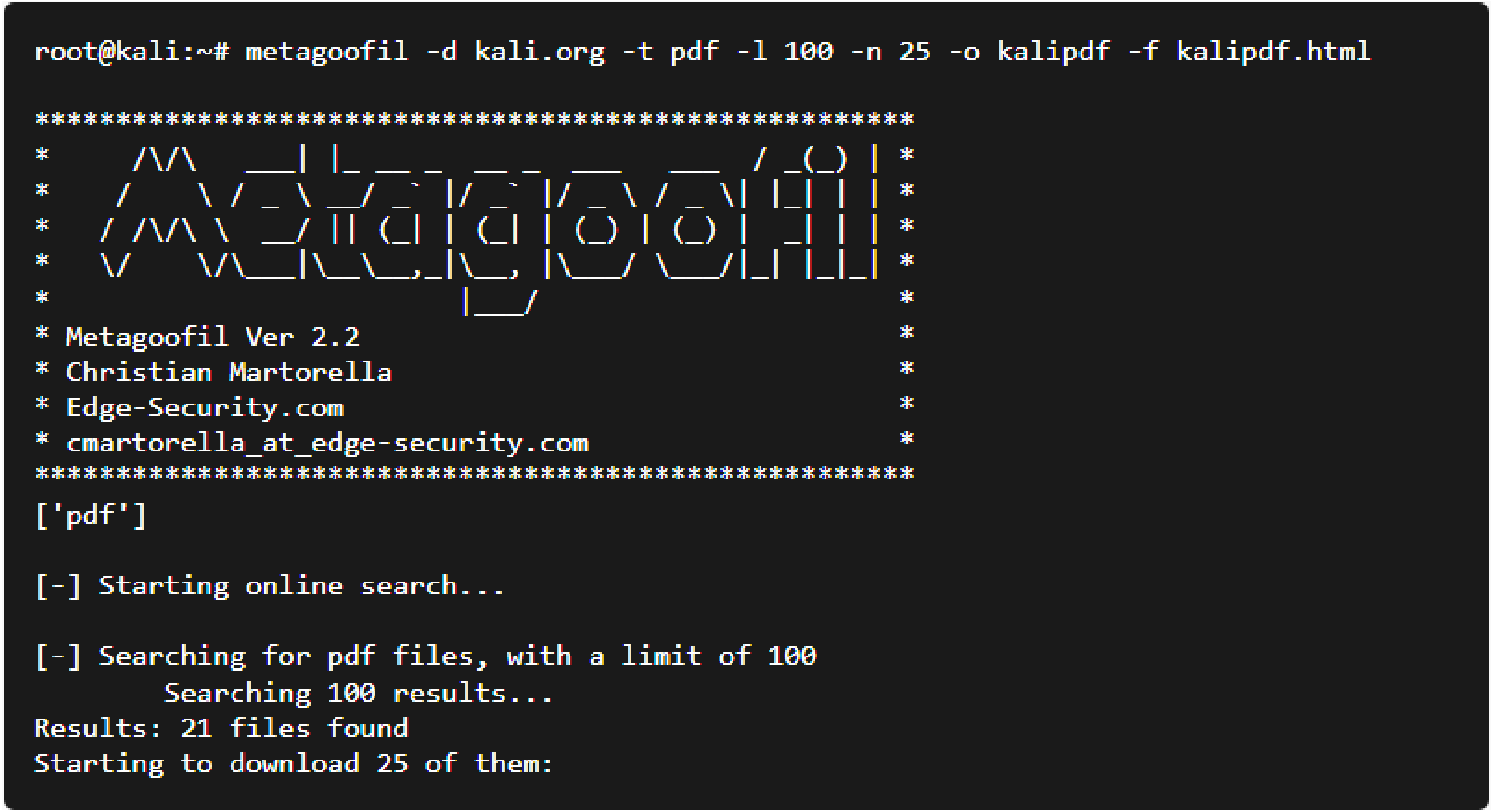
Time	Source	Severity	Message
11:46:15	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\ahlbeck_solar_activity (1).pdf
11:46:15	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\catchphrase-lesson-98 (1).pdf
11:46:16	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\mar (1).pdf
11:46:16	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\csr_report_2009_2010 (3).pdf
11:46:17	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\IRTNAB98 (1).PDF
11:46:17	MetadataSearch	low	Document metadata extracted: C:\Users\Mike\AppData\Local\Temp\newsletter_122.pdf

All documents were analized

METAGOOFIL

- Extracts metadata from publicly available documents belonging to a target company
  - pdf, doc, xls, ppt, docx, pptx, xlsx
- Uses Google hacks to find information in meta tags
- Generates a report of:
  - usernames, email addresses, software versions, server names, etc.

METAGOOFIL EXAMPLE



```
root@kali:~# metagoofil -d kali.org -t pdf -l 100 -n 25 -o kalipdf -f kalipdf.html

*******************************************************
*     /\/\   ___| |_ __ _  __ _  ___   ___  / _(_) |  *
*    /    \ / _ \ __/ _` |/ _` |/ _ \ / _ \| |_| | |  *
*   / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | |  *
*   \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_|  *
*                         |___/                       *
* Metagoofil Ver 2.2                                  *
* Christian Martorella                                *
* Edge-Security.com                                   *
* cmartorella_at_edge-security.com                    *
*******************************************************
['pdf']

[-] Starting online search...

[-] Searching for pdf files, with a limit of 100
        Searching 100 results...
Results: 21 files found
Starting to download 25 of them:
```

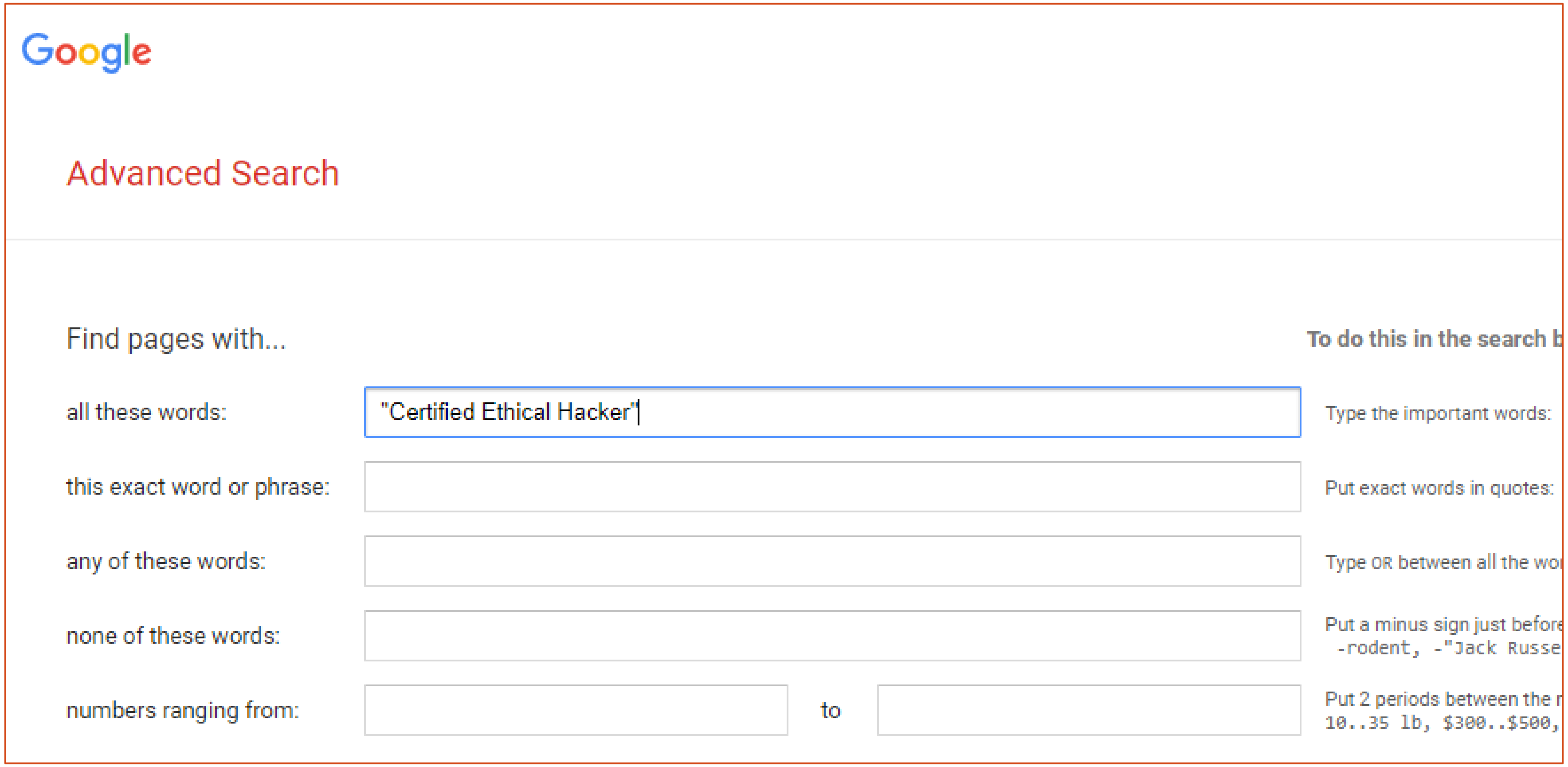
2.3 ADVANCED GOOGLE SEARCH

- Google Hacking
- Google Dorking
- Google Hacking Database

GOOGLE HACKING

- The use of specialized Google searches
- Find unusual information such as:
  - Sites that may link back to target's website
  - Information about partners, vendors, suppliers, clients, etc.
  - Error messages that contain sensitive information
  - Files that contain passwords
  - Sensitive directories
  - Pages that contain hidden login portals
  - Advisories and server vulnerabilities
  - Software version information
  - Web app source code

GOOGLE ADVANCED SEARCH



Advanced Search

Find pages with...

To do this in the search b

all these words: "Certified Ethical Hacker"

Type the important words:

this exact word or phrase:

Put exact words in quotes:

any of these words:

Type OR between all the wo

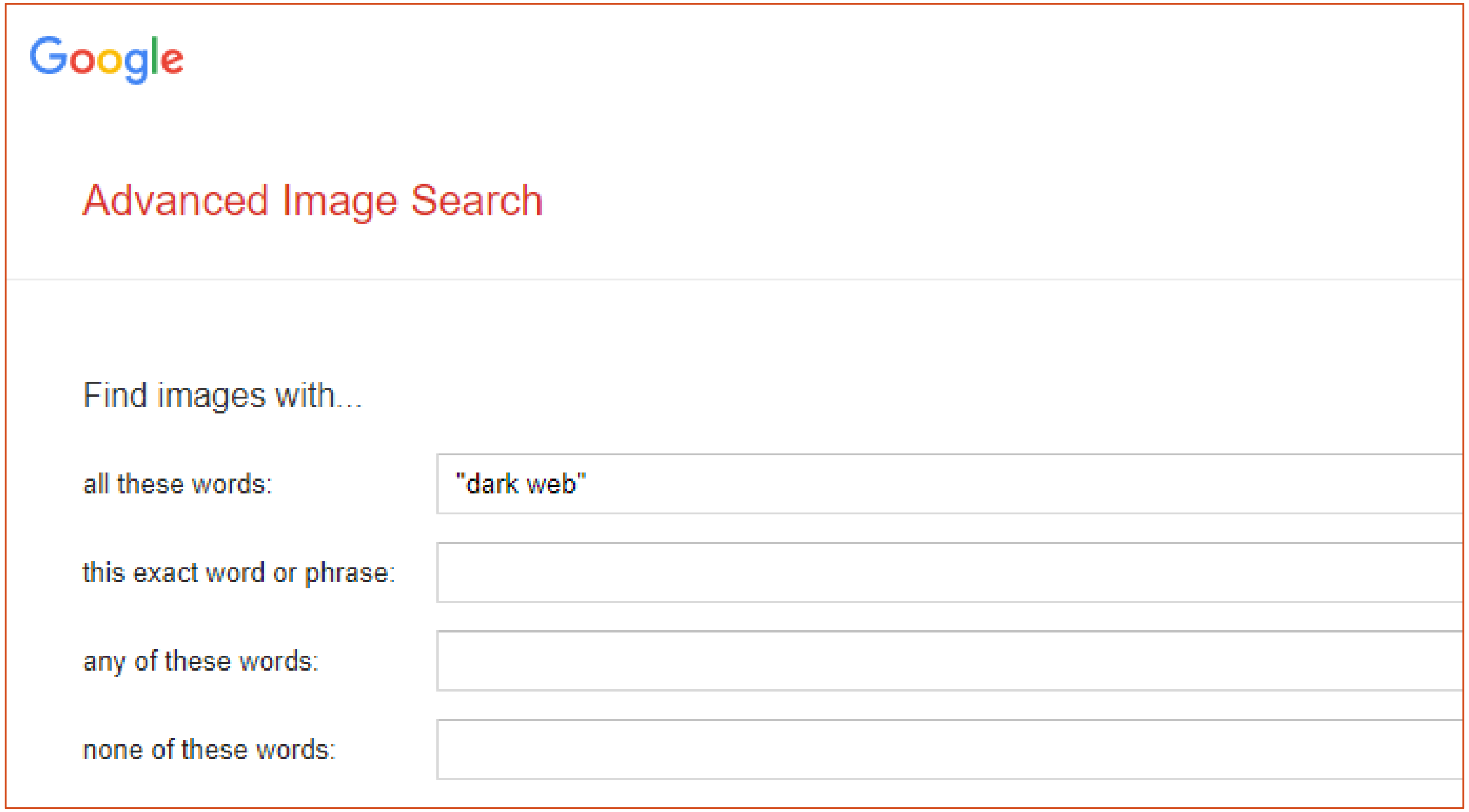
none of these words:

Put a minus sign just befor
-rodent, -"Jack Russe

numbers ranging from: to

Put 2 periods between the r
10..35 lb, $300..$500,

GOOGLE ADVANCED IMAGE SEARCH



Advanced Image Search

Find images with...

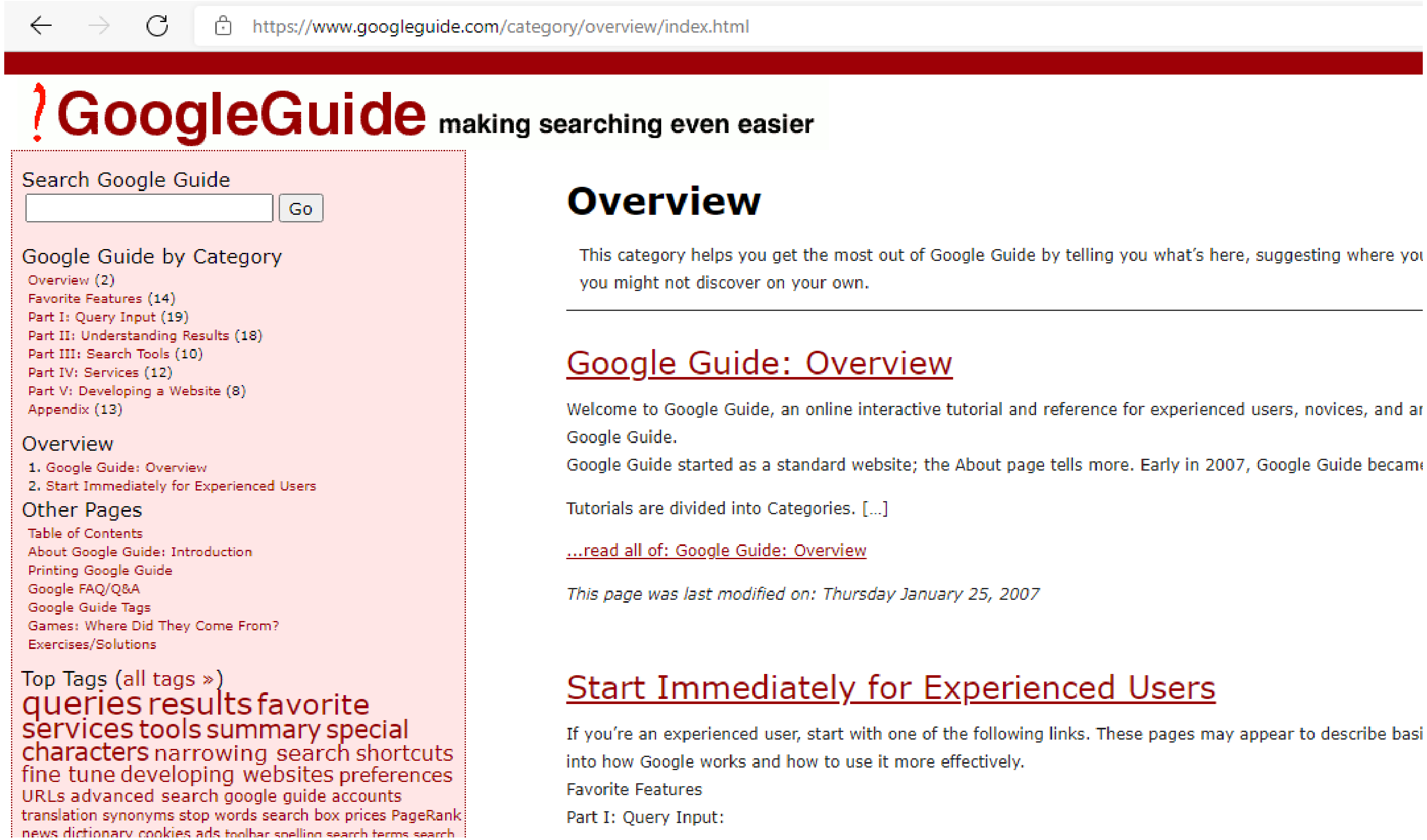
all these words: "dark web"

this exact word or phrase:

any of these words:

none of these words:

GOOGLE SEARCH GUIDE



https://www.googleguide.com/category/overview/index.html

GoogleGuide making searching even easier

Search Google Guide

Go

Google Guide by Category

- Overview (2)
- Favorite Features (14)
- Part I: Query Input (19)
- Part II: Understanding Results (18)
- Part III: Search Tools (10)
- Part IV: Services (12)
- Part V: Developing a Website (8)
- Appendix (13)

Overview

1. Google Guide: Overview
2. Start Immediately for Experienced Users

Other Pages

- Table of Contents
- About Google Guide: Introduction
- Printing Google Guide
- Google FAQ/Q&A
- Google Guide Tags
- Games: Where Did They Come From?
- Exercises/Solutions

Top Tags (all tags »)

queries results favorite services tools summary special characters narrowing search shortcuts fine tune developing websites preferences URLs advanced search google guide accounts translation synonyms stop words search box prices PageRank news dictionary cookies ads toolbar spelling search terms search

Overview

This category helps you get the most out of Google Guide by telling you what's here, suggesting where yo
you might not discover on your own.

Google Guide: Overview

Welcome to Google Guide, an online interactive tutorial and reference for experienced users, novices, and a
Google Guide.

Google Guide started as a standard website; the About page tells more. Early in 2007, Google Guide becam

Tutorials are divided into Categories. [...]

...read all of: Google Guide: Overview

This page was last modified on: Thursday January 25, 2007

Start Immediately for Experienced Users

If you're an experienced user, start with one of the following links. These pages may appear to describe bas
into how Google works and how to use it more effectively.

Favorite Features

Part I: Query Input:

GOOGLE DORKING

- Using search strings with advanced operators
- Find information not readily available on a website
- Can be used to find vulnerabilities, files containing passwords, lists of emails, log files, live camera feeds, and much more
- Considered an easy way of hacking

GOOGLE DORK OPERATORS

Operator	Description	Example
intitle:	find strings in the title of a page	intitle:”Your Text”
allintext:	find all terms in the title of a page	allintext:”Contact”
inurl:	find strings in the URL of a page	inurl:”news.php?id=”
site:	restrict a search to a particular site or domain	site:yeahhub.com “Keyword”
filetype:	find specific types of files (doc, pdf, mp3 etc) based on file extension	filetype:pdf “Cryptography”
link:	search for all links to a site or URL	link:”example.com”
cache:	display Google’s cached copy of a page	cache:yeahhub.com
info:	display summary information about a page	info:www.example.com

GOOGLE DORK OPERATORS (CONT'D)

Operator	Description	Example
OR	Match at least one keyword	google OR bing OR duckduckgo
AND	Match all keywords	Samsung AND Apple
“ “	Exact match	"Google Dorks Explained"
-	Exclude a keyword	Linux -site:Wikipedia.org
*	Wildcard of one or more words	"username * password"
( )	Grouping keywords	"google (dorks OR dorking OR hacking)" AND (explained OR tutorial OR guide)

GOOGLE DORK EXAMPLES

- Camera feeds – live feeds from AXIS cameras
  - intitle:"Live View / - AXIS" | inurl:/mjpg/video.mjpg?timestamp
- Email lists contained in Excel files
  - filetype:xls inurl:"email.xls"
- Log files containing passwords and corresponding emails
  - filetype:log intext:password intext:(@gmail.com | @yahoo.com | @hotmail.com)
- Open FTP Servers that can contain sensitive information
  - intext:"index of" inurl:ftp

GOOGLE DORK EXAMPLES

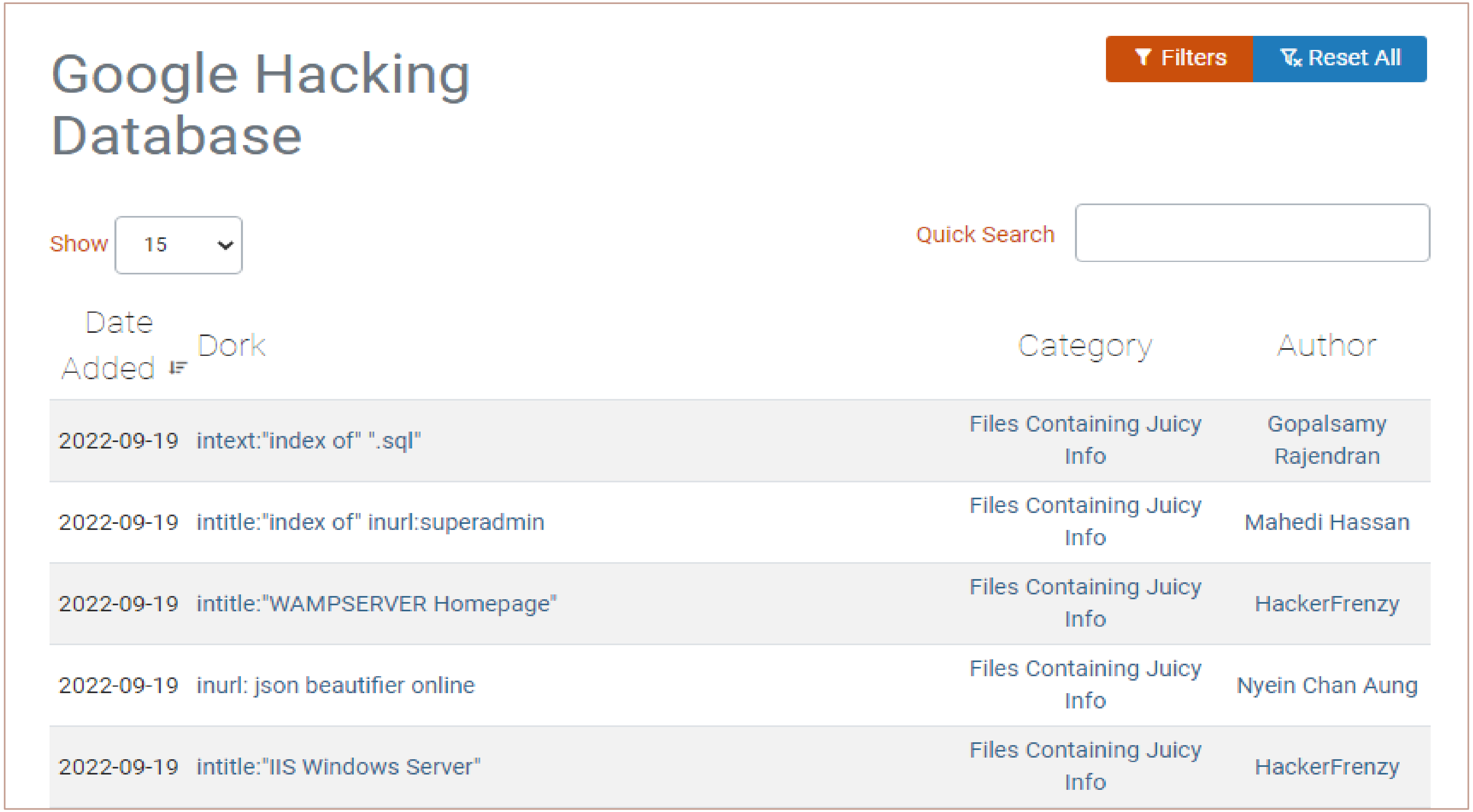
- Return results that match “accounting” from target.com, but NOT from marketing.target.com
  - `site:target.com -site:marketing.target.com accounting`
- Pages vulnerable to SQL injection attacks
  - `inurl:".php?id=" intext:(error AND sql)`
- Scanning reports – vulnerabilities in scanned systems
  - `intitle:report (nessus | qualys) filetype:pdf`
- SQL Database – contents of exposed databases, including usernames and passwords
  - `intitle:"index of" "dump.sql"`

GOOGLE HACKING DATABASE (GHDB)

- List of popular Google Dorks

https://www.exploit-db.com/google-hacking-database/

GHDB EXAMPLE



Google Hacking Database

Date Added	Dork	Category	Author
2022-09-19	intext:"index of" ".sql"	Files Containing Juicy Info	Gopalsamy Rajendran
2022-09-19	intitle:"index of" inurl:superadmin	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"WAMPSERVER Homepage"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	inurl: json beautifier online	Files Containing Juicy Info	Nyein Chan Aung
2022-09-19	intitle:"IIS Windows Server"	Files Containing Juicy Info	HackerFrenzy

2.4 WHOIS FOOTPRINTING

- Internet Authorities
- Whois
- Whois Tools

INTERNET AUTHORITIES

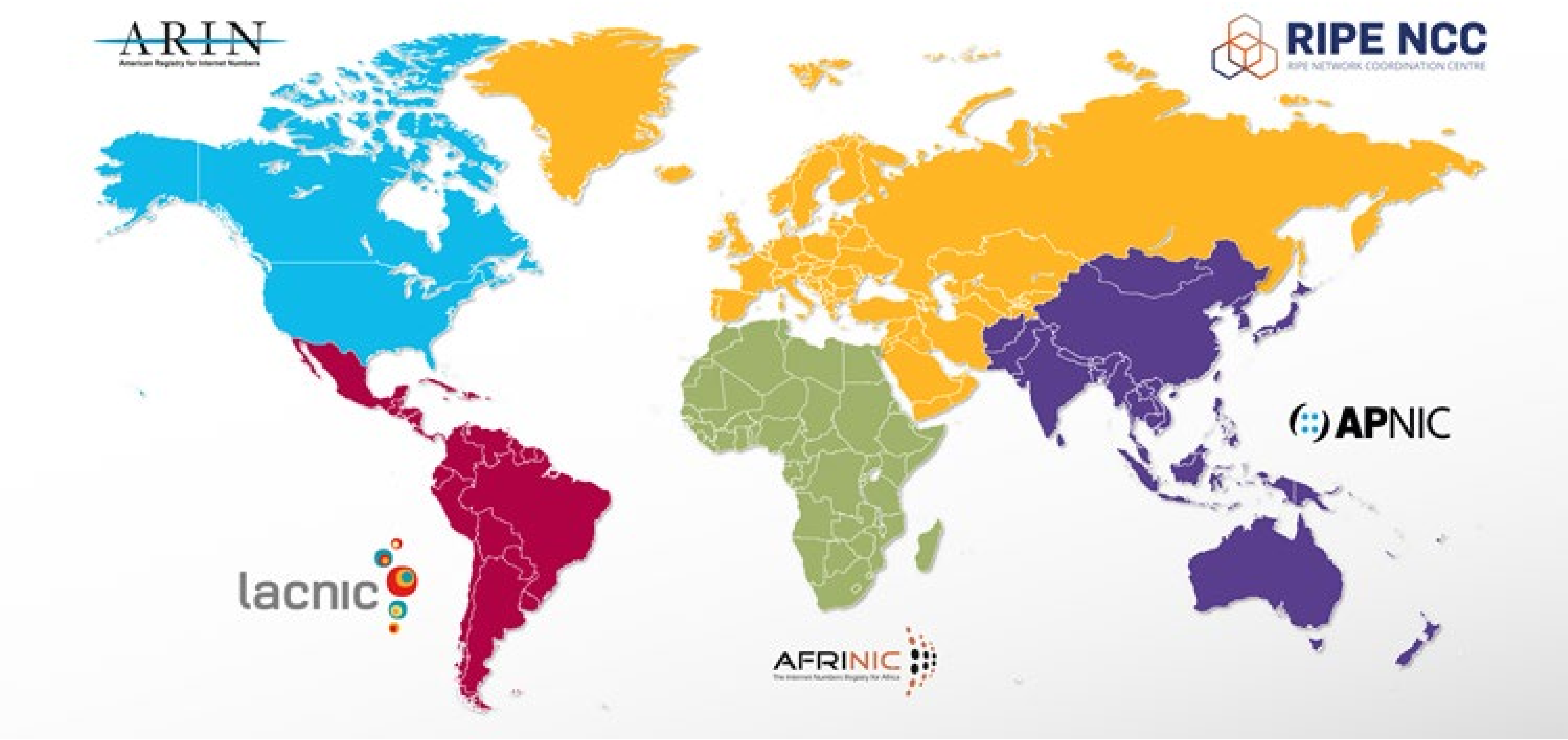
Organization	Description
Internet Corporation for Assigned Names and Numbers (ICANN)	• A not-for-profit public-benefit corporation • Dedicated to keeping the Internet secure, stable and interoperable • Promotes competition and develops policy on the Internet's unique identifiers • DNS names and Autonomous System (AS) numbers*
The Internet Assigned Numbers Authority (IANA)	• A department within ICANN • Maintains a central repository for Internet standards • Verifies and updates changes to Top Level Domain (TLD) information • Distributes Internet numbers to regions for Internet use
The Internet Engineering Task Force (IETF)	• An open standards organization • They develop and promote voluntary Internet standards (especially those related to IP)

* Every major network that is part of the Internet has an identifying Autonomous System number

REGIONAL INTERNET REGISTRIES (RIRS)

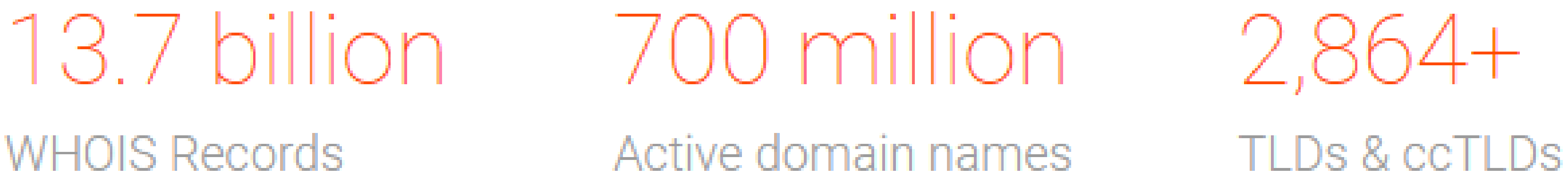
- Governing bodies that responsible for controlling all IP addresses and domain registrations in their operating region
- American Registry for Internet Numbers (ARIN)
  - U.S., Canada, Antarctica and parts of the Caribbean region
- Asia-Pacific Network Information Centre (APNIC)
  - Asia, Australia, New Zealand
- African Network Information Center (AfriNIC) - Africa and the Indian Ocean
- Reseaux IP Europeens Network Coordination Centre (RIPE NCC)
  - Europe, Russia, Central Asia, Middle East
- Latin America and Caribbean Network Information Center (LACNIC)
  - Latin America and parts of the Caribbean

REGIONAL INTERNET REGISTRIES (RIRS)


ARIN
American Registry for Internet Numbers
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
APNIC
lacnic
AFRINIC
The Internet Numbers Registry for Africa

WHOIS

- A widely-used query and response protocol
- Used to query databases that store the registered users or assignees of an Internet resource such as:
  - Domain names
  - IP address blocks
  - Autonomous system numbers
- The protocol stores and delivers database content in a human-readable format
- It is widely available for publicly available for use



13.7 billion
WHOIS Records

700 million
Active domain names

2,864+
TLDs & ccTLDs

Source: domainnamestat.com

WHO MAINTAINS THE WHOIS DATABASE?

- There is no single Whois database
- Registrars and registries each maintain their own respective Whois database
    - Registrars – companies and organizations that have ICANN accreditation and are registry certified to sell domain names
        - Also responsible for any resellers under them
    - Registries – organizations responsible for maintaining the records of a specific top level domain (TLD) such as .com, .net, .org, etc.
- ICANN requires that records remain accurate for the life of the domain registration

WHOIS LOOKUP

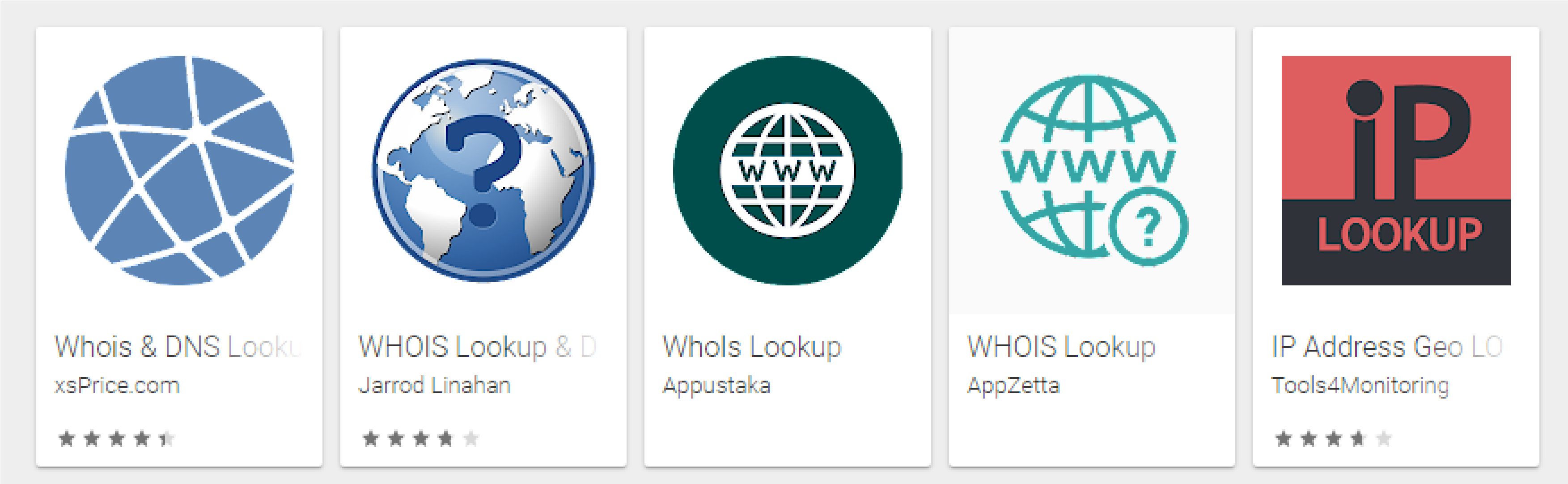
- WHOIS databases are maintained by Regional Internet Registries and hold personal information of domain owners
- WHOIS query
  - Domain name and details
  - Owner information
  - DNS servers
  - Network Blocks
  - Autonomous System Numbers
  - When created
  - Expiry
  - Last update
- Can aid attacker or ethical hacker with social engineering

POPULAR WHOIS LOOKUP TOOLS

- whois.com
- Domainnamestat.com
- LanWhoIs
- Batch IP Converter
- CallerIP
- WhoIs Lookup Multiple Addresses
- WhoIs Analyzer Pro
- HotWhoIs
- ActiveWhoIs
- WhoisThisDomain

- UltraTools
- SoftFuse Whois
- Domain Dossier
- BetterWhois
- Whois Online
- Web Wiz
- Network-Tools.com
- DNSstuff
- Network Solutions Whois
- WebToolHub

WHOIS MOBILE APPS



Whois & DNS Looku
xsPrice.com

WHOIS Lookup & D
Jarrod Linahan

WhoIs Lookup
Appustaka

WHOIS Lookup
AppZetta

IP Address Geo LO
Tools4Monitoring

2.5 DNS FOOTPRINTING

- DNS Information
- DNS Query Tools
- Location Search Tools

DNS INFORMATION

- Attackers use DNS data to find key hosts on the target’s network
- DNS record types:
  - A – IPv4 host address
  - AAAA - IPv6 host address
  - MX – mail server
  - NS – name server
  - CNAME – alias
  - SOA – authority for domain
  - SRV – service records
  - PTR – maps IP Address to hostname
  - RP – responsible person
  - HINFO – Host information record (CPU type/OS)
  - TXT – Unstructured text record

DNS QUERY TOOLS

- Nslookup
- dig
- host
- whatsmydns.net
- myDNSTools
- Professional Toolset
- DNS Records
- DNSData View
- DNSWatch
- DomainTools
- DNS Query Utility
- DNS Lookup

NSLOOKUP EXAMPLE

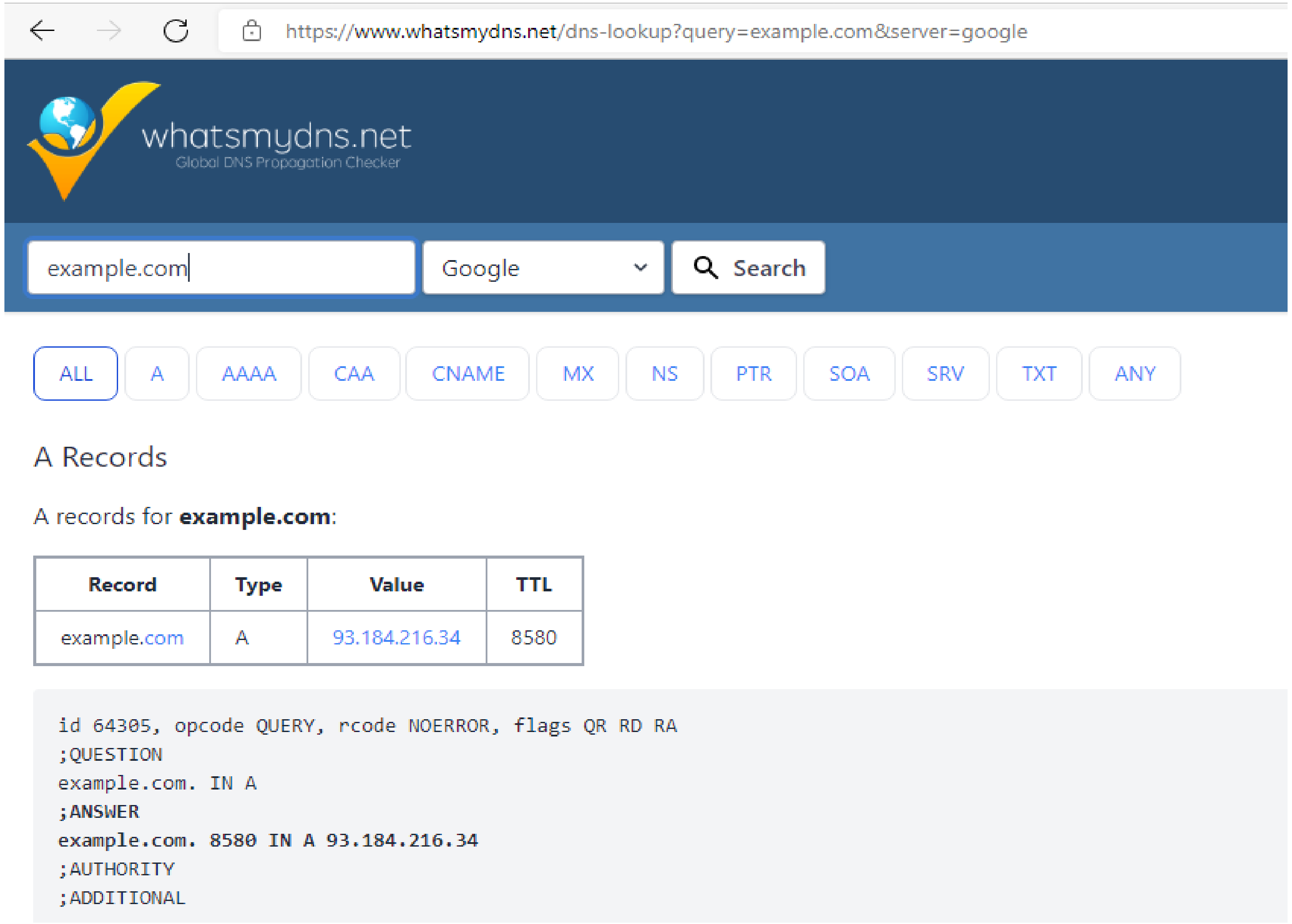
```
nslookup www.hackthissite.org
```

```
Server:         192.168.63.2
Address:          192.168.63.2#53

Non-authoritative answer:
Name:   www.hackthissite.org
Address: 137.74.187.103
Name:   www.hackthissite.org
Address: 137.74.187.102
```

DIG EXAMPLE

```
dig www.example.com
dig @8.8.8.8 www.example.com A
dig +short www.example.com A
dig example.com txt
dig example.com cname
dig example.com ns
dig example.com MX
dig axfr zonetransfer.me @nsztm1.digi.ninja.
```

ONLINE DNS LOOKUP EXAMPLE



https://www.whatsmydns.net/dns-lookup?query=example.com&server=google
whatsmydns.net
Global DNS Propagation Checker
example.com
Google
Search
ALL
A
AAAA
CAA
CNAME
MX
NS
PTR
SOA
SRV
TXT
ANY

A Records

A records for **example.com**:

Record	Type	Value	TTL
example.com	A	93.184.216.34	8580

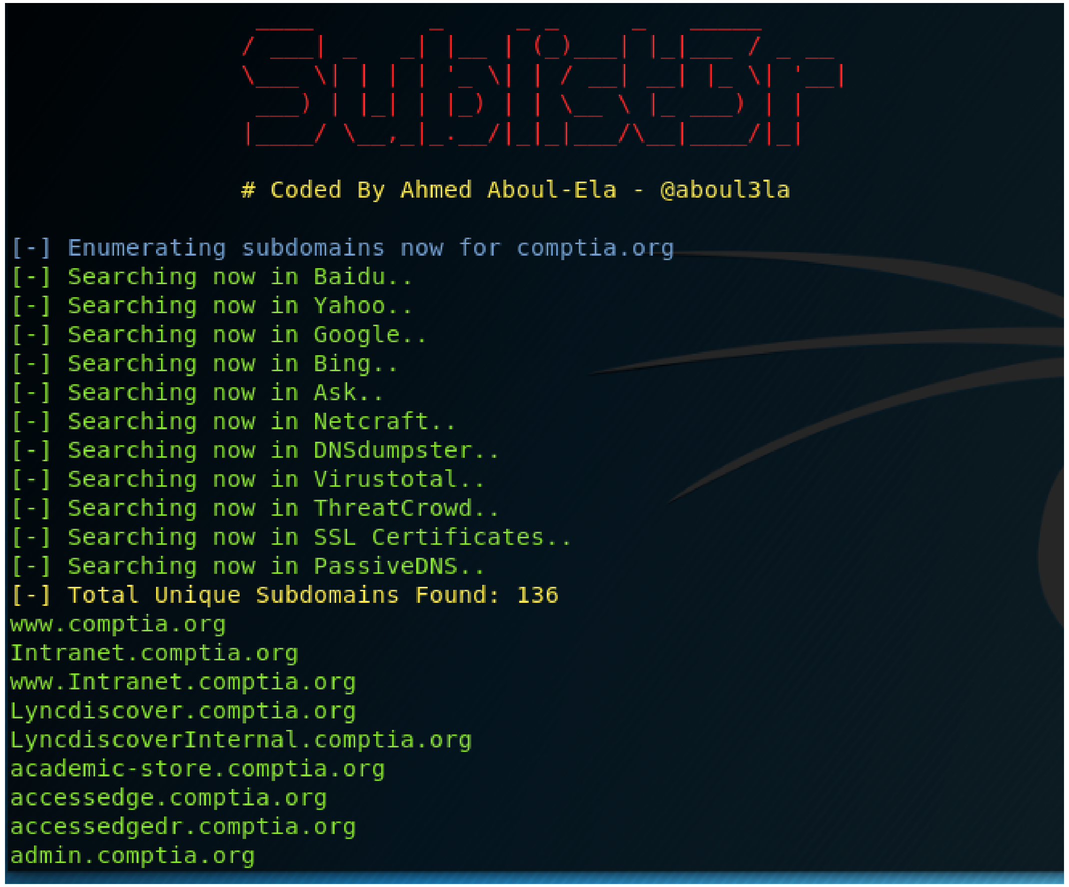
```
id 64305, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
example.com. IN A
;ANSWER
example.com. 8580 IN A 93.184.216.34
;AUTHORITY
;ADDITIONAL
```

SUBLIST3R

- Find subdomains for a domain
- Install in Kali:

```
apt install sublist3r
Sublist3r -d <domain>
```

- Subdomains are useful to investigate
  - They are often independently managed by the local business unit or child organization
- They typically have fewer resources (and thus fewer security controls) than the parent organization



```
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for comptia.org
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 136
www.comptia.org
Intranet.comptia.org
www.Intranet.comptia.org
Lyncdiscover.comptia.org
LyncdiscoverInternal.comptia.org
academic-store.comptia.org
accessedge.comptia.org
accessedgedr.comptia.org
admin.comptia.org
```

LOCATION SEARCH TOOLS

Helps you perform physical or aerial reconnaissance of a target

- Google Maps
- Google Earth
- Wikimapia
- National Geographic Maps
- Yahoo Maps
- Bing Maps

2.6 WEBSITE FOOTPRINTING

- Website Footprinting
- Tools
- Spiders
- Mirroring
- Update Monitoring

WEBSITE FOOTPRINTING

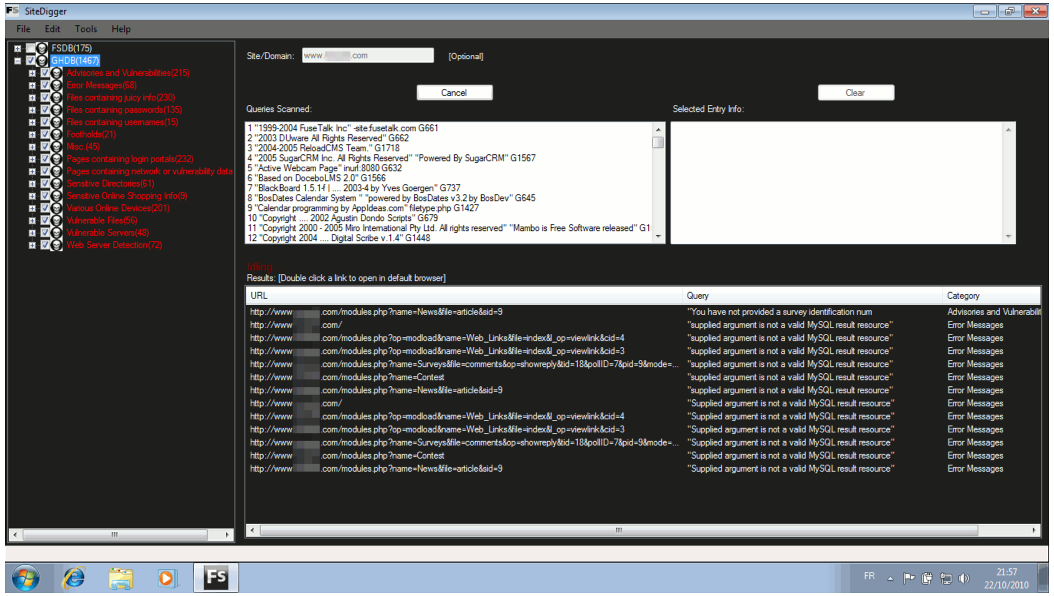
- Monitoring and analyzing the target's website for information
  - Browse the target website
- Use Burp Suite, Zaproxy, Paros Proxy, Website Informer, Firebug, etc. to determine:
  - Connection status and content-type
  - Accept-Ranges and Last-Modified information
  - X-Powered-By information
  - Web server version
- Examine HTML sources
- Examining cookies

WEB SEARCH ENUMERATION

- Use OSINT to discover additional information about a website
- Identify personnel, hostnames, domain names, and useful data residing on exposed web servers
- Search Google, Netcraft, Shodan, LinkedIn, PGP key servers, and other sites
- Search known domain names and IP blocks

SITEDIGGER

- Searches Google's cache
- Looks for vulnerabilities, errors, configuration issues, proprietary information, and interesting security nuggets on web sites
- Use it to find information that can be exposed through Google Dorking



- FSDB(175)
- GHDB(1467)
  - Advisories and Vulnerabilities(215)
  - Error Messages(68)
  - Files containing juicy info(230)
  - Files containing passwords(135)
  - Files containing usernames(15)
  - Footholds(21)
  - Misc.(45)
  - Pages containing login portals(232)
  - Pages containing network or vulnerability data
  - Sensitive Directories(61)
  - Sensitive Online Shopping Info(9)
  - Various Online Devices(201)
  - Vulnerable Files(56)
  - Vulnerable Servers(48)
  - Web Server Detection(72)

Site/Domain: www.[redacted].com [Optional]

Queries Scanned:

```
1 "1999-2004 FuseTalk Inc" -site:fusetalk.com G661
2 "2003 DUware All Rights Reserved" G662
3 "2004-2005 ReloadCMS Team." G1718
4 "2005 SugarCRM Inc. All Rights Reserved" "Powered By SugarCRM" G1567
5 "Active Webcam Page" inurl:8080 G632
6 "Based on DoceboLMS 2.0" G1566
7 "BlackBoard 1.5.1-f | .... 2003-4 by Yves Goergen" G737
8 "BosDates Calendar System " "powered by BosDates v3.2 by BosDev" G645
9 "Calendar programming by AppIdeas.com" filetype:php G1427
10 "Copyright .... 2002 Agustin Dondo Scripts" G679
11 "Copyright 2000 - 2005 Miro International Pty Ltd. All rights reserved" "Mambo is Free Software released" G1
12 "Copyright 2004 .... Digital Scribe v.1.4" G1448
```

Selected Entry Info:

Idling...

Results: [Double click a link to open in default browser]

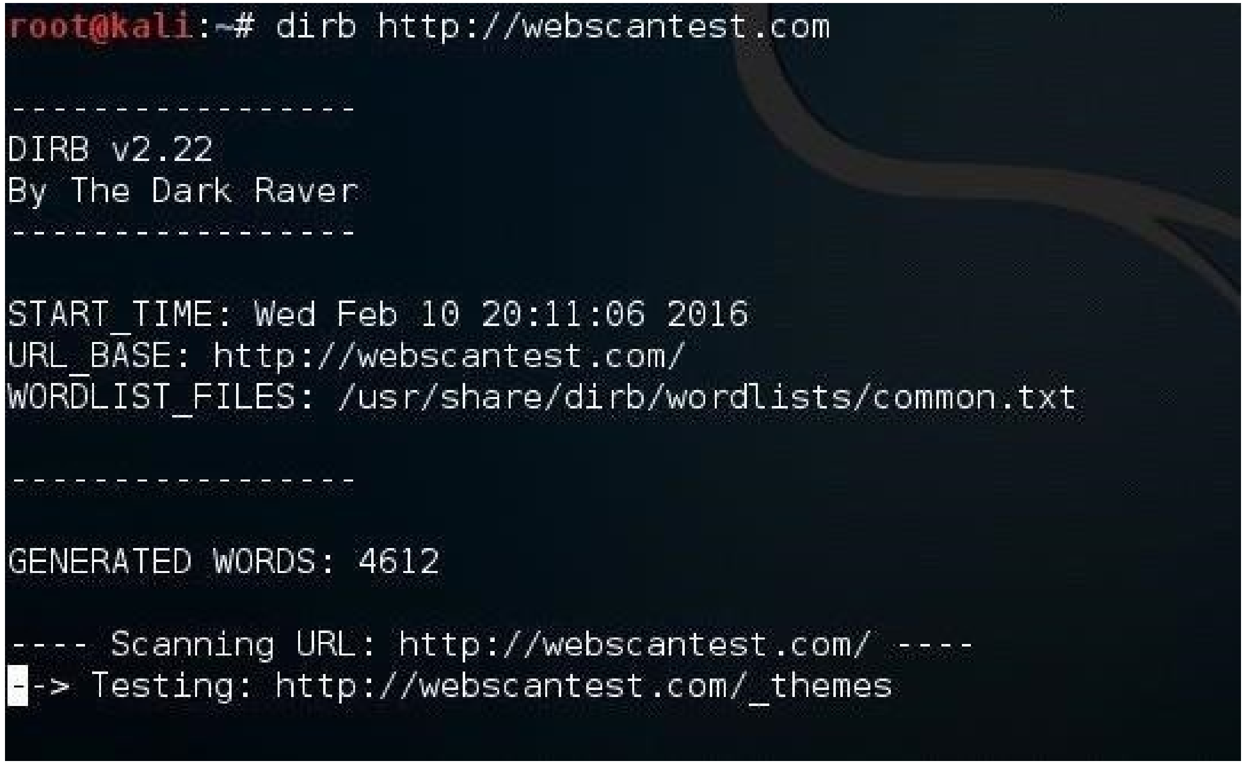
URL	Query	Category
http://www[redacted].com/modules.php?name=News&file=article&sid=9	"You have not provided a survey identification num	Advisories and Vulnerabilit
http://www[redacted].com/	"supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink&cid=4	"supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink&cid=3	"supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?name=Surveys&file=comments&op=showreply&tid=18&pollID=7&pid=9&mode=...	"supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?name=Contest	"supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?name=News&file=article&sid=9	"supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/	"Supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink&cid=4	"Supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?op=modload&name=Web_Links&file=index&l_op=viewlink&cid=3	"Supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?name=Surveys&file=comments&op=showreply&tid=18&pollID=7&pid=9&mode=...	"Supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?name=Contest	"Supplied argument is not a valid MySQL result resource"	Error Messages
http://www[redacted].com/modules.php?name=News&file=article&sid=9	"Supplied argument is not a valid MySQL result resource"	Error Messages

WEB SPIDERS

- Web spiders automate searches on the target website and collect information:
  - employee names, titles, addresses, email, phone and fax numbers, meta tags
- Helps with footprinting and social engineering attacks
- Tools
  - SpiderFoot
  - Visual SEO Studio
  - WildShark SEO Spider Tool
  - Beam Us Up SEO Spider SEO
  - Scrapy
  - Screaming Frog
  - Xenu

DIRB

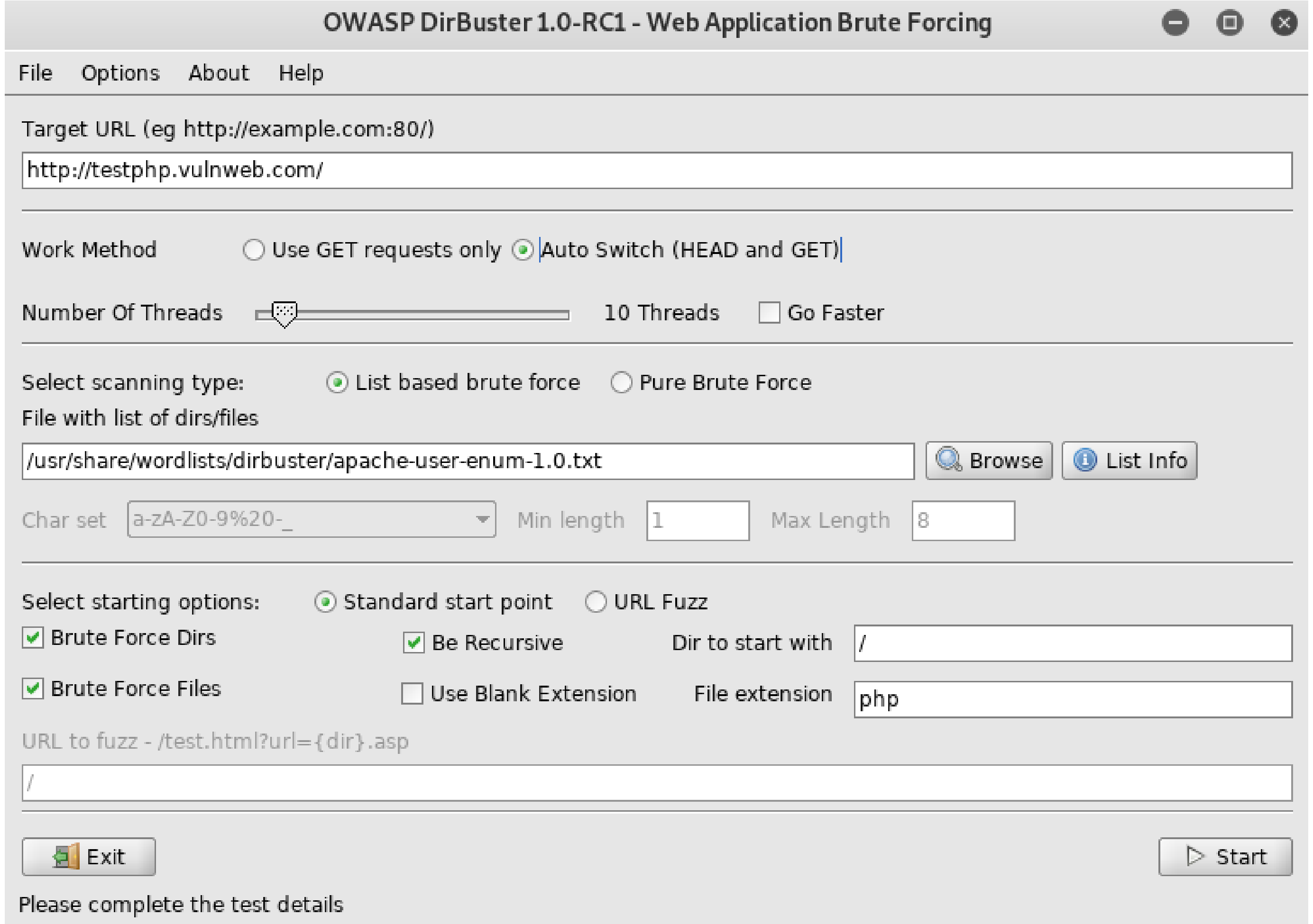
- Web content scanner
- Looks for existing and hidden web objects
- Useful for finding hidden subdirectories in a web app
- Works by launching a dictionary based attack against a web server
    - Analyzes the response



```
root@kali:~# dirb http://webscantest.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Feb 10 20:11:06 2016
URL_BASE: http://webscantest.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://webscantest.com/ ----
--> Testing: http://webscantest.com/_themes
```

DIRBUSTER

- Similar to DIRB
- GUI-based



Target URL (eg http://example.com:80/)

http://testphp.vulnweb.com/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/apache-user-enum-1.0.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp

/

Please complete the test details

WEBSITE MIRRORING

- Download an entire copy of the website to a local directory
- You can examine the entire website offline
- Helps gather information without making website requests that could be detected
- You can take your time searching
- Need to copy slowly

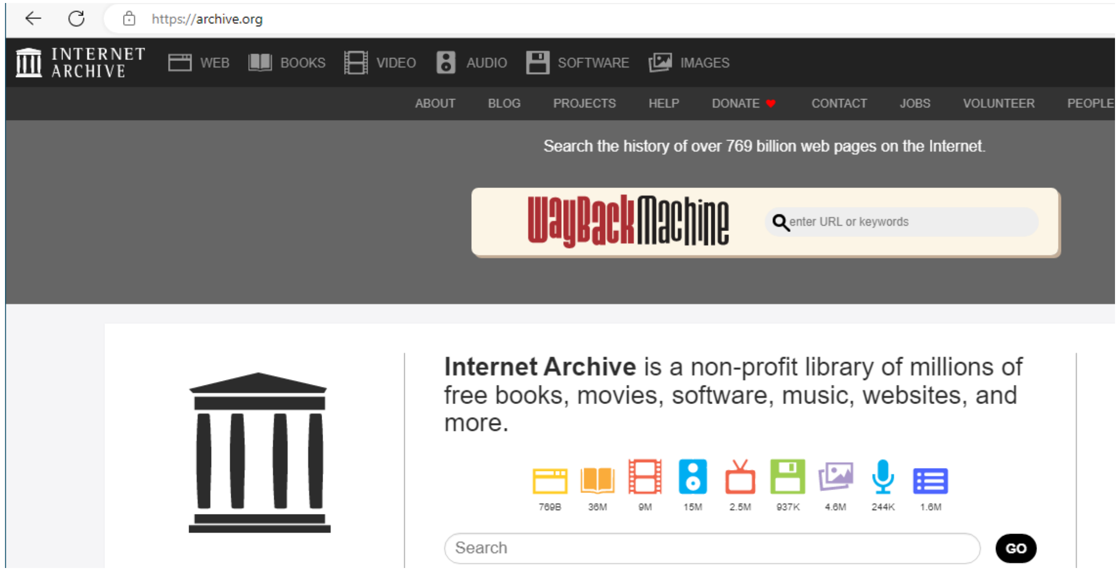
WEBSITE MIRRORING TOOLS

- HTTrack Web Site Copier
- SurfOffline
- Teleport Pro
- Portable Offline Browser
- Gnu Wget
- BlackWidow
- Ncollector Studio

- Website Ripper Copier
- PageNest
- Backstreet Browser
- Offline Explorer Enterprise
- Archive.org
- WebWatcher

ARCHIVE.ORG

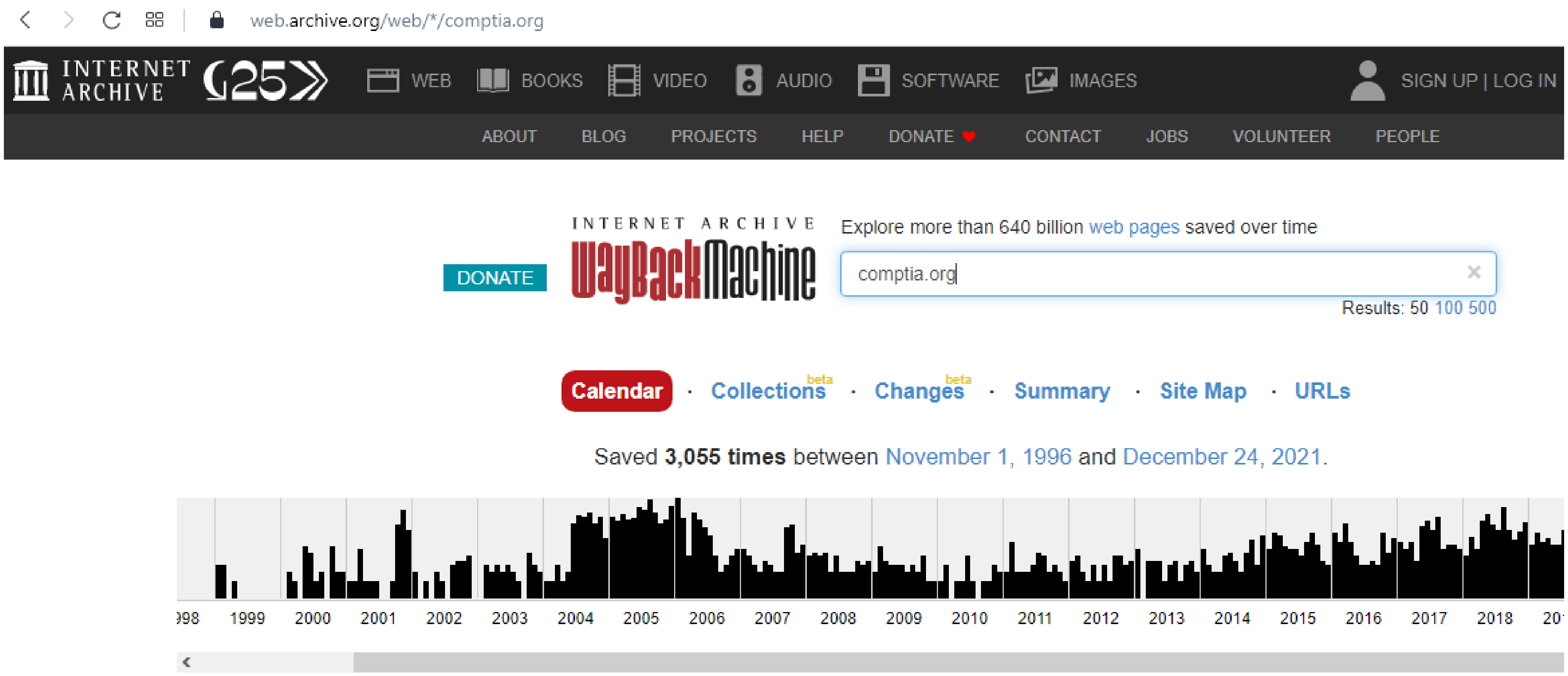
- Allows access to archived versions of the website
  - Copies the site as it was at the time
  - You can find information that was subsequently deleted
  - Archived sites may or may not include original downloads
- Also contains extensive content uploaded by the community



Search the history of over 769 billion web pages on the Internet.

Internet Archive is a non-profit library of millions of free books, movies, software, music, websites, and more.

ARCHIVE.ORG EXAMPLE



web.archive.org/web/*/comptia.org

Explore more than 640 billion web pages saved over time

comptia.org

Results: 50 100 500

Calendar · Collections beta · Changes beta · Summary · Site Map · URLs

Saved **3,055 times** between November 1, 1996 and December 24, 2021.

WEBSITE UPDATE MONITORING

- Automatically checks web pages for updates and changes
- Sends alerts to interested users
- Example tools:
  - Website Watcher
  - Visual Ping
  - Follow that Page
  - Watch that Page
  - Check4Change
  - OnWebChange
  - Infominder

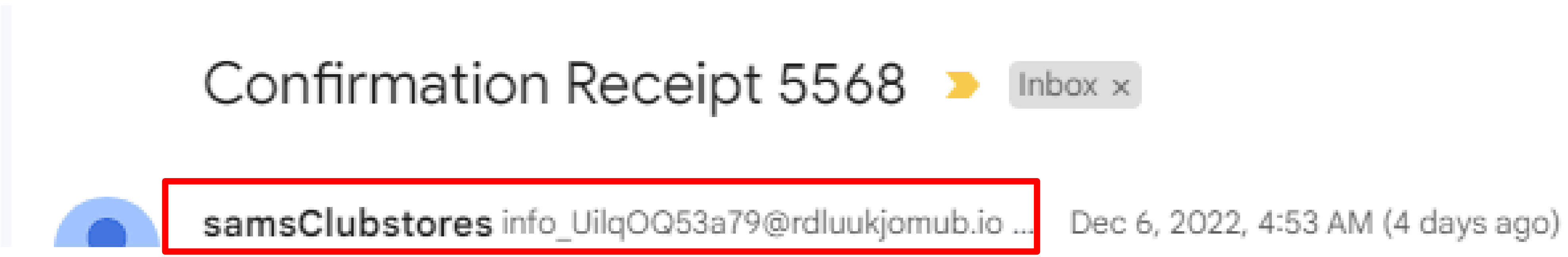
2.7 EMAIL FOOTPRINTING

- Email Source Header
- Email Tracking
- Email Tracking Tools

EMAIL SOURCE HEADER

- Reading the email source header can reveal:
  - Address from which the message was sent
  - Sender’s mail server
  - Authentication system used by sender’s mail server
  - Date and time of message
  - Sender’s name
- Also reveals:
  - Spoofed info
  - Bogus links and phishing techniques

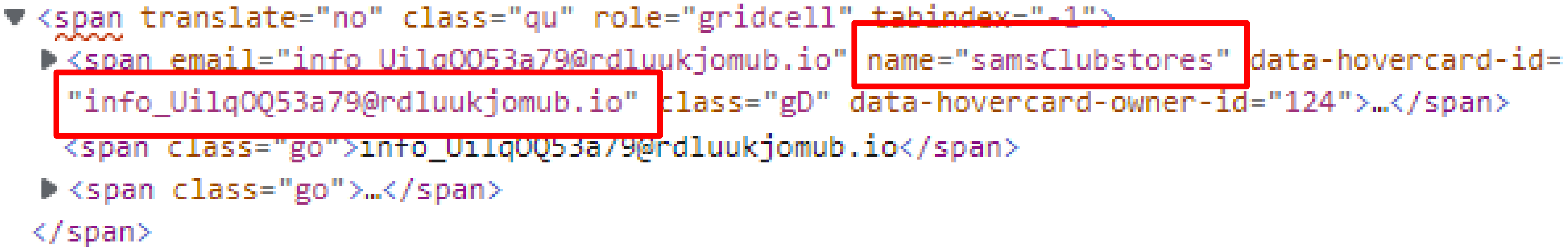
EMAIL SOURCE HEADER EXAMPLE



Confirmation Receipt 5568

samsClubstores info_UilqOQ53a79@rdluukjomub.io ...

Dec 6, 2022, 4:53 AM (4 days ago)



```
▼ <span translate="no" class="qu" role="gridcell" tabindex="-1">
  ▶ <span email="info_UilqOQ53a79@rdluukjomub.io" name="samsClubstores" data-hovercard-id=
   "info_UilqOQ53a79@rdluukjomub.io" class="gD" data-hovercard-owner-id="124">…</span>
   <span class="go">info_UilqOQ53a79@rdluukjomub.io</span>
  ▶ <span class="go">…</span>
 </span>
```

EMAIL TRACKING

Tracking emails can reveal:

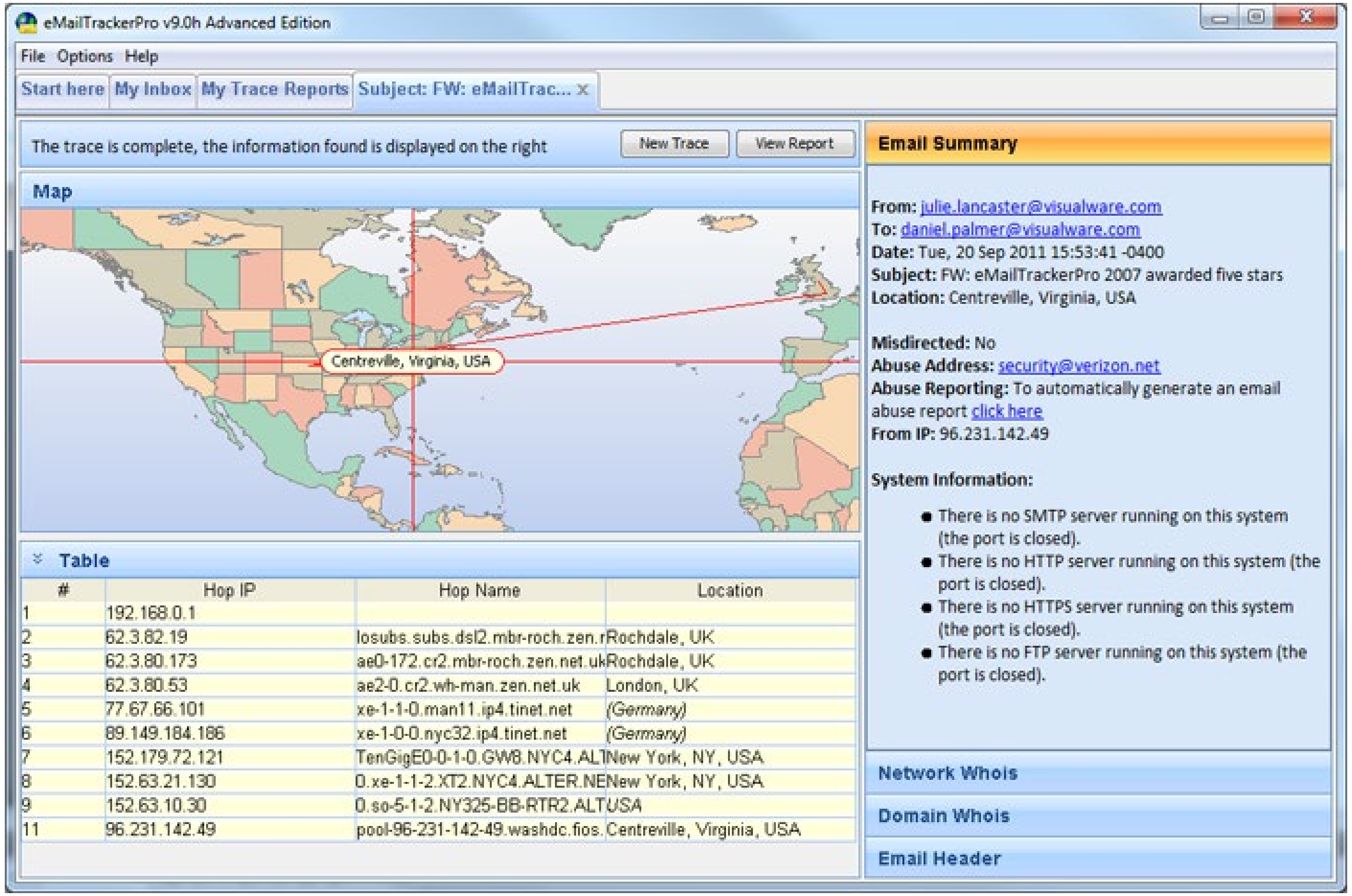
- Recipient IP address
- Geolocation
- Email received and read
- Read duration
- Proxy detection
- Links
- OS and Browser info
- Forwarded email
- Recipient device type

EMAIL TRACKING TOOLS

- EmailTrackerPro
- PoliteMail
- Yesware
- ContactMonkey
- Zendio
- ReadNotify
- DidTheyReadit

- Trace Email
- Email Lookup
- Pointofmail
- WhoReadMe
- GetNotigy
- G-Lock Analytics

EMAILTRACKERPRO EXAMPLE



The trace is complete, the information found is displayed on the right

#	Hop IP	Hop Name	Location
1	192.168.0.1		
2	62.3.82.19	losubs.subs.dsl2.mbr-roch.zen.r	Rochdale, UK
3	62.3.80.173	ae0-172.cr2.mbr-roch.zen.net.uk	Rochdale, UK
4	62.3.80.53	ae2-0.cr2.wh-man.zen.net.uk	London, UK
5	77.67.66.101	xe-1-1-0.man11.ip4.tinet.net	*(Germany)*
6	89.149.184.186	xe-1-0-0.nyc32.ip4.tinet.net	*(Germany)*
7	152.179.72.121	TenGigE0-0-1-0.GW8.NYC4.ALT	New York, NY, USA
8	152.63.21.130	0.xe-1-1-2.XT2.NYC4.ALTER.NE	New York, NY, USA
9	152.63.10.30	0.so-5-1-2.NY325-BB-RTR2.ALT	*USA*
11	96.231.142.49	pool-96-231-142-49.washdc.fios.	Centreville, Virginia, USA

Email Summary

From: julie.lancaster@visualware.com
To: daniel.palmer@visualware.com
Date: Tue, 20 Sep 2011 15:53:41 -0400
Subject: FW: eMailTrackerPro 2007 awarded five stars
Location: Centreville, Virginia, USA

Misdirected: No
Abuse Address: security@verizon.net
Abuse Reporting: To automatically generate an email abuse report click here
From IP: 96.231.142.49

System Information:

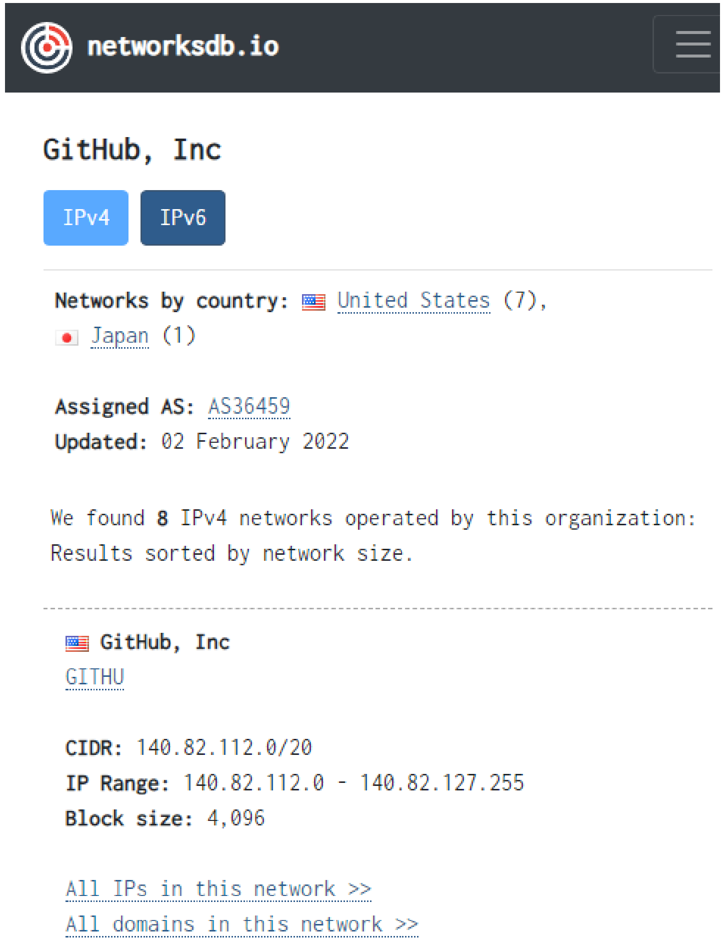
- There is no SMTP server running on this system (the port is closed).
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

2.8 NETWORK FOOTPRINTING

- Network Range
- Network Whois
- Traceroute

LOCATE NETWORK RANGE

- Map the target network
- Find in RIR whois database search
- Search online:
  - https://centralops.net/co/domaindossier.aspx
  - https://networksdb.io/ip-addresses-of/
- Use command prompt tools:
  - whois
  - curl



GitHub, Inc

Networks by country: United States (7), Japan (1)

Assigned AS: AS36459
Updated: 02 February 2022

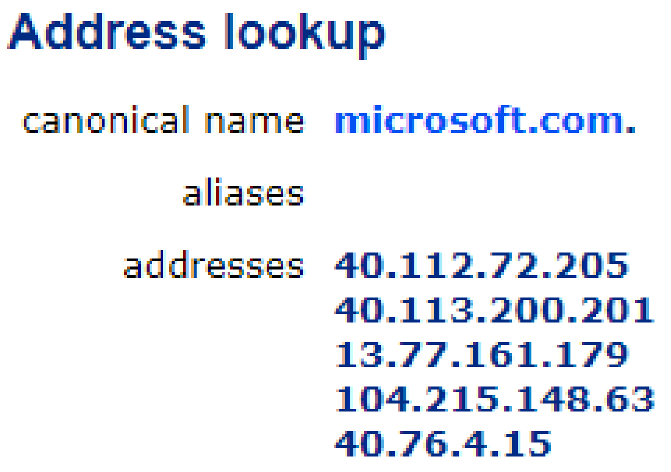
We found **8** IPv4 networks operated by this organization:
Results sorted by network size.

GitHub, Inc
GITHU

CIDR: 140.82.112.0/20
IP Range: 140.82.112.0 - 140.82.127.255
Block size: 4,096

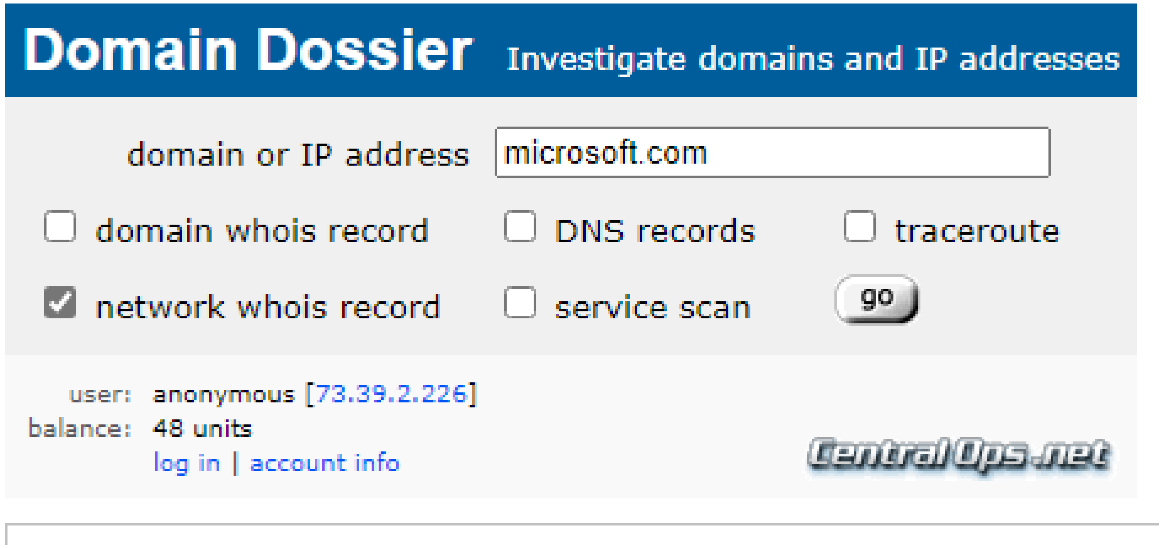
All IPs in this network >>
All domains in this network >>

NETWORK WHOIS EXAMPLE



Address lookup

```
canonical name   microsoft.com.
       aliases
     addresses   40.112.72.205
                 40.113.200.201
                 13.77.161.179
                 104.215.148.63
                 40.76.4.15
```



Domain Dossier

Investigate domains and IP addresses

domain or IP address: microsoft.com

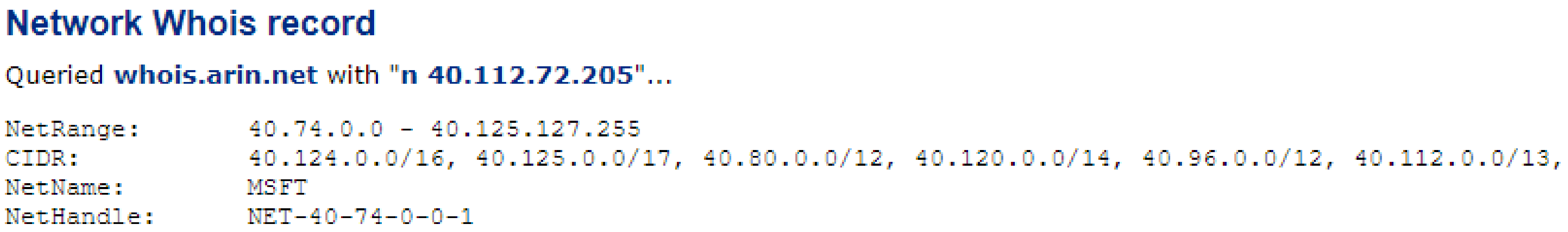
□ domain whois record　□ DNS records　□ traceroute

☑ network whois record　□ service scan　go

user: anonymous [73.39.2.226]

balance: 48 units

log in | account info



Network Whois record

Queried **whois.arin.net** with **"n 40.112.72.205"**...

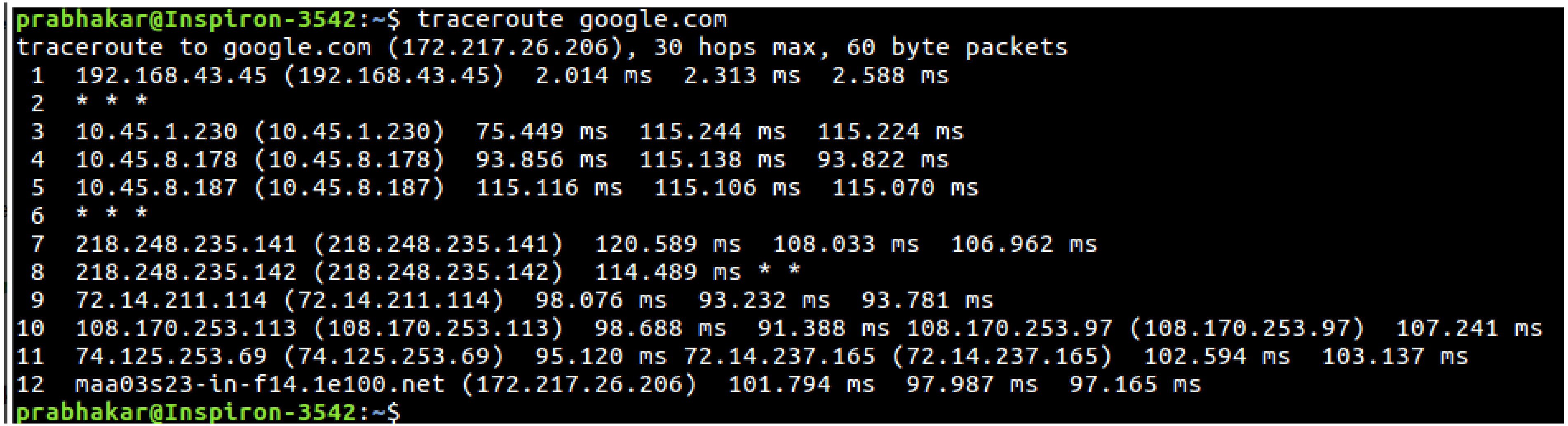
```
NetRange:       40.74.0.0 - 40.125.127.255
CIDR:           40.124.0.0/16, 40.125.0.0/17, 40.80.0.0/12, 40.120.0.0/14, 40.96.0.0/12, 40.112.0.0/13,
NetName:        MSFT
NetHandle:      NET-40-74-0-0-1
```

COMMAND LINE NETWORK WHOIS EXAMPLE

```
$ host -t a github.io
github.io has address 185.199.109.153

$ whois 185.199.109.153

inetnum:        185.199.108.0 - 185.199.111.255
netname:        US-GITHUB-20170413
country:        US

$ curl -s https://networksdb.io/ip-addresses-of/github-inc | grep 'IP Range' | awk '{print $3" - "$5}' | sort
140.82.112.0 - 140.82.127.255
148.62.46.150 - 148.62.46.151
```

TRACEROUTE

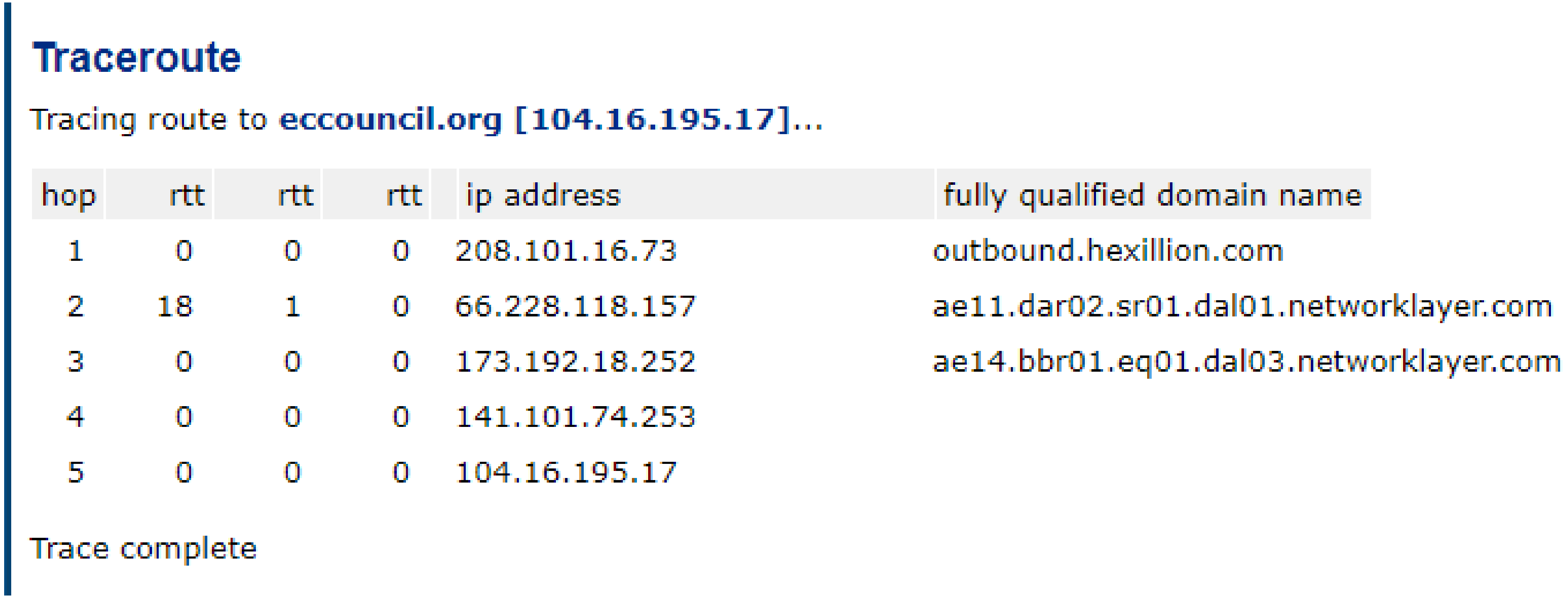
- Discover routers and firewalls along the path to a target
- Uses ICMP or UDP with an increasing TTL to elicit router identification
- Find the IP address of the target firewall
- Help map the target network



```
prabhakar@Inspiron-3542:~$ traceroute google.com
traceroute to google.com (172.217.26.206), 30 hops max, 60 byte packets
 1  192.168.43.45 (192.168.43.45)  2.014 ms  2.313 ms  2.588 ms
 2  * * *
 3  10.45.1.230 (10.45.1.230)  75.449 ms  115.244 ms  115.224 ms
 4  10.45.8.178 (10.45.8.178)  93.856 ms  115.138 ms  93.822 ms
 5  10.45.8.187 (10.45.8.187)  115.116 ms  115.106 ms  115.070 ms
 6  * * *
 7  218.248.235.141 (218.248.235.141)  120.589 ms  108.033 ms  106.962 ms
 8  218.248.235.142 (218.248.235.142)  114.489 ms * *
 9  72.14.211.114 (72.14.211.114)  98.076 ms  93.232 ms  93.781 ms
10  108.170.253.113 (108.170.253.113)  98.688 ms  91.388 ms 108.170.253.97 (108.170.253.97)  107.241 ms
11  74.125.253.69 (74.125.253.69)  95.120 ms 72.14.237.165 (72.14.237.165)  102.594 ms  103.137 ms
12  maa03s23-in-f14.1e100.net (172.217.26.206)  101.794 ms  97.987 ms  97.165 ms
prabhakar@Inspiron-3542:~$
```

ONLINE TRACEROUTE EXAMPLE

- https://www.monitis.com/traceroute/
- https://centralops.net/co/



Traceroute

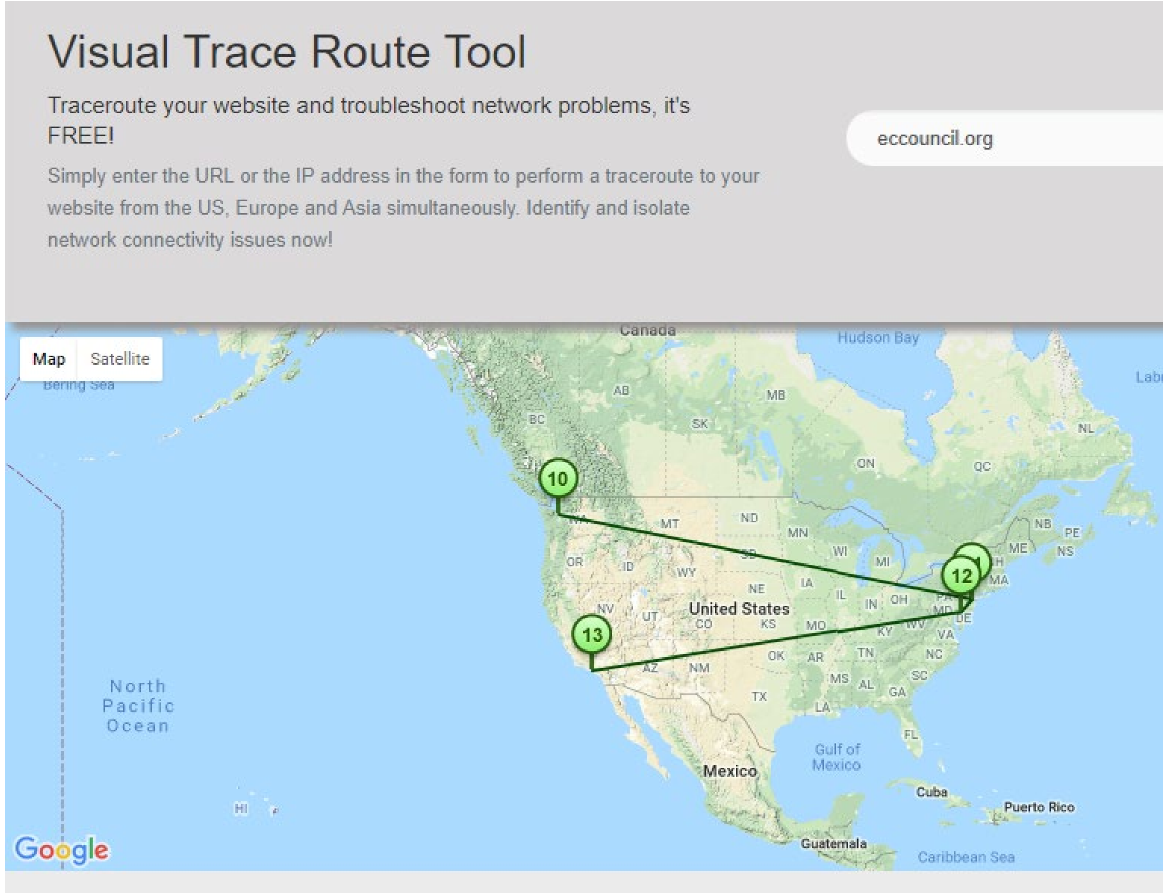
Tracing route to **eccouncil.org [104.16.195.17]...**

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	0	0	0	208.101.16.73	outbound.hexillion.com
2	18	1	0	66.228.118.157	ae11.dar02.sr01.dal01.networklayer.com
3	0	0	0	173.192.18.252	ae14.bbr01.eq01.dal03.networklayer.com
4	0	0	0	141.101.74.253	
5	0	0	0	104.16.195.17	

Trace complete

TRACEROUTE TOOLS

- Path Analyzer Pro
- VisualRoute
- Network Pinger
- GEOSpider
- vTrace
- Trout
- Roadkil's Trace Route
- Magic NetTrace
- 3D Traceroute
- AnalogX HyperTrace
- Network Systems Traceroute
- Ping Plotter



Visual Trace Route Tool

Traceroute your website and troubleshoot network problems, it's FREE!

Simply enter the URL or the IP address in the form to perform a traceroute to your website from the US, Europe and Asia simultaneously. Identify and isolate network connectivity issues now!

eccouncil.org

2.9 FOOTPRINTING THROUGH SOCIAL NETWORKING SITES

- Social Networking Sites
- Information
- People Search
- Social Media Groups

SOCIAL NETWORKING SITES

- Attackers use social networking sites to gain important and sensitive data about their target
  - They often create fake profiles through these social media
  - Aim is to lure their target and extract vulnerable information
- Employees may post :
  - Personal information such as DOB, educational and employment background, spouse’s names, etc.
  - Information about their company such as potential clients and business partners, trade secrets of business, websites, company’s upcoming news, mergers, acquisitions, etc.
- Common social networking sites used:
  - Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, YouTube, Instagram

INFORMATION FROM SOCIAL NETWORKING SITES

- Present activity/physical location
- Job activities
- Company information
- Contact details, names, numbers, addresses, date of birth, photos
- Family & friends
- Property information
- Bank details
- Background and criminal checks

PEOPLE SEARCH

- A great source of personal and organizational information
- Residential addresses, email addresses, phone number
  - Satellite photos of residences
- Date of birth
- Photos and social networking profiles
- Friends/family/associates
- Hobbies/current activities/blogs
- Work information
  - Projects and operating environment
  - Travel details

PEOPLE SEARCH SITES

- CheckPeople
- BeenVerified
- Truthfinder
- peopleWhiz
- PeopleLooker
- Intelius
- Checkmate
- Peoplefinders
- IDtrue

SOCIAL MEDIA GROUPS, FORUMS, BLOGS

- Social Media groups, forums, and blogs provide more intimate information about a person
  - Current interests
  - Current activities
  - Hobbies
  - Political and social viewpoints
- Can be used to cultivate a relationship with the target
- Attackers create fictious profiles and attempt to join groups
- Disinformation campaigns use bots to:
  - Automate posting
  - Increase visibility of an issue
  - Give malicious information traction
  - Make an opinion or idea seem to be popular

2.10 FOOTPRINTING AND RECONNAISSANCE COUNTER-MEASURES

- Mitigation and protection methods

OSINT COUNTERMEASURES

- Recognize that once information is on the Internet, it might never fully disappear
- Perform OSINT on yourself regularly to see what's out there
- Identify information that might be harmful
- When possible, go to the sites that publish that information and remove it
- Delete/deactivate unnecessary social media profiles
- Use an identity protection service
- Use Shodan and Google Dorks to search for exposed files and devices
  - If any are discovered, implement protective measures

OSINT COUNTERMEASURES (CONT'D)

- Set up a monitoring service such as Google Alerts to notify you if new information appears
- Train yourself (and your employees) to recognize the danger and be cautious about what they share on social media
- If possible, use a data protection solution to minimize data leakage from the company
- Turn off tracking features on your phone and configure privacy settings
- Disable location on photos you plan to post publicly on social media
- Remove metadata from images if you don't want others to know which device you are using to capture

OSINT COUNTERMEASURES (CONT'D)

- Conduct only private dialogues, trying to avoid public communication on forums and other sites
- Keep a close eye on which web pages and portals you visit
- Some of them may require too much information for registration: name, phone number, real address
- Use different nicknames on the Internet – it will be much more difficult to find you
- Switch your profile to private mode, if the social network allows you to do this
- When adding friends on social media, only add people you actually know in real life

2.11 FOOTPRINTING AND RECONNAISSANCE REVIEW

- Review

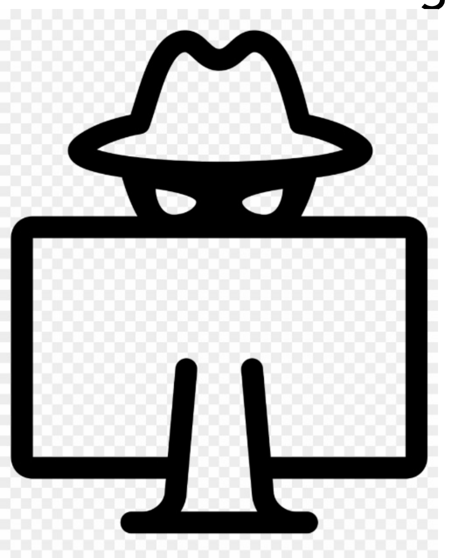
FOOTPRINTING RECONNAISSANCE REVIEW

- Footprinting gathers as much information as possible about a target in advance of the attack
  - You’re looking for any information that can help you break into the target network
- Footprinting can be passive or active
- It’s usually subtle / unnoticeable
- Small, random, seemingly unimportant details can together paint a bigger picture or become important later in your hacking efforts

- Research sources can include:
  - Search engines
  - Whois
  - Websites
  - Social media
  - Social networking sites
  - Job boards
  - Press releases
  - Advanced online services
  - DNS
  - Email
  - Competitive intelligence sites
  - Limited social engineering

FOOTPRINTING RECONNAISSANCE REVIEW

- OSINT is the use of publicly available sources and tools to footprint a target
- You can perform advanced Google searches using “dorks” (search strings with advanced operators)
- The Google Hacking Database (GHDB) lists popular dorks created by the community
- Whois is a protocol for searching domain registration information
- You can use dig, nslookup, and many other tools to query a DNS server for host



- You can footprint websites through the use of:
  - Spiders that automatically crawl through a website looking for specific types of information
  - Site mirroring so you can take your time examining an offline copy of the website
  - Tools like dirb and DirBuster that attempt to uncover hidden subdirectories on a website
  - Google cache and archive.org that maintain snapshots of websites over time

FOOTPRINTING RECONNAISSANCE REVIEW

- You can examine email headers and use email tracking tools to identify the actual source of an email
- You can use Whois, traceroute, and other tools to identify IP blocks, the firewall IP address, and other network-available points of entry to the target
- Social networking sites and social media can provide a wealth of information