The Bug Hunter's Methodology Live

THE MOST IMPORTANT THING

.ENV

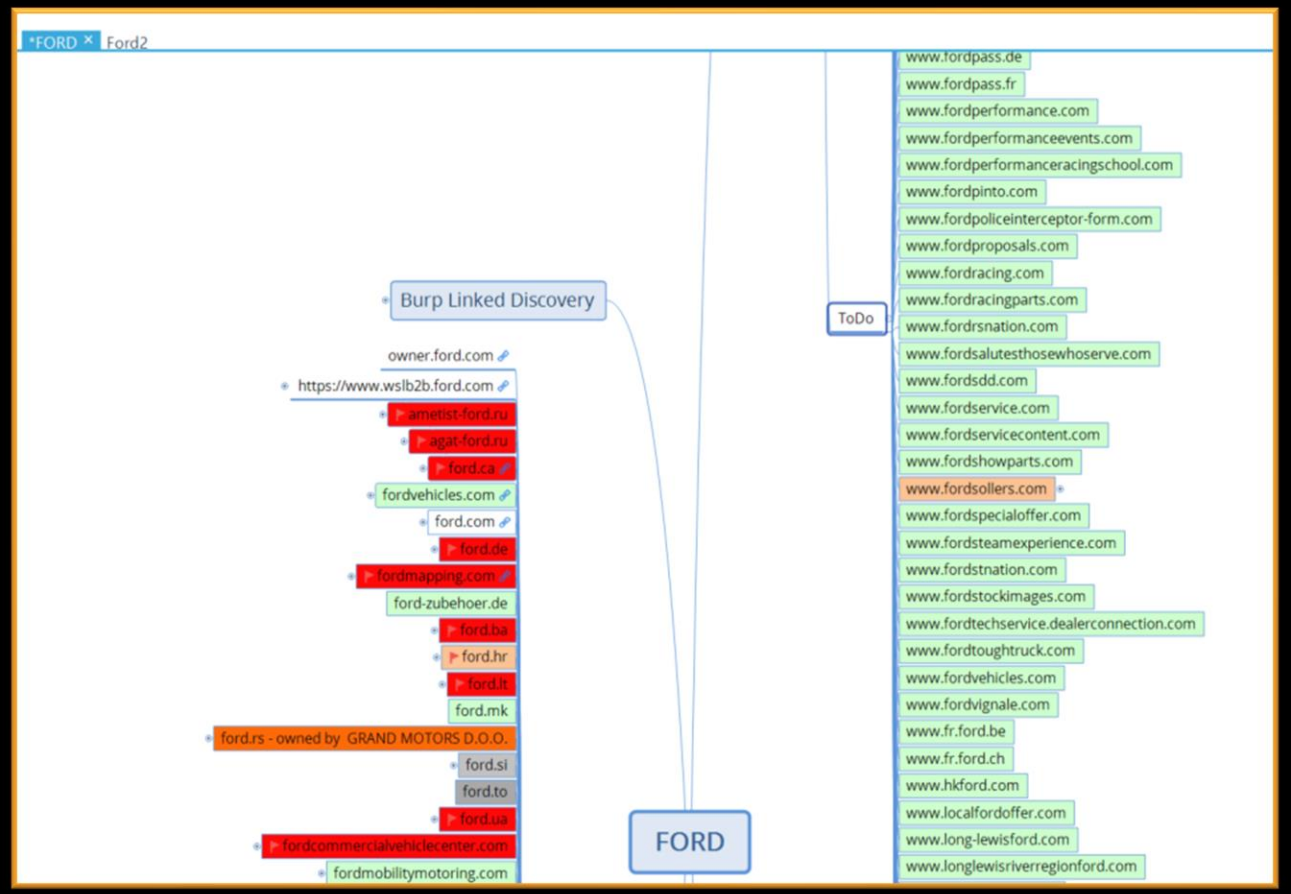
Sample Targets

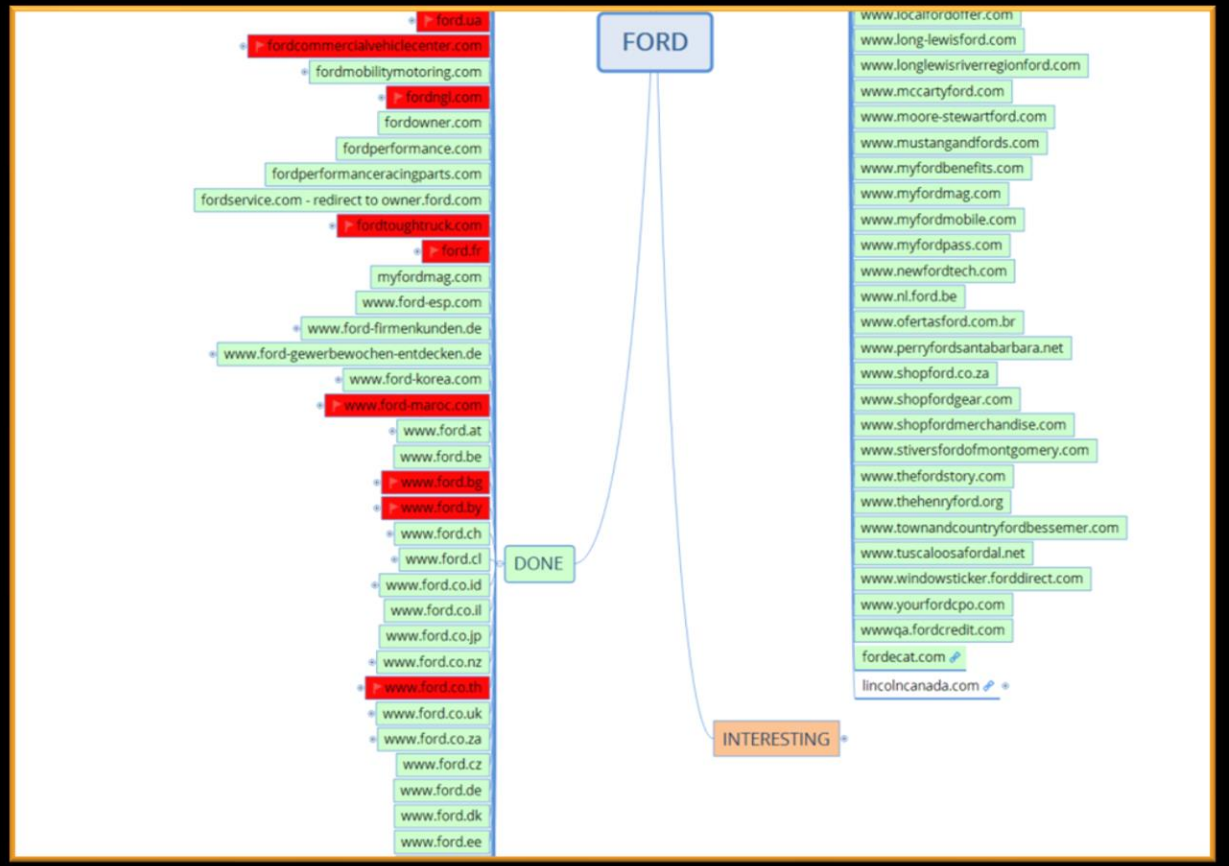
Note Taking

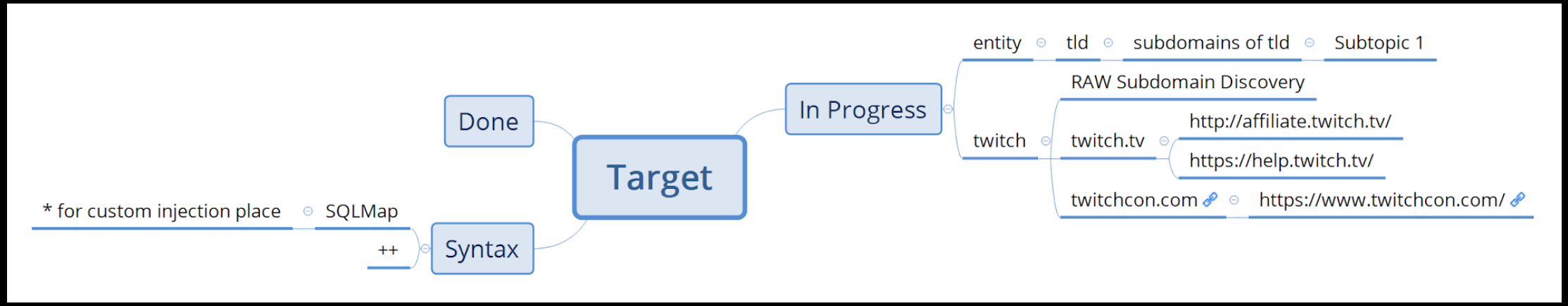
In many parts of the course, we will need to keep track of site-hierarchy, tools output, interesting notes, etc.

I will be using mind maps with Xmind throughout the course, but the same effect can be achieved through multiple different programs.

Mind maps allow me to visualize large-scope bug hunting targets and to break up methodology for in-depth bug hunting.


*FORD
Ford2
Burp Linked Discovery
owner.ford.com
https://www.wslb2b.ford.com
ametist-ford.ru
agat-ford.ru
ford.ca
fordvehicles.com
ford.com
ford.de
fordmapping.com
ford-zubehoer.de
ford.ba
ford.hr
ford.lt
ford.mk
ford.rs - owned by GRAND MOTORS D.O.O.
ford.si
ford.to
ford.ua
fordcommercialvehiclecenter.com
fordmobilitymotoring.com
FORD
ToDo
www.fordpass.de
www.fordpass.fr
www.fordperformance.com
www.fordperformanceevents.com
www.fordperformanceracingschool.com
www.fordpinto.com
www.fordpoliceinterceptor-form.com
www.fordproposals.com
www.fordracing.com
www.fordracingparts.com
www.fordrsnation.com
www.fordsalutesthosewhoserve.com
www.fordsdd.com
www.fordservice.com
www.fordservicecontent.com
www.fordshowparts.com
www.fordsollers.com
www.fordspecialoffer.com
www.fordsteamexperience.com
www.fordstnation.com
www.fordstockimages.com
www.fordtechservice.dealerconnection.com
www.fordtoughtruck.com
www.fordvehicles.com
www.fordvignale.com
www.fr.ford.be
www.fr.ford.ch
www.hkford.com
www.localfordoffer.com
www.long-lewisford.com
www.longlewisriverregionford.com

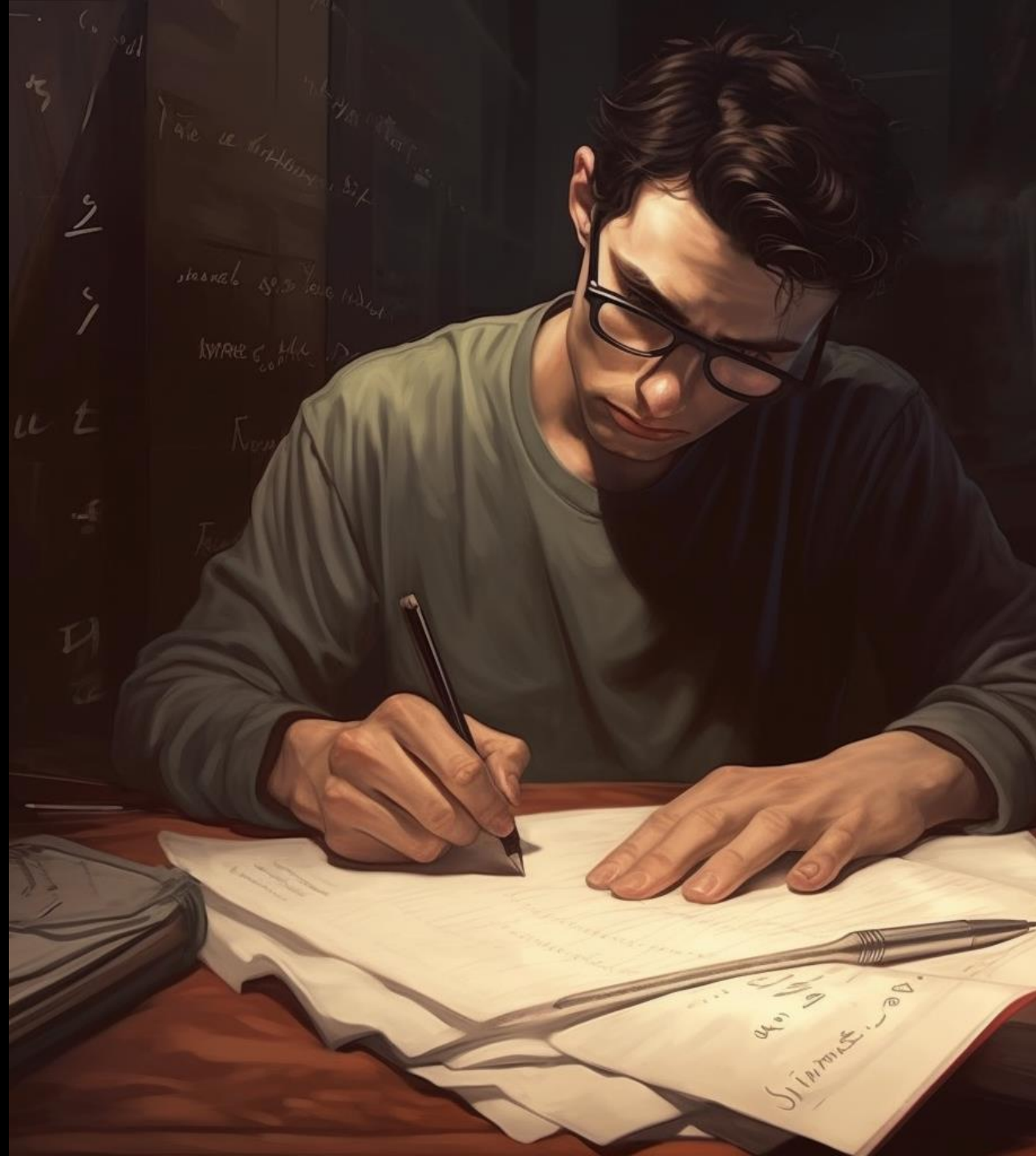

FORD
DONE
ford.ua
fordcommercialvehiclecenter.com
fordmobilitymotoring.com
fordngl.com
fordowner.com
fordperformance.com
fordperformanceracingparts.com
fordservice.com - redirect to owner.ford.com
fordtoughtruck.com
ford.fr
myfordmag.com
www.ford-esp.com
www.ford-firmenkunden.de
www.ford-gewerbewochen-entdecken.de
www.ford-korea.com
www.ford-maroc.com
www.ford.at
www.ford.be
www.ford.bg
www.ford.by
www.ford.ch
www.ford.cl
www.ford.co.id
www.ford.co.il
www.ford.co.jp
www.ford.co.nz
www.ford.co.th
www.ford.co.uk
www.ford.co.za
www.ford.cz
www.ford.de
www.ford.dk
www.ford.ee
INTERESTING
www.localfordoffer.com
www.long-lewisford.com
www.longlewisriverregionford.com
www.mccartyford.com
www.moore-stewartford.com
www.mustangandfords.com
www.myfordbenefits.com
www.myfordmag.com
www.myfordmobile.com
www.myfordpass.com
www.newfordtech.com
www.nl.ford.be
www.ofertasford.com.br
www.perryfordsantabarbara.net
www.shopford.co.za
www.shopfordgear.com
www.shopfordmerchandise.com
www.stiversfordofmontgomery.com
www.thefordstory.com
www.thehenryford.org
www.townandcountryfordbessemer.com
www.tuscaloosafordal.net
www.windowsticker.forddirect.com
www.yourfordcpo.com
wwwqa.fordcredit.com
fordecat.com
lincolncanada.com



That mind map grew from a simple template like the one above. Sometimes the format changes of how I notate but it's always similar.

Green = site / entity had no vulns
Orange = currently in progress of testing or saving for later
Red = vulns found
✅ Checkmark icon (or strikethrough) = completed

TEMPLATES AND REPORTING



Template Musings

You can keep track of targets, status/workflow, common tool syntax, and common reporting templates:

 # Technical Issue - Cross Site Scripting

The resource `payments` in the parameter `month` is vulnerable to reflected cross-site scripting. Once authenticated if a user is passed the URL:

* https://XXXX.com/payments?month=%3Cscript%3Ealert(%27XSS%27)%3C/script%3E

JavaScript will be executed against the person visiting the link.

* payload: `<script>alert('XSS')</script>`

 # Reproduction

* login (create a free account)
* visit the link to see the PoC alert

Templates

 # Impact

Attackers can leverage XSS to target, phish, and impersonate users of the application. This is possible because the vulnerability allows the attacker to gain the user's trust by using exploit links that appear to be from the application (xxxx.com).

In the context of this application, which handles highly sensitive user date, XSS attacks enable attackers to specifically target and access personally identifiable information (PII) of users. This poses a significant threat to the privacy and security of the affected individuals.

 # Developer and Remediation Notes

1. Always treat all user input as untrusted data.
2. Never insert untrusted data except in allowed locations.
3. Always input or output-encode all data coming into or out of the application.
4. Always whitelist allowed characters and seldom use blacklisting of characters except in certain use 5. cases.
5. Always use a well-known and security encoding API for input and output encoding such as the `OWASP ESAPI` or other framework provided solutions.
6. Never try to write input and output encoders unless absolutely necessary. Chances are that someone has already written a good one.
7. Never use the DOM function `innerHtml` and instead use the functions `innerText` and `textContent` to 8. prevent against DOM-based XSS.
8. As a best practice, consider using the `HTTPOnly` flag on cookies that are session tokens or sensitive tokens.
9. As a best practice, consider implementing `Content Security Policy` to protect against XSS and other injection type attacks.
10. As a best practice, consider using an auto-escaping templating system
11. As a best practice, consider using the `X-XSS-Protection` response header.

 # References

- https://www.owasp.org/index.php/Top_10_2013-A3-Cross-Site_Scripting_(XSS)
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
- http://projects.webappsec.org/Cross-Site+Scripting
- https://www.cvedetails.com/vulnerability-list/opxss-1/xss.html

Decent but generic

To enhance XSS security:

• While the field/parameter X inherits default framework protections from XSS, further validation and sanitization is needed to ensure it meets expected formats, length limits, and character sets. Consider whitelisting characters rather than blacklisting. Consider implementing DOMPurify an industry respected XSS sanitization library.

• Encode untrusted data before inserting it into HTML, JavaScript, CSS, or other contexts, using appropriate encoding methods. Use HTML entity encoding (<, >, etc.) or context-specific encoding libraries (e.g., OWASP Java Encoder) where possible.

• Safely manipulate the DOM by avoiding vulnerable methods like innerHTML and using safer alternatives such as textContent or createTextNode.

• Secure cookies by setting the HttpOnly flag to prevent client-side JavaScript access and the Secure flag to restrict transmission to secure connections.

• Implement a strict Content Security Policy (CSP) to restrict content loading and execution, specifying trusted sources and limiting inline scripts.

• Utilize auto-escaping templating systems that automatically encode untrusted data based on the output context.

• Enable the X-XSS-Protection response header with the value "1; mode=block" to activate the browser's XSS filter.

Better. More detail. Specific.

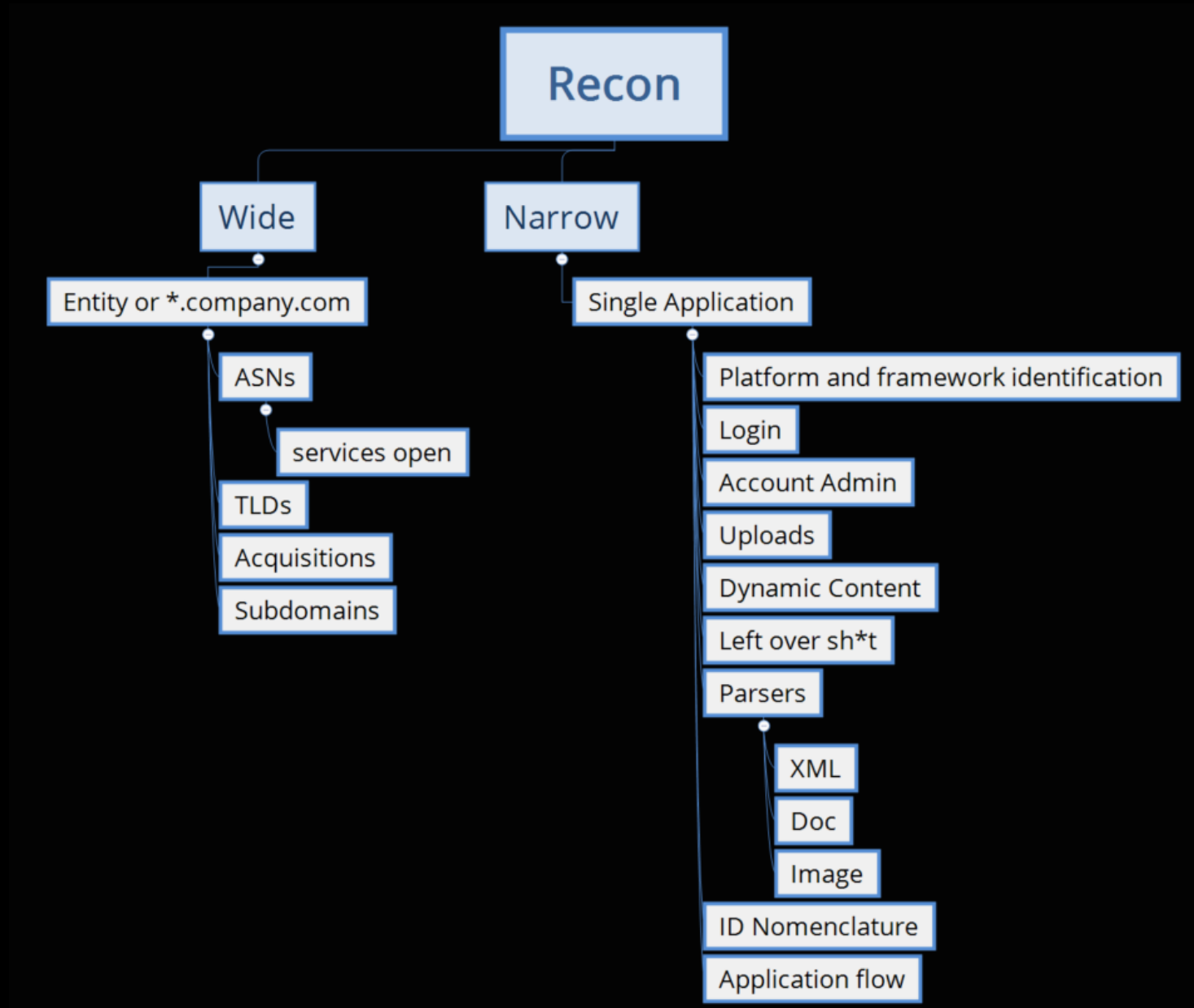
RECON INTRO

RECON CONCEPTS

Depending on your security testing engagement (bounty, pentest, etc.) it's important to understand your scope and what kind of testing you prefer to do.

Going "wide" results in finding sites that have often been left less secure than a "flagship" application. Some of these wide scope sites may be worth less due to their threat profile to the entity, but bugs are plentiful.

Focusing "narrow" is more involved and yields much higher payouts (normally) but requires you to invest a lot of time to understand the application.



What are we after?

APEX DOMAINS - www.twitch.tv

SUBDOMAINS - www.twitch.tv

IP Addresses

Services

Contextual Business & Tech Intel

Why?

For every subdomain you find you 2x your chance of hacking the target.

For every apex domain you find you 4x your chance of hacking the target.

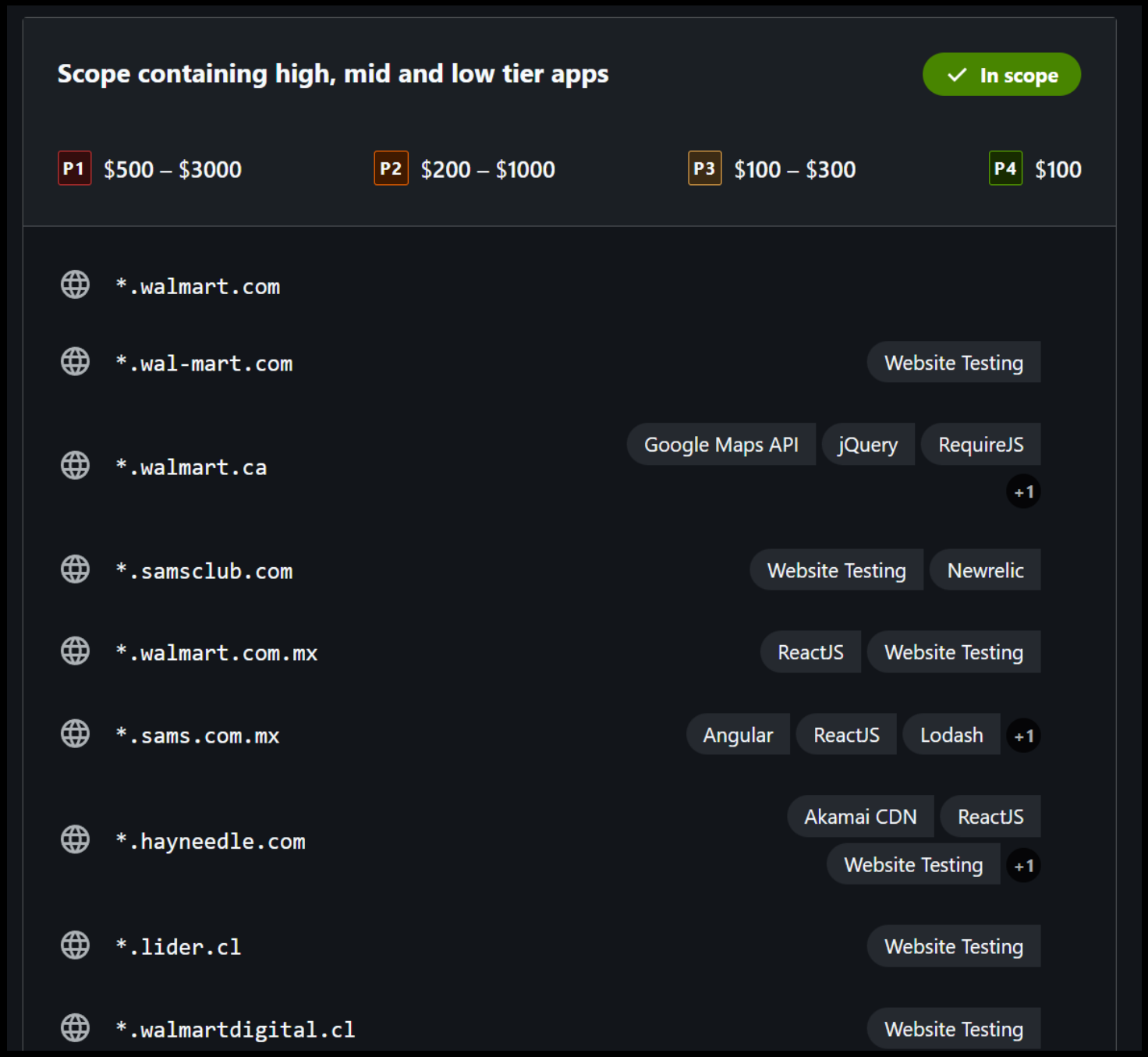
RECON IS A CYCLE

Good recon has a lot of “jumping” around.

It’s not a linear process.

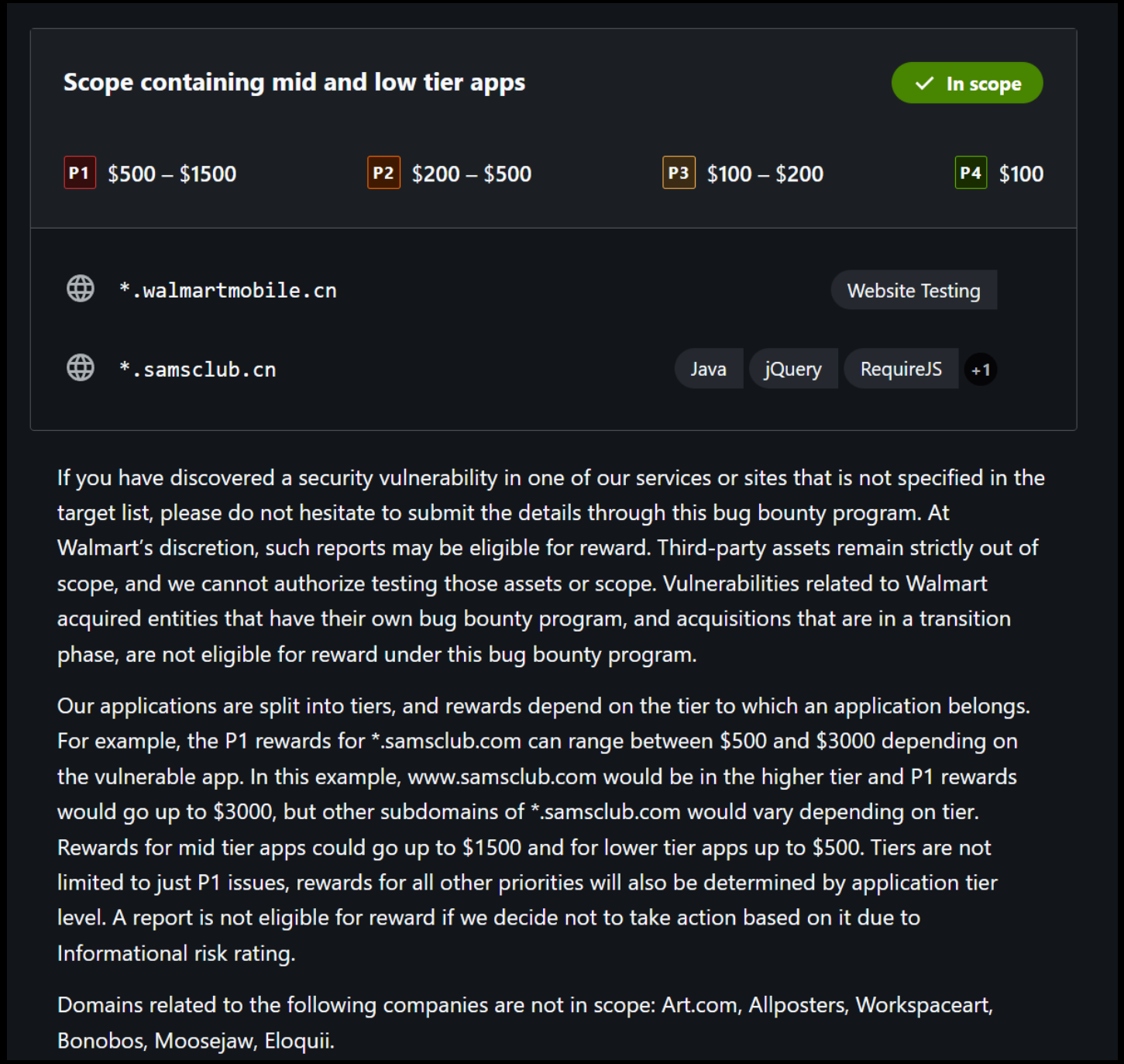
RECON

CREATING WIDER SCOPE



The * represents that we have permission to enumerate and hack any subdomains for the apex domain.

Watch for “catch all” statements at the bottom of the scope sections for all programs



Scope containing mid and low tier apps — In scope

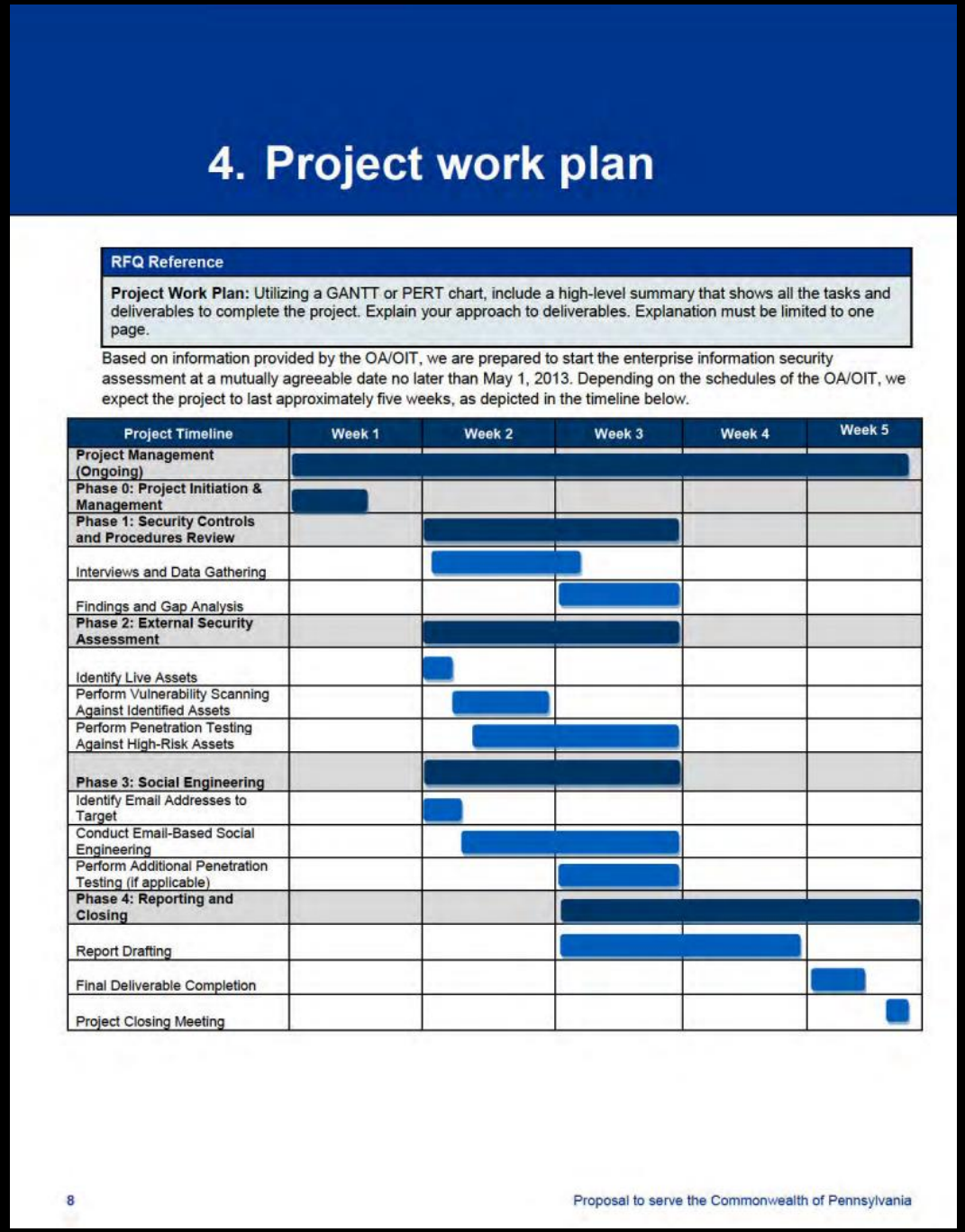
P1	P2	P3	P4
$500 – $1500	$200 – $500	$100 – $200	$100

*.walmartmobile.cn	Website Testing
*.samsclub.cn	Java, jQuery, RequireJS, +1

If you have discovered a security vulnerability in one of our services or sites that is not specified in the target list, please do not hesitate to submit the details through this bug bounty program. At Walmart’s discretion, such reports may be eligible for reward. Third-party assets remain strictly out of scope, and we cannot authorize testing those assets or scope. Vulnerabilities related to Walmart acquired entities that have their own bug bounty program, and acquisitions that are in a transition phase, are not eligible for reward under this bug bounty program.

Our applications are split into tiers, and rewards depend on the tier to which an application belongs. For example, the P1 rewards for *.samsclub.com can range between $500 and $3000 depending on the vulnerable app. In this example, www.samsclub.com would be in the higher tier and P1 rewards would go up to $3000, but other subdomains of *.samsclub.com would vary depending on tier. Rewards for mid tier apps could go up to $1500 and for lower tier apps up to $500. Tiers are not limited to just P1 issues, rewards for all other priorities will also be determined by application tier level. A report is not eligible for reward if we decide not to take action based on it due to Informational risk rating.

Domains related to the following companies are not in scope: Art.com, Allposters, Workspaceart, Bonobos, Moosejaw, Eloquii.



4. Project work plan

RFQ Reference

Project Work Plan: Utilizing a GANTT or PERT chart, include a high-level summary that shows all the tasks and deliverables to complete the project. Explain your approach to deliverables. Explanation must be limited to one page.

Based on information provided by the OA/OIT, we are prepared to start the enterprise information security assessment at a mutually agreeable date no later than May 1, 2013. Depending on the schedules of the OA/OIT, we expect the project to last approximately five weeks, as depicted in the timeline below.

Project Timeline	Week 1	Week 2	Week 3	Week 4	Week 5
Project Management (Ongoing)					
Phase 0: Project Initiation & Management					
Phase 1: Security Controls and Procedures Review					
Interviews and Data Gathering					
Findings and Gap Analysis					
Phase 2: External Security Assessment					
Identify Live Assets					
Perform Vulnerability Scanning Against Identified Assets					
Perform Penetration Testing Against High-Risk Assets					
Phase 3: Social Engineering					
Identify Email Addresses to Target					
Conduct Email-Based Social Engineering					
Perform Additional Penetration Testing (if applicable)					
Phase 4: Reporting and Closing					
Report Drafting					
Final Deliverable Completion					
Project Closing Meeting					

8 Proposal to serve the Commonwealth of Pennsylvania

In your Scope of Work and Rules of engagement, in a Red Team Engagement, push for objective based testing and keep them broad:

- “Access to privileged user or corporate data”
- “Provable disruption of services”

Old-school example of ROE and SoW:

- https://www.halock.com/wp-content/uploads/2019/01/HALOCK-Pen-Test-Deliverables-12-18.pdf

ASNs++

WHAT ARE WE AFTER?

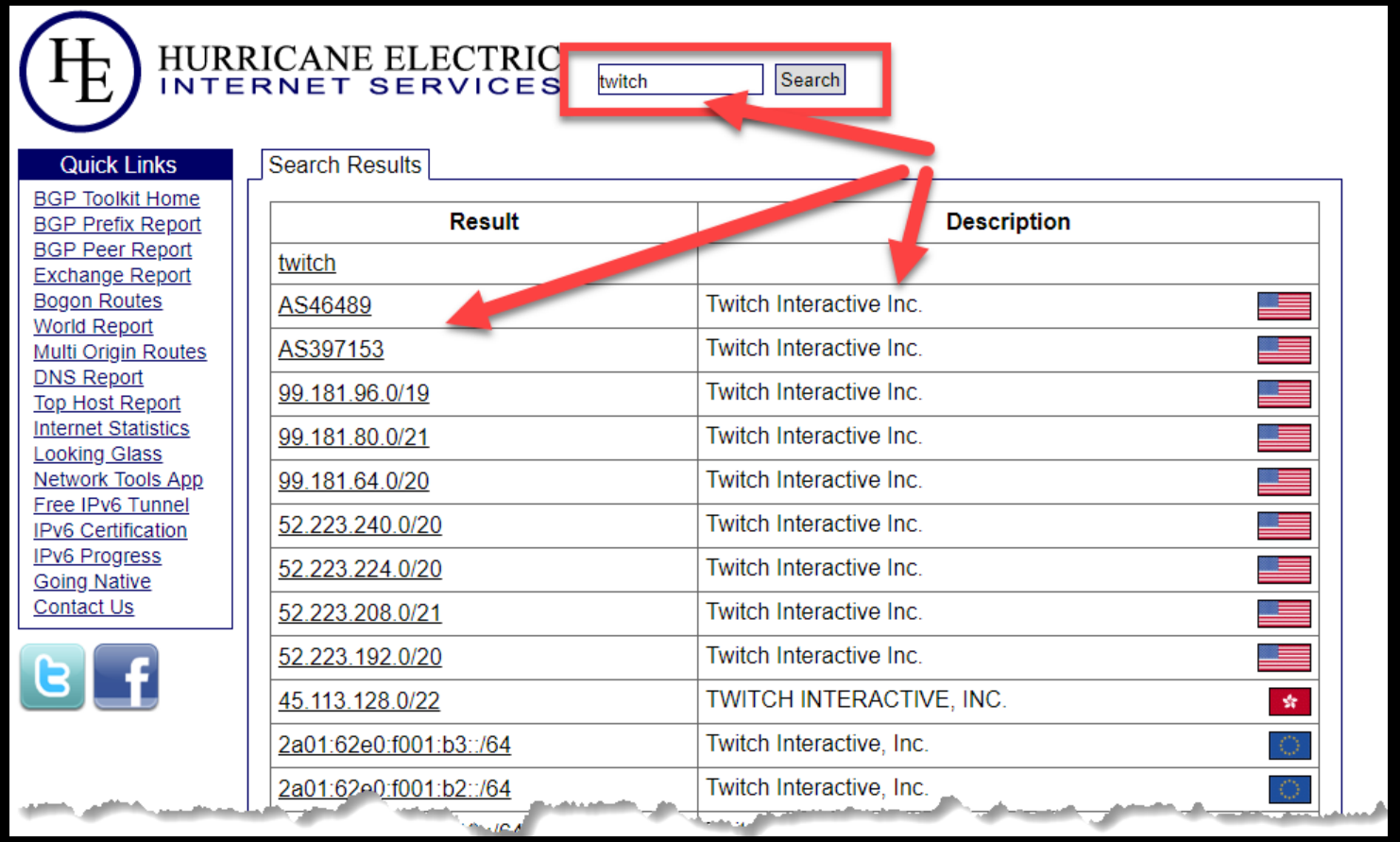
ASNs will give us IP Addresses of owned servers

These IPs will lead to more apex domains, websites, & services.

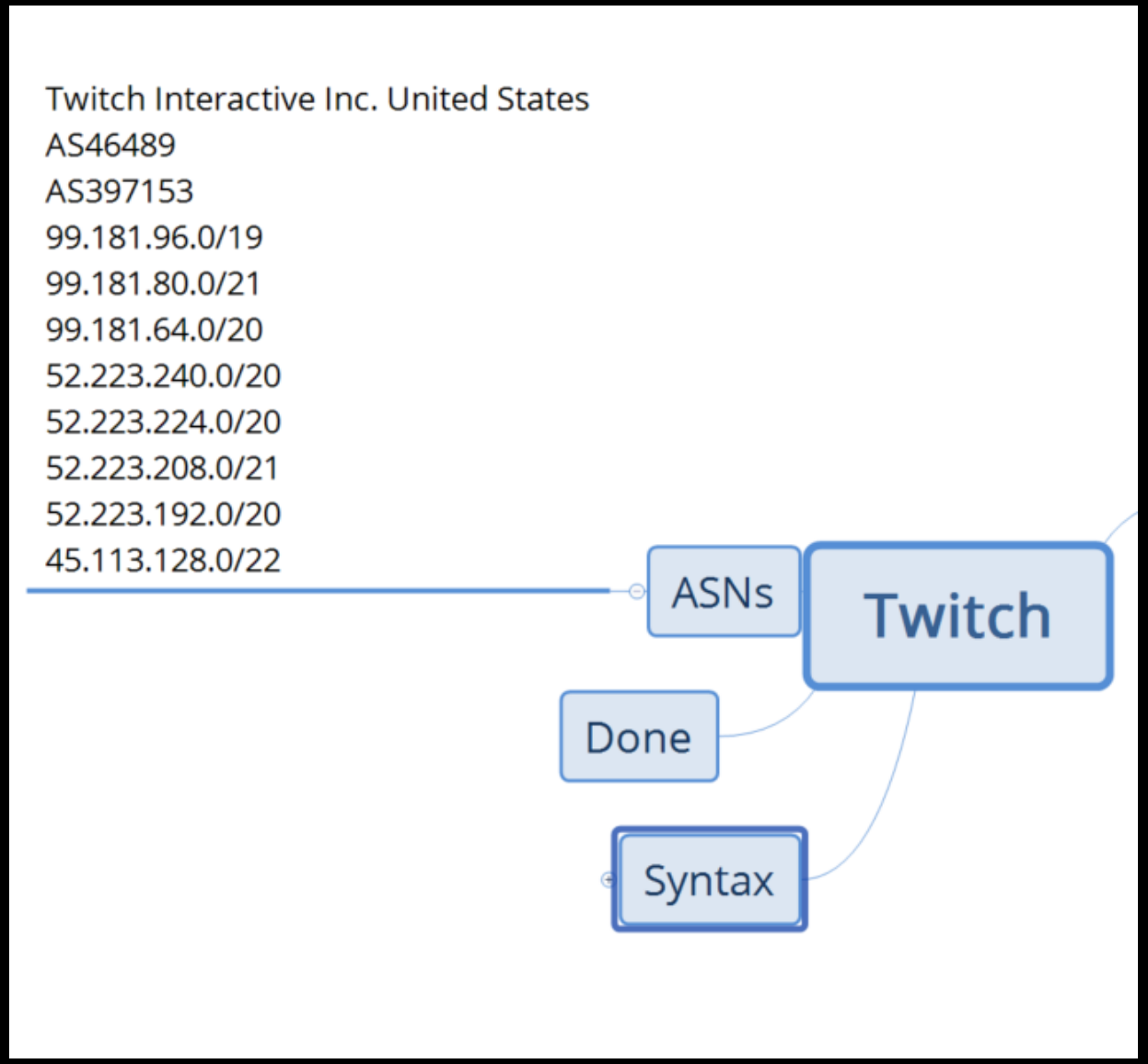
Autonomous System Numbers are given to large enough networks. These ASNs will help us track down some semblance of an entity's IT infrastructure. The most reliable way to get these is manually through Hurricane Electric's free-form search:

http://bgp.he.net

Because of the advent of cloud infrastructure, ASNs aren't always a complete picture of a network. Rogue assets could exist on cloud environments like AWS and Azure. Here we can see several IP ranges.



Update our notes...



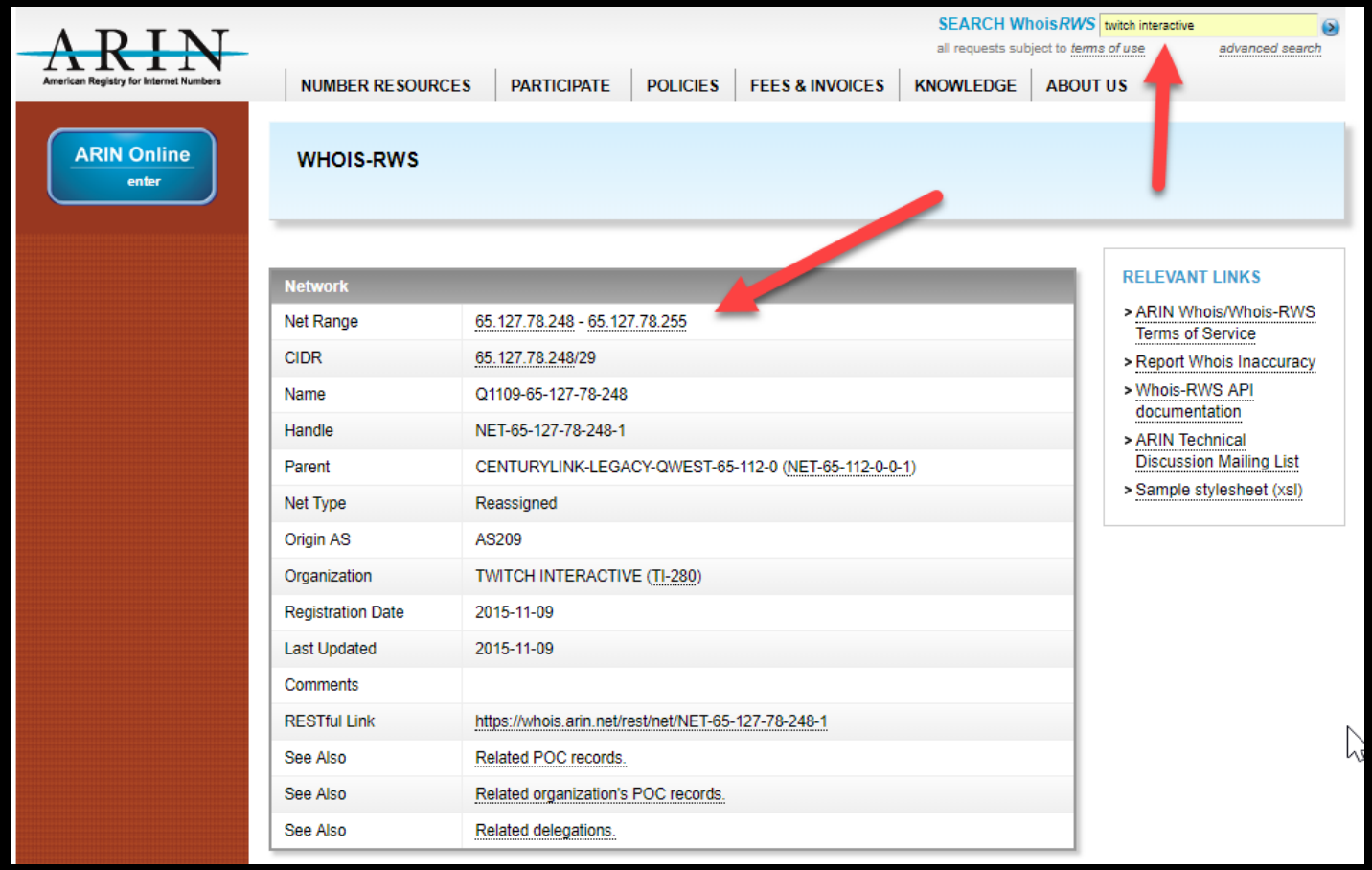
IP Enumeration: Registrars

ARIN and RIPE are Regional Registrars who allow full text searches for address space:

"As a Regional Internet Registry, we allocate and register blocks of Internet number resources to Internet service providers (ISPs) and other organizations in our geographical service region. These Internet number resources are mainly in the form of IPv4 and IPv6 address space and Autonomous System Numbers (ASNs)."

(US Region)
https://whois.arin.net/ui/query.do

(EU, Central Asia regions)
https://apps.db.ripe.net/db-web-ui/#/fulltextsearch



SHODAN++

WHAT ARE WE AFTER?

Shodan will give us passive subdomains, IP addresses, vulnerability data, and more...

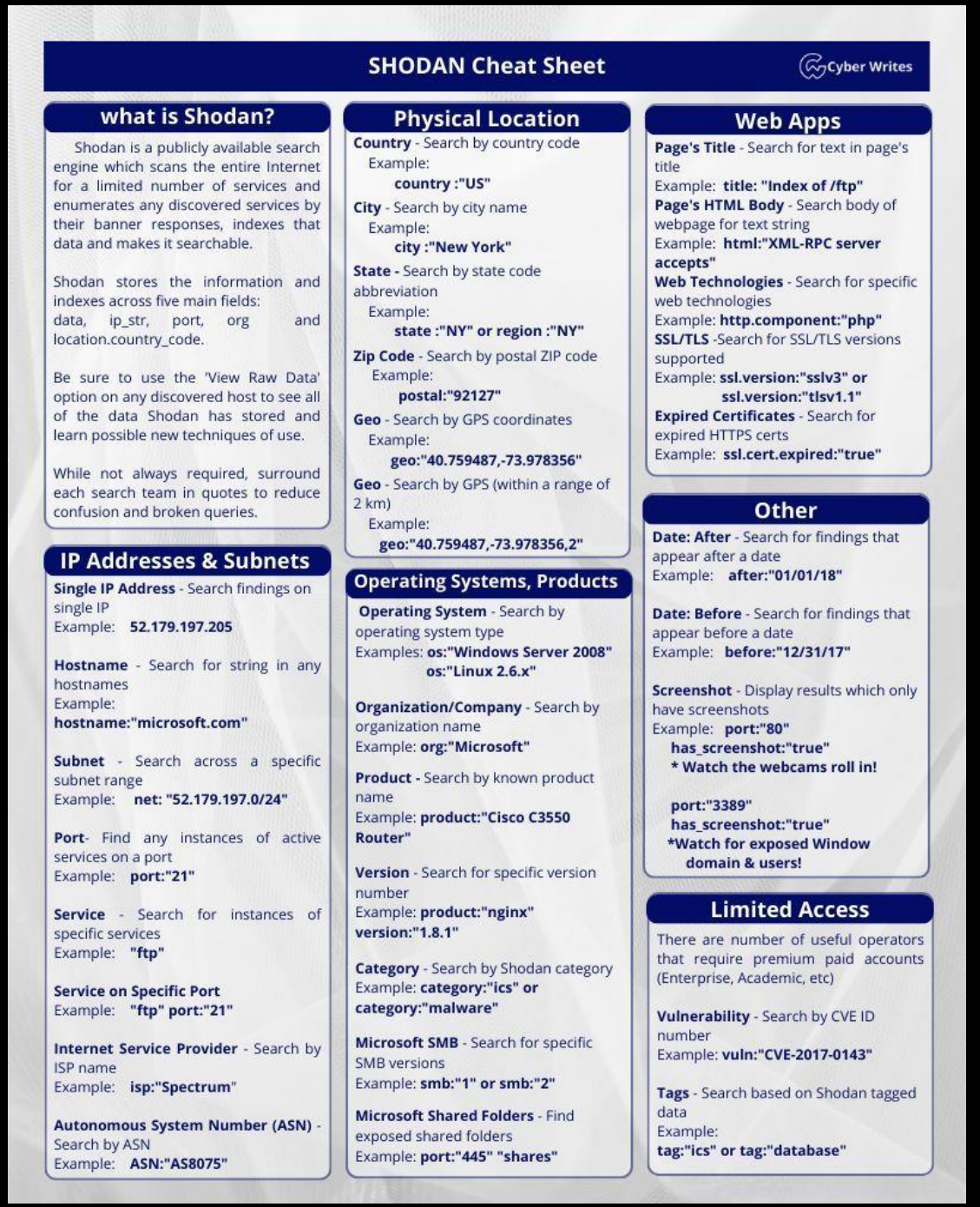
MANUAL SHODAN

Shodan is a tool that continuously spiders infrastructure on the internet. It is much more verbose than regular spiders. It captures response data, cert data, stack profiling data, and more. It requires registration.

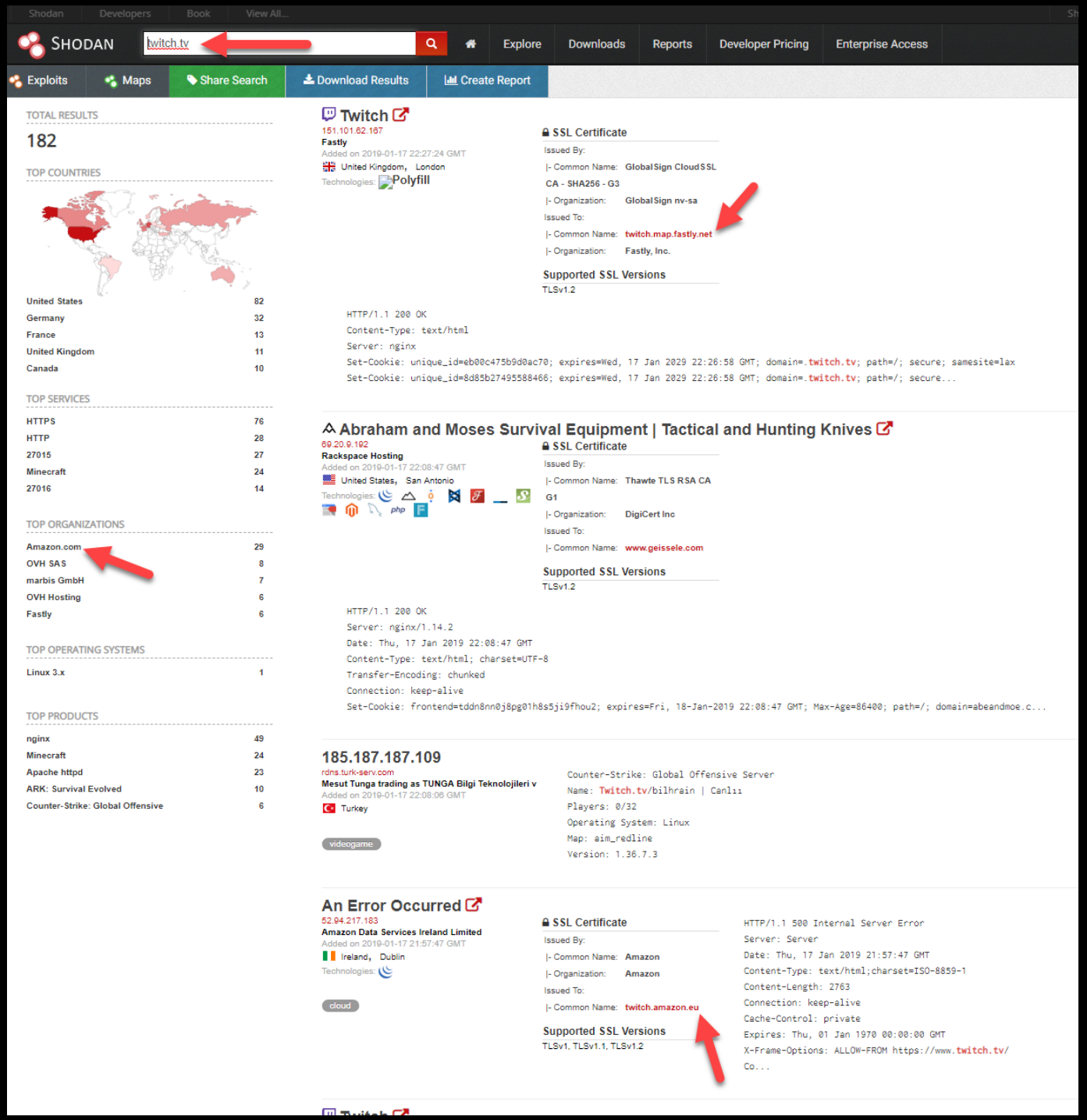
Example:

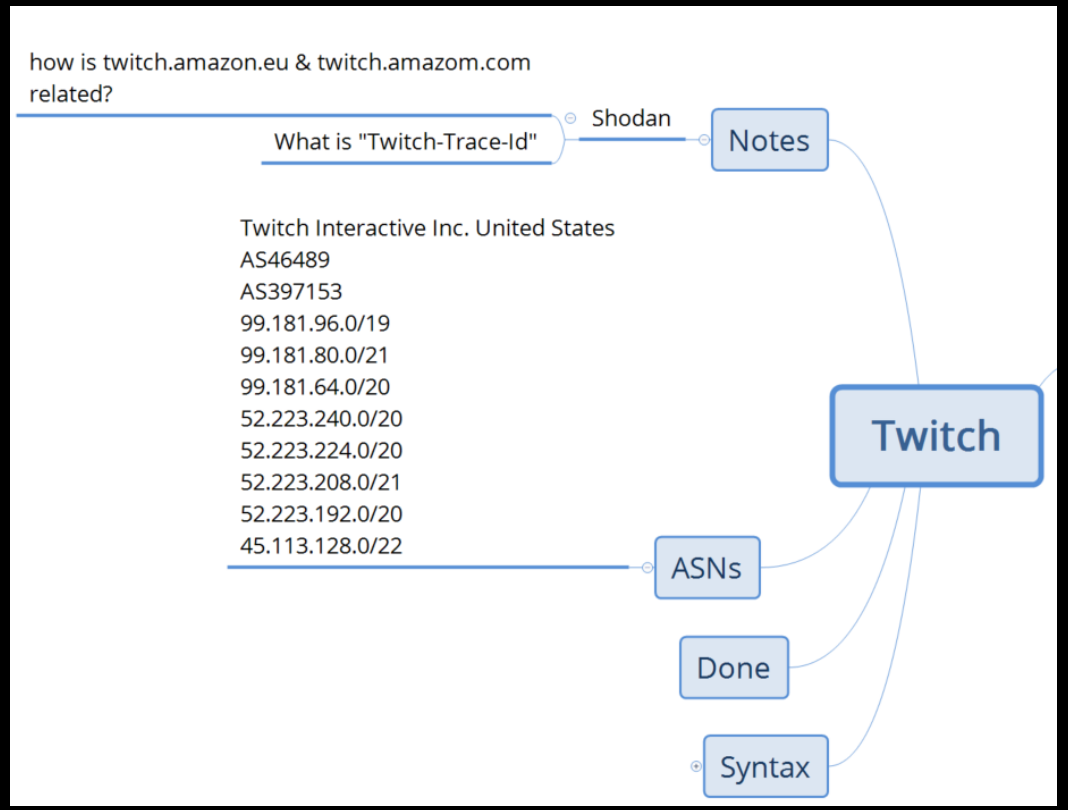
https://www.shodan.io/search?query=twitch.tv

It's often used for threat hunting and passive security research.



https://www.linkedin.com/feed/update/urn:li:activity:7073267561278095361/


Shodan
Developers
Book
View All...
SHODAN
twitch.tv
Explore
Downloads
Reports
Developer Pricing
Enterprise Access
Exploits
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
182
TOP COUNTRIES
United States 82
Germany 32
France 13
United Kingdom 11
Canada 10
TOP SERVICES
HTTPS 76
HTTP 28
27015 27
Minecraft 24
27016 14
TOP ORGANIZATIONS
Amazon.com 29
OVH SAS 8
marbis GmbH 7
OVH Hosting 6
Fastly 6
TOP OPERATING SYSTEMS
Linux 3.x 1
TOP PRODUCTS
nginx 49
Minecraft 24
Apache httpd 23
ARK: Survival Evolved 10
Counter-Strike: Global Offensive 6
Twitch
151.101.62.167
Fastly
Added on 2019-01-17 22:27:24 GMT
United Kingdom, London
Technologies: Polyfill
SSL Certificate
Issued By:
|- Common Name: GlobalSign CloudSSL CA - SHA256 - G3
|- Organization: GlobalSign nv-sa
Issued To:
|- Common Name: twitch.map.fastly.net
|- Organization: Fastly, Inc.
Supported SSL Versions
TLSv1.2
HTTP/1.1 200 OK
Content-Type: text/html
Server: nginx
Set-Cookie: unique_id=eb00c475b9d0ac70; expires=Wed, 17 Jan 2029 22:26:58 GMT; domain=.twitch.tv; path=/; secure; samesite=lax
Set-Cookie: unique_id=8d85b27495588466; expires=Wed, 17 Jan 2029 22:26:58 GMT; domain=.twitch.tv; path=/; secure...
Abraham and Moses Survival Equipment | Tactical and Hunting Knives
69.20.9.192
Rackspace Hosting
Added on 2019-01-17 22:08:47 GMT
United States, San Antonio
Technologies:
SSL Certificate
Issued By:
|- Common Name: Thawte TLS RSA CA G1
|- Organization: DigiCert Inc
Issued To:
|- Common Name: www.geissele.com
Supported SSL Versions
TLSv1.2
HTTP/1.1 200 OK
Server: nginx/1.14.2
Date: Thu, 17 Jan 2019 22:08:47 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: frontend=tddn8nn0j8pg01h8s5ji9fhou2; expires=Fri, 18-Jan-2019 22:08:47 GMT; Max-Age=86400; path=/; domain=abeandmoe.c...
185.187.187.109
rdns.turk-serv.com
Mesut Tunga trading as TUNGA Bilgi Teknolojileri v
Added on 2019-01-17 22:08:06 GMT
Turkey
videogame
Counter-Strike: Global Offensive Server
Name: Twitch.tv/bilhrain | Canlı
Players: 0/32
Operating System: Linux
Map: aim_redline
Version: 1.36.7.3
An Error Occurred
52.94.217.183
Amazon Data Services Ireland Limited
Added on 2019-01-17 21:57:47 GMT
Ireland, Dublin
Technologies:
cloud
SSL Certificate
Issued By:
|- Common Name: Amazon
|- Organization: Amazon
Issued To:
|- Common Name: twitch.amazon.eu
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2
HTTP/1.1 500 Internal Server Error
Server: Server
Date: Thu, 17 Jan 2019 21:57:47 GMT
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 2763
Connection: keep-alive
Cache-Control: private
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Frame-Options: ALLOW-FROM https://www.twitch.tv/
Co...

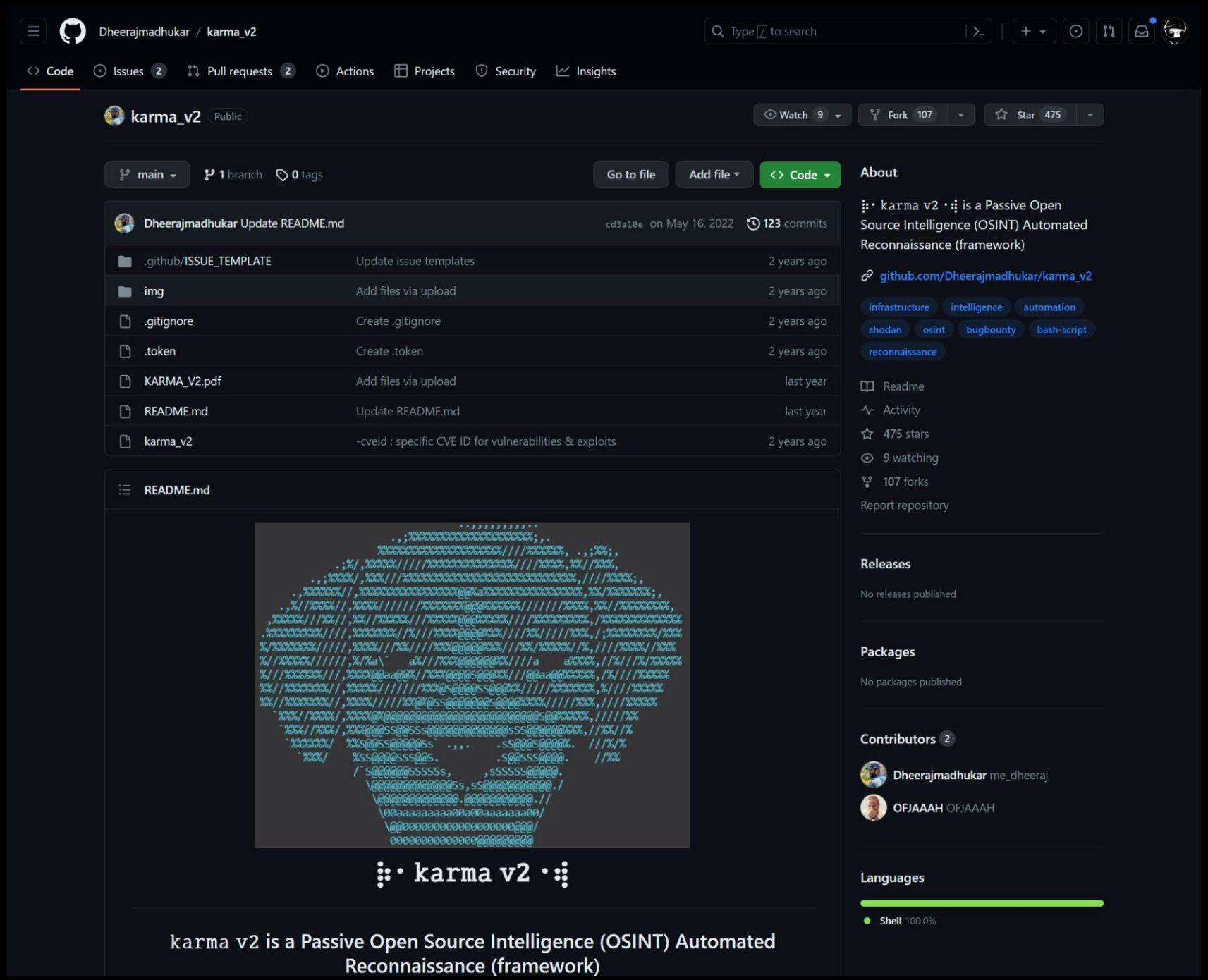

how is twitch.amazon.eu & twitch.amazom.com related?
What is "Twitch-Trace-Id"
Shodan
Notes
Twitch Interactive Inc. United States
AS46489
AS397153
99.181.96.0/19
99.181.80.0/21
99.181.64.0/20
52.223.240.0/20
52.223.224.0/20
52.223.208.0/21
52.223.192.0/20
45.113.128.0/22
ASNs
Twitch
Done
Syntax

AUTOMATED SHODAN (Karma v2)

For red team engagements and bounty, utilizing Shodan can be powerful.

One of the best methods to get passive recon data and possible passive vuln data from our target is Karma v2.

Also check out WTFIS



```
 Shodan Result Count  [ No API Credits Use ]

Indexing_Hostname                | 4
Indexing_SSL                     | 2
LogIn_title_SSL_subject          | 69
LogIn_title_SSL                  | 125
LogIn_title_Hostname             | 238
LogIn_body_SSL_subject           | 13
LogIn_body_SSL                   | 28
LogIn_body_Hostname              | 48
403_Forbidden_SSL_subject        | 51
403_Forbidden_SSL                | 68
403_Forbidden_Hostname           | 61
500_Status_html_SSL_subject      | 3
500_Status_html_SSL              | 3
500_Status_html_Hostname         | 3
500_Status_SSL_subject           | 32
500_Status_SSL                   | 45
500_Status_Hostname              | 40
Jetty_Detect_Hostname            | 4
Grafana_Detect_SSL_subject       | 6
Grafana_Detect_SSL               | 6
MongoDB_Server_Metrics_Hostname  | 8
MongoDB_Server_Metrics_SSL       | 8
Spring_Boot_SSL                  | 1

Query credits available: 199551
Scan credits available: 65536

>> Saved 4 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/Indexing_Hostname_ford.com.json.gz
>> Saved 2 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/Indexing_SSL_ford.com.json.gz
>> Saved 69 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/LogIn_title_SSL_subject_ford.com.json.gz
>> Saved 124 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/LogIn_title_SSL_ford.com.json.gz
>> Saved 237 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/LogIn_title_Hostname_ford.com.json.gz
>> Saved 13 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/LogIn_body_SSL_subject_ford.com.json.gz
>> Saved 28 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/LogIn_body_SSL_ford.com.json.gz
>> Saved 48 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/LogIn_body_Hostname_ford.com.json.gz
>> Saved 50 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/403_Forbidden_SSL_subject_ford.com.json.gz
>> Saved 67 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/403_Forbidden_SSL_ford.com.json.gz
>> Saved 60 results into file /opt/hackerone/TOOLS/me_dheeraj/karma/v2/output/ford.com-2021-08-31/Collect/403_Forbidden_Hostname_ford.com.json.gz
```

AUTOMATED SHODAN (Shosubgo)

For strictly subdomain discovery using shodan, Shusubgo is the most reliable tool.

A savvy hacker might ask;

Why use this tool when Amass has a module for this?

I find for Shodan enumeration and for GitHub enumeration, these stand-alone tools give back more results due to their narrow focus. About 3-10% increased discoveries.

```
✔ /home/temp/go/mytools/shosubgo >> go run main.go -d uber.com
Credits: 84
Scan Credits: 100

accessibility.uber.com
accounts.uber.com
advantage.uber.com
amp.uber.com
api.uber.com
ar.uber.com
assets-share.uber.com
auth.uber.com
azkaban.uber.com
backup.uber.com
bastion.uber.com
bastion-geo.uber.com
beacon.uber.com
biz.uber.com
bizblog.uber.com
blackswan.uber.com
bliss-events.uber.com
blog.uber.com
blogapi.uber.com
blogcdn.uber.com
bonjour.uber.com
brand.uber.com
business.uber.com
businesses.uber.com
careers.uber.com
careersinfo.uber.com
central.uber.com
ci.uber.com
cleopatra.uber.com
click.uber.com
click.et.uber.com
clients.uber.com
cn.uber.com
cn-dc1.uber.com
cn-dca1.uber.com
cn-dca1.cfe.uber.com
cn-ecg.cfe.uber.com
cn-freight.uber.com
cn-geo1.uber.com
```

OTHER SHODAN RESOURCES

While the web interface is useful for small to medium scale research, Shodan CLI is better for larger projects.

Ben does a banger video on using Shodan CLI. It also has some great parsing tips for Shodan data and passing to httpx.

https://www.youtube.com/watch?v=4CL_8GRNVTE

OTHER SHODAN RESOURCES

Official Shodan Documentation	Data reference: *https://datapedia.shodan.io/* List of search filters: *https://www.shodan.io/search/filters* Query syntax: *https://help.shodan.io/the-basics/search-query-fundamentals* Official Examples: *https://www.shodan.io/search/examples*
The Shodan Pentesting Guide	*https://community.turgensec.com/shodan-pentesting-guide/*
***Cert.sh* and Shodan Recon with @GodfatherOrwa**	*https://www.youtube.com/watch?v=YoXM4m1VEM0*
Shodan Filters and Hacks	*https://www.youtube.com/watch?v=GyZFM5laH2Y*
100 Shodan Queries for Discovery	*https://www.osintme.com/index.php/2021/01/16/ultimate-osint-with-shodan-100-great-shodan-queries/*
Org filter dorks for technologies	*https://mr-koanti.github.io/shodan#*
General other interesting queries	*https://github.com/jakejarvis/awesome-shodan-queries*

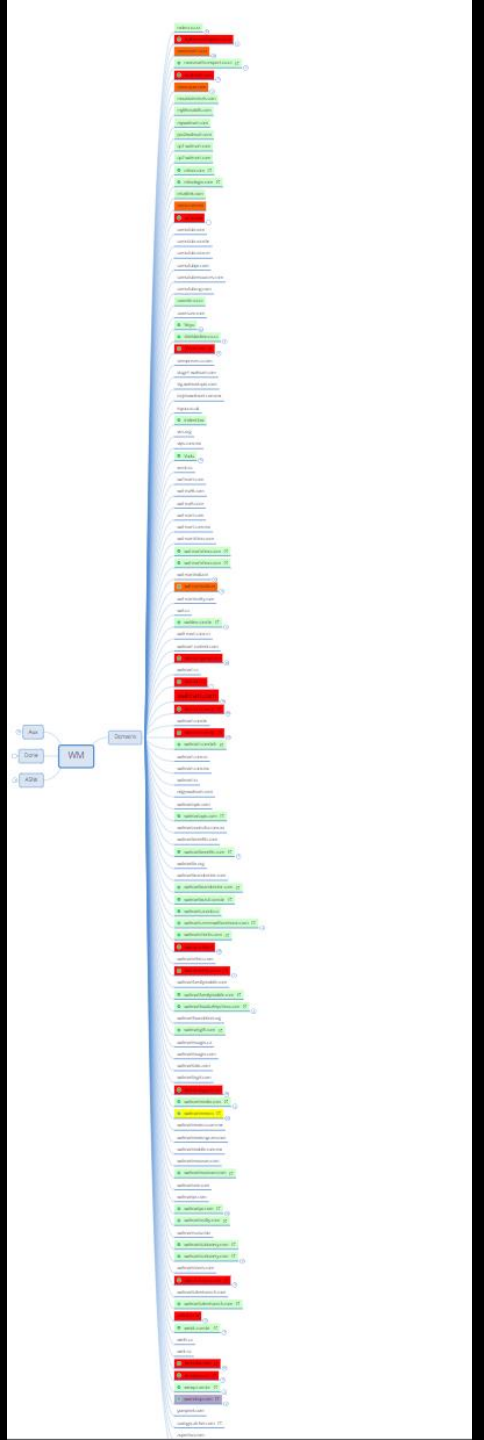
INTERLUDE FOR TRACKING

SO FAR WE HAVE...

- Apex Domains
- Subdomains
- IP Addresses / Ranges
- Interesting hosts from Shodan

With a large target, tracking this can get crazy.

So we need to talk about it...

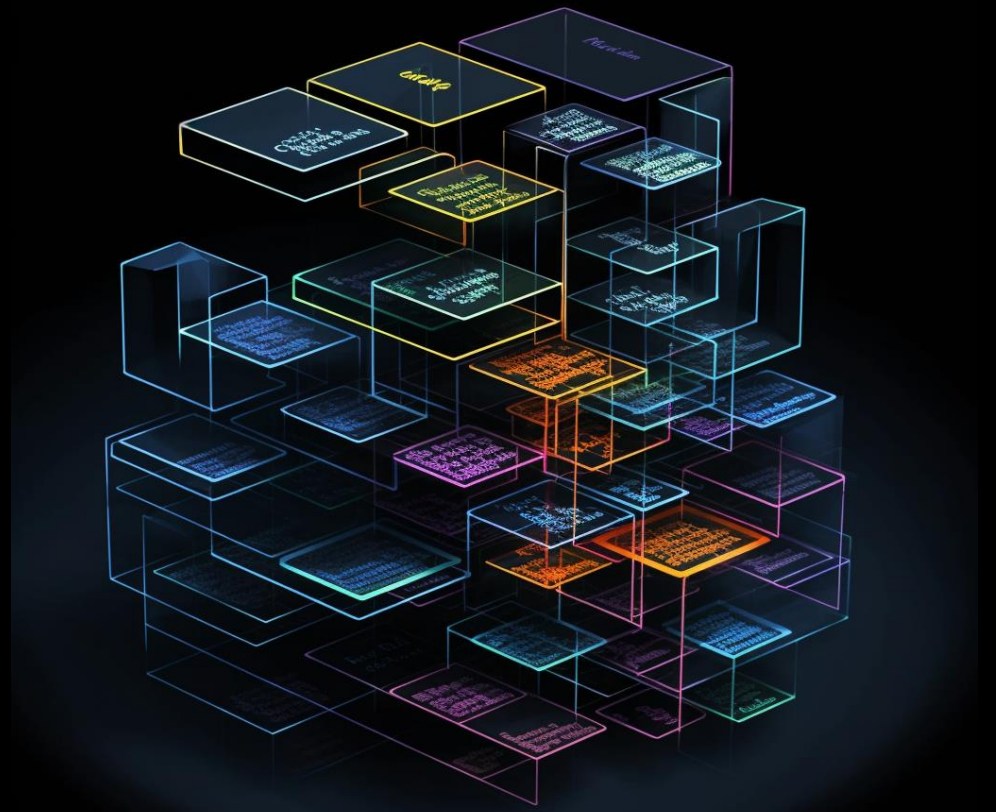


HOW I DO IT (TODAY)

- Apex Domains (db)
- Subdomains (db)
- IP Addresses / Ranges (Spreadsheet/Mindmap)
- Interesting hosts from Shodan (Spreadsheet/Mindmap)
- Re-used syntax (Spreadsheet/Mindmap)

Questions to ask...

Are you hacking with a team?



BOUNTYCATCH.PY

- Python3 around simple Redis DB
- Handles domains from txt files
- Dedupes and gives stats upon input
- Could use more love
- No warranty

```
~ (master*) # python3 bountycatch.py --project 1 -o add -f githubdell9.txt

10495 out of 10497 domains were duplicates (99.98%).
```

https://gist.github.com/jhaddix/91035a01168902e8130a8e1bb383ae1e

BOUNTYCATCH.PY

Start a project called “dell”, add your 1st set of subdomains:

python3 bountycatch.py --project dell --file dell.txt

Print the current project:

python3 bountycatch.py --project dell -o print

Add new subdomains to the project:

python3 bountycatch.py --project dell -o add -f githubdell8.txt

```
~ (master*) # python3 bountycatch.py --project 1 -o print
auspwctiweb04.aus.amer.dell.com
emf3gtidev01.bray.ie.dell.com
ie-edc-rtr2-e0.bray.ie.dell.com
sig.us.dell.com
omnidrdb02.us.dell.com
solvengine-app-sit.us.dell.com
pc-smtp2.us.dell.com
auspc1rpad01-ext.us.dell.com
auslafpsitgw.us.dell.com
apjom1.sit1.osb.us.dell.com
drm04gw4-myconnect.dell.com
ui-api.test2.insights.dell.com
dellcloudfoundry.cfapps.prod1.vc1.pcf.dell.com
premtool.jp.dell.com
sell1.dit2.osb.us.dell.com
bo-stress-forms.bray.ie.dell.com
myc-gw-l2-emea-lim.lim.emea.dell.com
domino.dell.com
sd01.bray.ie.dell.com
res.uk.home.dell.com
dyn206093.shonline.dell.com
ausevrdmsdb02.production.online.dell.com
spprdvss01.aus.amer.dell.com
ausximlog01.aus.amer.dell.com
s3besxu232-drac.us.dell.com
auspc1esg01.us.dell.com
kul02gw2-myconnect.dell.com
otct-ias-ap2.us.dell.com
cms-sp1-pkg.dell.com
auspwtabwrk104.aus.amer.dell.com
scl01gw5-myconnect.dell.com
ausx2kmpc100.aus.amer.dell.com
svt3-coresvcs.amds.dell.com
acritelli-1.frontier.dell.com
identity.svc.dell.com
```

BBRF

BBRF does the same stuff but uses couchdb and has a GUI and handles more datatypes!

45	242	23	0
Programs	Domains	IPs	URLs
	39 resolved (16.12%)		

Programs

Select a program below to load data tables.

intigriti

Domains | IPs | URLs

- ○ Show all
- ◉ Resolved only
- ○ Unresolved only

Domain	IPs	Source
filter	filter	filter
1337up.intigriti.io	["216.239.32.21"]	sublister
api.intigriti.com	["52.85.79.58"]	sublister
challenge-1120.intigriti.io	["34.77.172.4"]	sublister
challenge-1220.intigriti.io	["34.77.172.4"]	sublister

CRUNCHBASE ++

WHAT ARE WE AFTER?

Crunchbase and sites like it will give us acquisitions and phishing targets.

Acquisitions are new apex domains.

CRUNCHBASE

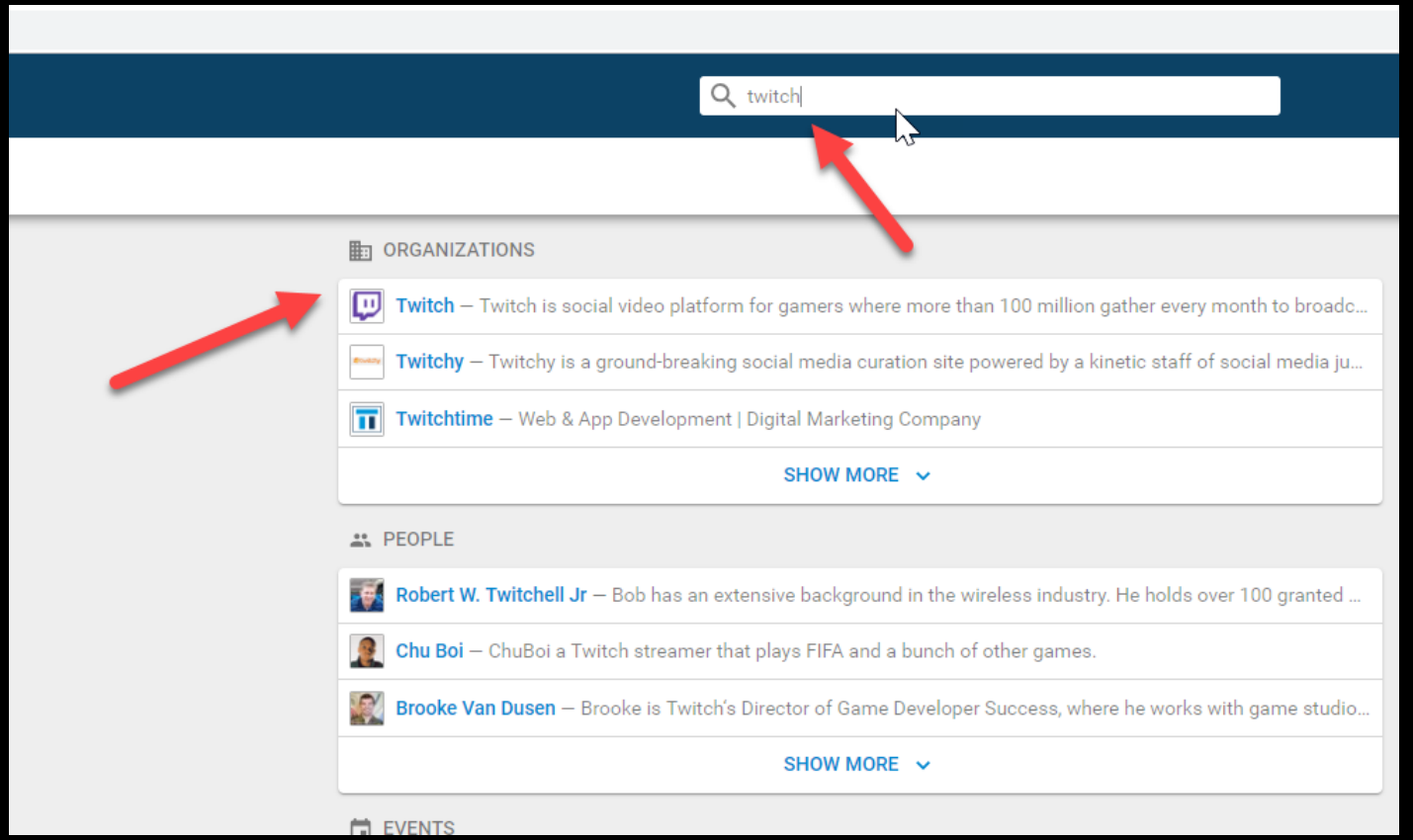
So far, we've been sniffing around an entity with one name. There are however entities that operate under many brand names or parent organizations who have acquired other brands. When these acquisitions happen, IT groups are folded together, and infrastructure is decommissioned... or are they? When doing wide recon, it's important to look at this.

Crunchbase is a business analytics aggregator which tracks acquisitions.

We can use it to expand our scope: https://www.crunchbase.com/

It also offers a **wealth** of contextual data about our target.

Wikipedia can also have this data.



Overview

Acquired by: Amazon

Number of Acquisitions: 4

Twitch

Twitch is social video platform for gamers where more than 100 million gather every month to broadcast, watch and talk about video games.

San Francisco, California, United States

Categories	Social Media, Video, Video Games, Video Streaming
Headquarters Regions	San Francisco Bay Area, West Coast, Western US
Sub-Organization of	Amazon
Founded Date	2007
Founders	Emmett Shear, Justin Kan, Kyle Vogt
Operating Status	Active
Funding Status	M&A
Last Funding Type	Series C
Number of Employees	251-500
Also Known As	twitch.tv, Twitch Interactive
Legal Name	Twitch Interactive, Inc.
IPO Status	Private
Company Type	For Profit
Website	www.twitch.tv/
Facebook	View on Facebook
LinkedIn	View on LinkedIn
Twitter	View on Twitter

Twitch is social video for gamers. It is a video platform and community for gamers where more than 100 million gather every month to watch and talk about video games. Twitch's video platform is the backbone of both live and on-demand distribution for the entire video ecosystem. This includes game developers, publishers, media...

Read More

Acquisitions

Number of Acquisitions: 4

Twitch has acquired 4 organizations. Their most recent acquisition was Revlo on Dec 13, 2018.

Which types of acquisition does this organization make most frequently? pro Show

Acquired Organization Name	Announced Date	Price	Transaction Name
Revlo	Dec 13, 2018	–	Revlo acquired by Twitch
ClipMine	Aug 17, 2017	–	ClipMine acquired by Twitch
Curse	Aug 16, 2016	–	Curse acquired by Twitch
GoodGame	Dec 9, 2014	–	GoodGame acquired by Twitch

Company Tech Stack by Siftery

Active Products

Twitch uses 61 technology products and services including Google Analytics, WordPress, and G Suite (formerly Google Apps for Work).

UNLOCK MORE TECHNOLOGIES DATA ›

Website Tech Stack by BuiltWith

Active Technology

Twitch is actively using 12 technologies for its website. These include SSL by Default, Content Delivery Network, and nginx.

UNLOCK WEBSITE TECHNOLOGIES DATA ›

Competitors & Revenue by Owler

Twitch has $30M in revenue annually. Twitch competes with Azubu, Dailymotion, and Plays.tv.

UNLOCK MORE COMPETITORS & REVENUE DATA ›

Current Team

Number of Current Team Members 40

Twitch has 40 current team members, including CEO and Founder Emmett Shear.

Emmett Shear
CEO and Founder

Justin Kan
Founder

Colin Carrier
Chief Strategy Officer

Sara Clemens
COO

Jonathan Simpson-Bint
CRO

Kym Nelson
SVP Sales

Khudor Annous
Head of Marketing & Partnerships

Mark Weiler
SVP, Head of Platform & Services

VIEW ALL ›

Past Team

Number of Past Team Members 7

Twitch has 7 past team members, including COO Kevin Lin.

Person Name	Title At Company	Start Date	End Date
Kevin Lin	COO	2008	2018
Christina Nguyen	UI/UX Designer	2016	2017
Anne Lin	4GAMERS(Twitch's agency) - Business Development Director	May 2015	Apr 2016
Andrew Shifflett	Internet Personality	Jan 2012	Feb 2014
Kyle Vogt	Co-Founder	Jun 2011	Oct 2013

VIEW ALL >

Events

Number of Events 17

Twitch has participated in 17 events. Recently, they attended TwitchCon 2018 on Oct 26, 2018.

TwitchCon 2018
Organizer
Oct 26, 2018

TwitchCon 2018
Sponsor
Oct 26, 2018

VidCon 2018
Sponsor
Jun 20, 2018

E3 2018
Sponsor
Jun 12, 2018

OMR Festival 2018
Exhibitor
Mar 22, 2018

Lesbians Who Tech London Summit 2017
Sponsor
Nov 10, 2017

TwitchCon 2017
Sponsor
Oct 20, 2017

TwitchCon 2017
Organizer
Oct 20, 2017

VIEW ALL >

Recent News & Activity

Number of Articles 4,189

Date	Activity
Dec 13, 2018	Twitch acquired Revlo for an undisclosed amount
Nov 12, 2018	Twitch: TechCrunch — What's next? The top media executives on the job market
Nov 6, 2018	Twitch: TechCrunch — How to stream U.S. elections coverage if you don't have TV
Oct 26, 2018	Twitch: TechCrunch — Twitch announces group streaming and a karaoke game for its 1M concurrent viewers
Oct 26, 2018	Twitch: TechCrunch — Snapchat's new Camera desktop camera app brings AR masks to Twitch, Skype...
Oct 25, 2018	Twitch: TechCrunch — YouTube is closing the gap with Twitch on live streaming, report finds
Oct 17, 2018	Twitch: TechCrunch — These are the most successful companies to emerge from Y Combinator
Sep 22, 2018	Twitch: Digital Trends — How to sign up for Amazon Prime
Sep 17, 2018	Twitch: GameSpot — Overwatch: Free Golden Loot Box For Amazon / Twitch Prime Members
Sep 14, 2018	Twitch: TechCrunch — Twitch updates security for its TwitchCon event following the Jacksonville esports shooting

VIEW ALL >

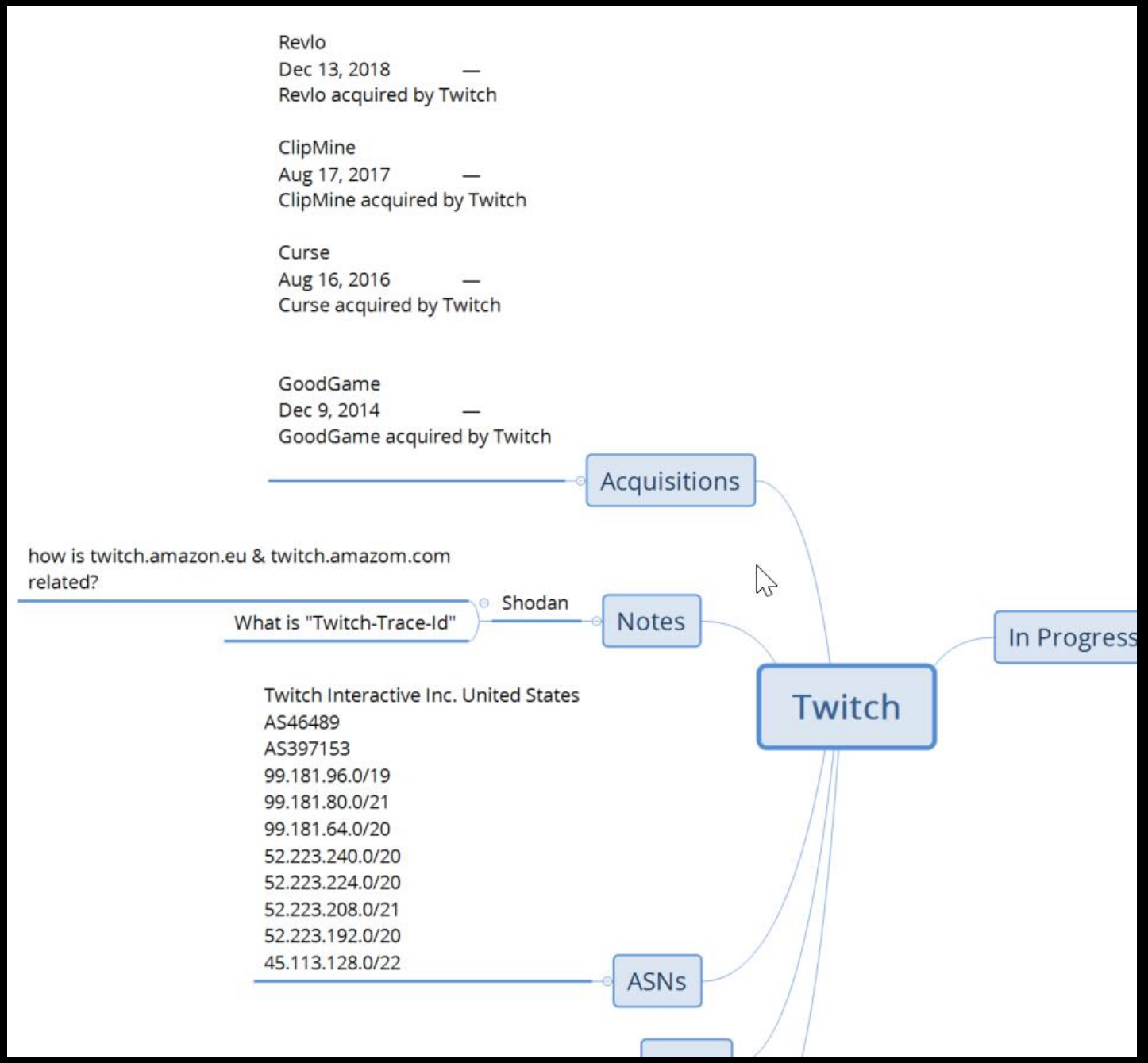
Twitter

Jan 14, 2019

Twitch
@Twitch
The dark spirit thanked @Asmongold for the follow.

Asmongold Gets Jebaited

Updates to our notes...



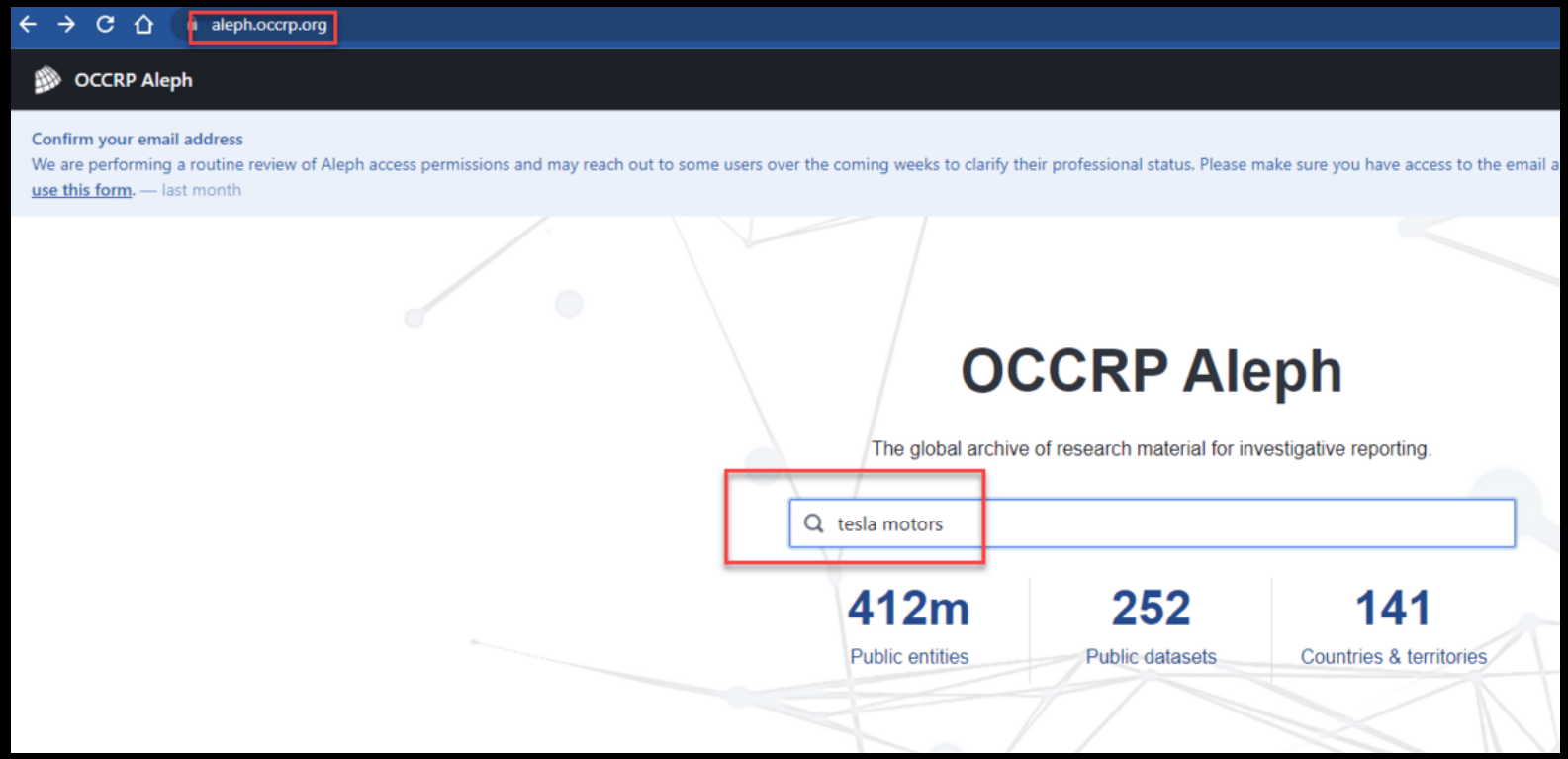

A new foe has appeared!
CHALLENGER APPROACHING

OCCRP.ORG

OCCRP Aleph is a global archive of research material for investigative reporting. They keep track of 414 million public entities and parse over 252 discrete datasets in more than 141 countries.

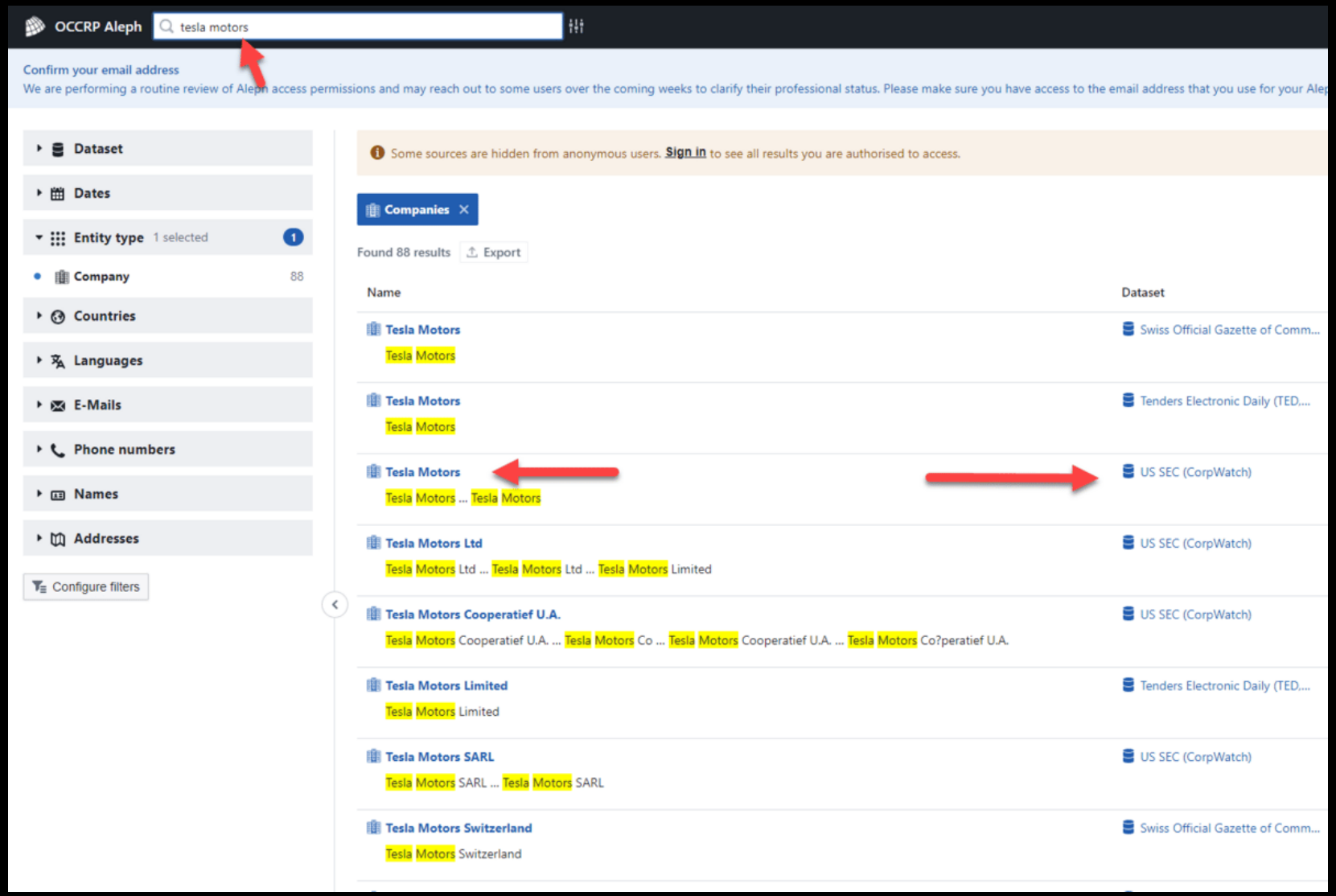
Here's how to use it for reconnaissance, red teaming, and bug bounty.

Head over to the site, register, and then search on the main page for your target company (in this case, Tesla Motors).



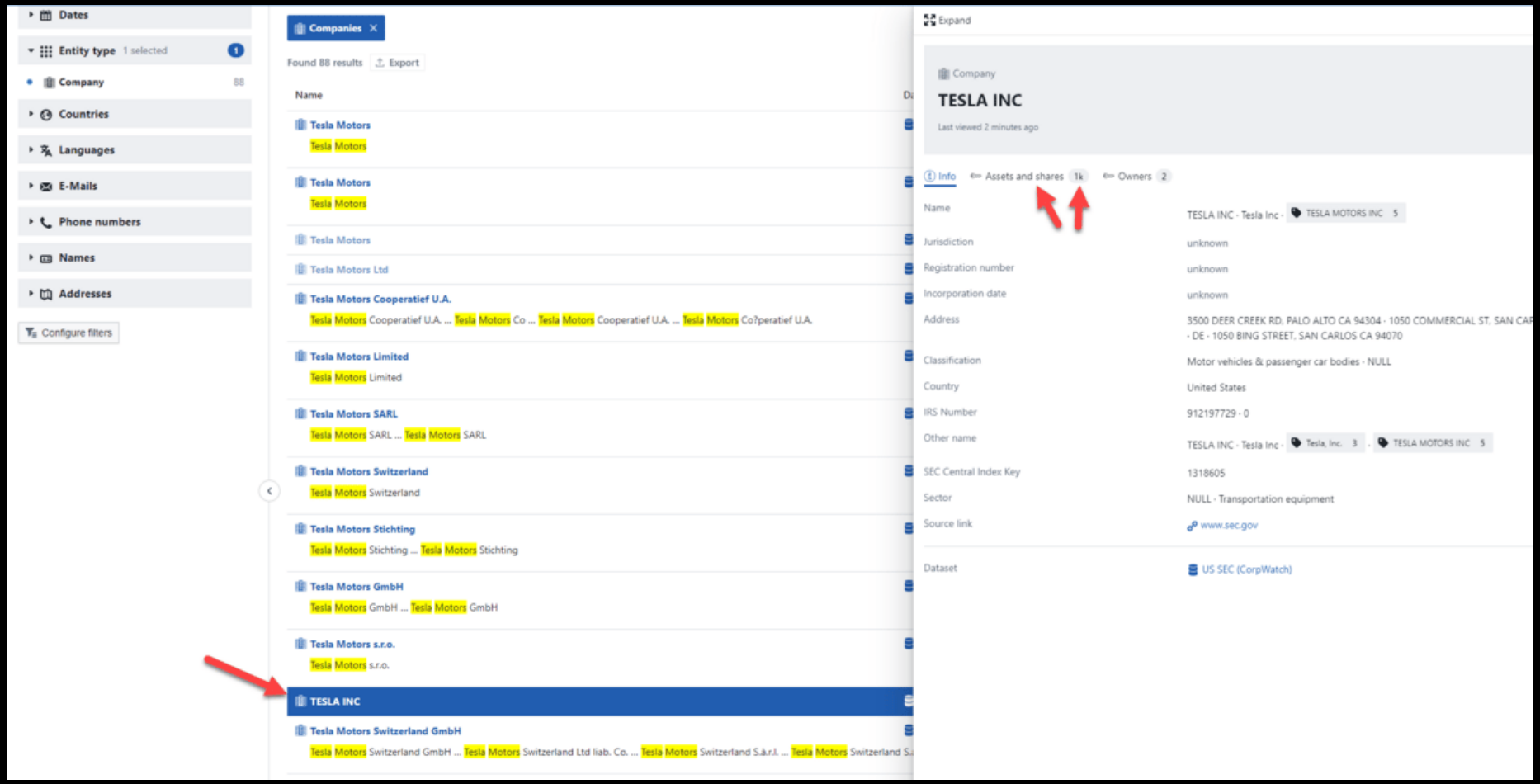
OCCRP.ORG

Once the search is complete, find the entry that comes up, closely related to your company and associated with the dataset "US SEC CorpWatch."



OCCRP.ORG

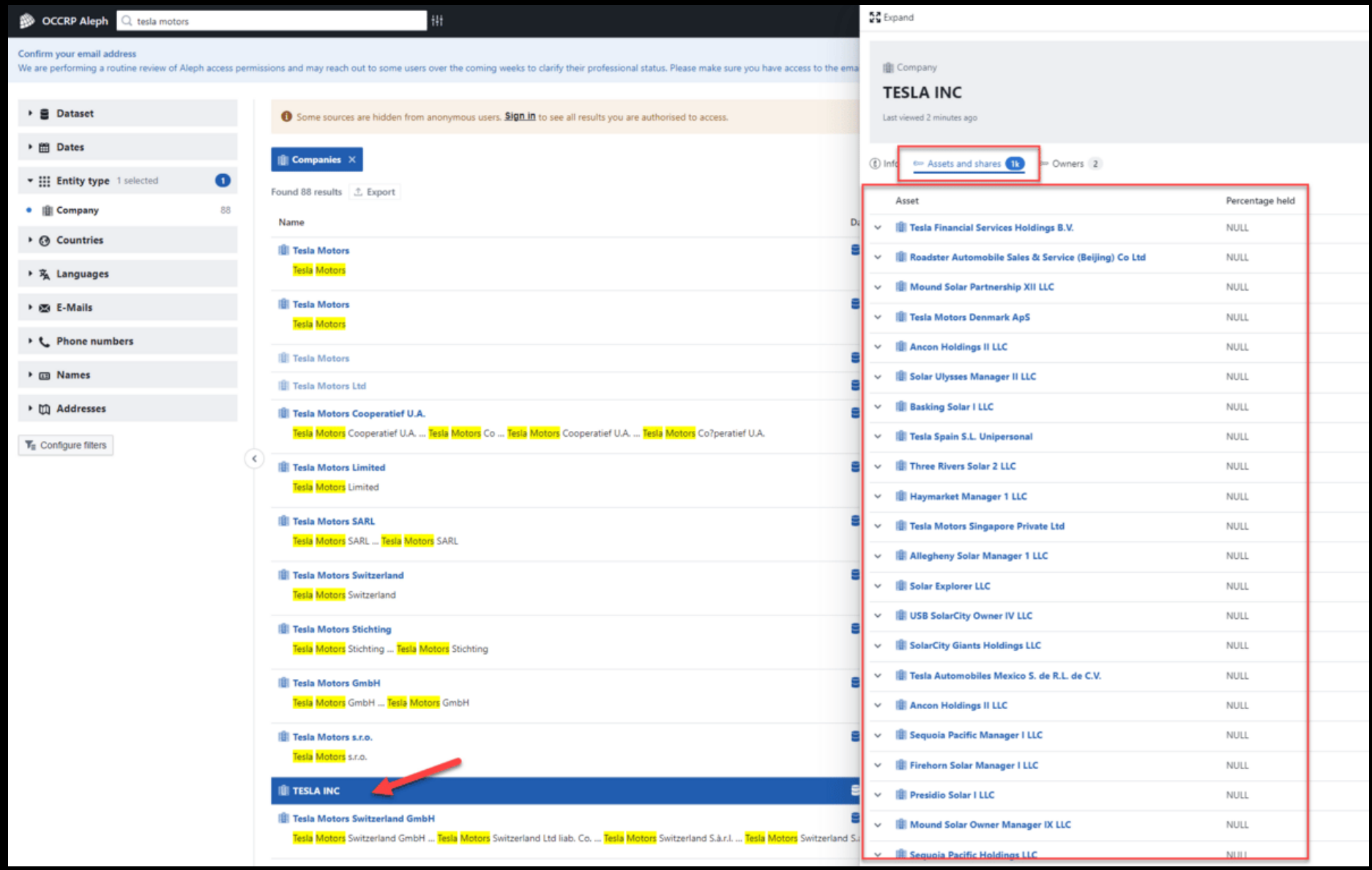
You might have to click around on a couple of these datasets until you find one with a substantial list of assets and shares, as pictured:



OCCRP.ORG

Upon clicking on "assets and shares", you'll be given a list of all your target's investments and acquisitions.

Using this method on a site, I've discovered some fascinating, small, and seldom-mentioned acquisitions and companies tied to targets in both my bounty work and my red team work.



CLOUD RECON

WHAT ARE WE AFTER?

We will be using SSL certificate enumeration to find subdomains of our targets.

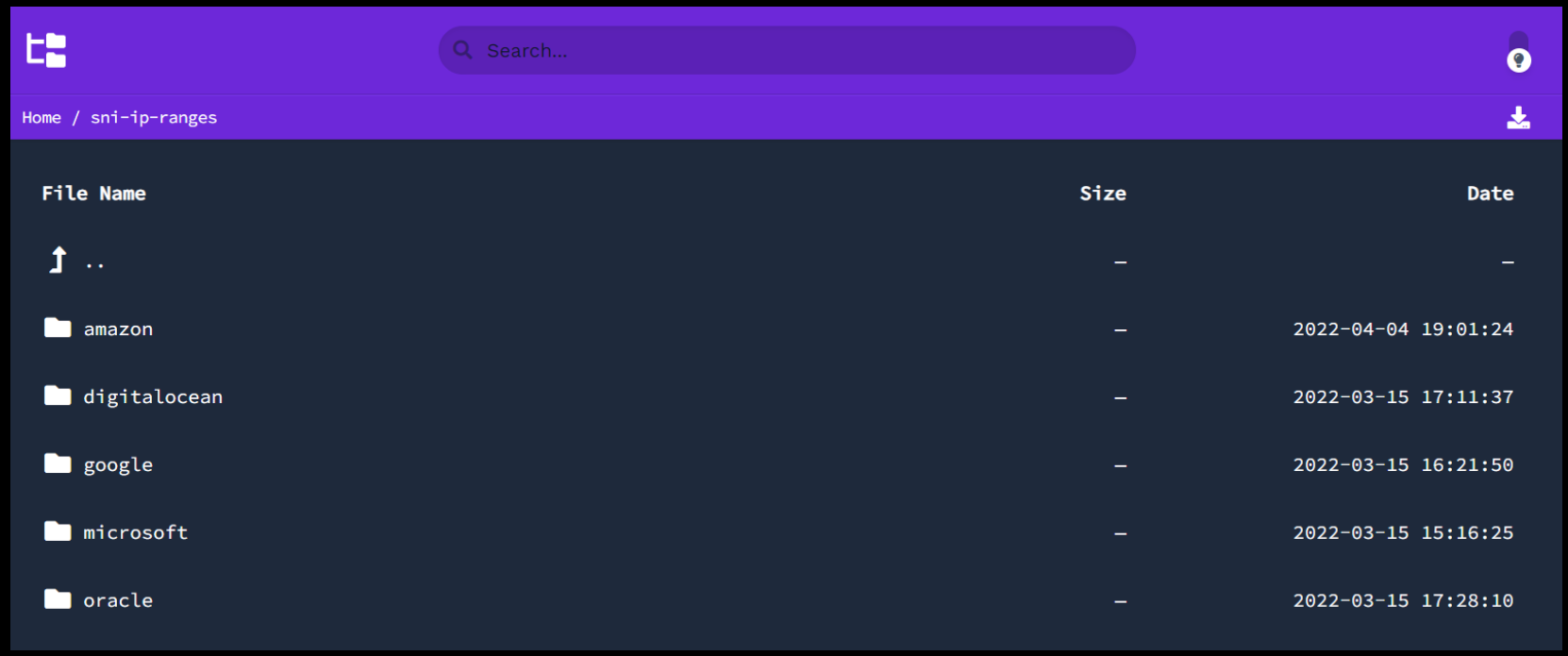
This can also yield apex domains and internal domain names.

CLOUD RECON (http://kaeferjaeger.gay/)

The hacker collective kaeferjaeger scans all the major cloud providers every week. They pull down every IPs SSL certificate data.

They offer it for download.

We can search this cert data for our target.



http://kaeferjaeger.gay/?dir=sni-ip-ranges

```
~/recon/SNI (master*) # ls -al
drwxr-xr-x root root 4.0 KB Thu Jun 15 15:21:40 2023 .
drwxr-xr-x root root 4.0 KB Thu May 25 03:12:23 2023 ..
.rw-r--r-- root root 710 MB Tue Mar 21 19:15:56 2023 aws_ipv4_merged_sni.txt
.rw-r--r-- root root 389 MB Tue Mar 21 20:01:59 2023 azure_ipv4_merged_sni.txt
.rw-r--r-- root root  61 MB Tue Mar 21 19:57:53 2023 DO_ipv4_merged_sni.txt
.rw-r--r-- root root 121 MB Tue Mar 21 19:59:32 2023 Google_ipv4_merged_sni.txt
.rw-r--r-- root root  17 MB Tue Mar 21 20:08:44 2023 oracle_ipv4_merged_sni.txt
```

CLOUD RECON (http://kaeferjaeger.gay/)

Here we are looking at Dell.com as part of their bug bounty. It does take some shell scripting to get the output desired:

```
cat *.txt | grep -F ".dell.com" | awk -F'-- ' '{print $2}' | tr ' ' '\n' | tr '[' ' ' | sed 's/ //' | sed 's/\]//' | grep -F ".dell.com" | sort -u
```

```
~/recon/SNI (master*) # cat *.txt |grep -F ".dell.com" |awk -F'-- ' '{print $2}'| tr ' ' '\n'| tr '[' ' '|sed 's/ //'|sed 's/\]//'|grep -F ".dell.com"|sort -u
*.cms.dell.com
*.corp.connect.dell.com
*.dell.com
*.deoutlet.dell.com
*.mdm.dell.com
*.staging-auoutlet.dell.com
DellCMG01.dell.com
DellCMG02.dell.com
DellPOCCMG.dell.com
Myconnect-NG.dell.com
Myconnect-NGPoC.dell.com
Pexscprox.dell.com
Pexscprox01.dell.com
Pexscprox02.dell.com
agent.api.astra-dev.dell.com
agent.api.astra-stage.dell.com
agent.api.astra-test.dell.com
agent.api.astra.dell.com
anz.business.dell.com
anz.home.dell.com
api.agent.dcca-dev.dell.com
api.agent.dcca-staging.dell.com
api.agent.dcca-test.dell.com
api.agent.dcca.dell.com
api.analytics.dcca-dev.dell.com
api.analytics.dcca-staging.dell.com
api.analytics.dcca-test.dell.com
api.analytics.dcca.dell.com
api.astra-dev.dell.com
```

REVWHOIS ++

WHAT ARE WE AFTER?

Reverse WHOIS will help up identify new apex domains.

REVERSE WHOIS

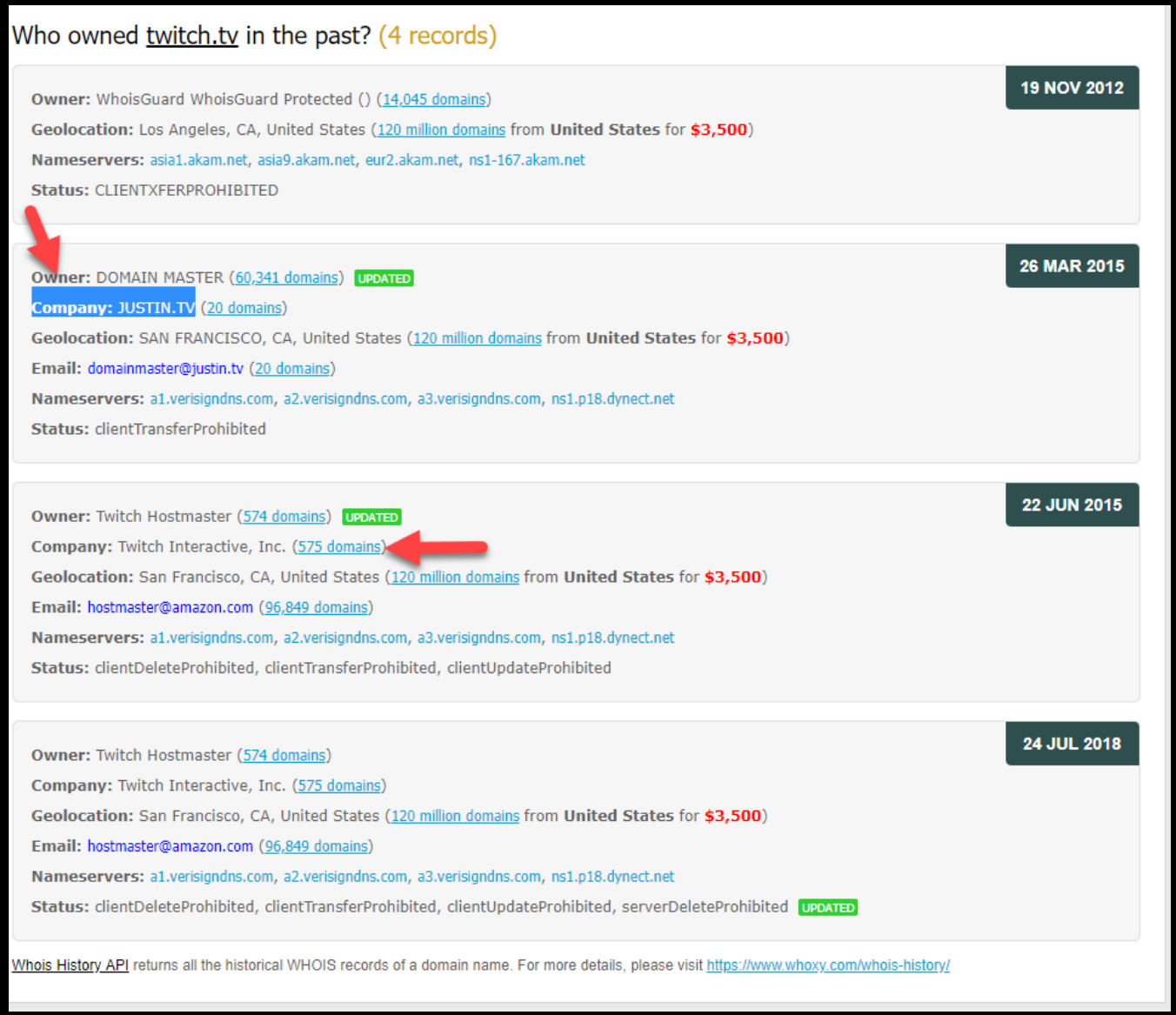
Here we are looking at a WHOIS query on Google.com

We would want to do a reverse WHOIS, in this case, on “Organization Name” or “Registrant Email” to find other sites of Google’s.

```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2017-09-07T08:50:36-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: DNS Admin
Registrant Organization: Google Inc.
Registrant Street: 1600 Amphitheatre Parkway,
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6502530000
Registrant Phone Ext:
Registrant Fax: +1.6502530001
Registrant Fax Ext:
Registrant Email: dns-admin@google.com
```

REVERSE WHOIS (whoxy.com)

Whoxy.com is the cheapest place on the net for access to revwhois and whois data.



REVERSE WHOIS (using whoxy.com API)

1000 Reverse WHOIS API Queries= $10

https://api.whoxy.com/?key=xxxxx&reverse=whois&keyword=google&mode=domains


```
{
    "status": 1,
    "api_query": "reverse_whois",
    "search_identifier": {
        "keyword": "google"
    },
    "total_results": 36049,
    "total_pages": 1,
    "current_page": 1,
    "domain_names": "google.no, google.com.pe, google.fr, google.ca, google.co.uk, google.com, google.com.
google.com.au, google.je, google.ae, google.com.ag, google.pt, google.com.gi, google.co, google.co.kr, goo
google.co.nz, google.com.af, google.com.ec, google.com.ly, google.li, google.lu, google.mn, google.org.cn,
google.com.pt, google.com.sb, google.com.sg, google.com.ua, google.com.vc, google.fi, google.ga, google.gy
google.bf, google.by, google.co.hu, google.gg, google.hr, google.ir, google.lt, google.md, google.mg, goog
google.com.gh, google.com.np, google.com.qa, google.com.kh, google.com.mm, google.com.py, google.com.ni, g
google.com.et, google.us, google.tg, google.ng, google.dj, google.cv, google.au, google.com.ve, google.fm,
google.press, google.ink, google.host, google.bar, google.eus, google.xyz, google.gal, google.cymru, googl
google.kiwi, google.frl, google.xn--kput3i, google.wales, google.sydney, google.green, google.voto, google
google.ovh, google.irish, google.versicherung, google.markets, google.sucks, google.plus, google.express,
google.miami, google.alsace, google.trading, google.xn--hxt814e, google.film, google.study, google.srl, goo
google.xn--tckwe, google.guru, google.discount, google.pet, google.mom, google.istanbul, google.ist, googl
google.yoga, google.lat, google.xn--6qq986b3xl, google.jobs, google.xn--q9jyb4c, google.lol, google.how, g
google.net.au, google.org.il, google.org.nz, google.rent, google.tv, google.mx, google.sg, google.co.rs, g
google.travel, google.co.at, google.tokyo, google.gl, google.mk, google.com.do, google.dz, google.cc, goog
market.com, google-web.org, googlebril.org, googledirectorio.com, googleforum.org, googlegroups.com, googl
googlerank.it, google-adsense-templates.co.uk, google-online.net, google-sucks.org, google404.net, googlen
optimisation.com, googlepluscommunity.com, googler.com, googlesri.com, googlethem.com, googleusercontent.i
googletopper.com, googletrends.com, googleartproject.com, googlermania.com, googletutor.com, googleadsserv
googlevideositemap.com, google-melange.com, google-panda.com, googlebestpractices.com, googlegoro.com, goo
googleplustips.com, googleprs.info, googlerankchecker.net, google-success.com, googleadwordsmockexam.com,
googleseouzmani.net, googlezeitgeist.com, google-bookmark.com, googlepagerankupdates.com, googleredirectvi
googledocs.com, googlegooru.com, googlemapsguru.com.au, googleocity.com, googlesy.com, googletrafficmonste
googlecode.com, googleegypte.com, googleespionnage.com, googlefacile.info, googlefight.com, googlehosted.c
googleplussuomi.com, googlerankings.com, googleretargeting.com, googleshortcuts.org, googlesniper2.com, go
```

RECONGPT

WHAT ARE WE AFTER?

AI can help in finding acquisitions and guess subdomains.

Acquisitions are new apex domains.

RECONGPT (using chatgpt4)

Remember the dataset cuts off in 2021. Verify all results!

What can you tell me about Tesla's acquisitions?

It finds 2 items Crunchbase does not list: “Compass Automation” and “DeepScale”. Crunchbase has the most recent one though, “Wiferion.”

As of my knowledge cutoff in September 2021, Tesla, Inc. had made a few key acquisitions to help it advance its electric vehicle and energy storage business.

1. **Riviera Tool LLC** - In 2015, Tesla acquired this Michigan-based auto supplier to expand its manufacturing capabilities.
2. **SolarCity** - In 2016, Tesla purchased this company, which was one of the largest solar energy services in the United States. SolarCity was already closely tied to Tesla, as Elon Musk was the chairman and his cousins Lyndon and Peter Rive were the founders. The acquisition was a major step in Tesla's strategy to create a sustainable energy ecosystem that includes energy generation, storage, and transportation.
3. **Grohmann Engineering** - In 2016, Tesla bought this German firm to create Tesla Advanced Automation Germany, which designs, builds, and sells automated manufacturing systems. The acquisition was aimed at increasing Tesla's production rate for its cars.

RECONGPT (using chatgpt4)

We can also use GPT4 to intelligently guess subdomain names for us:

For each input subdomain, the script will print out the AI's guesses for similar subdomains and whether each guess resolves:

```
Subdomain = admin.kroger.com
Guesses: dev, qa, test, prod, secure

dev.kroger.com does not resolve.
qa.kroger.com does not resolve.

*** test.kroger.com RESOLVES to 192.0.2.123 ***

prod.kroger.com does not resolve.
secure.kroger.com does not resolve.
```

Resolved subdomains are printed with a clear message and their IP address. The IP address 192.0.2.123 is a placeholder used for illustrative purposes.

https://github.com/jhaddix/SubreconGPT

LINKED DISCOVERY

WHAT ARE WE AFTER?

Linked discovery can help in finding apex domains and subdomains.

LINKED DISCOVERY (using Burp Pro)

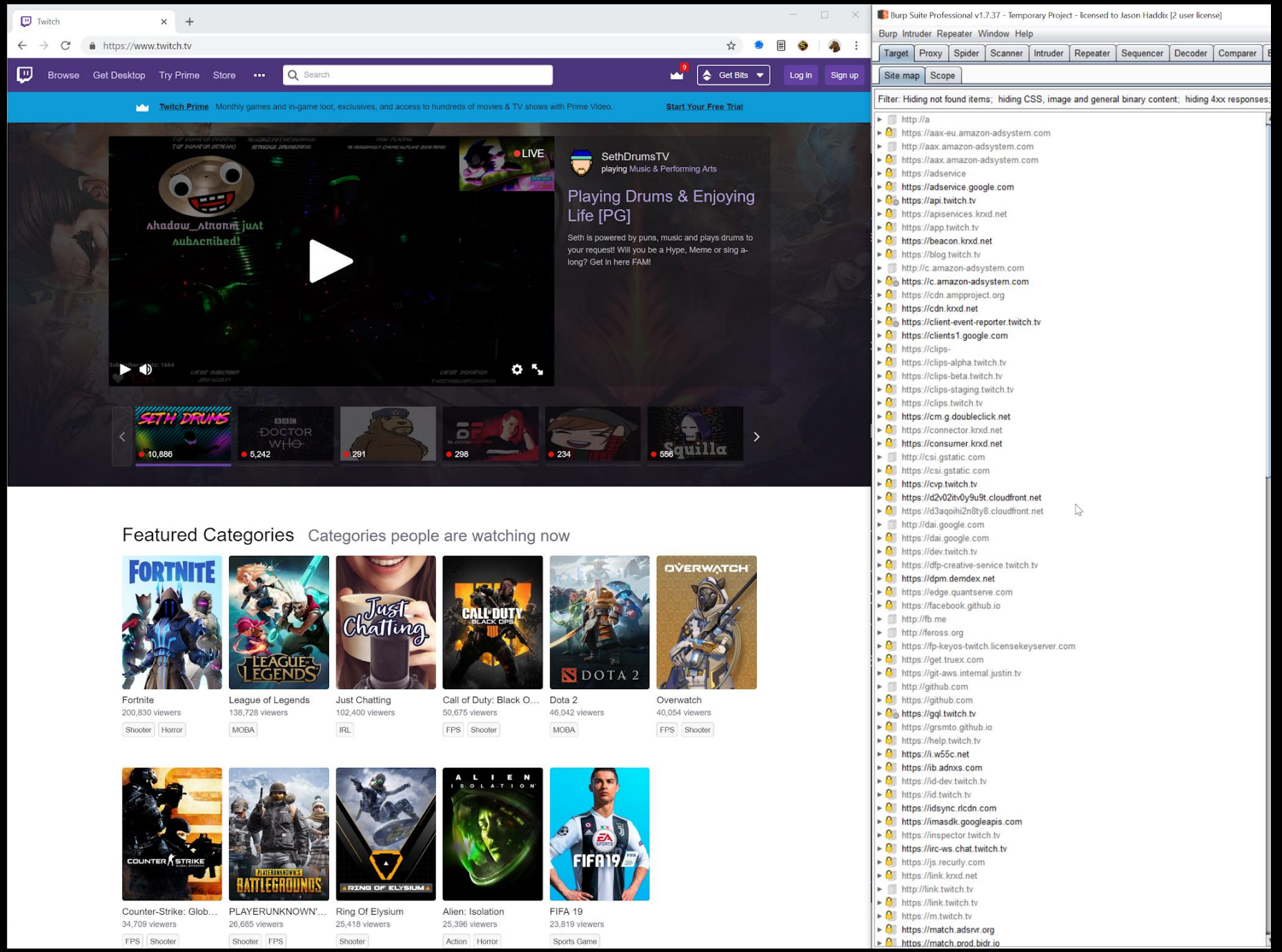
Another way to to widen our scope is to examine all the links of our main target. We can do this using Burp Suite.

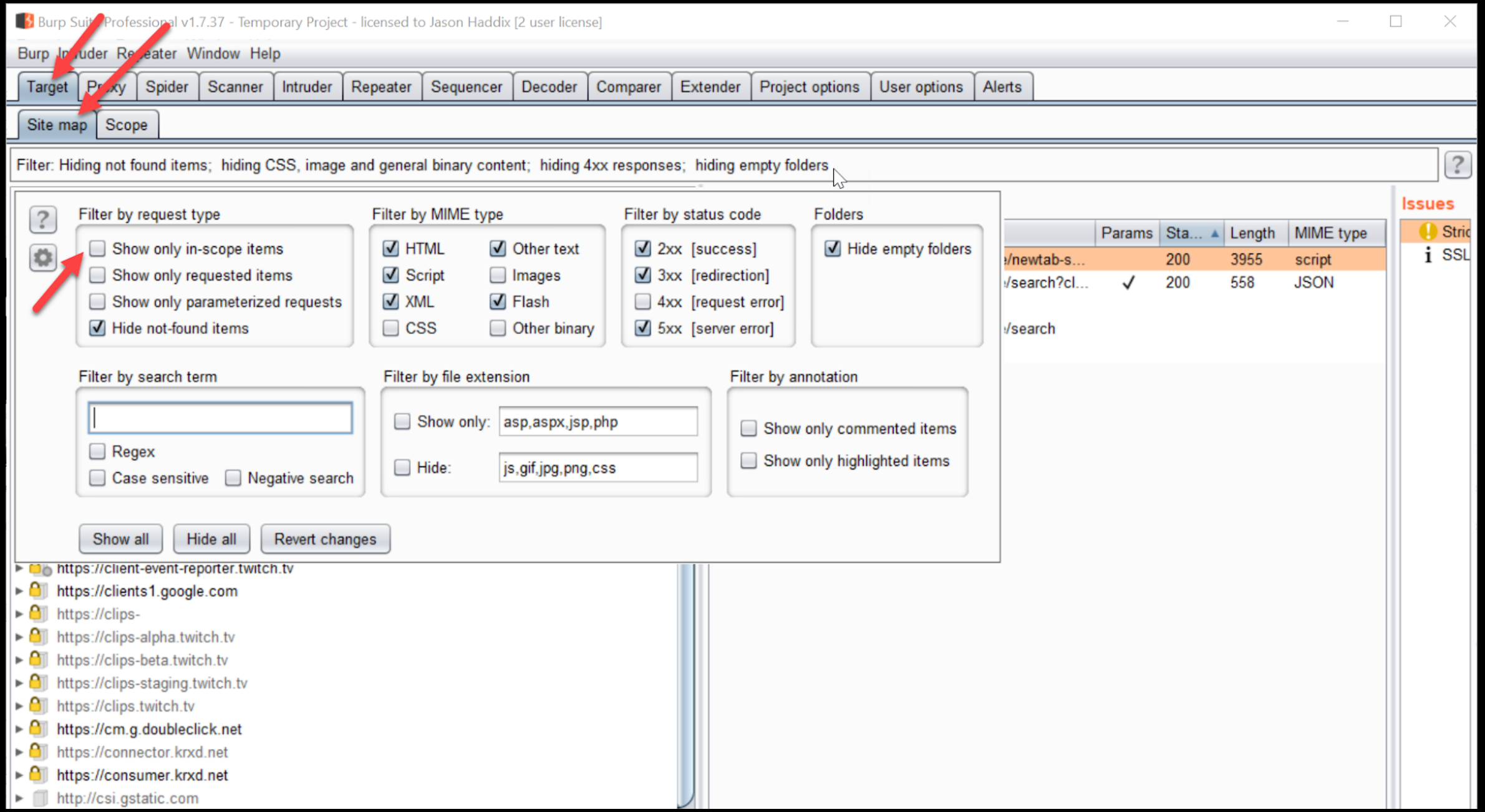
We can then recursively spider all those links for a term with regex, examining those links... and their links, and so on... until we have found all sites that could be in our scope.

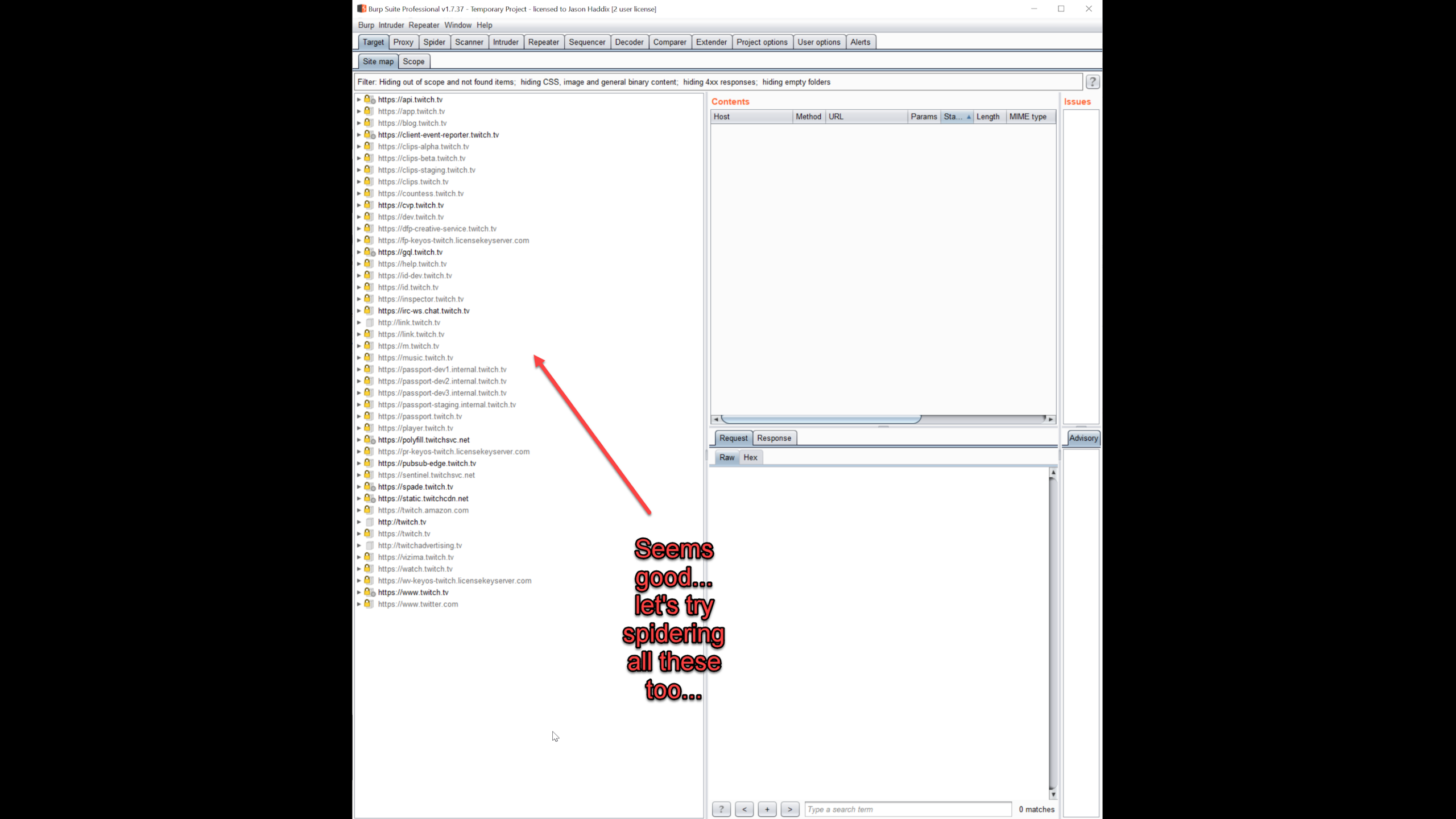
Instructor DEMO

1. Turn off passive scanning
2. Set forms auto to submit (if you're feeling frisky)
3. Set scope to advanced control and use "keyword" of target name (not a normal FQDN)
4. Walk+browse main site, then spider all hosts recursively!
5. Profit

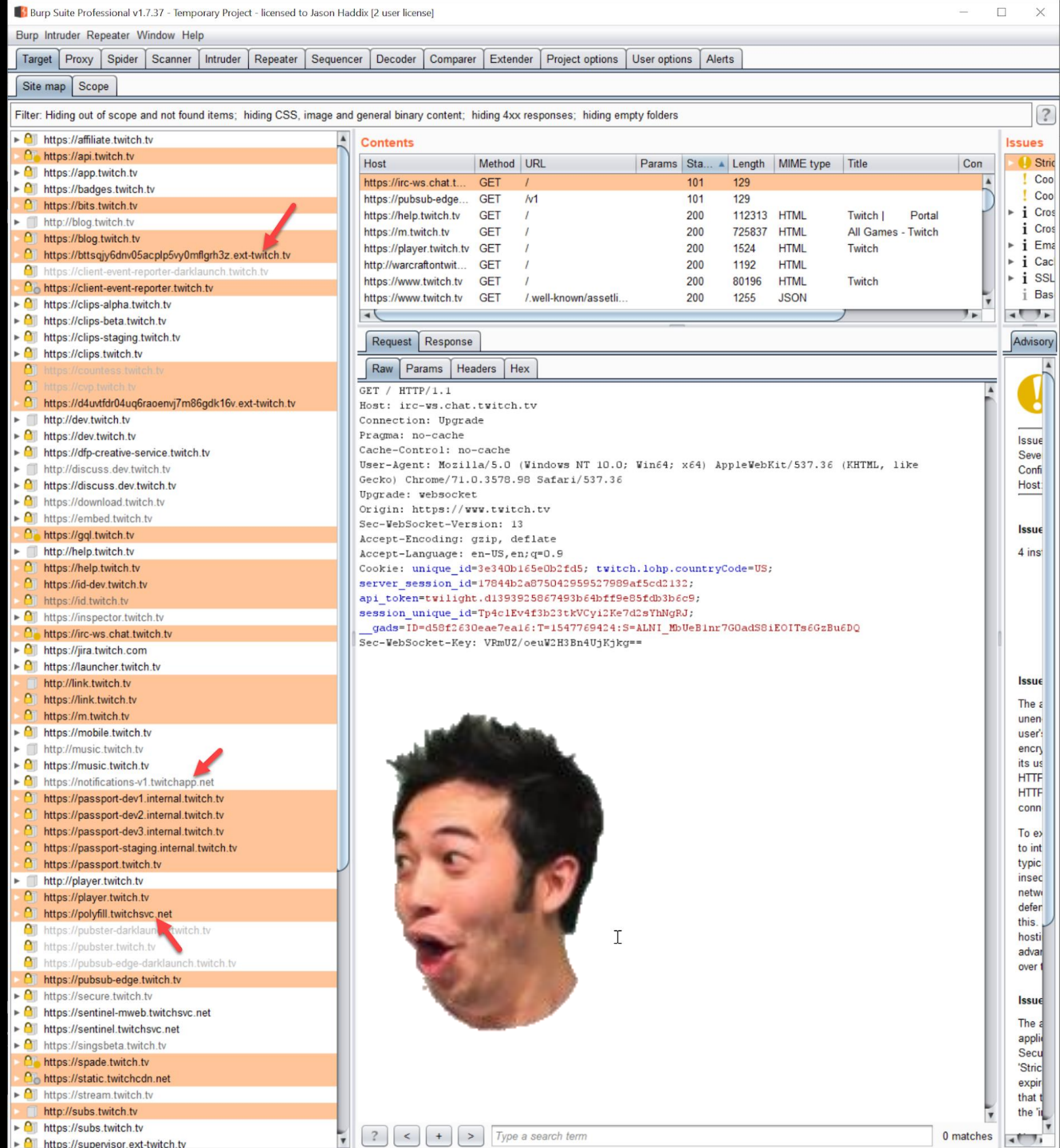
Burp site tree after one request...




Burp Suite Professional v1.7.37 - Temporary Project - licensed to Jason Haddix [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Filter by request type
Show only in-scope items
Show only requested items
Show only parameterized requests
Hide not-found items
Filter by MIME type
HTML
Script
XML
CSS
Other text
Images
Flash
Other binary
Filter by status code
2xx [success]
3xx [redirection]
4xx [request error]
5xx [server error]
Folders
Hide empty folders
Filter by search term
Regex
Case sensitive
Negative search
Filter by file extension
Show only: asp,aspx,jsp,php
Hide: js,gif,jpg,png,css
Filter by annotation
Show only commented items
Show only highlighted items
Show all
Hide all
Revert changes
Params
Sta...
Length
MIME type
/newtab-s...
200
3955
script
/search?cl...
200
558
JSON
/search
Issues
SSL
https://client-event-reporter.twitch.tv
https://clients1.google.com
https://clips-
https://clips-alpha.twitch.tv
https://clips-beta.twitch.tv
https://clips-staging.twitch.tv
https://clips.twitch.tv
https://cm.g.doubleclick.net
https://connector.krxd.net
https://consumer.krxd.net
http://csi.gstatic.com


Burp Suite Professional v1.7.37 - Temporary Project - licensed to Jason Haddix [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
https://api.twitch.tv
https://app.twitch.tv
https://blog.twitch.tv
https://client-event-reporter.twitch.tv
https://clips-alpha.twitch.tv
https://clips-beta.twitch.tv
https://clips-staging.twitch.tv
https://clips.twitch.tv
https://countess.twitch.tv
https://cvp.twitch.tv
https://dev.twitch.tv
https://dfp-creative-service.twitch.tv
https://fp-keyos-twitch.licensekeyserver.com
https://gql.twitch.tv
https://help.twitch.tv
https://id-dev.twitch.tv
https://id.twitch.tv
https://inspector.twitch.tv
https://irc-ws.chat.twitch.tv
http://link.twitch.tv
https://link.twitch.tv
https://m.twitch.tv
https://music.twitch.tv
https://passport-dev1.internal.twitch.tv
https://passport-dev2.internal.twitch.tv
https://passport-dev3.internal.twitch.tv
https://passport-staging.internal.twitch.tv
https://passport.twitch.tv
https://player.twitch.tv
https://polyfill.twitchsvc.net
https://pr-keyos-twitch.licensekeyserver.com
https://pubsub-edge.twitch.tv
https://sentinel.twitchsvc.net
https://spade.twitch.tv
https://static.twitchcdn.net
https://twitch.amazon.com
http://twitch.tv
https://twitch.tv
http://twitchadvertising.tv
https://vizima.twitch.tv
https://watch.twitch.tv
https://ww-keyos-twitch.licensekeyserver.com
https://www.twitch.tv
https://www.twitter.com
Contents
Host Method URL Params Sta... Length MIME type
Issues
Request Response
Raw Hex
Advisory
Type a search term
0 matches
Seems good... let's try spidering all these too...

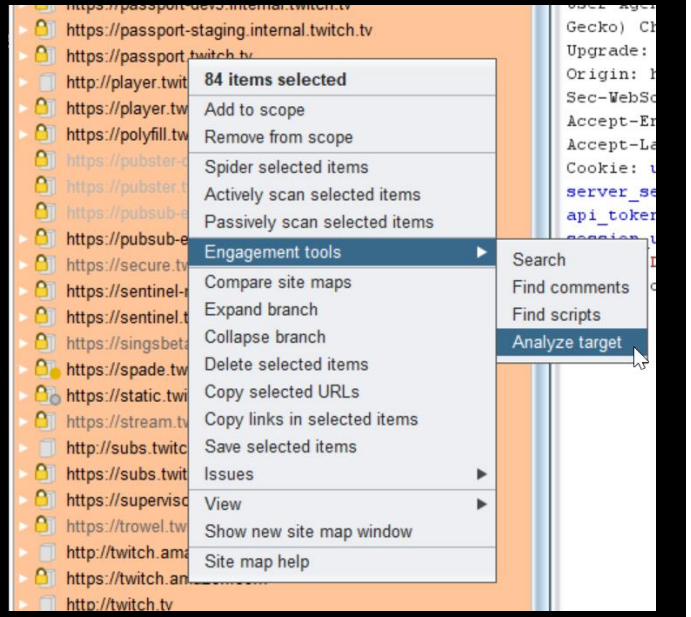
We've now discovered a TON of linked URLs that belong to our entity. Not only subdomains, but completely **NEW apex** domains we can do analysis later on in the subdomain discovery section.We can also now spider these hosts.



Now that we have this data, how do we export it?

Clumsily =(

1. Select all hosts in the site tree
2. In PRO ONLY right click the selected hosts
3. Go to “Engagement Tools” -> “Analyze target”
4. Save report as an html file
5. Copy the hosts from the “Target” section



Target analysis

Targets

- https://affiliate.twitch.tv/
- https://api.twitch.tv/
- https://app.twitch.tv/
- https://badges.twitch.tv/
- https://bits.twitch.tv/
- http://blog.twitch.tv/
- https://blog.twitch.tv/
- https://bttsqjy6dnv05acplp5vy0mflgrh3z.ext-twitch.tv/
- https://client-event-reporter-darklaunch.twitch.tv/
- https://client-event-reporter.twitch.tv/
- https://clips-alpha.twitch.tv/
- https://clips-beta.twitch.tv/
- https://clips-staging.twitch.tv/
- https://clips.twitch.tv/
- https://countess.twitch.tv/
- https://cvp.twitch.tv/
- https://d4uvtfdr04uq6raoenvj7m86gdk16v.ext-twitch.tv/
- http://dev.twitch.tv/
- https://dev.twitch.tv/
- https://dfp-creative-service.twitch.tv/
- http://discuss.dev.twitch.tv/
- https://discuss.dev.twitch.tv/
- https://download.twitch.tv/
- https://embed.twitch.tv/
- https://gql.twitch.tv/
- http://help.twitch.tv/
- https://help.twitch.tv/
- https://id-dev.twitch.tv/
- https://id.twitch.tv/
- https://inspector.twitch.tv/
- https://irc-ws.chat.twitch.tv/
- https://jira.twitch.com/
- https://launcher.twitch.tv/
- http://link.twitch.tv/
- https://link.twitch.tv/
- https://m.twitch.tv/
- https://mobile.twitch.tv/
- http://music.twitch.tv/
- https://music.twitch.tv/
- https://notifications-v1.twitchapp.net/
- https://passport-dev1.internal.twitch.tv/
- https://passport-dev2.internal.twitch.tv/
- https://passport-dev3.internal.twitch.tv/
- https://passport-staging.internal.twitch.tv/
- https://passport.twitch.tv/
- http://player.twitch.tv/

LINKED DISCOVERY (NEW Burp Pro)

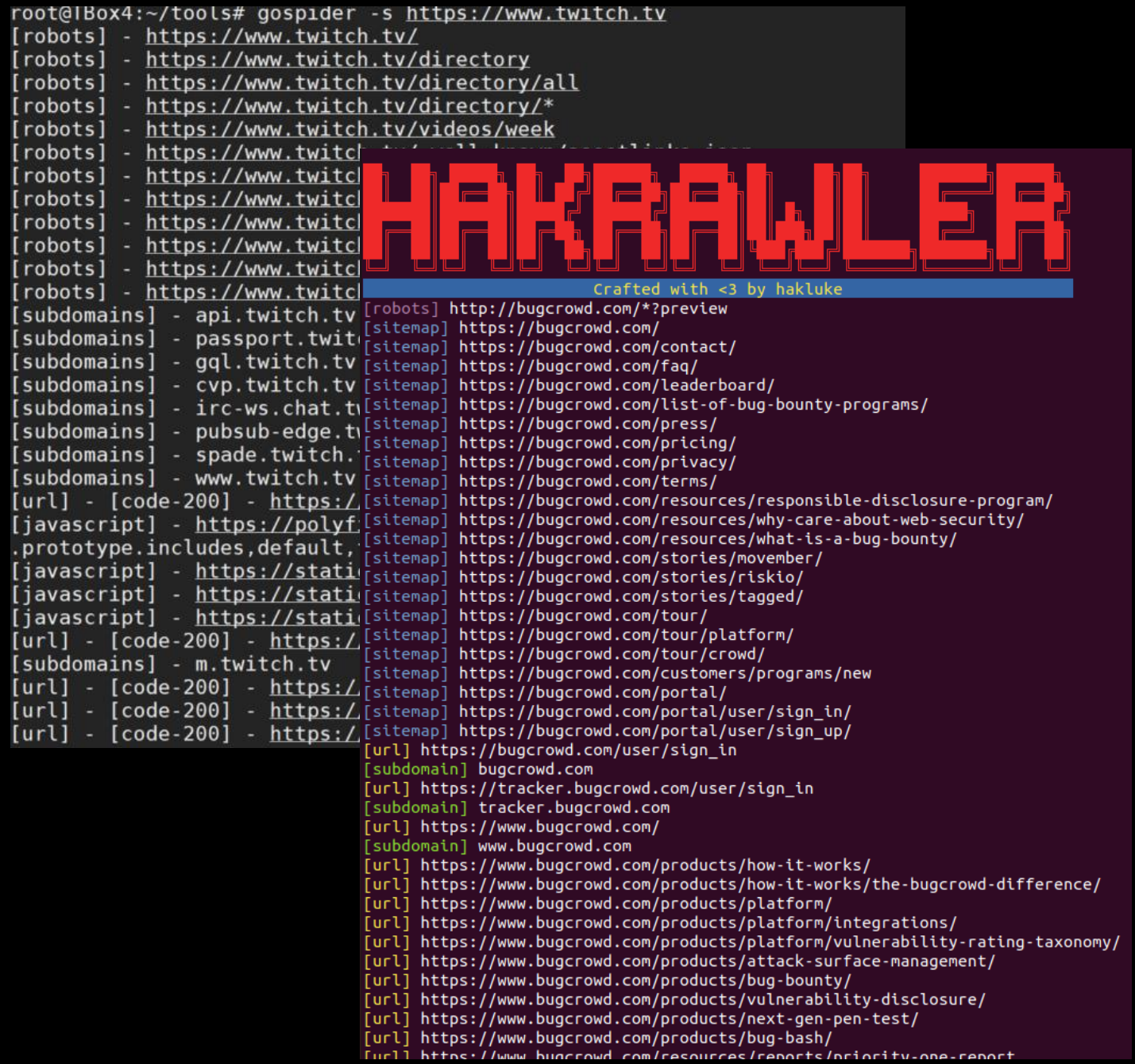
Demo w/ new Burp

LINKED DISCOVERY (Spiders)

Linked discovery really just counts on using a spider recursively.

One of the most extensible spiders for general automation is GoSpider written by j3ssiejjj which can be used for many things and supports parsing js very well.

In addition hakrawler by hakluke has many parsing strategies that interest bug hunters.



AD & ANALYTICS++

WHAT ARE WE AFTER?

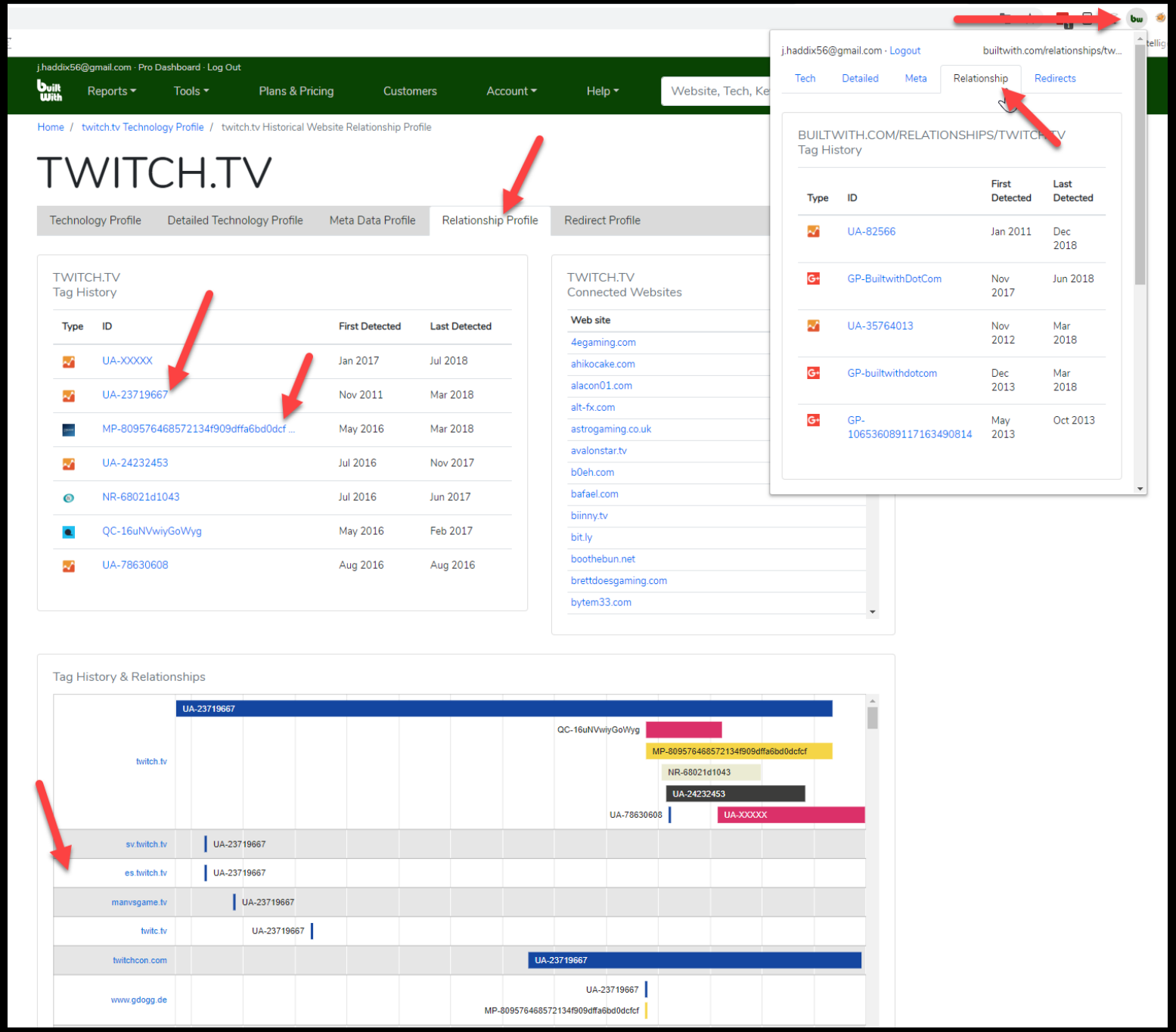
Ad & Analytics relationships can help in finding apex domains and subdomains.

Ad/Analytics Relationships (using builtwith.com)

You can also glean related domains and subdomains by looking at a target's ad/analytics tracker codes. Many sites use the same codes across all their domains. Google analytics and New Relic codes are the most common. We can look at these "relationships" via a site called BuiltWith. Builtwith also has a Chrome and Firefox extension to do this on the fly.

- https://builtwith.com/relationships/twitch.tv

BuiltWith is also a tool we'll use to profile the technology stack of a target later.



Ad/Analytics Relationships (getrelationship.py)

You can do this on the command line with your session cookie and this script by Mall0k:

https://raw.githubusercontent.com/m4ll0k/Bug-Bounty-Toolz/master/getrelationship.py

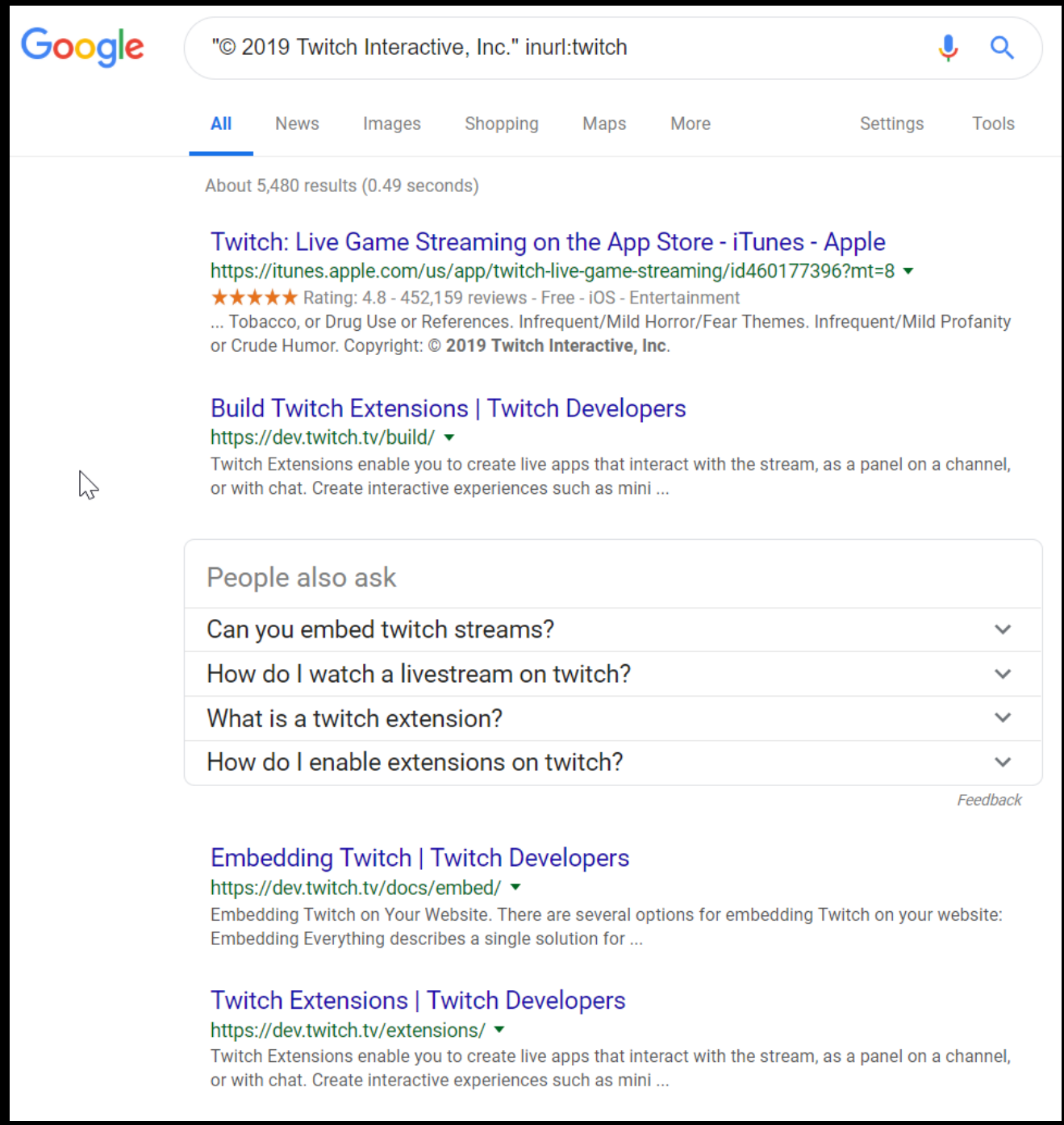
```
~ (master*) # python3 getrelationship.py tesla.com FgMABMlf4RoJrjFXjTBTi/l3WHxgN
/gy9qDXU=
167sscar.com
1solarbid.com
airboard.co
amtesla.homes
anquantec.com
anubisgraphics.com
askneuron.com
atr.ru
tesla-com.aurebeshtranslator.net
baoxianpzh.cn
bellalead.com
bestvoipchoice.com
birthdaycards.com
bizibetiko.com
bjbroad.net
bjsjmy.com
bonusnames.com
casolarcity.com
chiablue.org
chiabluechip.com
chiabluechip.org
chiasolid.com
chiasolid.org
chiassdrive.com
chiassdrive.org
```

Trademark, Terms of Service, Copyright, & Privacy Policy Recon (using Google)

"© 2019 Twitch Interactive, Inc." inurl:twitch

"© 2018 Twitch Interactive, Inc." inurl:twitch

You can Google the copyright and terms of service text from a main target to glean related hosts.



SUBDOMAIN SCRAPING

WHAT ARE WE AFTER?

Subdomain scraping will give us passive subdomains.

Subdomain scraping will by far be the biggest contributor to your subdomain enumeration.

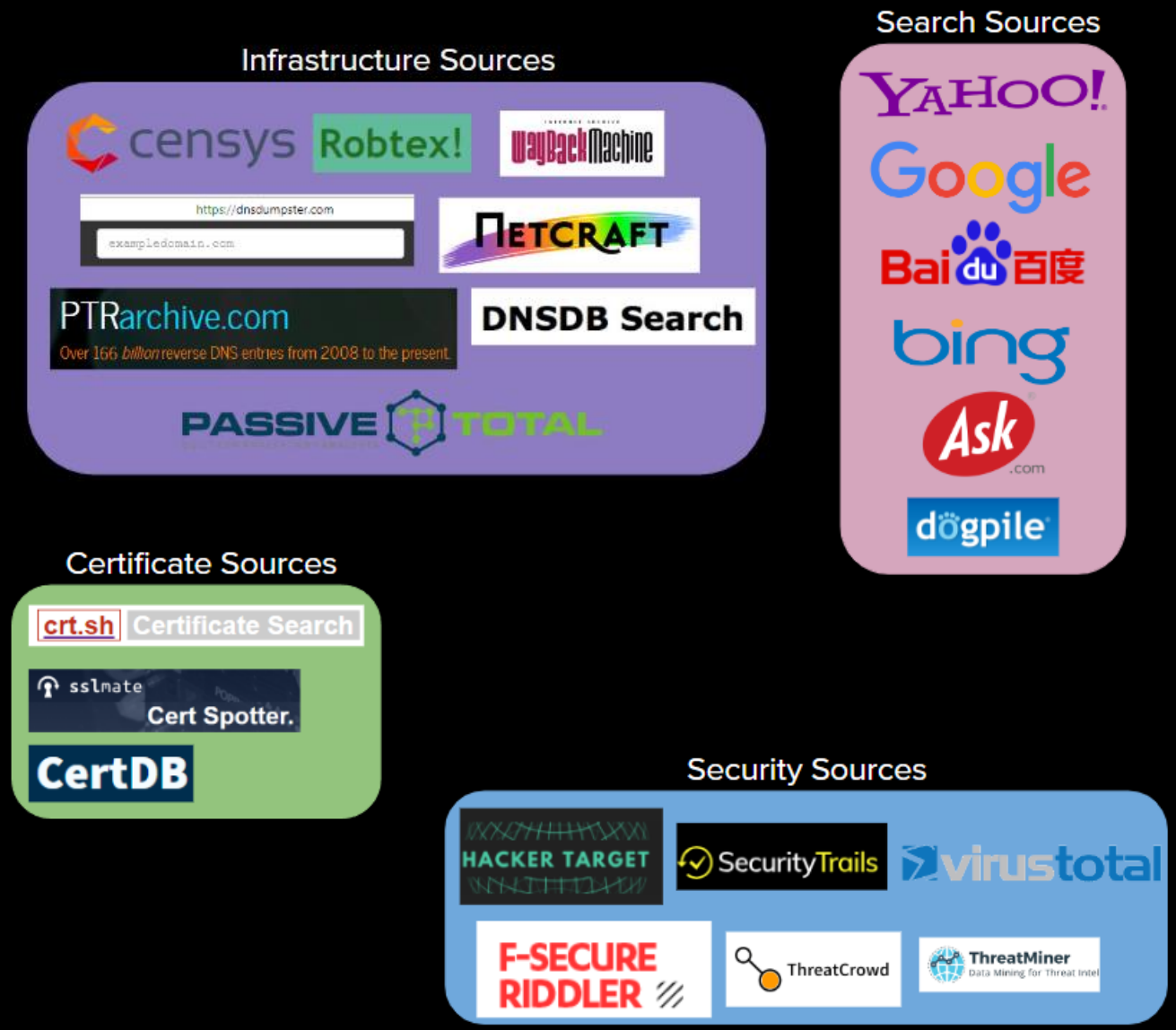
Web Scraping for Subdomains

Domain and URL information gets used across the internet for a multitude of reasons. There are all sorts of data projects that expose databases of URLs or domains they store.

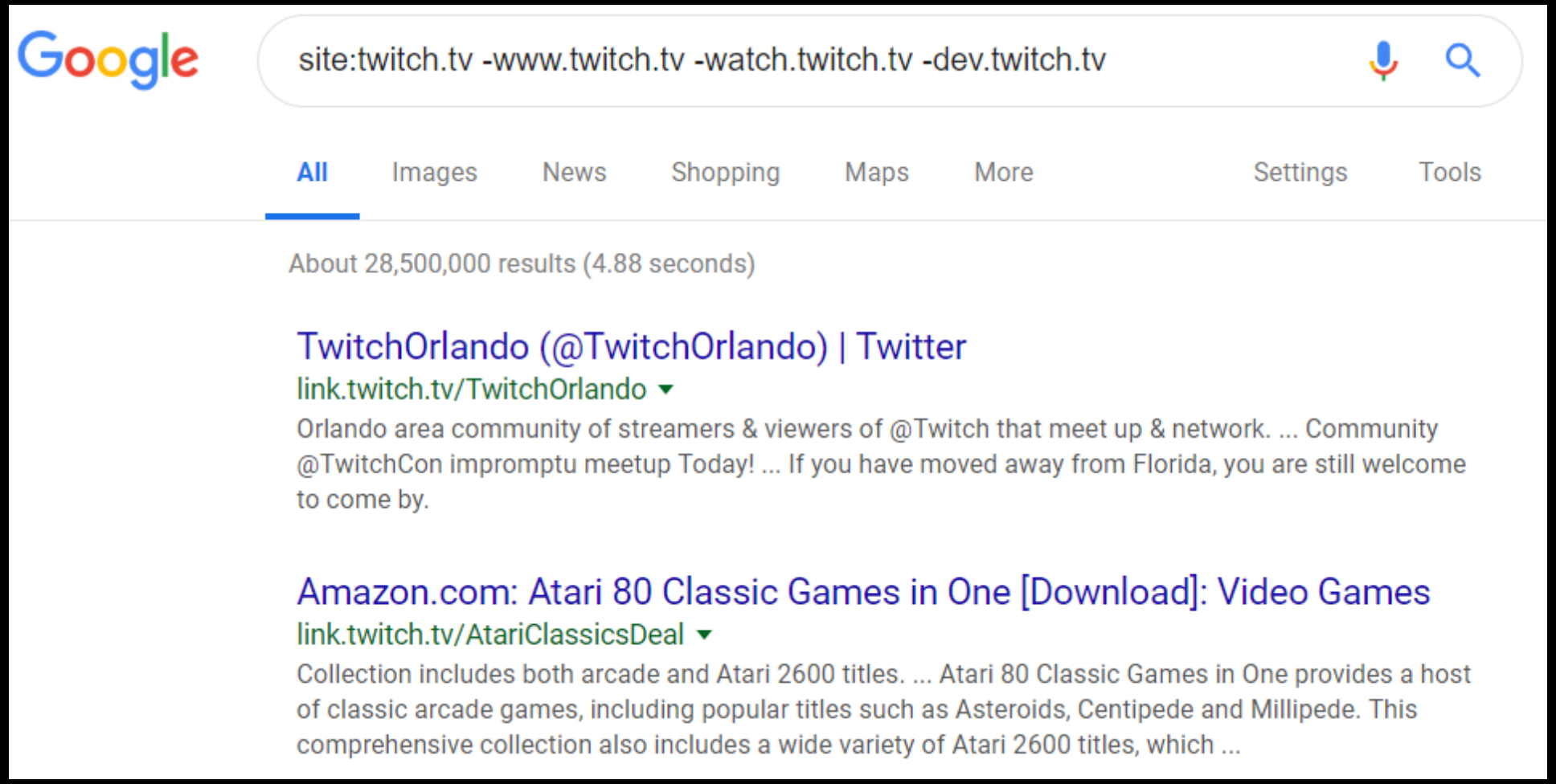
In a wide scope project, we want to query these sites and APIs to discover what subdomains they might know about related to our target.

Luckily, we don't have to do this manually. There are tools for this.

This is only a small list of sources. Many more exist.



1. site:twitch.tv -www.twitch.tv
2. site:twitch.tv -www.twitch.tv -watch.twitch.tv
3. site:twitch.tv -www.twitch.tv -watch.twitch.tv -dev.twitch.tv
4. ...



Subdomain Scraping (using Amass)

For scraping subdomain data, there are currently two industry leading tools, Amass and Subfinder.

They parse all the “sources” referenced in the previous slide, and more.

Amass has extensible output, brute forcing, and more.

Amass is written by Jeff Foley

```
root@Test2:~/tools/amass# amass -d twitch.tv
twitch.tv
passport-external.aws.twitch.tv
gql.twitch.tv
pubsub-edge.twitch.tv
pubsub-edge.chat.twitch.tv
passport.twitch.tv
www.twitch.tv
m.twitch.tv
irc-ws-edge.chat.twitch.tv
irc-ws.chat.twitch.tv
app.twitch.tv
download.twitch.tv
discuss.dev.twitch.tv
invite.twitch.tv
join.twitch.tv
edgecast.hls.twitch.tv has a static DNS wildcard
blog.twitch.tv
polls.twitch.tv
th.blog.twitch.tv
link.twitch.tv
servers.twitch.tv
cis.blog.twitch.tv
graphql.prod.us-west2.twitch.tv
it.blog.twitch.tv
rc.twitch.tv
de.blog.twitch.tv
tr.blog.twitch.tv
release.twitch.tv
nl.blog.twitch.tv
canary.twitch.tv
ccu.event-engineering.twitch.tv
pong.prod.us-west2.twitch.tv
jp.blog.twitch.tv
event-panel.event-engineering.twitch.tv
assets.help.twitch.tv
uploads-regional.twitch.tv
websub-test-proxy.twitch.tv
```

Amass also groups these scraped domains to ASNs, Owners, and IP Ranges.

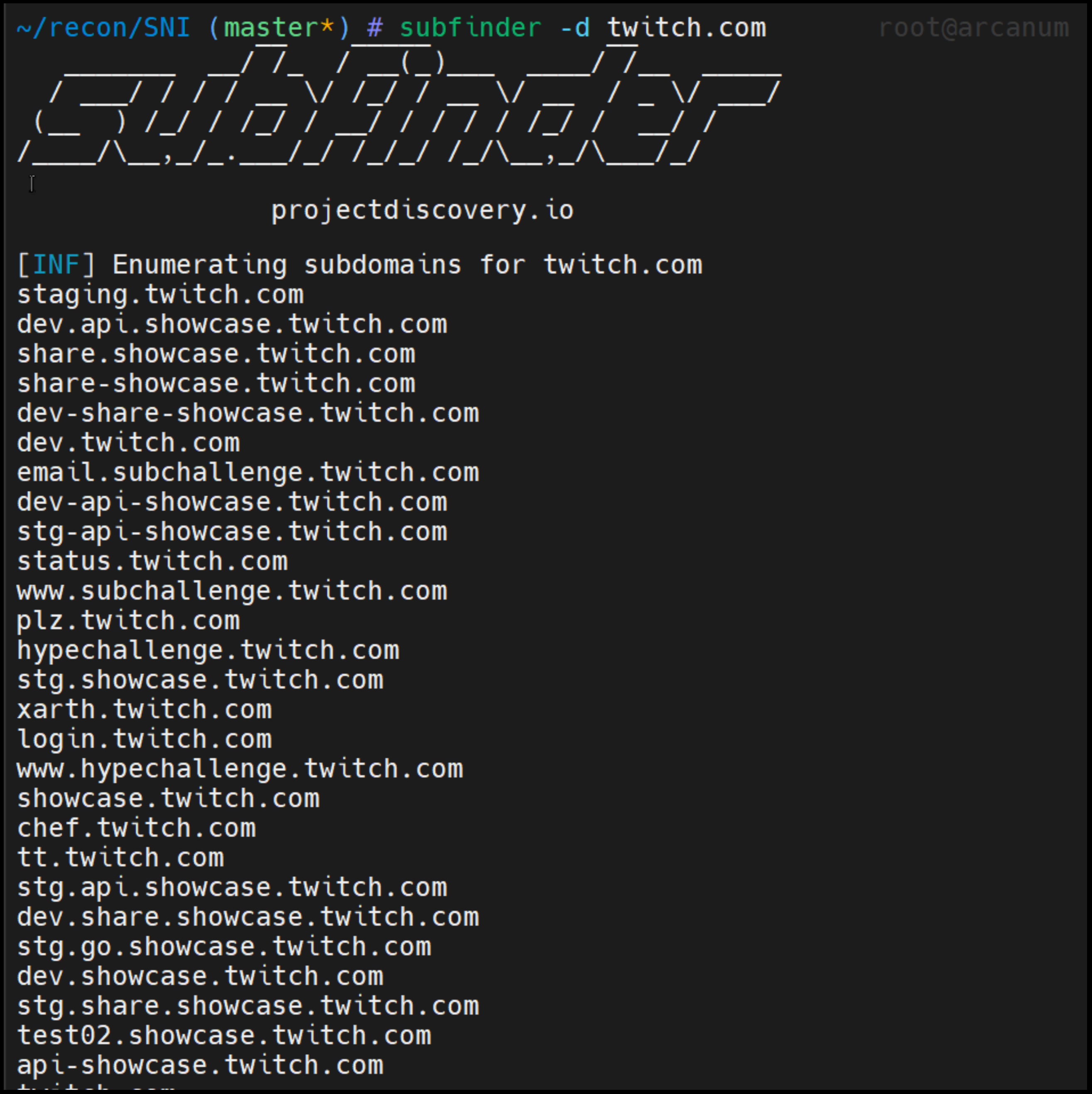
Useful.

```
Average DNS names processed: 49/sec

OWASP Amass v2.9.0                                https://github.com/OWASP/Amass
-------------------------------------------------------------------------------
439 names discovered - alt: 77, dns: 3, cert: 105, archive: 24, scrape: 218, api: 12
-------------------------------------------------------------------------------
ASN: 54113 - FASTLY - Fastly, US
       151.101.64.0/22          2    Subdomain Name(s)
       151.101.0.0/22           2    Subdomain Name(s)
       151.101.188.0/22         52   Subdomain Name(s)
       151.101.40.0/22          1    Subdomain Name(s)
       151.101.244.0/22         1    Subdomain Name(s)
       151.101.192.0/22         2    Subdomain Name(s)
       151.101.128.0/22         2    Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc., US
       52.24.0.0/14             35   Subdomain Name(s)
       52.84.48.0/23            4    Subdomain Name(s)
       13.35.8.0/23             4    Subdomain Name(s)
       34.208.0.0/12            15   Subdomain Name(s)
       35.160.0.0/13            16   Subdomain Name(s)
       54.254.128.0/17          1    Subdomain Name(s)
       54.186.0.0/15            9    Subdomain Name(s)
       52.18.0.0/15             2    Subdomain Name(s)
       52.36.0.0/14             6    Subdomain Name(s)
       35.178.0.0/15            1    Subdomain Name(s)
       2600:9000:202d::/48      54   Subdomain Name(s)
       52.40.0.0/14             5    Subdomain Name(s)
       54.192.144.0/22          12   Subdomain Name(s)
       52.220.0.0/15            1    Subdomain Name(s)
       54.171.0.0/16            2    Subdomain Name(s)
       3.8.0.0/14               1    Subdomain Name(s)
       54.192.12.0/22           55   Subdomain Name(s)
       2600:9000:2001::/48      26   Subdomain Name(s)
       54.148.0.0/15            10   Subdomain Name(s)
       2600:9000:204b::/48      8    Subdomain Name(s)
       52.10.0.0/15             3    Subdomain Name(s)
       2600:9000:201d::/48      8    Subdomain Name(s)
       52.84.44.0/22            1    Subdomain Name(s)
       52.88.0.0/15             7    Subdomain Name(s)
       2600:9000:2145::/48      8    Subdomain Name(s)
       184.169.128.0/17         1    Subdomain Name(s)
       52.208.0.0/13            3    Subdomain Name(s)
       52.32.0.0/14             11   Subdomain Name(s)
       13.35.124.0/22           44   Subdomain Name(s)
       50.112.128.0/19          3    Subdomain Name(s)
       52.52.0.0/15             3    Subdomain Name(s)
       54.215.128.0/18          2    Subdomain Name(s)
       54.68.0.0/15             2    Subdomain Name(s)
       54.191.0.0/16            3    Subdomain Name(s)
       54.70.0.0/15             2    Subdomain Name(s)
       54.200.0.0/15            6    Subdomain Name(s)
       50.18.0.0/18             1    Subdomain Name(s)
ASN: 0 - Private Networks
       10.0.0.0/8               66   Subdomain Name(s)
ASN: 46489 - JUSTINTV - Twitch Interactive Inc., US
       52.223.240.0/20          21   Subdomain Name(s)
       192.16.64.0/21           32   Subdomain Name(s)
       99.181.64.0/20           2    Subdomain Name(s)
       52.223.224.0/20          27   Subdomain Name(s)
       45.113.128.0/22          10   Subdomain Name(s)
       192.108.239.0/24         4    Subdomain Name(s)
       52.223.208.0/21          28   Subdomain Name(s)
       199.9.248.0/21           164  Subdomain Name(s)
       185.42.204.0/22          15   Subdomain Name(s)
       23.160.0.0/24            8    Subdomain Name(s)
       52.223.192.0/20          11   Subdomain Name(s)
ASN: 40341 - Q9-AS-CAL2 - Q9 Networks Inc., CA
       162.219.8.0/21           1    Subdomain Name(s)
ASN: 14618 - AMAZON-AES - Amazon.com, Inc., US
       54.84.0.0/15             1    Subdomain Name(s)
       52.72.0.0/15             1    Subdomain Name(s)
       52.0.0.0/15              71   Subdomain Name(s)
       2600:1f18::/33           1    Subdomain Name(s)
       52.2.0.0/15              2    Subdomain Name(s)
       18.204.0.0/14            3    Subdomain Name(s)
       52.200.0.0/13            4    Subdomain Name(s)
       52.4.0.0/14              137  Subdomain Name(s)
       52.20.0.0/14             1    Subdomain Name(s)
ASN: 395224 - BITLY-AS - Bitly Inc, US
       67.199.248.0/24          4    Subdomain Name(s)
ASN: 15169 - GOOGLE - Google LLC, US
       35.185.0.0/19            1    Subdomain Name(s)
ASN: 22606 - EXACT-7 - ExactTarget, Inc., US
       13.111.18.0/24           5    Subdomain Name(s)
       13.111.19.0/24           1    Subdomain Name(s)
       13.111.20.0/24           1    Subdomain Name(s)
       13.111.97.0/24           1    Subdomain Name(s)
ASN: 11377 - SENDGRID - SendGrid, Inc., US
       167.89.64.0/19           1    Subdomain Name(s)
ASN: 38895 - AMAZON-AS-AP Amazon.com Tech Telecom, JP
       2600:9000:20c7::/48      8    Subdomain Name(s)
```

Subdomain Scraping (using Subfinder)

Subfinder written by Project Discovery is also a best-in-class tool to gather this data from various websites and APIs

I use both tools and concatenate and uniq the outputs.



Subdomain Scraping (using BBOT)

BBOT is a new entry to subdomain scraping. It wraps around some other tools and adds a few new sources. I have added it to my workflow.

It does much more than just subdomain scraping as well.

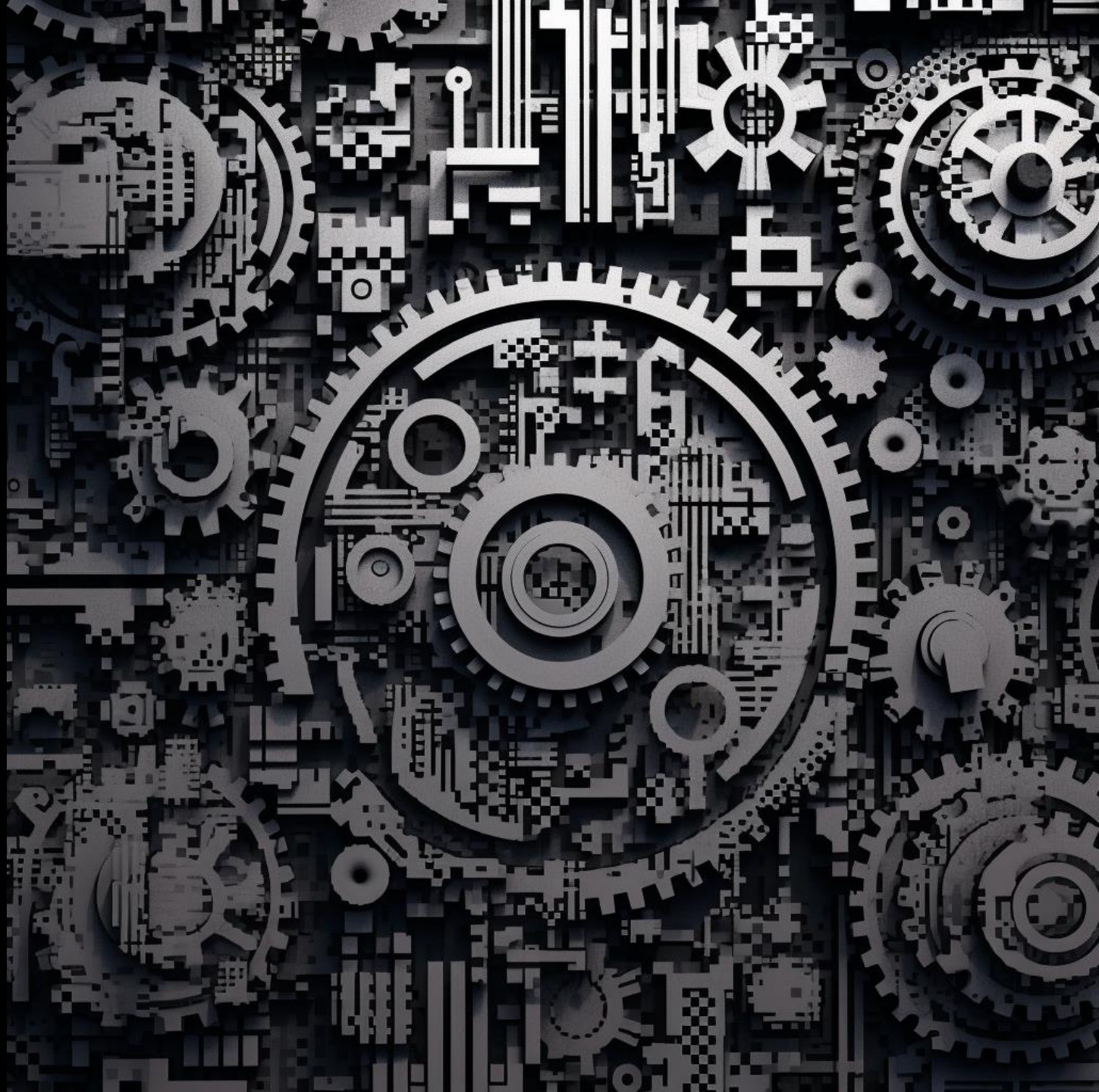
```
bls bbot $ bbot -m otx -t tesla.com
[INFO] bbot: Loaded defaults from /home/bls/Downloads/code/bbot/bbot/defaults.yml
[INFO] bbot: Loaded config from /home/bls/.config/bbot/bbot.yml
[INFO] bbot: Loaded secrets from /home/bls/.config/bbot/secrets.yml
[INFO] bbot.cli:
[INFO] bbot.cli: ### MODULES ###
[INFO] bbot.cli:
[INFO] bbot.cli: +----------+--------+---------+-----------------------------------------+---------------------------+------------------+
[INFO] bbot.cli: | Module   | Type   | Needs   | Description                             | Flags                     | Produced Events  |
[INFO] bbot.cli: |          |        | API     |                                         |                           |                  |
[INFO] bbot.cli: |          |        | Key     |                                         |                           |                  |
[INFO] bbot.cli: +==========+========+=========+=========================================+===========================+==================+
[INFO] bbot.cli: | otx      | scan   |         | Query otx.alienvault.com for subdomains | passive,safe,subdomain-enum | DNS_NAME       |
[INFO] bbot.cli: +----------+--------+---------+-----------------------------------------+---------------------------+------------------+
[INFO] bbot.scanner: Scan with 1 modules seeded with 1 targets
[INFO] bbot.scanner: Loaded 1/1 scan modules (otx)
[INFO] bbot.scanner: Loaded 1/1 internal modules (aggregate)
[INFO] bbot.scanner: Loaded 1/1 output modules, (human)
[INFO] bbot.scanner: Setting up modules...
[SUCC] bbot.scanner: Setup succeeded for 3 modules.
[SUCC] bbot.cli: Scan ready. Press enter to execute philosophical_sauron

[SUCC] bbot.scanner: Starting scan philosophical_sauron
[SCAN]                  philosophical_sauron (SCAN:a6d54ea493057713316121184[illegible]c88a3e9)    TARGET  (distance-0)
[DNS_NAME]              tesla.com       TARGET  (distance-0, domain, in-scope, resolved, target)
[DNS_NAME]              acme-sentry-4a.eng.use1.vn.cloud.tesla.com      otx     (distance-0, in-scope, subdomain, unresolved)
[DNS_NAME]              mobile.kronos.tesla.com otx     (a-record, cloud-amazon, cloud-aws, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              sso-dev.tesla.com       otx     (a-record, aaaa-record, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              employeefeedback.tesla.com      otx     (a-record, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              energydesk.tesla.com    otx     (a-record, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              digitalassets-shop.tesla.com    otx     (a-record, aaaa-record, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              fleetview.fn.tesla.com  otx     (a-record, cloud-amazon, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              sc-cppm.tesla.com       otx     (a-record, cloud-amazon, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              integration.kronos.tesla.com    otx     (a-record, cloud-amazon, cloud-aws, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              apacvpn1.tesla.com      otx     (a-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              digitalassets-contents.tesla.com        otx     (a-record, aaaa-record, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              digitalassets.tesla.com otx     (a-record, aaaa-record, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              feedback.tesla.com      otx     (a-record, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              api.kronos.tesla.com    otx     (a-record, cloud-amazon, cloud-aws, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              sso.tesla.com   otx     (a-record, aaaa-record, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              toolbox.tesla.com       otx     (a-record, aaaa-record, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              wdm.kronos.tesla.com    otx     (a-record, cloud-amazon, cloud-aws, cname-record, distance-0, in-scope, resolved, subdomain)
[DNS_NAME]              kronos.tesla.com        otx     (a-record, aaaa-record, cname-record, distance-0, in-scope, resolved, subdomain)
```

Subdomain Scraping (using BBOT, working with BBOT output)

The output is a file at “/root/.bbot/scans/{scan_name}/” You can clean up the output to just found subdomains per line like so:

```
cat /root/.bbot/scans/{scan_name}/output.txt | grep -F '[DNS_NAME]' | awk '{print $2}'
```

SUBDOMAIN SCRAPING CONFIG



WHY?

Configuring the APIs for the tools increases their efficacy by up to 50%

Subdomain Scraping Configurations

As you saw in a few of the screenshots many of these tools need API keys to access certain sources.

You absolutely need these to be effective

If you look at my Amass, you can see it has x data sources:

amass enum –list

I want to enable any NOT enabled by providing API keys (if they are free)

amass enum -list | grep -v "*"

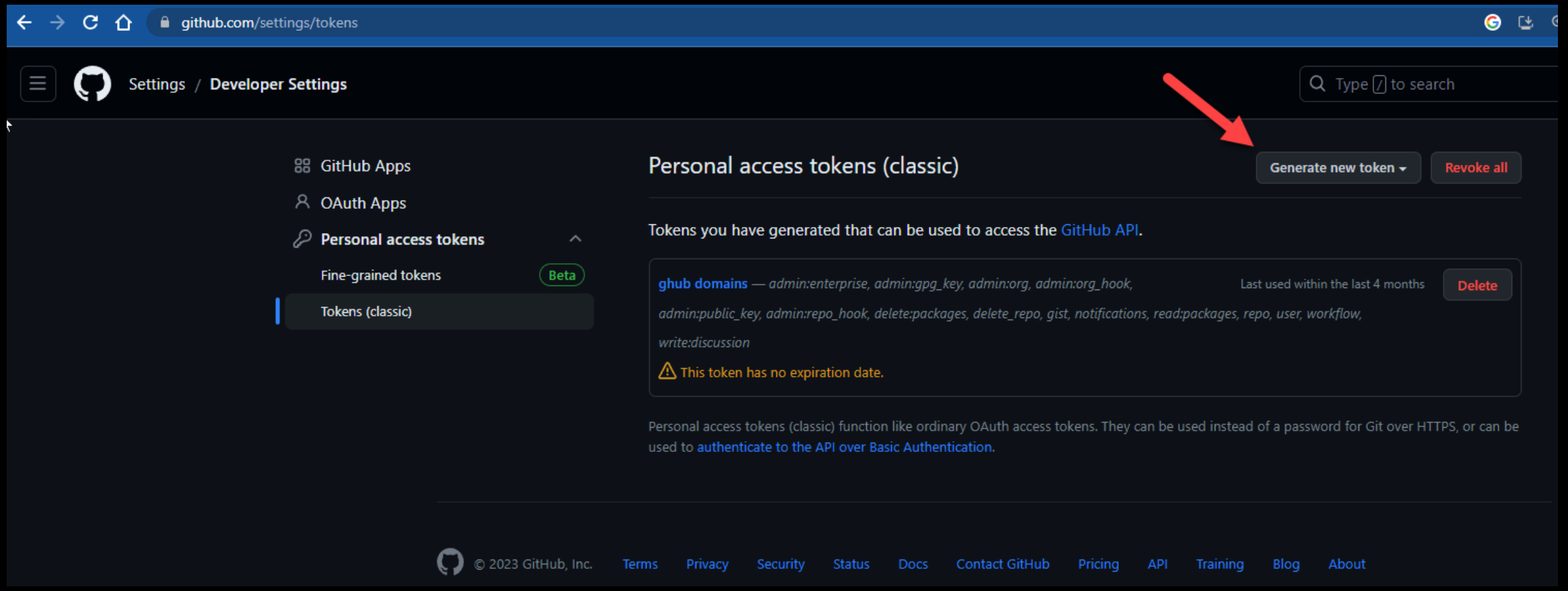
```
~ (master*) # amass enum -list

Data Source                | Type                    | Available
---------------------------------------------------------------------
360PassiveDNS              api
ASNLookup                  api
AbuseIPDB                  scrape                    *
Active Crawl               crawl                     *
Active DNS                 dns                       *
Ahrefs                     api
AlienVault                 api                       *
Alterations                alt                       *
AnubisDB                   api                       *
Arquivo                    archive                   *
Ask                        scrape                    *
AskDNS                     scrape                    *
BGPTools                   misc                      *
BGPView                    api                       *
Baidu                      scrape                    *
BeVigil                    api
BigDataCloud               api
BinaryEdge                 api
Bing                       scrape                    *
Brute Forcing              brute                     *
BufferOver                 api
BuiltWith                  api
C99                        api
CIRCL                      api
Censys                     cert
CertCentral                cert
CertSpotter                cert                      *
Chaos                      api                       *
CommonCrawl                crawl                     *
Crtsh                      cert                      *
DNS SRV                    dns                       *
DNSDB                      api
DNSDumpster                scrape                    *
```

Priority #1 (Chaos)

https://chaos.projectdiscovery.io/#/

Let's talk about Chaos secret...

Priority #2 (GitHub)



https://github.com/settings/tokens

How many can you get?

The Rest (free)

- FacebookCT
  - Open https://developers.facebook.com and Sign in as a facebook (developer)
  - Go to apps, create app
  - Create app > Your app page
  - Get apikey
  - setting > advance setting > security > client token
  - Get Secret

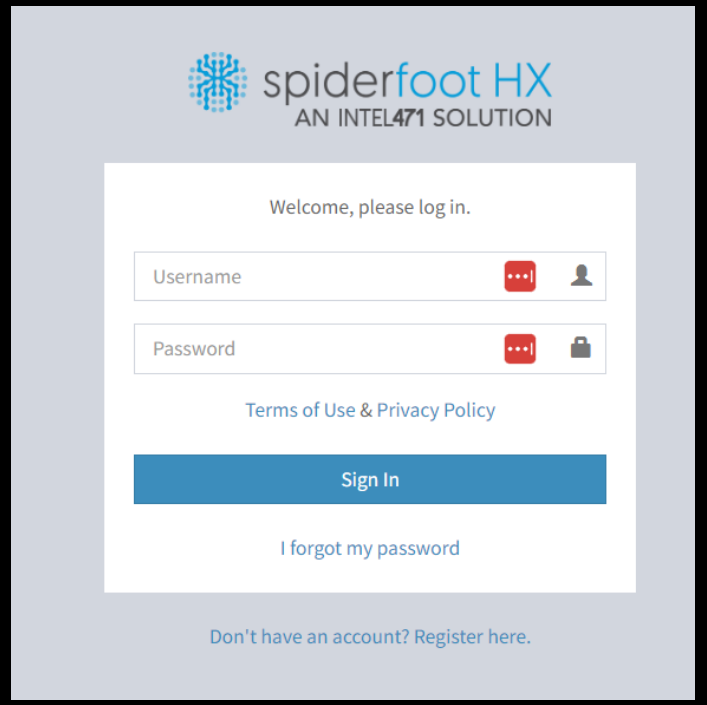
- PassiveTotal
  - https://community.riskiq.com/settings

- Shodan (Cheap)

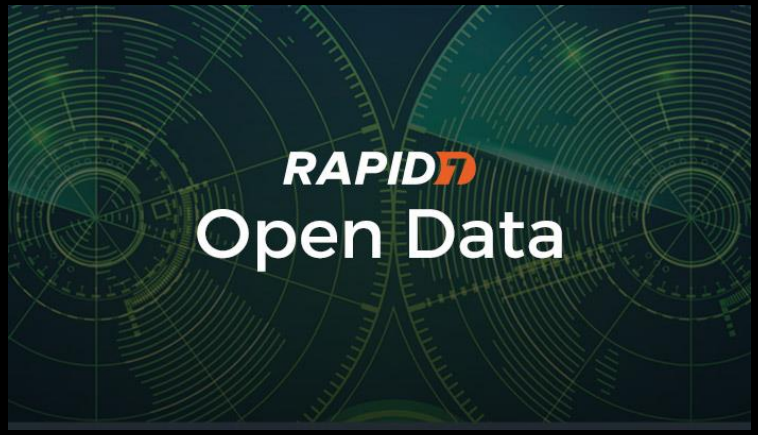
Put them all in: ~/.config/amass/config.ini

Paid / Limited Sources

- Rapid 7 Sonar
  - Good dataset but only avail upon req, no one has it recently
- SecurityTrails
  - The best paid API
- SpiderFootHX
  - 2nd best paid API
  - Acquired, trying to DM vendor



SecurityTrails



GITHUB ENUMERATION

WHAT ARE WE AFTER?

Github Enumeration can give us passive subdomains, IP addresses, vulnerability data, and more...

GITHUB ENUMERATION

Note:

Most tools in this arena that offer automation to find things are targeted at scanning a single repo or organization. This is the opposite of what we want. We want to scour all repos, especially personal ones, to find the following data.

GITHUB ENUMERATION (subdomains with github-subdomains)

We want to extract any referenced subdomains of our target that are on GitHub.

Why use a stand-alone tool?

It's simply the best and the API is random.

You need many API keys and many runs to complete this method.

```
~ (master*) # github-subdomains -d dell.com -t ghp_q
Wv68vXF7xAjf94Fgb7m -o githubdell10.txt

github subdomains
by @gwendallecoguic

[12:15:55] Domain:dell.com, Output:githubdell10.txt
[12:15:55] Tokens:3, Delay:866ms
[12:15:55] Token rehab:true, Quick mode:false
[12:15:55] Languages:20, Noise:7
[12:15:55] keyword:%22dell.com%22, sort:indexed, order:desc, language:, noise:[]
[12:15:56] https://api.github.com/search/code?per_page=100&s=indexed&type=Code&o=desc&q=%22dell.com%22&page
[12:15:57] current search returned 22816 results, language filter added for later search
[12:15:57] https://github.com/trickest/cve/blob/d740a037a3cac6cc34626c6d5c43f8d4712b1edc/2022/CVE-2022-2685
[12:15:57] www.dell.com
[12:15:57] https://github.com/AdguardTeam/AdguardBrowserExtension/blob/1e5d5f8b7c1b74d8c345e58949d2fc7e6cd7
7.txt
[12:15:57] dell.com
[12:15:57] https://github.com/digoal/blog/blob/32cc6204e0fba8280f091c5f4a540e38b6bb1cad/201805/20180524_01.
[12:15:57] en.community.dell.com
[12:15:57] https://github.com/felixonmars/dnsmasq-china-list/blob/895e9f2517d9849a6cfcfcb835347939ec78f3a1/
[12:15:57] configure.ap.dell.com
[12:15:57] topics-cdn.dell.com
[12:15:57] https://github.com/fwupd/fwupd/blob/87c0651c2a46c888322cf1b97c0de9be9483461e/contrib/firmware_pa
[12:15:57] downloads.dell.com
[12:15:57] www1-cdn.dell.com
[12:15:57] https://github.com/Kaustubh-Natuskar/moreThanFAANGM/blob/a7ae9f2ecff8ad71397b82bdb43e9da765d15de
[12:15:57] jobs.dell.com
[12:15:57] https://github.com/FreeRDP/FreeRDP/blob/e18918356f7669ab347d97ce06fdddb31e772a27/libfreerdp/core
[12:15:57] software.dell.com
[12:15:57] https://github.com/git/git/blob/061c58647eb4b3f0e2c898333577d4b2af115b1d/.mailmap
[12:15:57] pig.linuxdev.us.dell.com
[12:15:57] https://github.com/Homebrew/homebrew-cask/blob/fff71217768fe8a83e871407244079b49125ea65/Casks/dd
[12:15:57] dl.dell.com
```

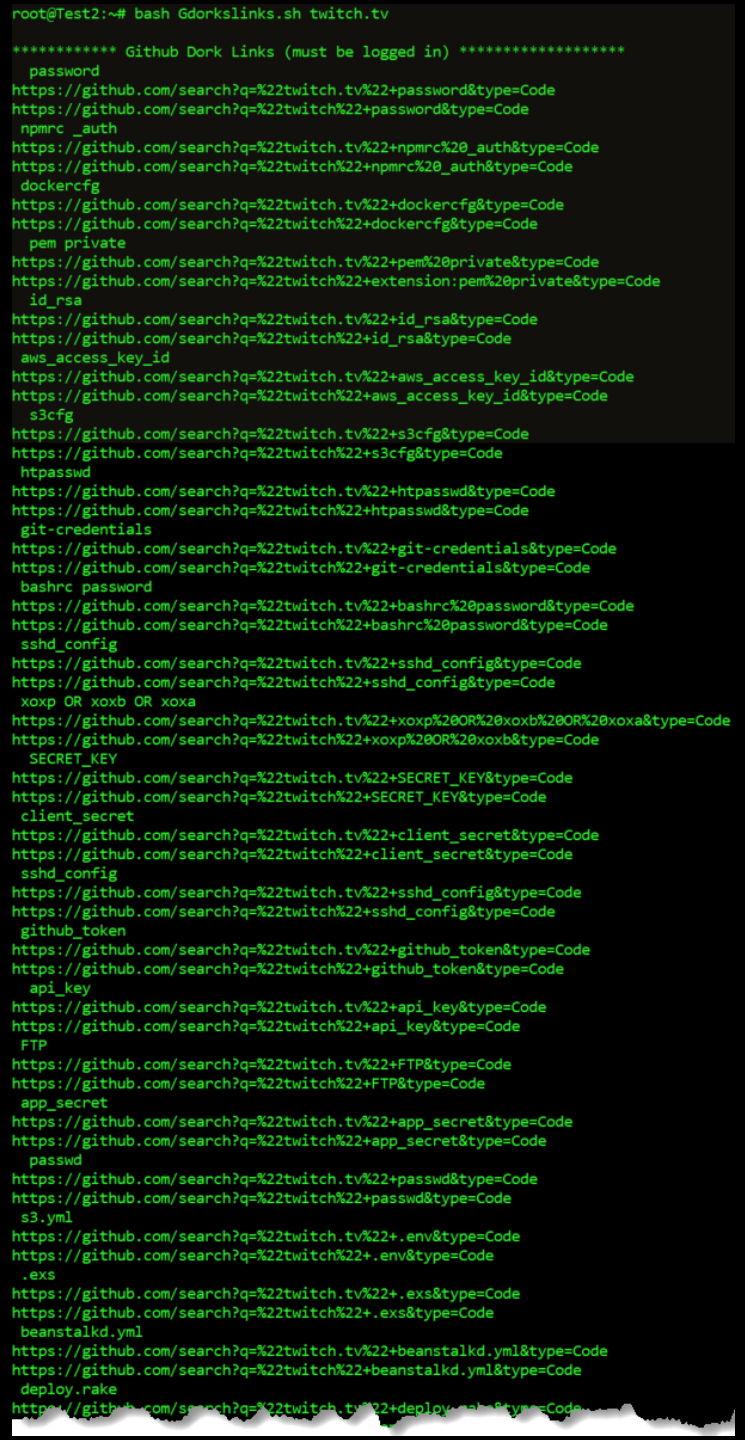
GITHUB ENUMERATION (Manually)

Many organizations quickly grow in their engineering teams. Sooner or later a new developer, intern, contractor, or other staff will leak source code online, usually through a public Github repo that they mistakenly thought they had set private.

Enjoy my github dork collection… They win… a lot.

*** Helps if your console supports clickable hyperlinks*

https://gist.github.com/jhaddix/1fb7ab2409ab579178d2a79959909b33



Github Recon (cont.)

The last list and script was designed to find sensitive source code, most often exposure of sensitive credentials (very common).

You can also learn a lot about:

- New hosts and TLDs
  - Be sure to keep a lookout for cloud storage (AWS and Azure)
    - amazonaws.com
- Host naming patterns
  - bender.company.com, fry.company.com, zoidberg.company.com, ...
- Technology stacks
  - DBMS type for injection
  - OSS components for CVE's

The repo mentioned earlier by Gwendal Le Coguic called "github- search" has some automated github tools as well.

Also check out @th3g3ntelman's full module on Github and Sensitive data Exposure.

SUBDOMAIN BRUTEFORCE

WHAT ARE WE AFTER?

Subdomain brute forcing will give us subdomains.

We will run it on all discovered apex domains.

Brute forcing for Subdomains

The other option to discover subdomains is brute force.

If we try and resolve thistotallydoesntexist.company.com we will *usually* not get a record. So, we can use a large list of common subdomain names and just try and resolve them analyzing if they succeed.

```
root@Test2:~# host thistotallydoesntexist.twitch.com
Host thistotallydoesntexist.twitch.com not found: 3(NXDOMAIN)
```

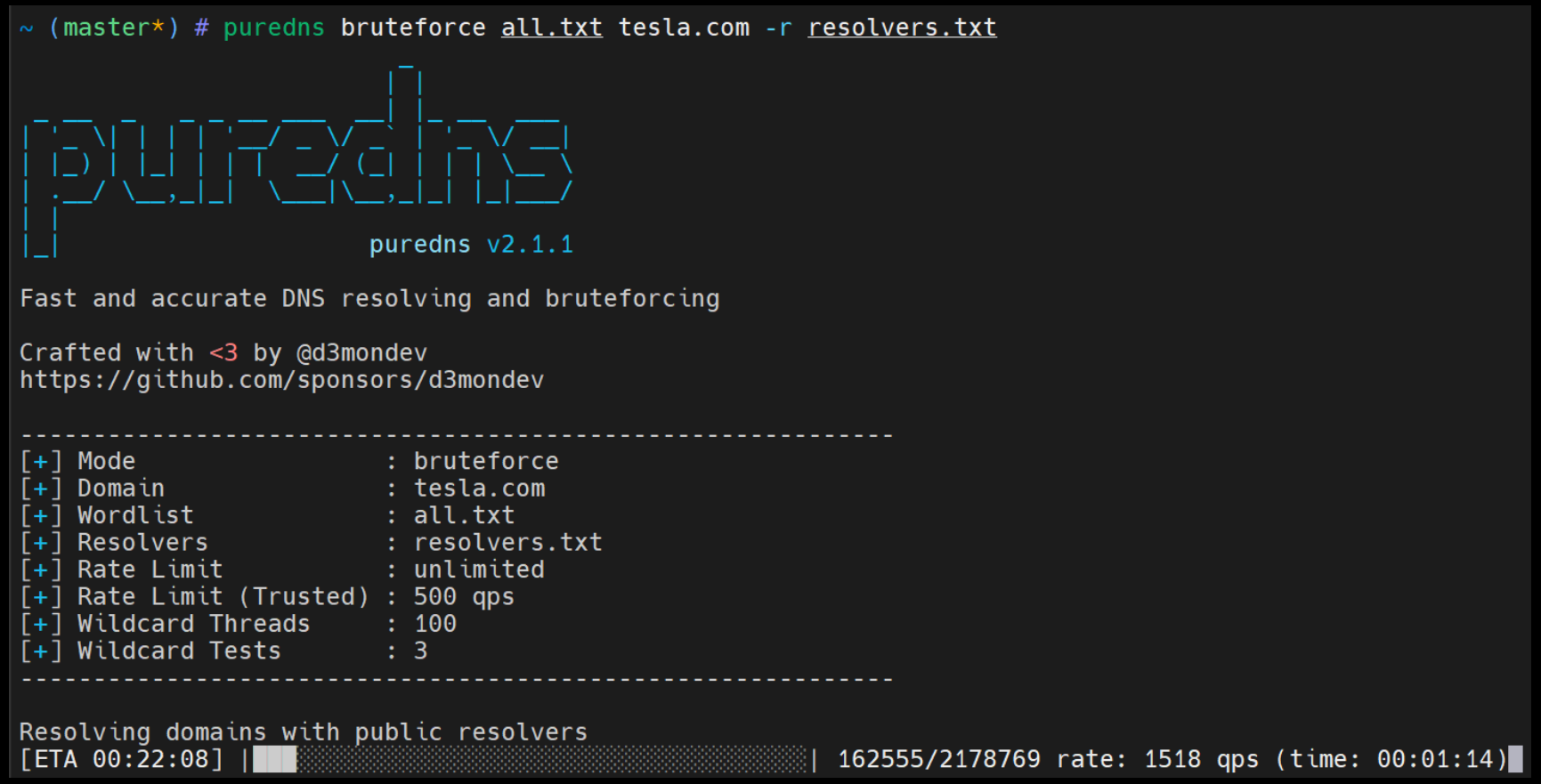
Brute forcing for Subdomains (Puredns)

The issue with brute forcing is that it's SLOW.

Some tools have come out that are both threaded and can use multiple DNS resolvers simultaneously. This speeds up this process significantly. massdns pioneered this idea.

While Amass does have a brute force module it is not optimal for this task.

I use Puredns by d3mondev. It is a wrapper and feature enhancer to massdns.



What about fresh, reliable DNS resolvers?

Resolvers Tweet

The most exhaustive list of reliable DNS resolvers

- resolvers.txt: A simple list of resolver IP addresses, which you can pass directly to your DNS enumeration tool.
- resolvers-extended.txt: All of the resolvers in `resolvers.txt` with additional information about each server, including the organization it belongs to, its country, and how many times it has been detected as valid. If a resolver is valid enough times, it may earn its place in the next file.
- resolvers-trusted.txt: A list of trusted resolvers from organizations like Cloudflare, Google, etc. We recommend you use this list to re-validate the results you get with the main resolvers.

https://github.com/trickest/resolvers

ALTERATION / PERMUTATION BRUTEFORCE

WHAT ARE WE AFTER?

This will give us even more esoteric subdomains.

Permutation / Alteration Scanning

When an admin names a subdomain, sometimes its' straightforward.

Other times... it's not.

While traditional subdomain bruteforce uses lists, it historically had no ability to find patterned naming of subdomains. The first tool to attempt to recognize these patterns and brute force for some of them was altdns written by Nathaniel Wakelam and Shubham Shah.

dev.company.com

dev1.company.com
dev2.company.com

dev-1.company.com
dev-2.company.com

dev.1.company.com
dev.2.company.com

Permutation / Alteration Scanning (with dnsgen)

Using tokenizing and pattern generation...

AKA magic

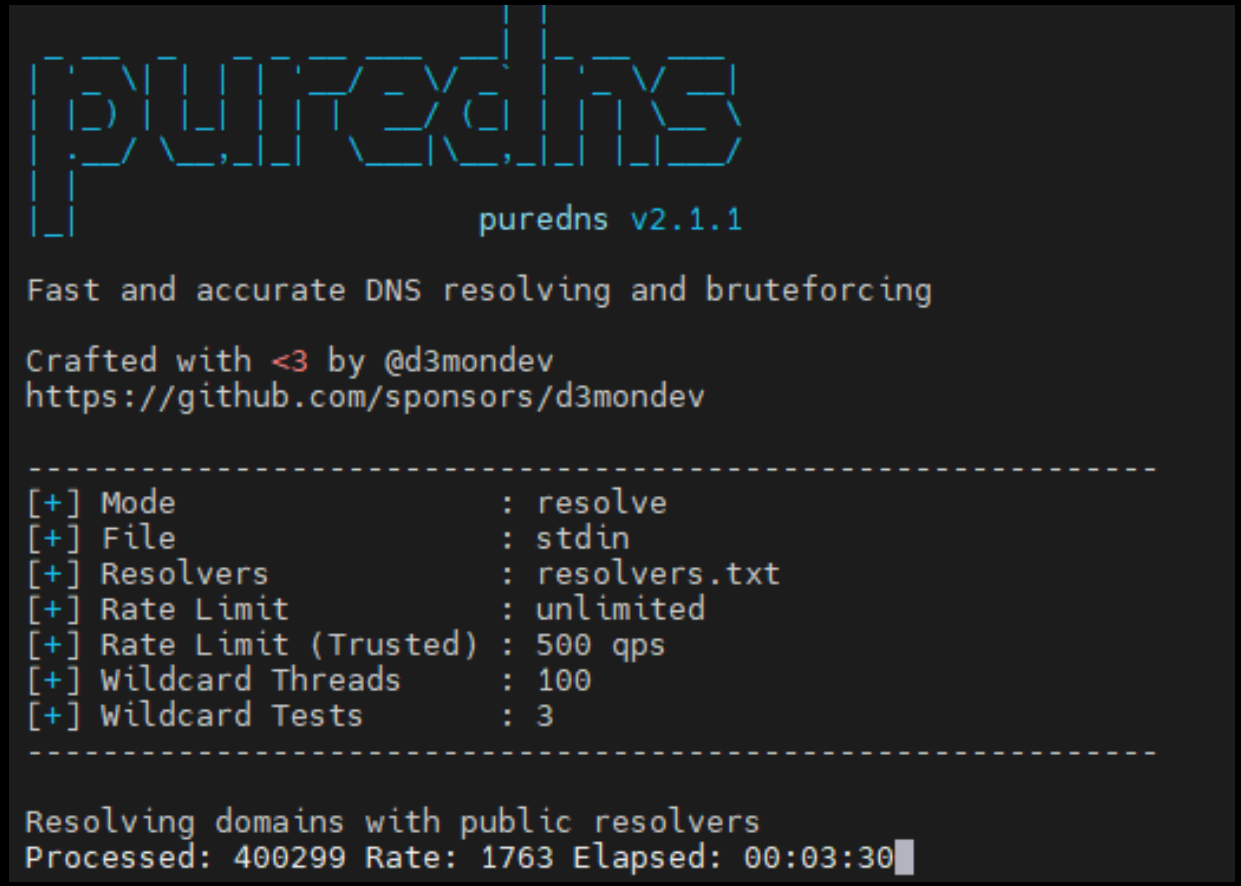
dnsgen builds lists of possible permutations / alterations of subdomains.

You feed it the results of amass, subfinder, bbot, etc.

It only generates these subdomain names, it does not resolve them. So, we use puredns with it.

Permutation / Alteration Scanning (with dnsgen)

cat <file_of_subdomains.txt> | dnsgen - | puredns resolve --resolvers resolvers.txt



SCREEN SHOTTING

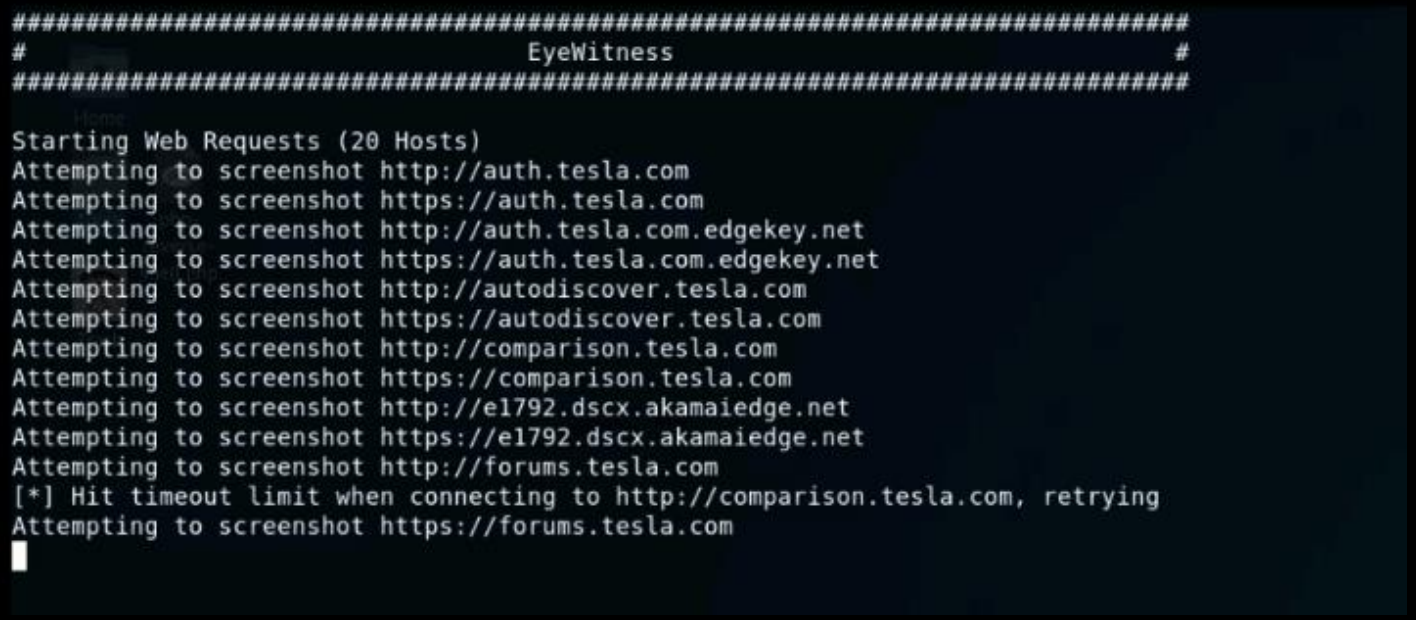
WHAT ARE WE AFTER?

This will give us a visual of all our gathered data.

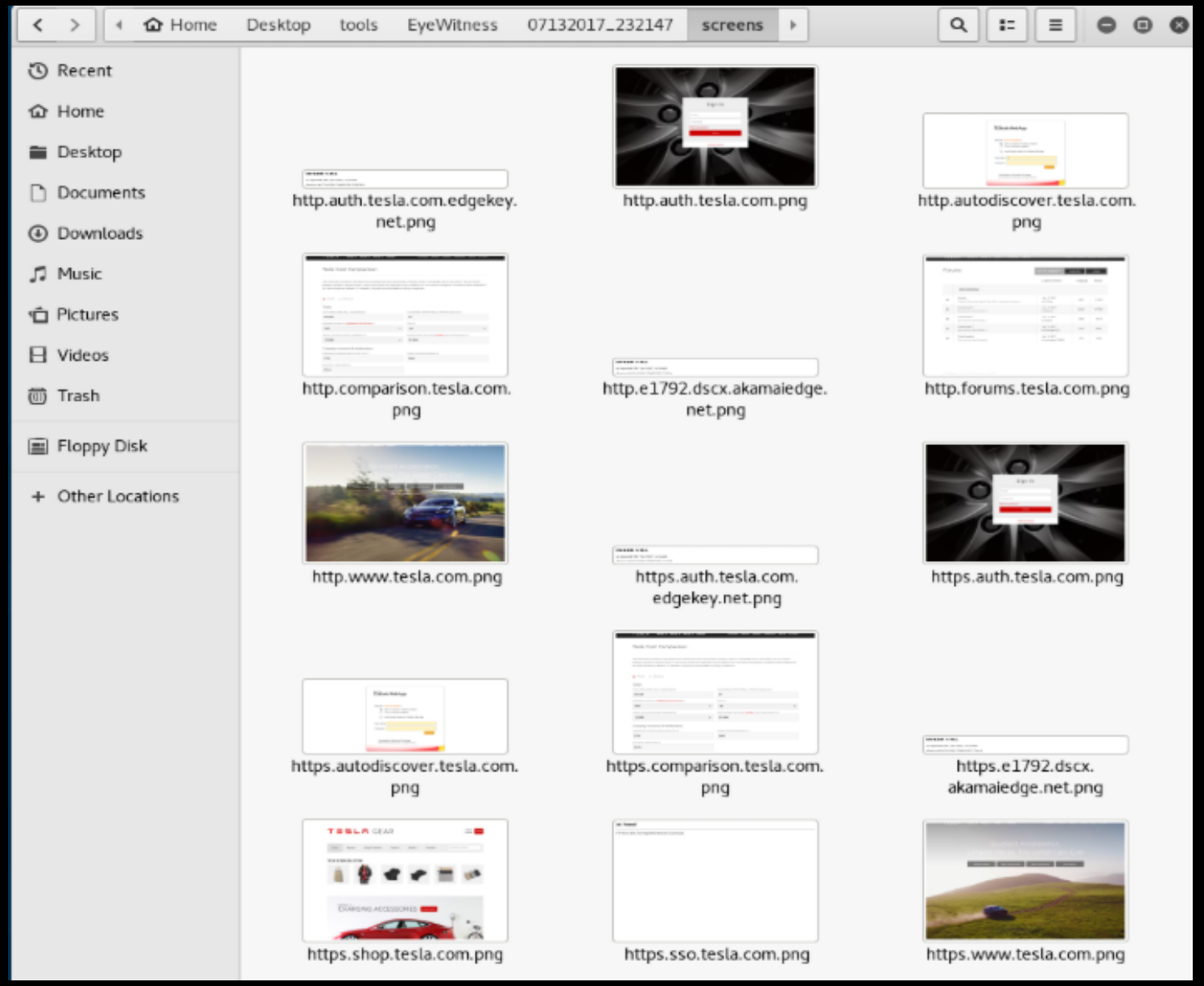
Screenshotting

At this point we have a lot of attack surface. We can feed possible sites to a tool and attempt to screenshot the results. This will allow us to "eyeball" things that might be interesting.

There are many tools for this. Aquatone is a wider recon framework that does this, HTTPscreenshot, and Eyewitness. I use Eyewitness because it will prepend both the http and https protocol for each domain we have observed. I'm not highly tied to this tool though, find one that works for you.



Screenshotting for Prioritization (cont.)



EDGE CASE RECON

Stuff to watch for (origin domains)

Content delivery networks (CDNs) are used to deliver website content/traffic more efficiently and to reduce heavy loads on servers.

When using a CDN, it is not a proxy for the real webserver. The real webserver is the origin.

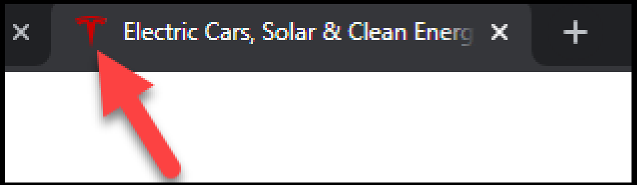
Many times, in security testing a CDN will block security testing payloads.

If you find the origin server, you do not get blocked.

Stuff to watch for (other)

- Logins
- Default content
- Bypass domains (dev,stage qa, ww1,ww2,)
- 302's
- Basic Auth
- Old looking frameworks
- Outdated Priv Pol / Trademark

Favicon Analysis (FavFreak)



What if you have a large scope and several hundred web servers to analyze?

What if screenshots aren't enough?

What if many of the roots of the webservers are black pages?

You can attempt to fingerprint COTS application by their favicon using favfreak.

```
levi@Asm0d3us-Hackb0x:~/Desktop/proc$ cat urls.txt | python3 favfreak.py -o output

- Coded with <3 by Devansh Batham

[ERR] Not Fetched 'http://accounts-[redacted]com'
[INFO]Fetched 'http://apiproxy-movi[redacted]
[ERR] Not Fetched 'http://abossmoni[redacted]
[ERR] Not Fetched 'https://apiproxy[redacted]
[ERR] Not Fetched 'https://android-[redacted]
[ERR] Not Fetched 'https://appcdn.[redacted]
[ERR] Not Fetched 'https://accounts[redacted].com'
[ERR] Not Fetched 'http://apiproxy.[redacted]
[INFO]Fetched 'https://credit-card.[redacted]
[INFO]Fetched 'https://apiproxy-mov[redacted]
```

```
[FingerPrint Based Detection Results] -

[spring-boot] 116323821 - count : 2
[big-IP] 878647854 - count : 2
[slack-instance] 99395752 - count : 1
```

RECON FRAMEWORKS

Recon Frameworks

Some people dislike deep recon. It comes with data management, tooling updates, environment upkeep, needs cmdline knowledge, etc.

For those of you that wish to get the results of great (not superb) recon, there exists several frameworks that automate some of the stuff we covered today.

I've tested many of these.

These are my current favorite free ones.

Also investigating OsmedeusNG

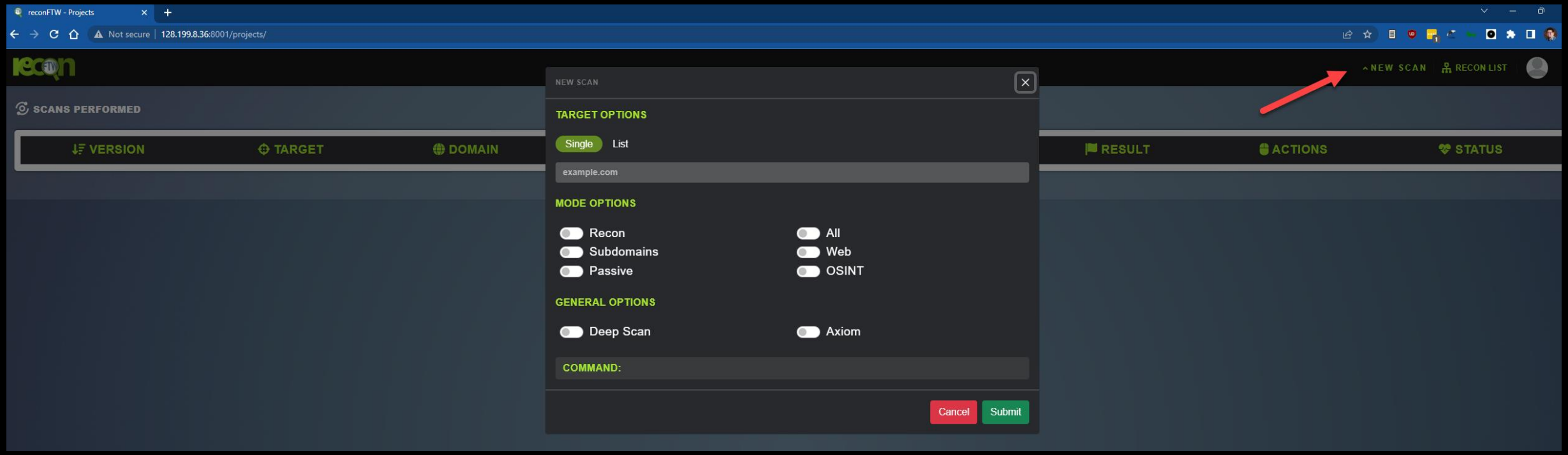
Frameworks (ReconFTW)

Arguably my most used and favorite.

- Web GUI – Yes (NEW)
- Passive scraping - Yes
- Brute force - Yes
- Permutations - Yes
- Certificate transparency - Yes
- Github source code scraping - Yes
- Analytics analysis - Yes
- Screenshotting - Yes
- De-duplication - Yes
- Port Scanning - Yes
- Introductory content discovery – Yes

[Full Blog on ReconFTW]

Frameworks (ReconFTW)



Frameworks (reNgine)

My 2nd favorite but many people's 1st choice atm.

- Web GUI - Yes
- Passive scraping - Yes
- Brute force - Yes
- Permutations - Yes
- Certificate transparency - Yes
- Github source code scraping - Yes
- Analytics analysis - Yes
- Screenshotting - Yes
- De-duplication - Yes
- Port Scanning - Yes
- Introductory content discovery - Yes