QOMPLX:CYBER

What you don't know can hurt

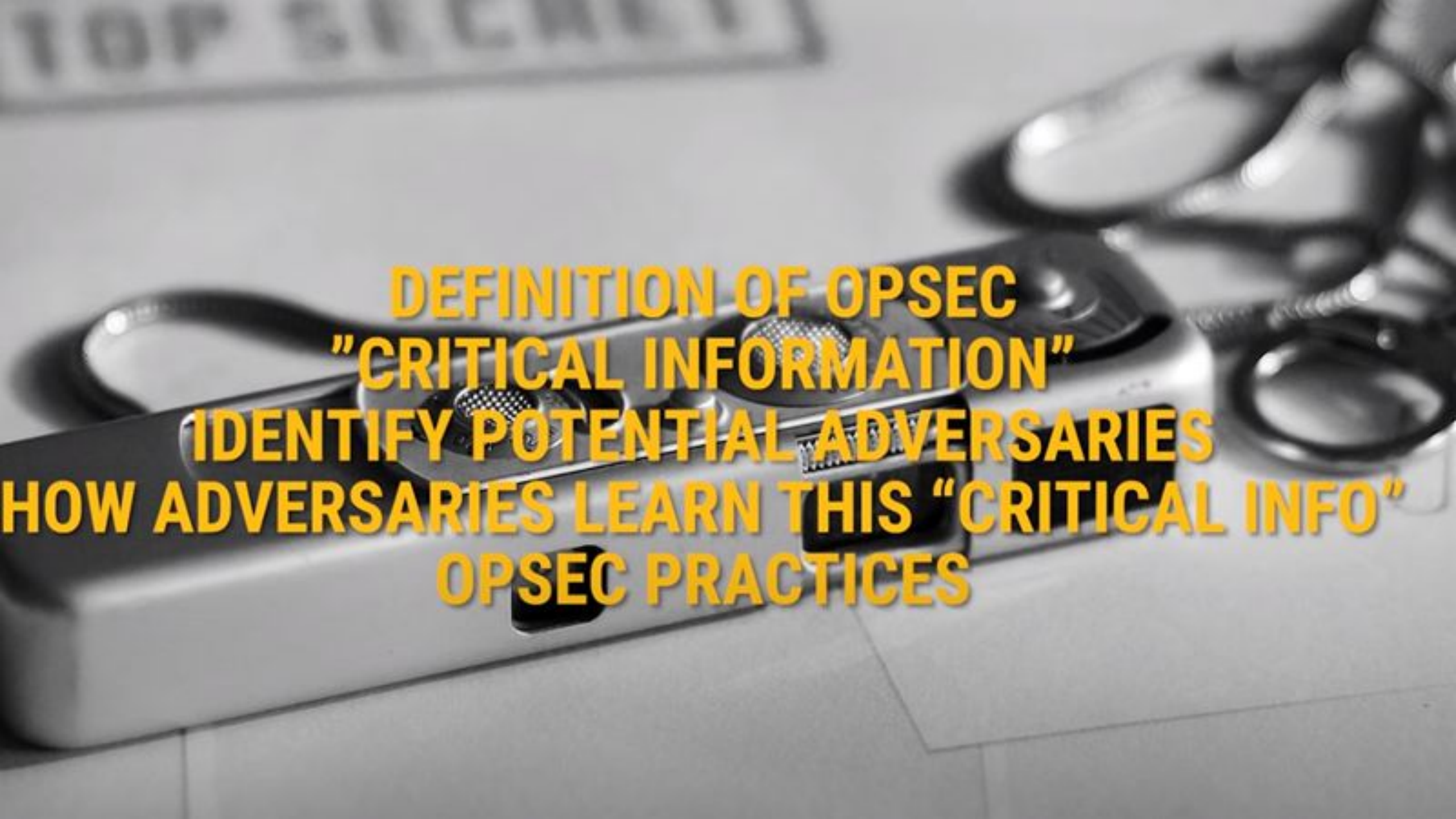
Archiving, social media and data breach for investigation

QOMPLX:CYBER

QOMPLX Intelligence Unit

QOMPLX:CYBER

OpSec for the Investigator


DEFINITION OF OPSEC
"CRITICAL INFORMATION"
IDENTIFY POTENTIAL ADVERSARIES
HOW ADVERSARIES LEARN THIS "CRITICAL INFO"
OPSEC PRACTICES

QOMPLX:CYBER

Archiving for Investigators

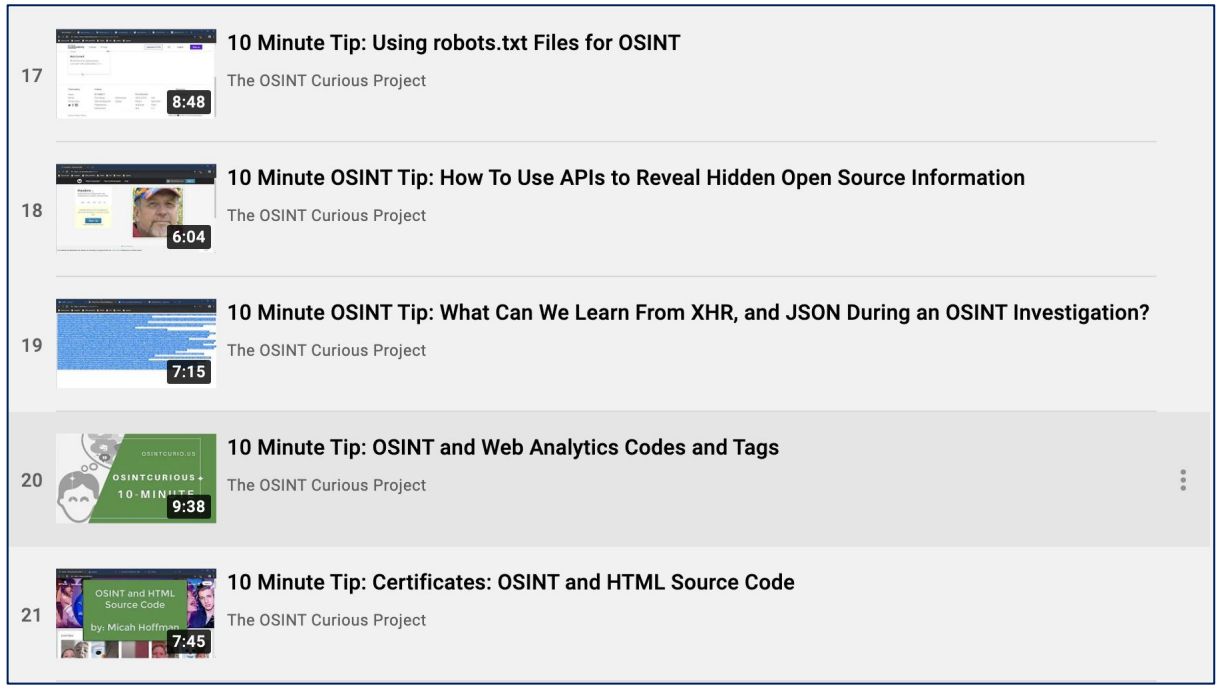
Beyond the Screenshot

Keith Turner
OSINT Specialist
QOMPLX Intelligence Unit
keith.turner@qomplx.com

Why Archive?

#OSINTCURIOUS
OSINTCURIO.US

YouTube - The OSINT Curious Project

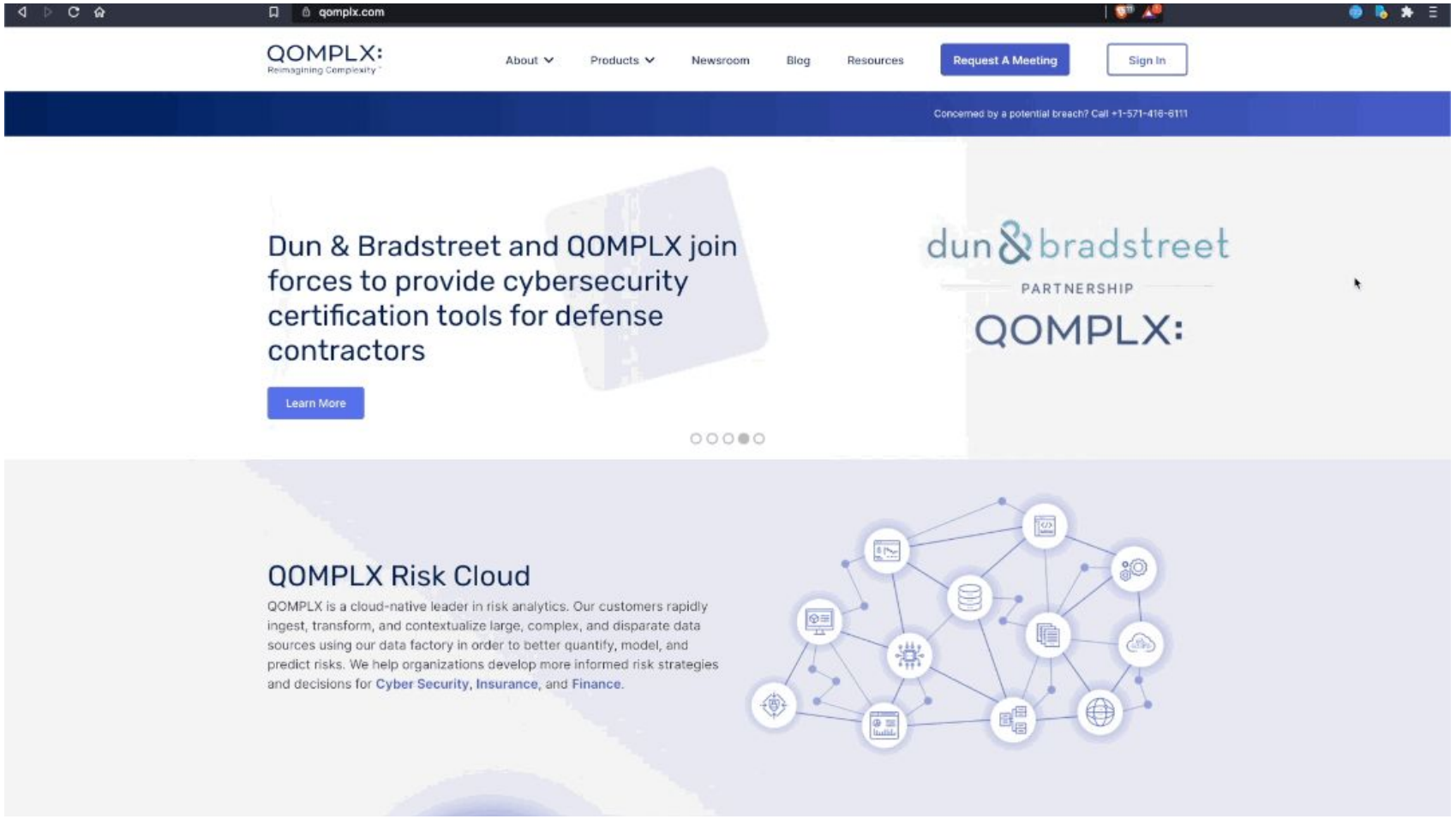


Browser Extensions

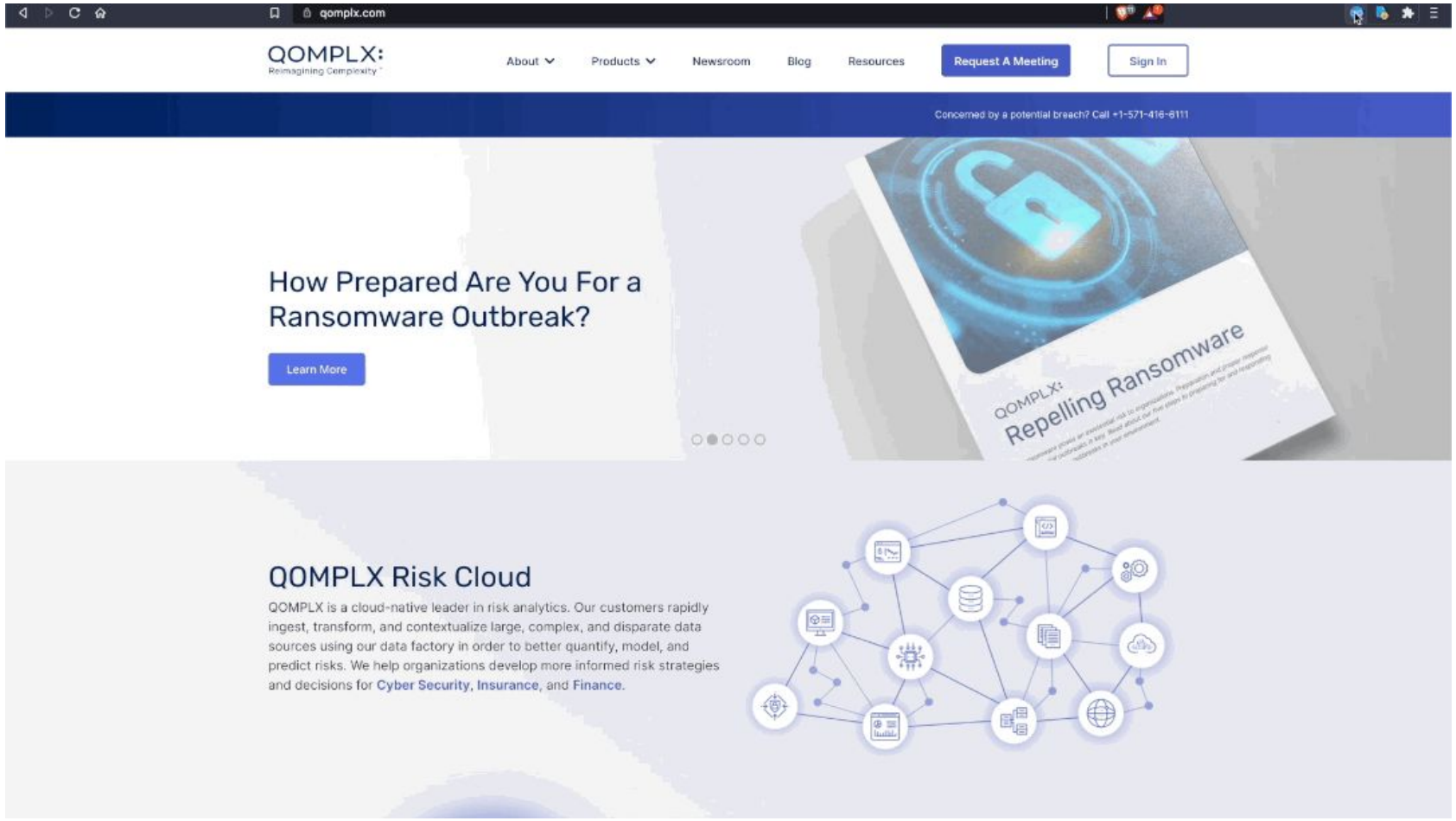
SingleFile

Webrecorder.net

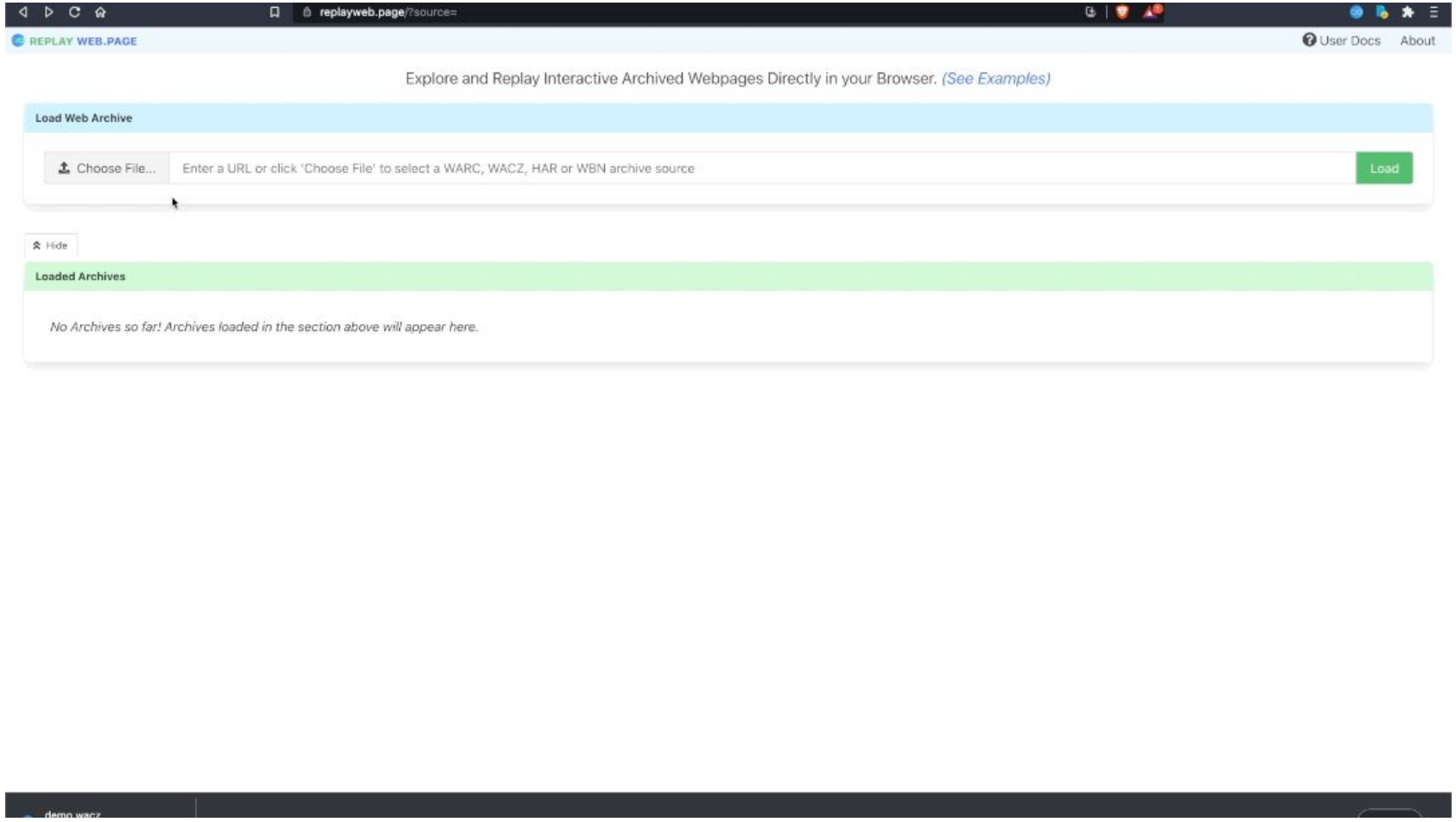
SingleFile


qomplx.com
QOMPLX:
Reimagining Complexity
About
Products
Newsroom
Blog
Resources
Request A Meeting
Sign In
Concerned by a potential breach? Call +1-571-416-6111
Dun & Bradstreet and QOMPLX join forces to provide cybersecurity certification tools for defense contractors
Learn More
dun & bradstreet
PARTNERSHIP
QOMPLX:
QOMPLX Risk Cloud
QOMPLX is a cloud-native leader in risk analytics. Our customers rapidly ingest, transform, and contextualize large, complex, and disparate data sources using our data factory in order to better quantify, model, and predict risks. We help organizations develop more informed risk strategies and decisions for Cyber Security, Insurance, and Finance.

WebRecorder Project - ArchiveWeb



WebRecorder Project – ReplayWeb



Online Archives

archive.today
webpage capture

https://archive.today

WayBack Machine

https://archive.org

Perma.cc ∞

https://perma.cc

ArchiveBox.io

Standalone Tools

https://hunch.ly

https://vortimo.com

https://calluna-software.com (NCollector)

https://httrack.com

Mobile Device Capture

https://hunch.ly

Online investigations. Now pocket sized.

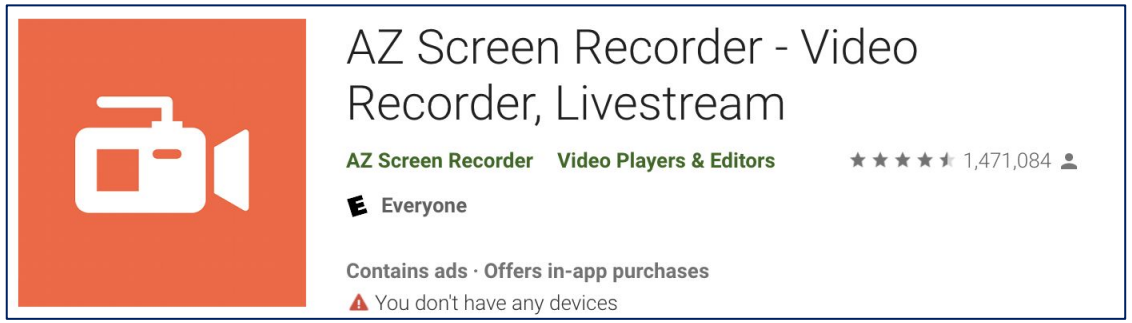
Digital evidence collection for investigators, witnesses, and victims

Hunchly Mobile is now available for free on iOS and Android

Download on the App Store | GET IT ON Google Play

GitHub SCNCPY

https://github.com/Genymobile/scncpy



Play Store - AZ Screen Recorder

QOMPLX:CYBER

Archiving for Investigators

Part 2 - ArkScrape Tool

Nate Johnson

Brief introduction...

Nate Johnson

AKA **Caprico**

OSINT Specialist
QOMPLX Intelligence Unit

@C4pr1c0

Archiving Tool for the Investigator

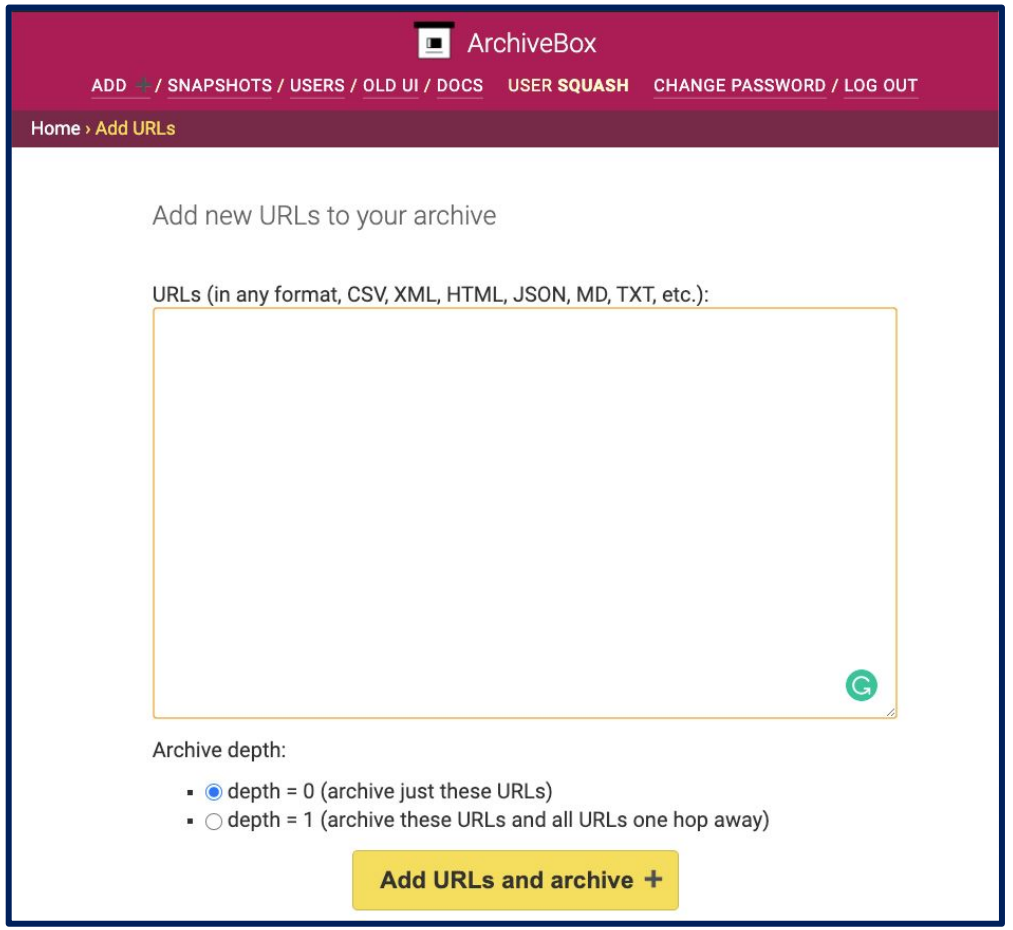
Brief introduction...

- Continuation of Archiving Data
- Shodan
- Archive Case Management tool

Archiving Tool for the Investigator

Archiving websites (ArchiveBox)

- Keith talked through using this
- Use a url to archive it
  - etc.
- How do we organize this?

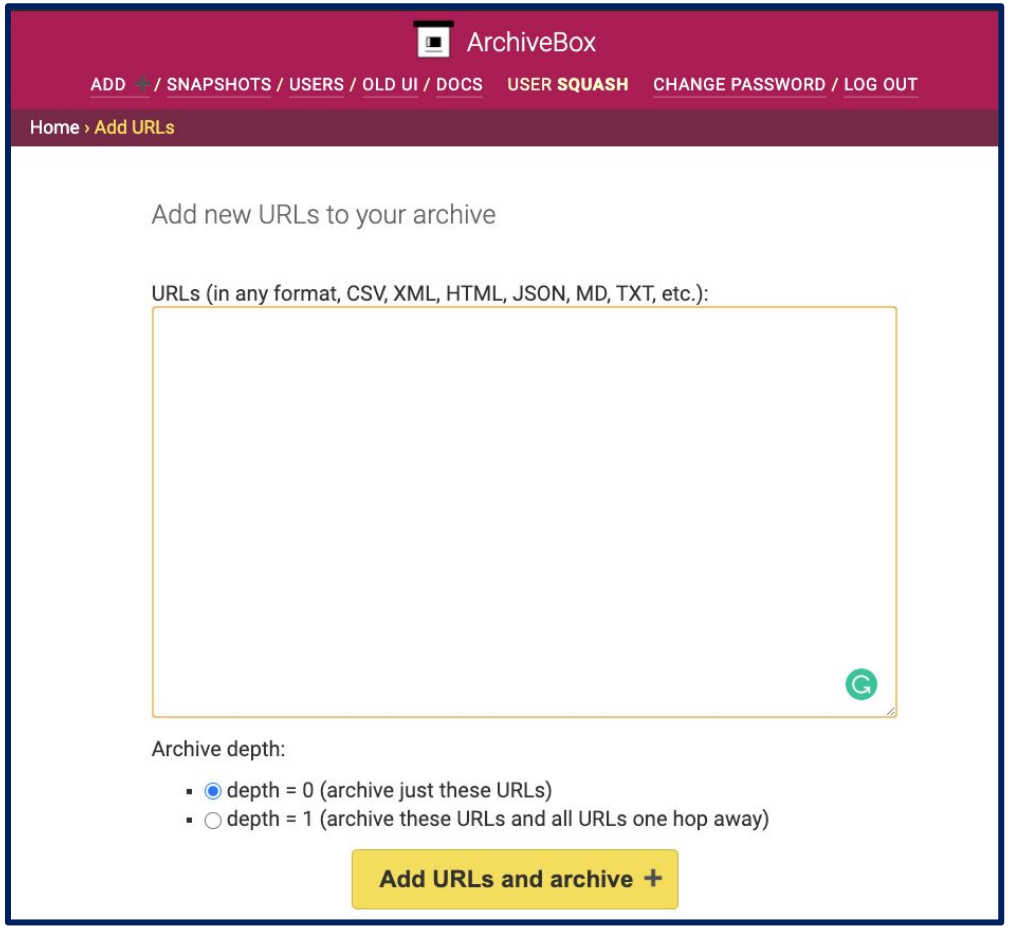


Archiving Tool for the Investigator

Archiving websites (ArchiveBox)

- If you have a single server there is the possibility of cross contamination of data
  - URL 1 has nothing to do with Investigation 2

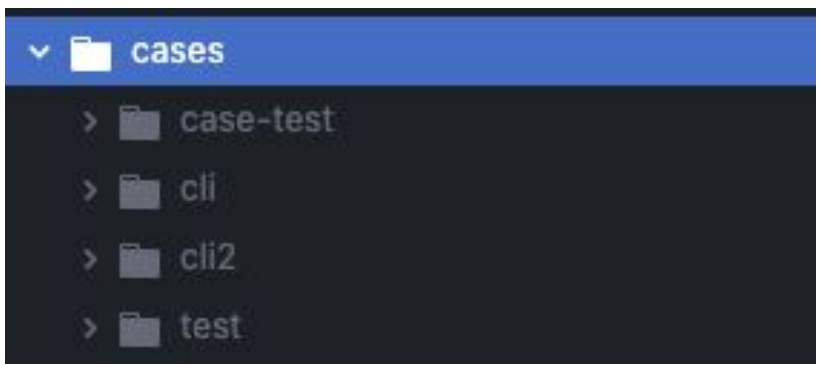
How do you fix that?



Archiving Tool for the Investigator

Archiving websites (ArchiveBox)

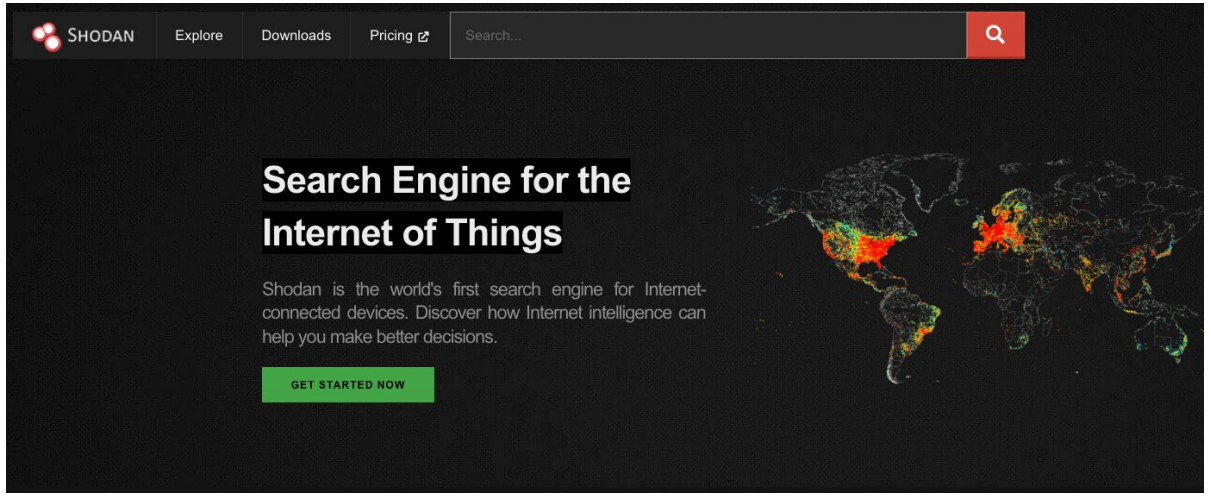
- Scripting (Python 3)
- Separate Archive Databases Into different Cases
- Let’s you run databases per operations



Archiving Tool for the Investigator

Archiving Infrastructure (shodan)

- Internet Scanning Tool
  - Price
    - Account ($)
    - Subscription ($-$$$$)
- Archive
  - Location Data
  - How long the site has been up.
  - Who is hosting it.



Archiving Tool for the Investigator

Using our tool

Usage

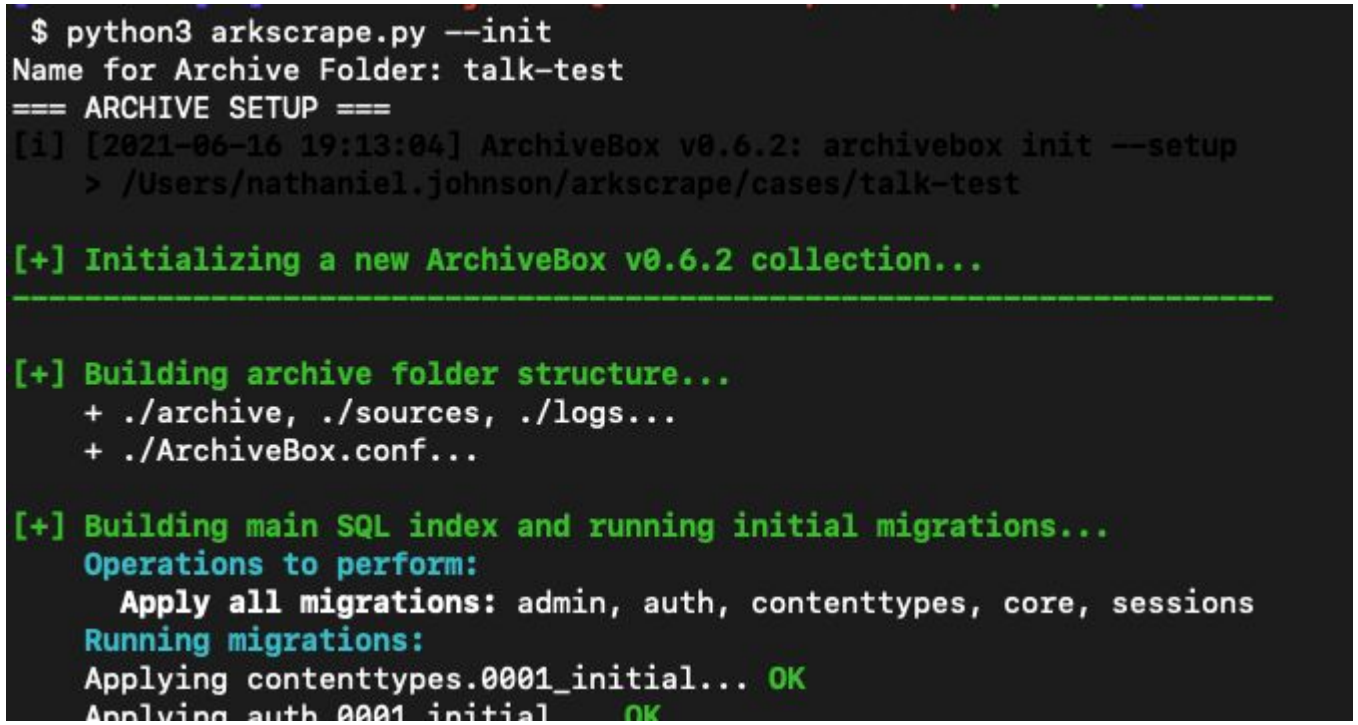
```
usage: arkscrape.py [-h] [--init] [--shodan SHODAN] [--server SERVER] [--domain DOMAIN]
                    [--scrape SCRAPE]

Archive websites, Shodan scan results, and webscraper per a domain

optional arguments:
  -h, --help       show this help message and exit
  --init           First run setup
  --shodan SHODAN  Shodan check: --shodan <archive folder>
  --server SERVER  Archive box server start: --server <archive folder>
  --domain DOMAIN  Target domain
  --scrape SCRAPE  Scrape Urls from a list: --scrape <archive folder>
```

Archiving Tool for the Investigator

Using our tool



Archiving Tool for the Investigator

Using our tool

```
 $ python3 arkscrape.py --server talk-test
=== Starting Server ===
[i] [2021-06-16 19:37:10] ArchiveBox v0.6.2: archivebox server
    > /Users/nathaniel.johnson/arkscrape/cases/talk-test

[+] Starting ArchiveBox webserver...
    > Logging errors to ./logs/errors.log
Performing system checks...

System check identified no issues (0 silenced).
June 16, 2021 - 19:37:11
Django version 3.1.8, using settings 'core.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
```

Archiving Tool for the Investigator

Using our tool

```
 $ python3 arkscrape.py --shodan talk-test --domain qomplx.com
Search query:                    domain qomplx.com
Total number of results:         0
Query credits left:              9920
Output file:                     2021_6_16-export.json.gz
  [########################################]  100%
Saved 0 results into file 2021_6_16-export.json.gz
```

Archiving Tool for the Investigator

Using our tool

```
 $ python3 arkscrape.py --shodan talk-test --domain qomplx.com
Search query:                    domain qomplx.com
Total number of results:         0
Query credits left:              9920
Output file:                     2021_6_16-export.json.gz
  [########################################]  100%
Saved 0 results into file 2021_6_16-export.json.gz
```

Archiving Tool for the Investigator

Using our tool

```
 $ shodan parse --fields ip_str,location.longitude,location.latitude cases/talk-test/shodan/2021_6_18-export.json.gz
121.178.254.145 126.39181       34.81282
216.107.134.6   -97.51643       35.46756
91.201.107.99   30.5238 50.45466
92.118.108.175  28.8575 47.00556
145.239.62.168  2.12807 50.98651
77.223.131.231  27.13838        38.41273
52.33.125.148   -119.70058      45.83986
172.105.59.29   72.88261        19.07283
45.166.51.71    -34.88111       -8.05389
106.14.226.189  114.0683        22.54554
113.43.133.106  139.69171       35.6895
78.46.162.158   7.77746 48.21884
185.225.1.45    -3.70256        40.4165
```

Archiving Tool for the Investigator

Conclusion

- You can find the tool within the leaflet for this presentation
- Feel free to contact me on twitter if you have any questions or suggestions.

QOMPLX:CYBER

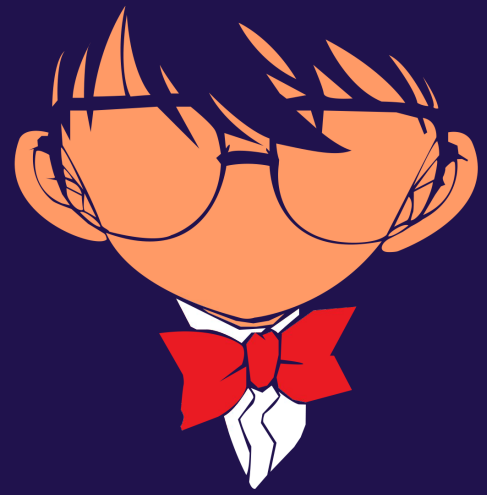
Where The kids Hangout

Salah

OSINT Specialist

QOMPLX Intelligence Unit

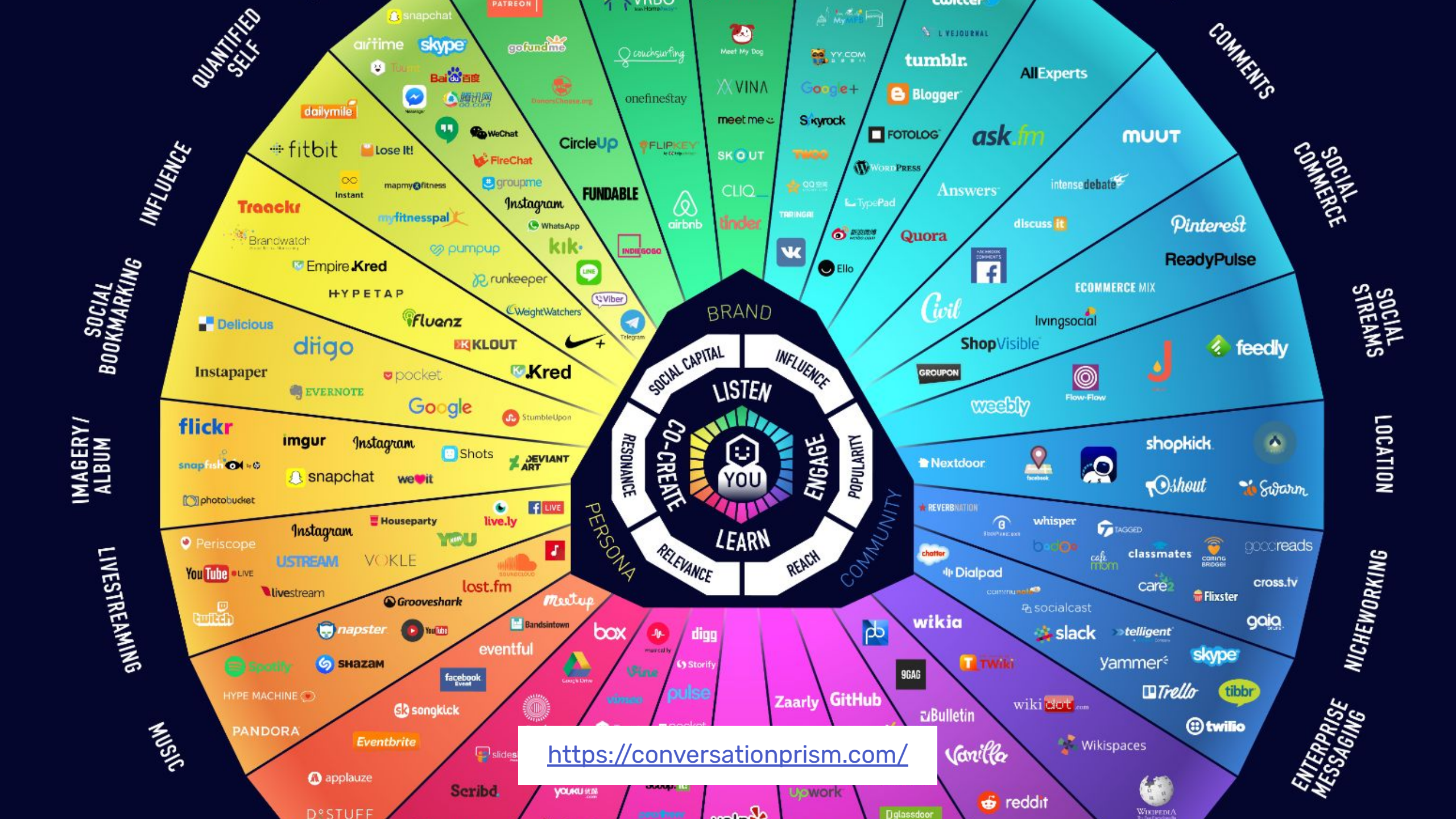
@Salaheldinaz



Social Media 🤔

Interactive technologies that allow the creation or sharing/exchange of information, ideas, career interests, and other forms of expression via virtual communities and networks.

- https://en.wikipedia.org/wiki/Social_media


QUANTIFIED SELF
INFLUENCE
SOCIAL BOOKMARKING
IMAGERY / ALBUM
LIVESTREAMING
MUSIC
COMMENTS
SOCIAL COMMERCE
SOCIAL STREAMS
LOCATION
NICHEWORKING
ENTERPRISE MESSAGING
BRAND
SOCIAL CAPITAL
INFLUENCE
LISTEN
ENGAGE
POPULARITY
CO-CREATE
RESONANCE
PERSONA
LEARN
RELEVANCE
REACH
COMMUNITY
YOU
https://conversationprism.com/

1 What Are They Looking For?

What Are They Looking For?

 Access to basic needs

 Sense of security

 Love and support

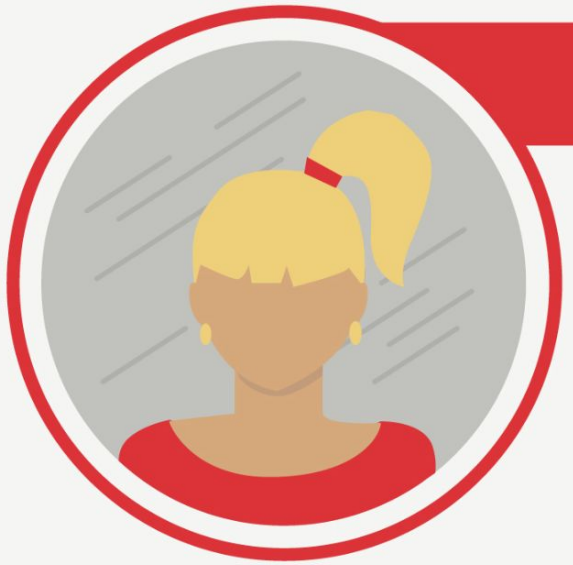
 Fun and play

 Education

Understand Generations

Name	Births Start	Births Ends	Youngest Age Today	Oldest Age Today
Gen Next (Millennials)	1980	1995	26	41
Gen Z	1996	2010	11	25
Gen Alpha	2011	2025	1	10

Understand Generations



Gen Z

Birth Years: 1996 to 2012/15

Current Age: 6 to 24

Size: 68 million

Media Consumption: The average Gen Zer received their first mobile phone at age 10.3 years. Many of them grew up playing with their parents' mobile phones or tablets. They have grown up in a hyper-connected world and the smartphone is their preferred method of communication. On average, they spend 3 hours a day on their mobile device.

Shaping Events: Smartphones, social media, never knowing a country not at war, and seeing the financial struggles of their parents (Gen X).

Finances: Similar to Gen X (their parents) in financial attitudes, but wanting to avoid debt after seeing Millennials struggle.

KASASA

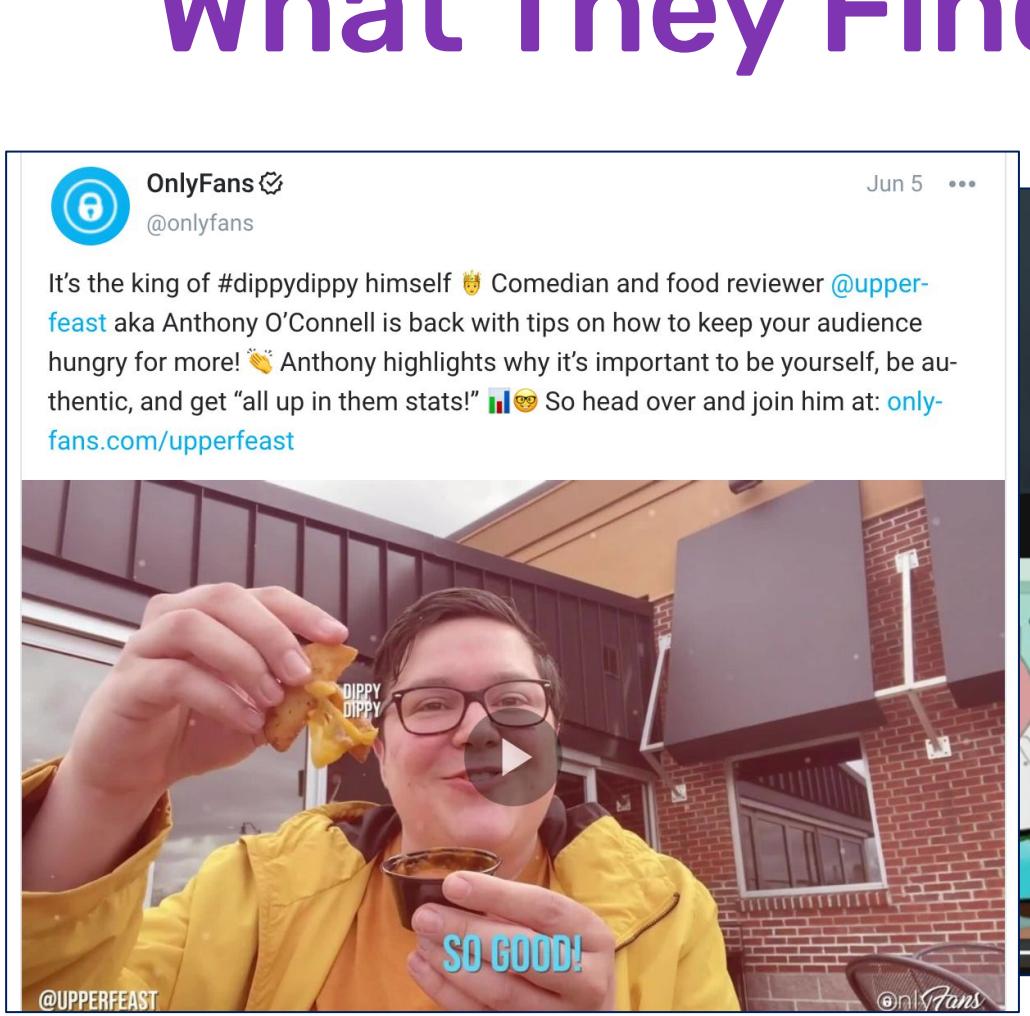
https://www.kasasa.com/articles/generations/gen-x-gen-y-gen-z

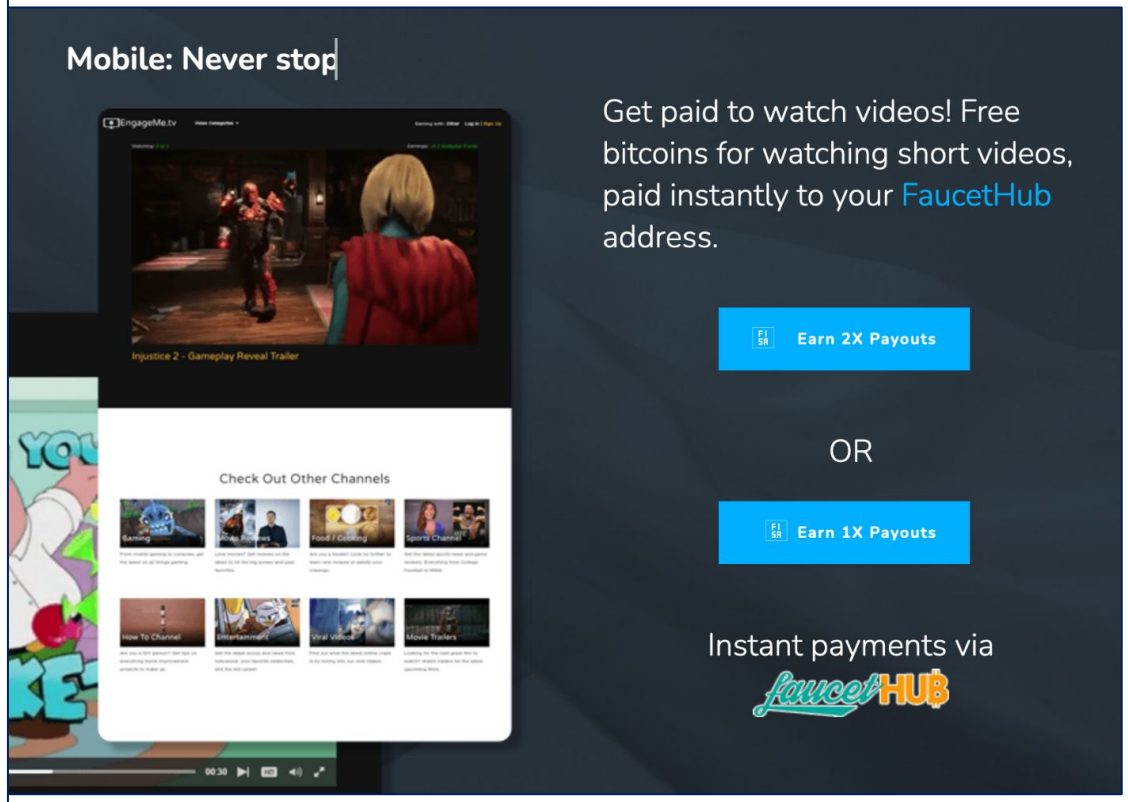
Understand Generations

https://www.verywellfamily.com/a-teen-slang-dictionary-2610994

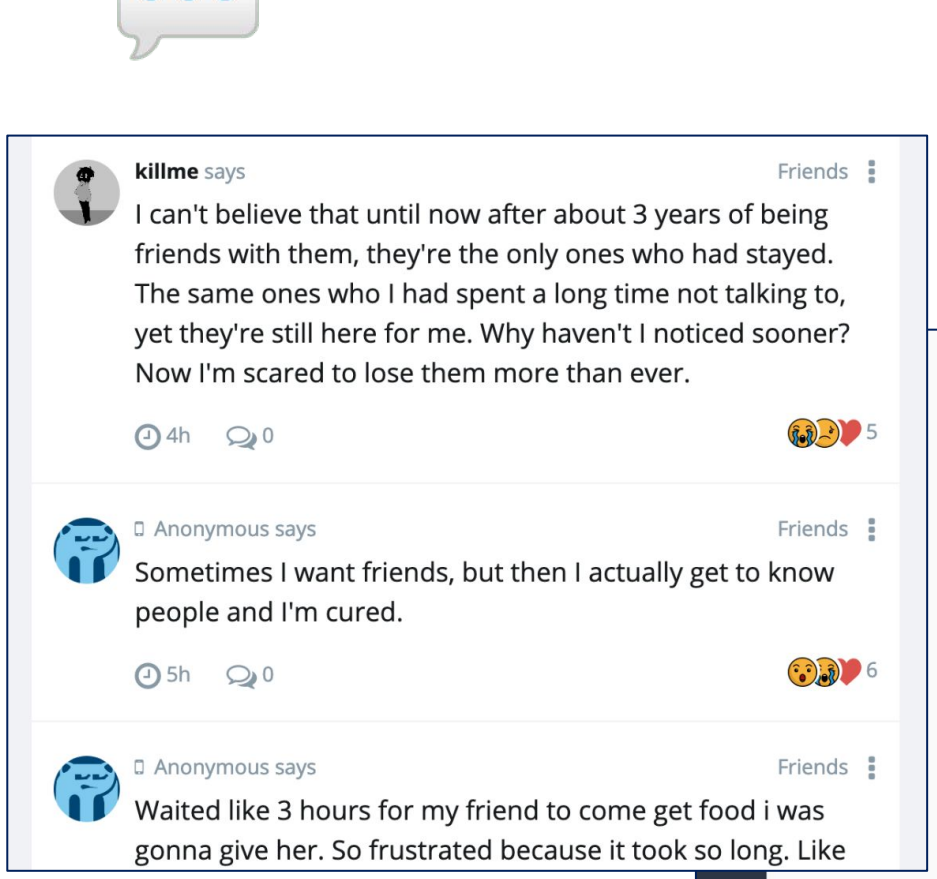
2 What They Finding Online !

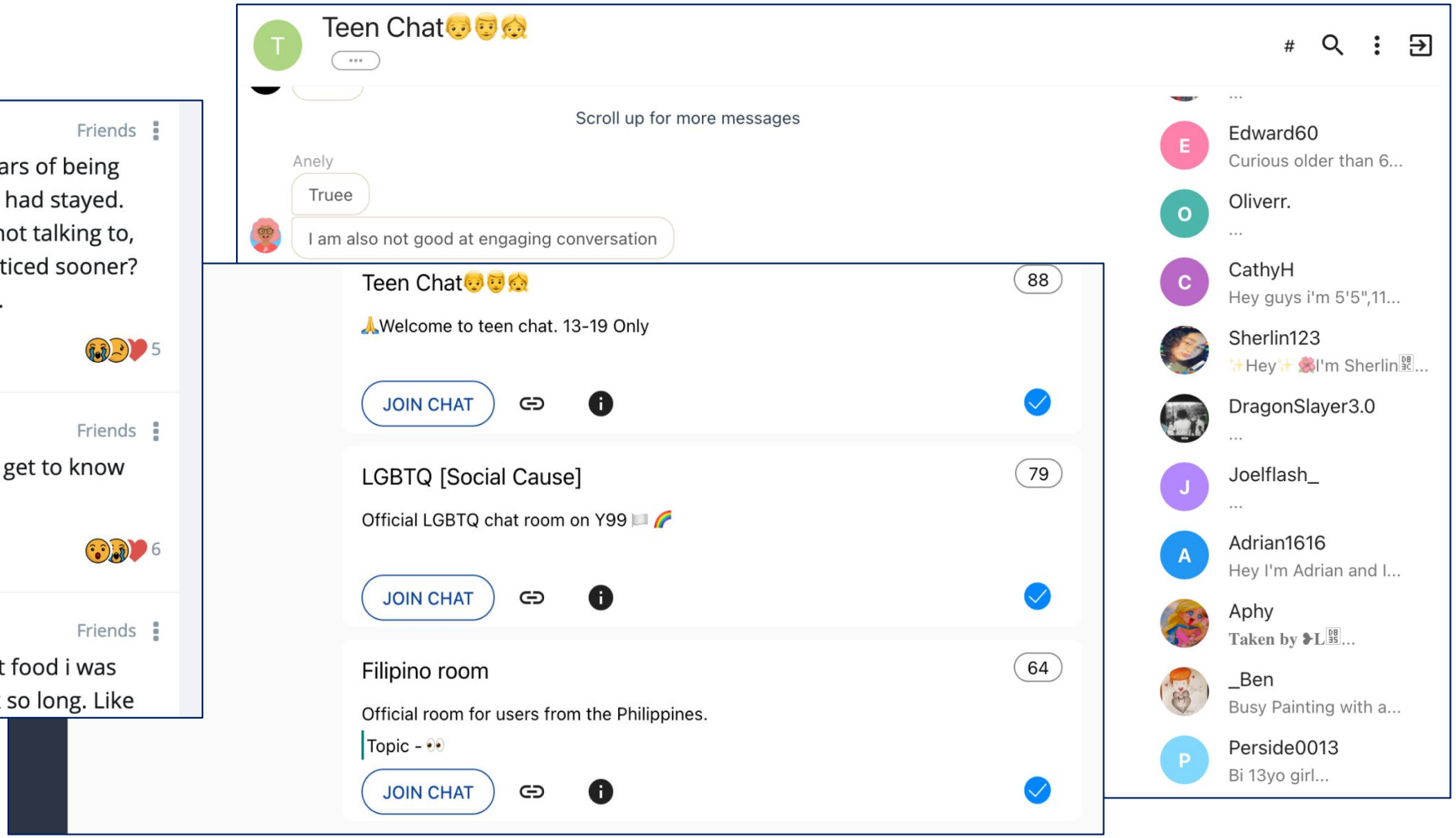
What They Finding Online !



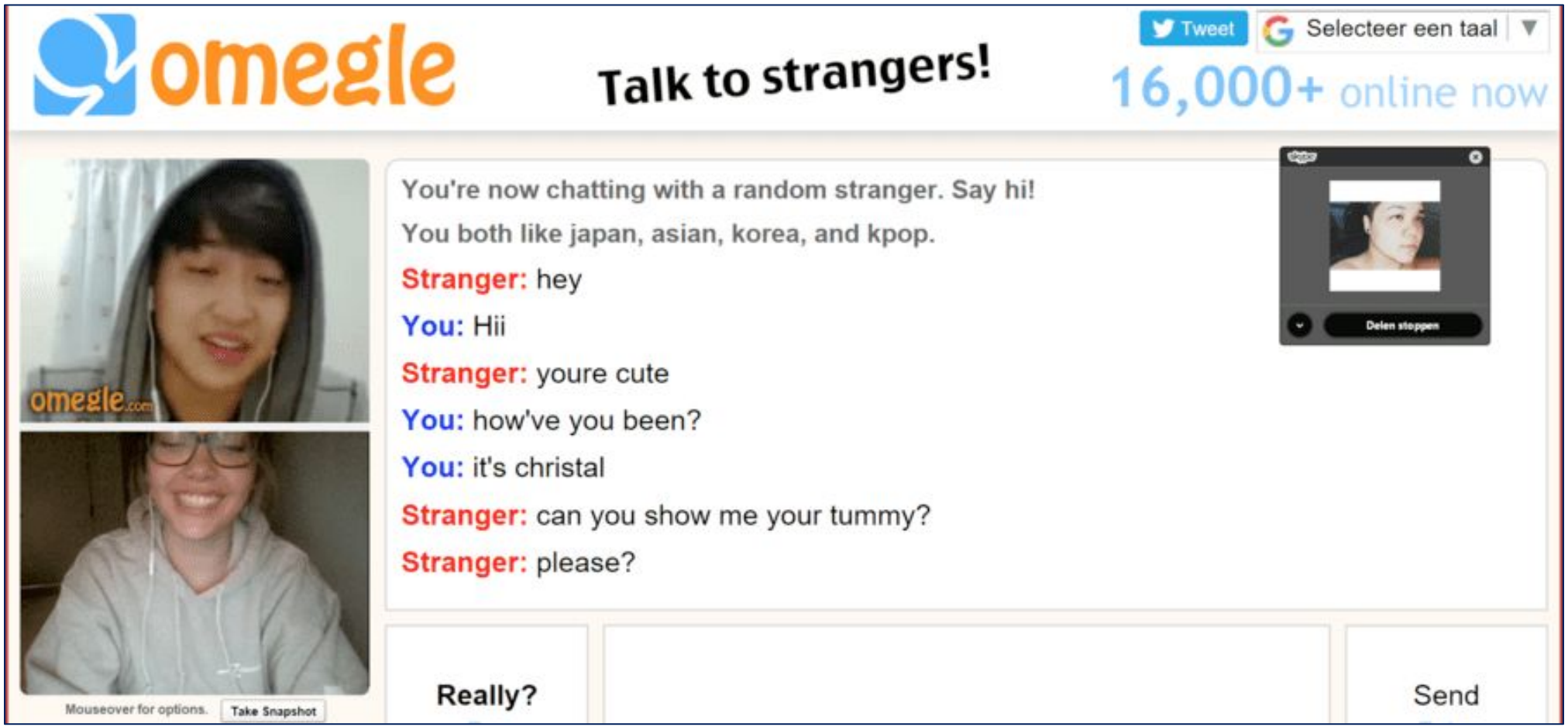


What They Finding Online !





What They Finding Online !



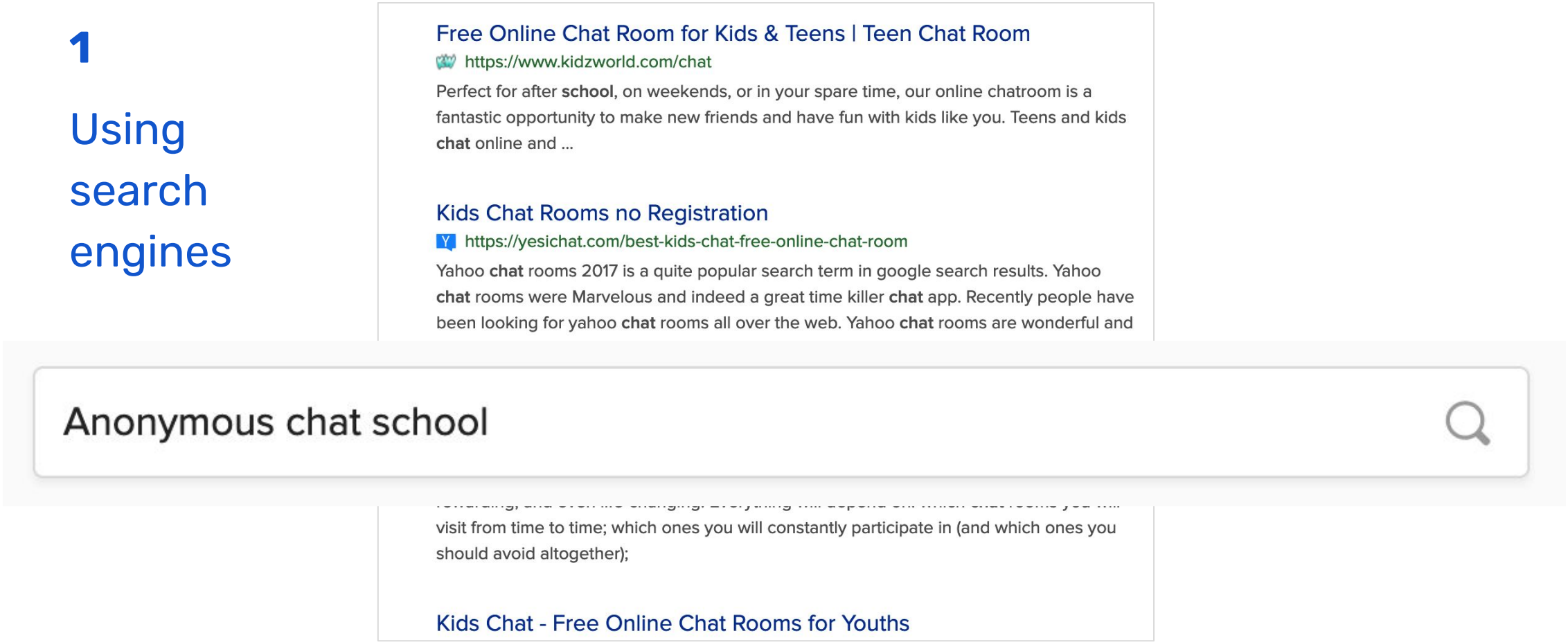
What They Finding Online !

3 Finding The Unknown

Finding The Unknown

1

Using search engines



Finding The Unknown

2 Lists, Collections

https://www.ovrdrv.com/knowledge/social-media-map/

Finding The Unknown

3 Mobile Apps Stores

Apple

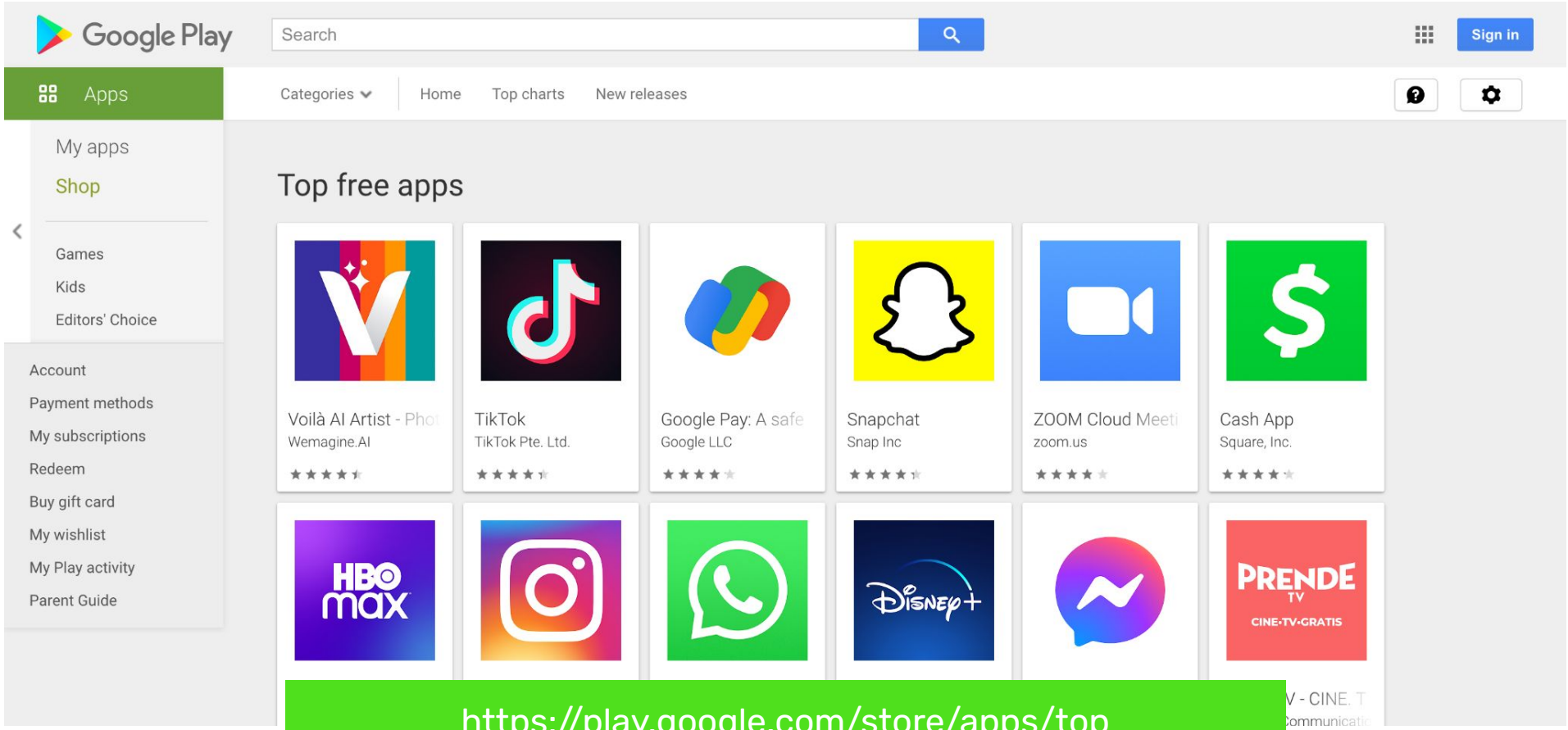
Google

Huawei

Amazon

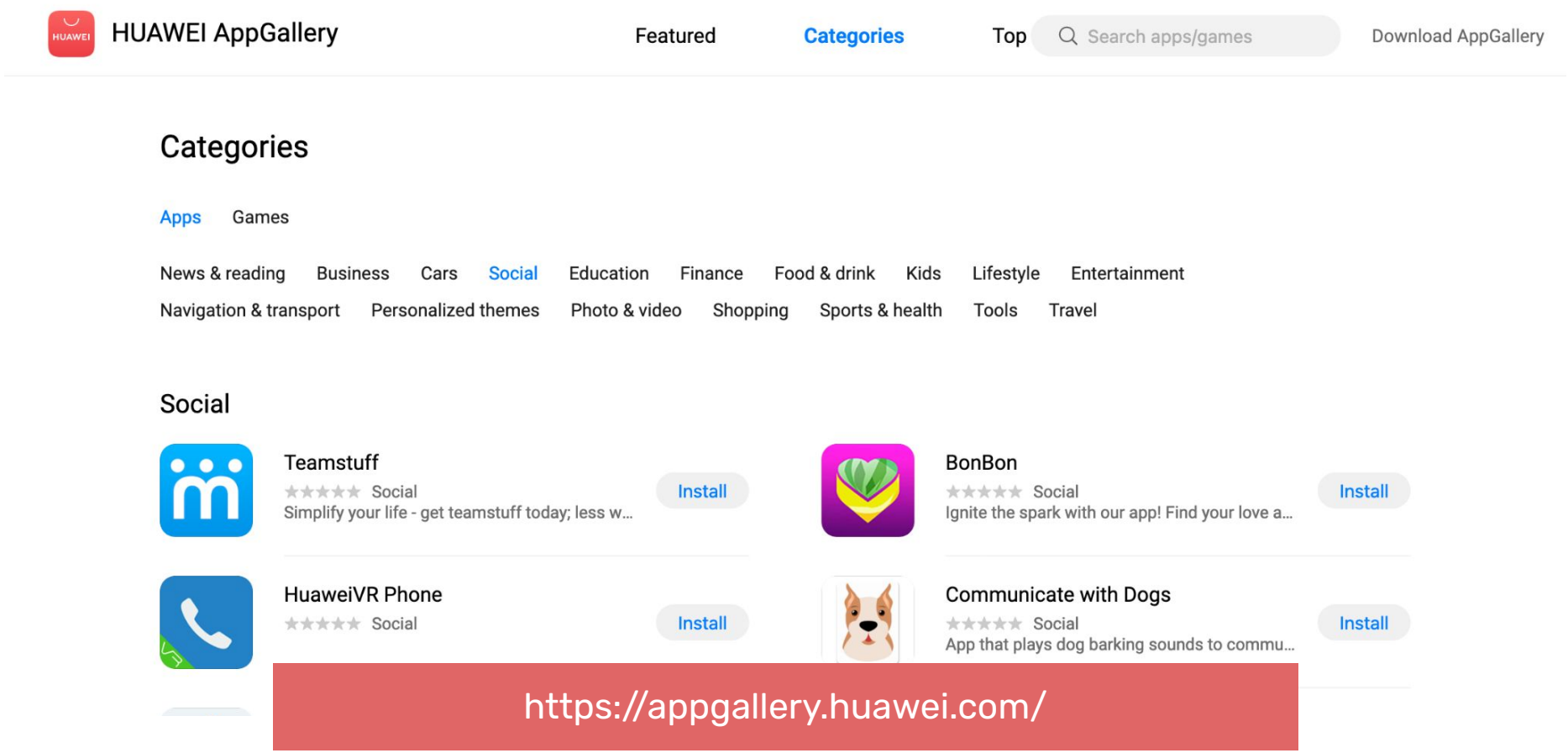
Microsoft

Finding The Unknown

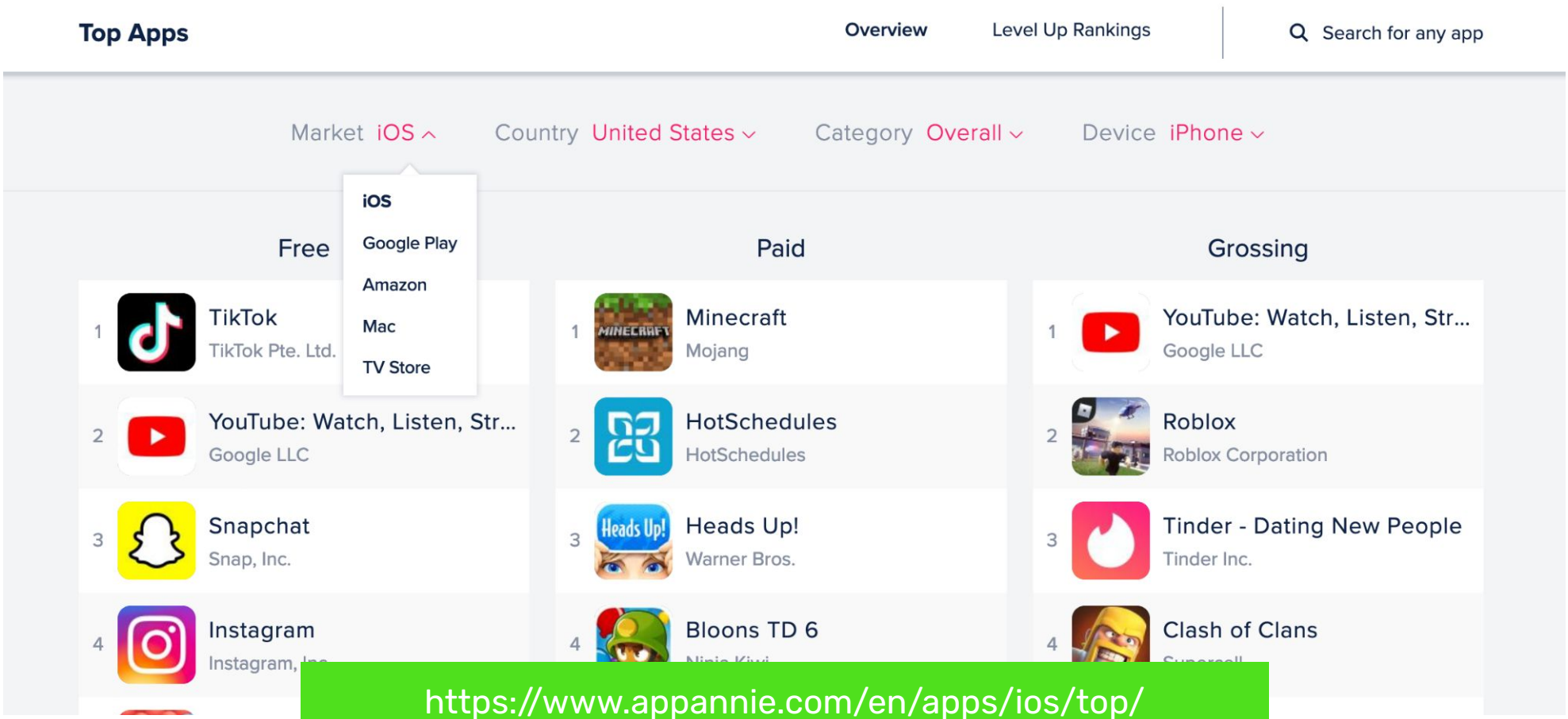


https://play.google.com/store/apps/top

Finding The Unknown

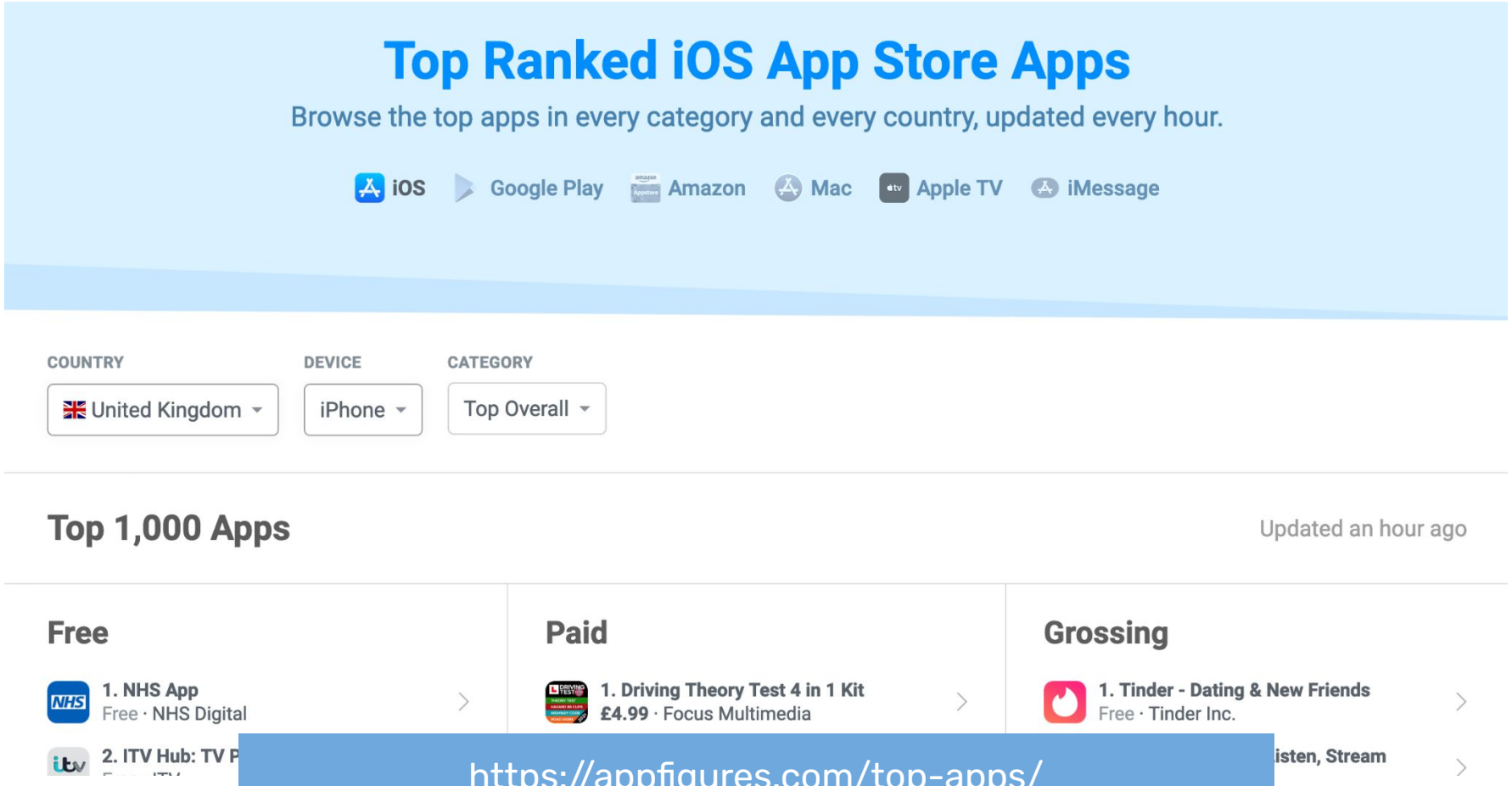


Finding The Unknown



https://www.appannie.com/en/apps/ios/top/

Finding The Unknown

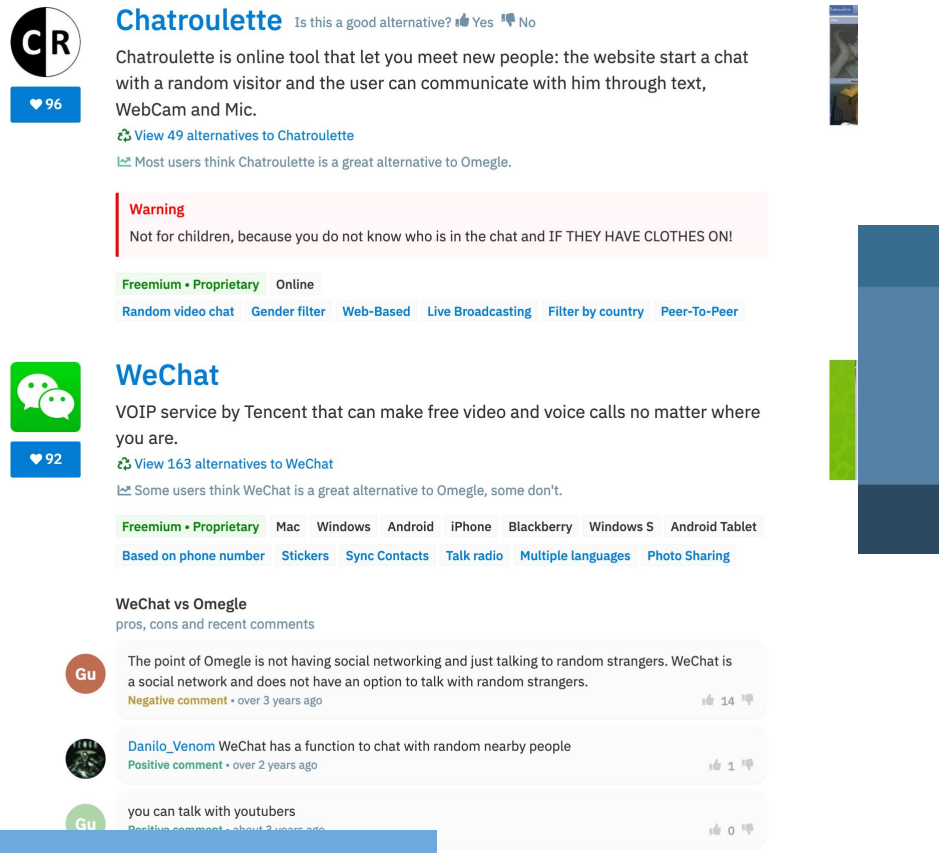


https://appfigures.com/top-apps/

Where The kids Hangout

Finding The Unknown

4 Apps Comparisons/Reviews



https://alternativeto.net/

Finding The Unknown

5

Games

Platforms

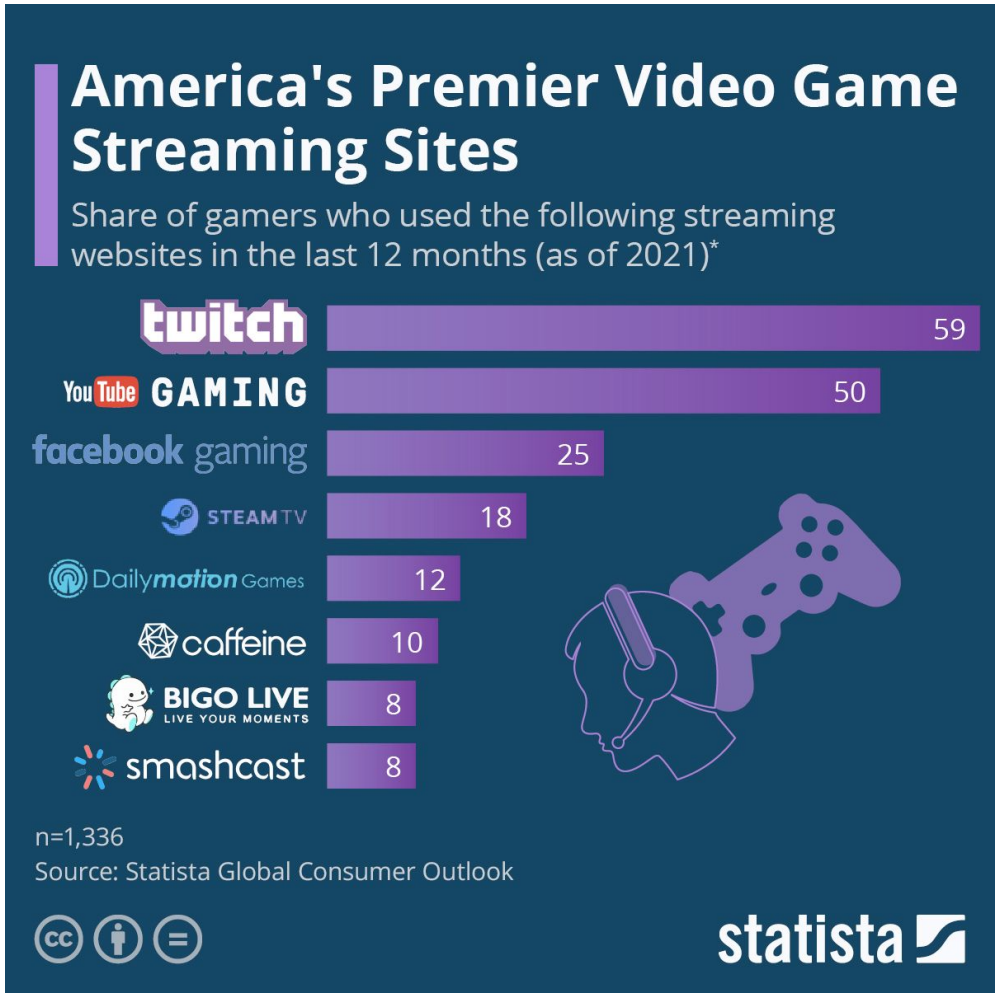
Xbox Nintendo PlayStation PC Gaming

PC
PCMAG.COM

Finding The Unknown

6

Games Streaming



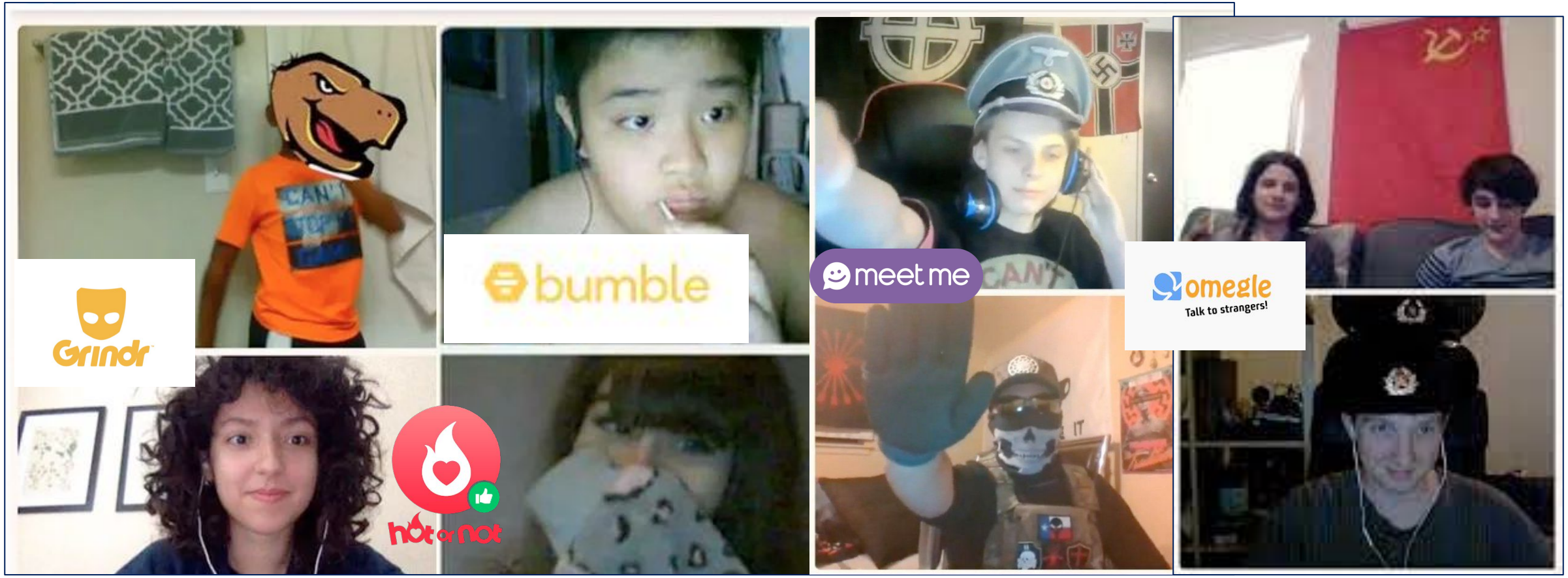
Finding The Unknown

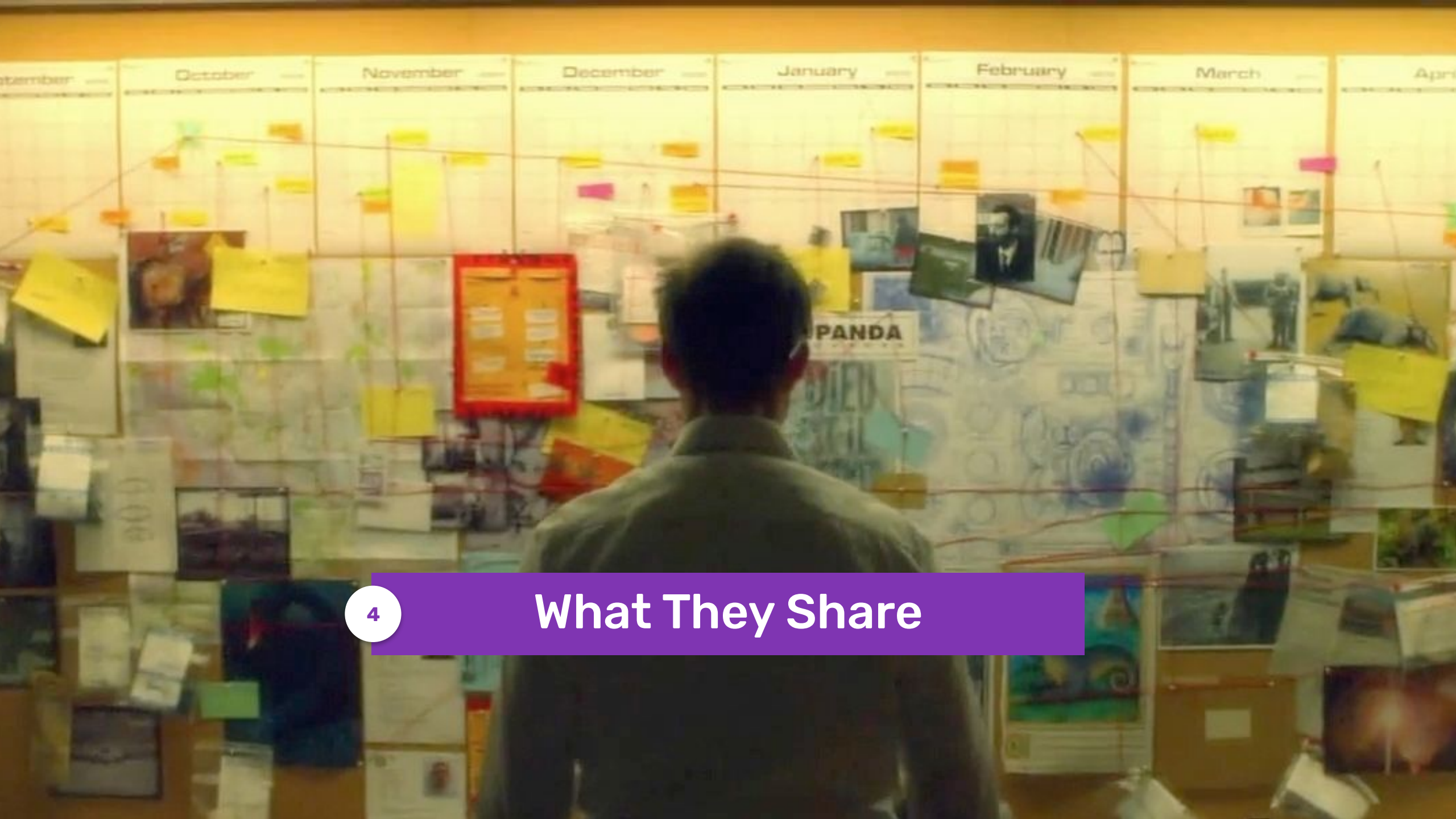
7 Gamers Communities

Site Name	Forum/Community URL or main URL	user URL format	user s	login t	locatic	birthd	join da	last ac	option	notes	indexe	Google Dork
Adventure Gamers	https://adventuregamers.com/forums	https://adventuregamers.com/forums/member/userid/	y	n	x		x	x		written bio & contact info section	x	site:armorgames.com/community intext:username
Armor Games	https://armorgames.com/community	https://armorgames.com/user/username	y	n	x		x	x	x	can list contact info on profile	x	site:armorgames.com/community intext:username
Blizzard Games	https://us.forums.blizzard.com/en/blizzard/	https://us.forums.blizzard.com/en/blizzard/u/username-userid/	y	n			x	x			x	site:us.forums.blizzard.com/en/blizzard intext:username
Choice of Games	https://forum.choiceofgames.com/	https://forum.choiceofgames.com/u/username/	y	n			x	x			x	site:forum.choiceofgames.com/ intext:username
Edge Gamers	https://www.edgegamers.com/	https://www.edgegamers.com/members/userid/	n	n	x	x	x	x			x	site:edgegamers.com intext:username
Euro Gamer	https://community.eurogamer.net/	https://www.eurogamer.net/profiles/username	n	n	x		x	x	x	written bio & contact info section	x	site:community.eurogamer.net/ intext:username
Game Revolution	https://forums.gamerevolution.com/	https://forums.gamerevolution.com/members/username.userid/	y	n	x	x	x	x	x	written bio & contact info section	x	site:forums.gamerevolution.com/ intext:username
GameFAQs	https://gamefaqs.gamespot.com/community	https://gamefaqs.gamespot.com/community/username	y	n			x	x	x	written bio & contact info section		no dork
GameSpot Boards	http://www.gamespot.com/forums/	https://www.gamespot.com/profile/username/	y	n			x				x	site:gamespot.com/forums/ intext:username
Gaming Latest	https://gaminglatest.com/	https://gaminglatest.com/members/username.userid/	y	n	x	x	x	x	x	can list contact info on profile	x	site:gaminglatest.com/ intext:username
Giant Bomb	https://www.giantbomb.com/forums/	https://www.giantbomb.com/profile/username/	y	n			x			written bio section	x	site:giantbomb.com/forums/ intext:username
IGN Boards	https://www.ignboards.com/	https://www.ignboards.com/members/username.userid	y	y	x	x	x	x	x	written bio & contact info section	x	site:ignboards.com/ intext:username
Kongregate	https://www.kongregate.com/forums	https://www.kongregate.com/accounts/username	y	n	x		x	x	x	written bio & contact info section	x	site:kongregate.com/forums intext:username
Minecraft Forum	http://www.minecraftforum.net/forums	https://www.minecraftforum.net/members/username	y	n			x	x	x	can list contact info on profile	x	site:minecraftforum.net/forums intext:username
MMORPG	https://www.mmorpg.com/	https://forums.mmorpg.com/profile/username	y	n			x	x	x	can list contact info on profile	x	site:forums.mmorpg.com/ intext:username
Mod DB	https://www.moddb.com/forum	https://www.moddb.com/members/username	y	n	x		x	x	x	written bio & contact info section	x	site:moddb.com/forum intext:username
NameMC (minecraft)	https://namemc.com/	https://namemc.com/name/username	y	n						shows entire username history	x	site:namemc.com/ intext:username
NeoGAF	http://www.neogaf.com/forum/	http://www.neogaf.com/members/username	y	y	x		x	x		written bio & contact info section	x	site:neogaf.com/forum/ intext:username
Nintendo Life	https://www.nintendolife.com/forums	https://www.nintendolife.com/users/username	n	n	x		x			can add bio & contact to profile	x	site:nintendolife.com/forums intext:username
Penny Arcade	https://forums.penny-arcade.com/	https://forums.penny-arcade.com/profile/discussions/username	y	n	x		x	x	x	can list contact info on profile	x	site:forums.penny-arcade.com/ intext:username
PSN Profiles	https://forum.psnprofiles.com/	https://forum.psnprofiles.com/profile/userid-username/	y	n	x	x	x	x	x	can add bio & contact to profile	x	site:forum.psnprofiles.com/ intext:username
Roblox Developer Forum	https://devfor											ox.com/ intext:username
RPG	https://forum.											/index.php intext:username

https://drive.google.com/file/d/1xZ8n5PiEviB70aOLDtKZ2GrduKY8GWEq/view

The Most Interesting One





4

What They Share

What They Share

- Username
- Real name
- Gender
- Birth date
- Education
- Profession
- Relationship status
- Friends/Following/Followers
- Groups entered
- Interests
- Hobbies
- Linked accounts
- Languages
- Status updates
- Likes
- Reactions
- Emoji used
- Uploaded media
- Media metadata
- People tagged on media
- Public posts
- Comments
- Hashtags used
- Social media handles
- Email(s) used
- Phone number(s)

Privacy Research

https://en.panoptykon.org/articles/three-layers-your-digital-profile

What They Share

- Addresses
- Current Location
- Events attended
- Places visited
- Links Shared
- Tests and Surveys
- Products reviewed and ranked
- Petitions signed
- Accepted invitations
- File names and types

- Liked Games/toys
- Fan pages
- Biography
- Tagged accounts
- Time zone

And more...

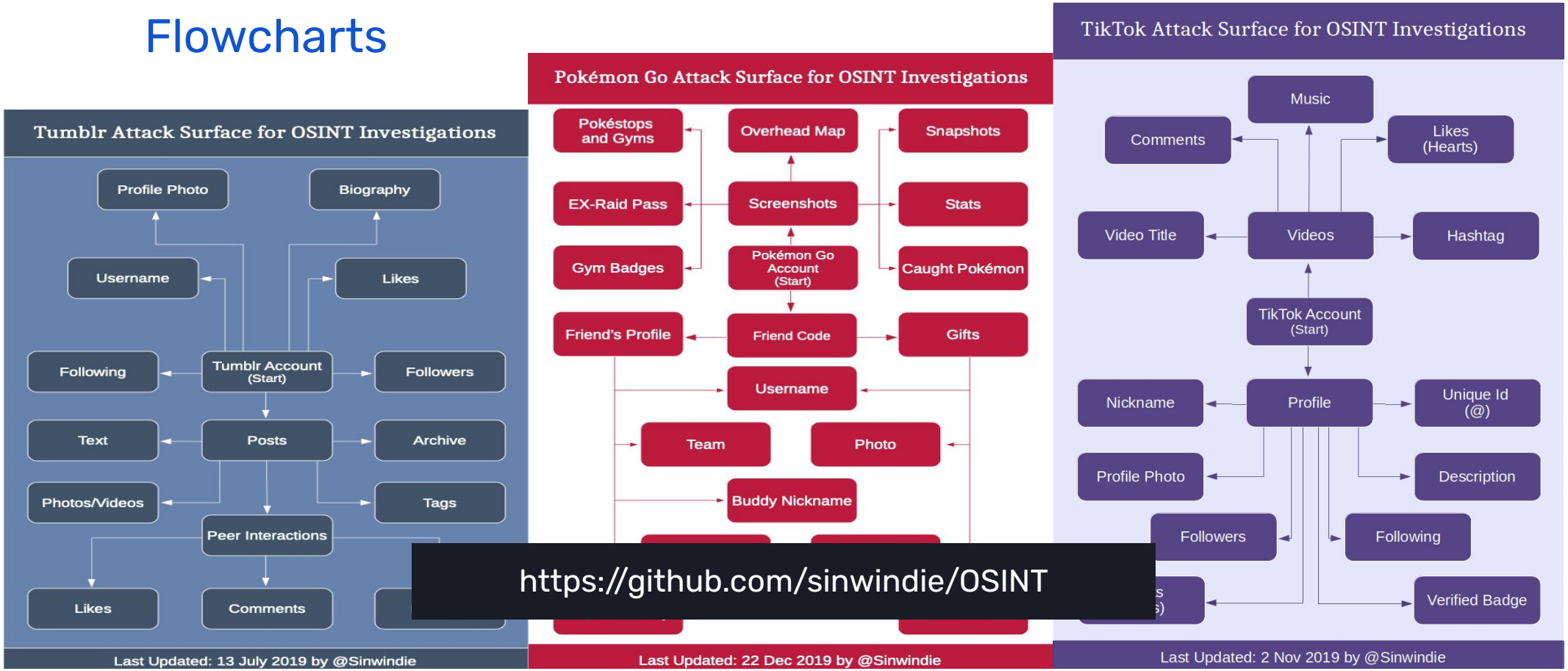
- Fingerprints
- IDs
- Credit/Bank cards
- Logins and passwords
- Devices used
- Private family details

Privacy Research

https://en.panoptykon.org/articles/three-layers-your-digital-profile

What They Share

Flowcharts



https://github.com/sinwindie/OSINT

Darknet...

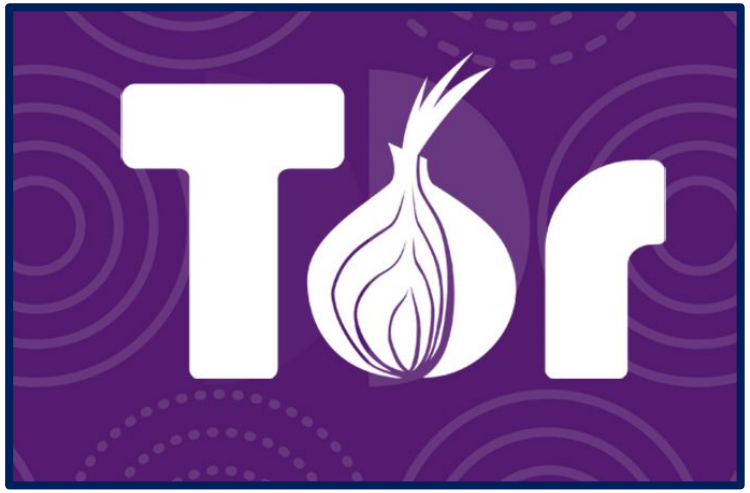
QOMPLX:CYBER

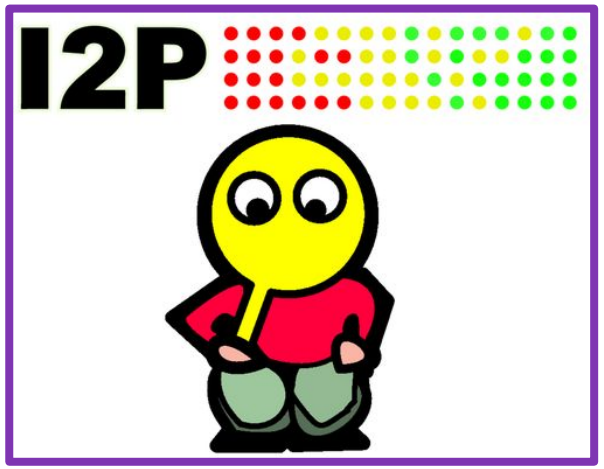
Michael James

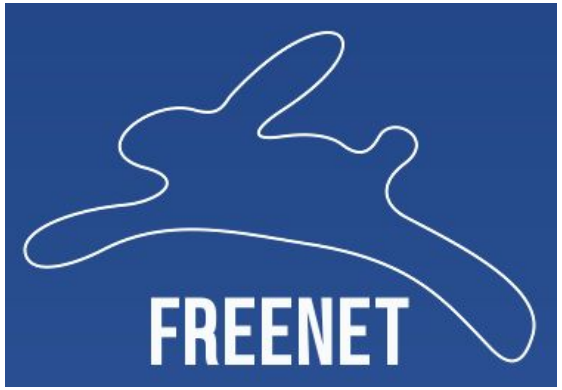
Principle OSINT Specialist
QOMPLX Intelligence Unit

@Ginsberg5150

Deep Web: areas of search

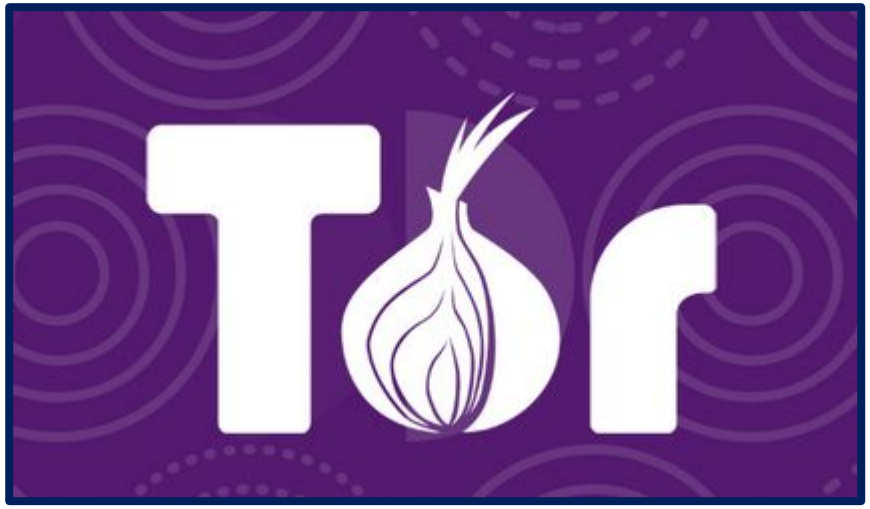






Where do we look for .onion sites?

- OSINT Party Fresh Links
- Hunch.ly DarkNet Daily Update
- TOR 66 fresh links

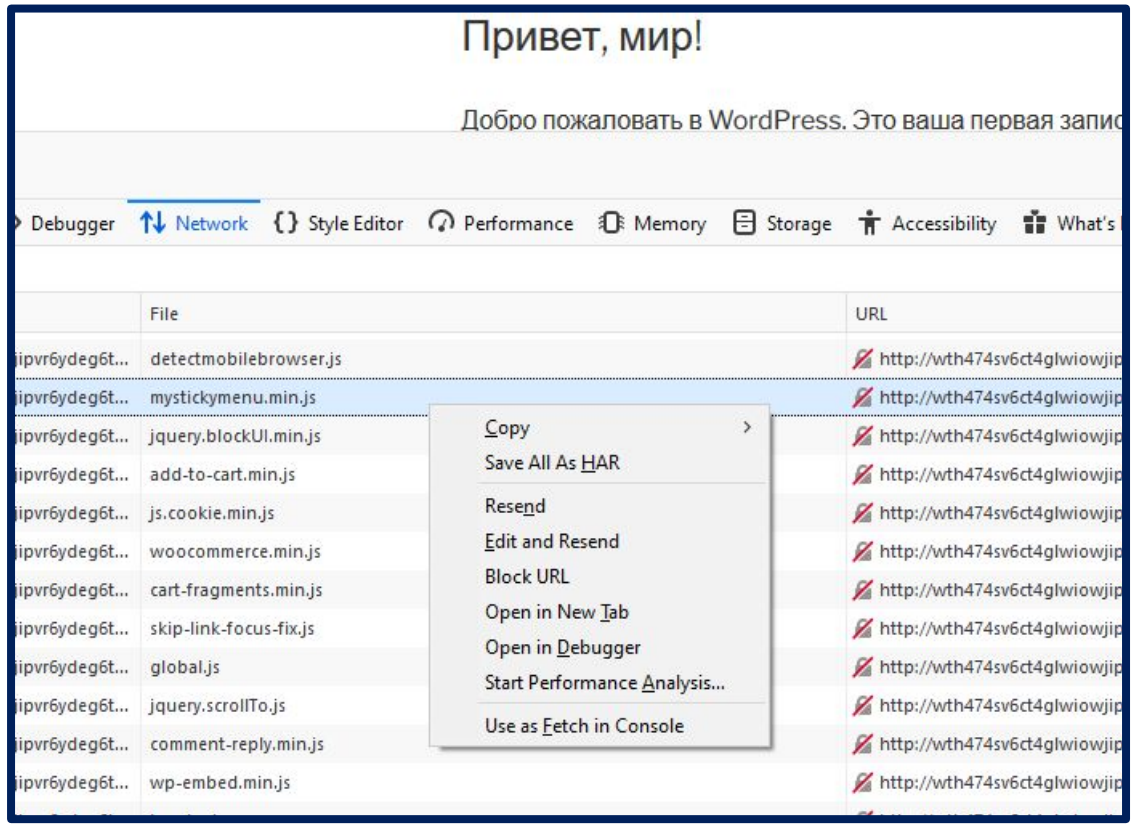


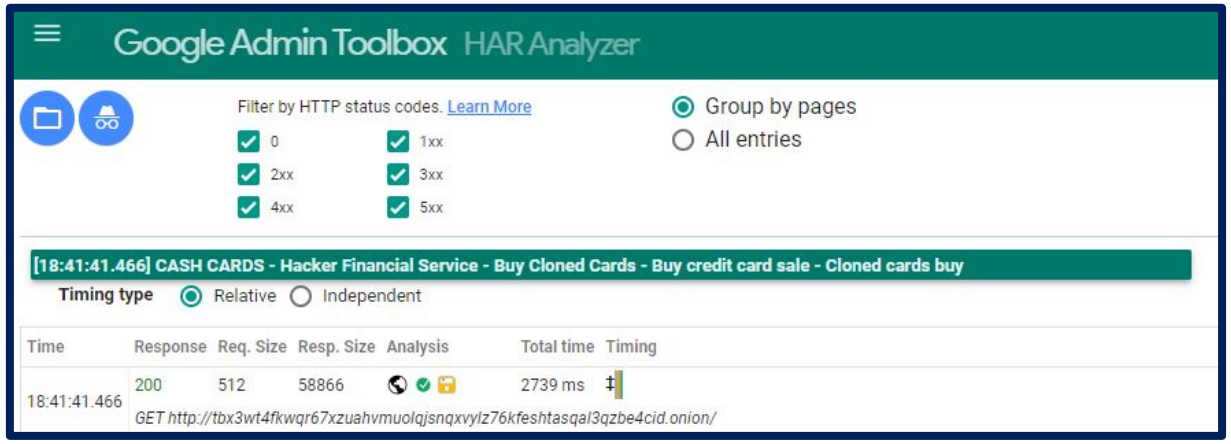
qd43byl2pgq5b7k3.onior	en	200	OnionDir
x2btcvwtemaqaoa2.onior	en	200	OnionDir - Adult
lt6ychu3k6fx3apu.onion	en	200	OnionDir
chemspain7iw2zby.onion	en	200	Store
svyagrufqojpw2ge.onion	en	200	OnionDir
7a5eaokoytoqpp6jgklwg5	en	200	Home | Towards Liberty
caseygdp6ledkxai.onion	en	200	OnionDir
infantilefb6ovh4.onion	en	200	Infantile - No Rules Communications

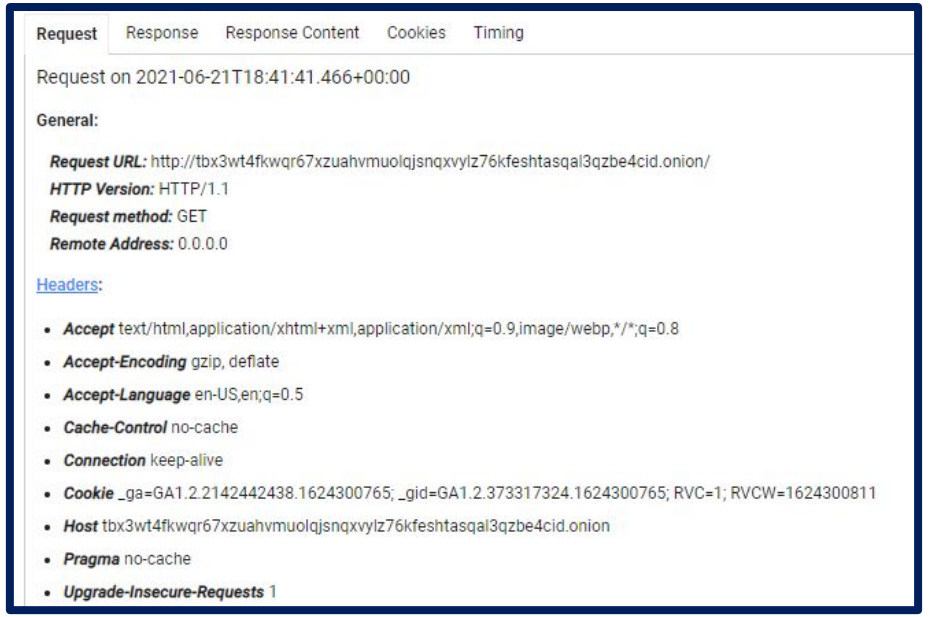
QOMPLX:CYBER

HTTP ARchive format - HAR files

https://toolbox.googleapps.com/apps/har_analyzer/



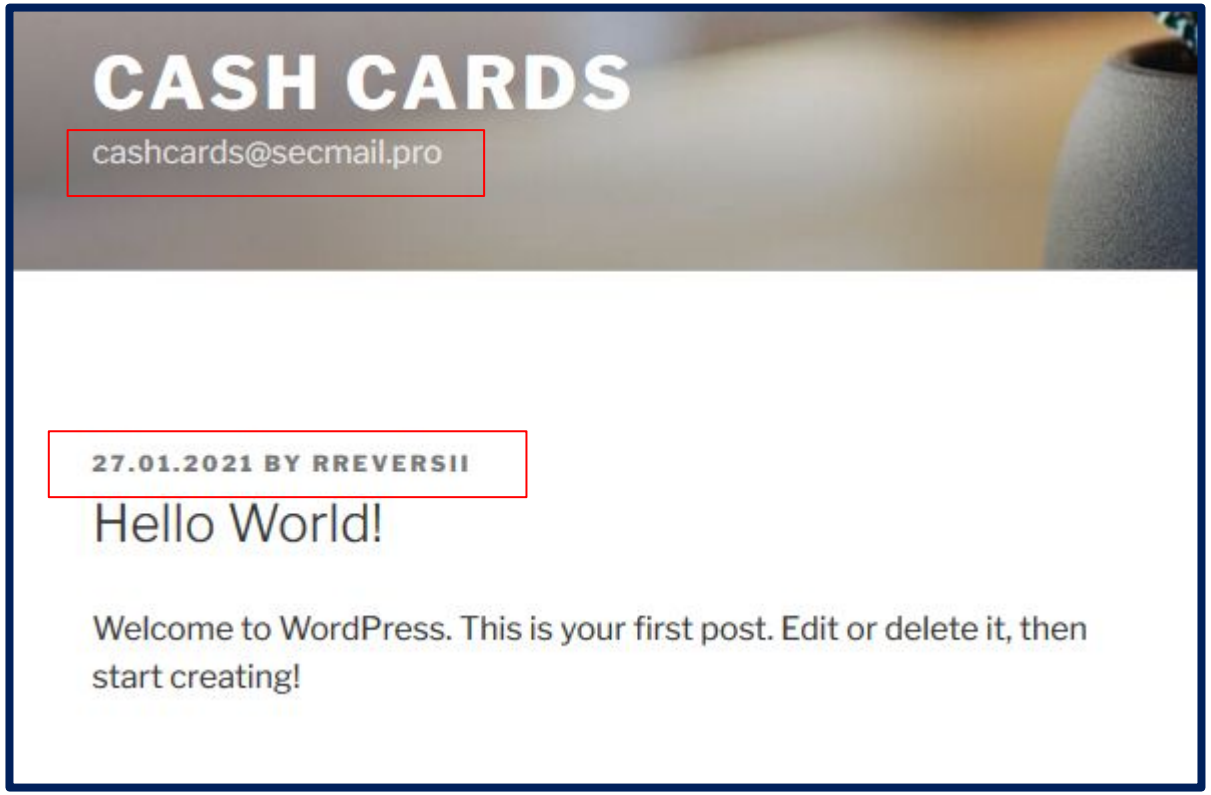




```
−<oembed>
   <version>1.0</version>
   <provider_name>CASH CARDS</provider_name>
  −<provider_url>
      http://wth474sv6ct4glwiowjipvr6ydeg6tbxlenxqibe5vno7ivmeqlumnid.onion
   </provider_url>
   <author_name>rreversii</author_name>
  −<author_url>
      http://wth474sv6ct4glwiowjipvr6ydeg6tbxlenxqibe5vno7ivmeqlumnid.onion/author/rreversii/
   </author_url>
   <title>CASH CARDS</title>
```

Author Name

Author login/blog




```
from:              "response_body"
identifier_type:   "email_address"
identifier:        "ccards@mailfence.com"
created_at:        "2021-06-21T17:30:13.000000Z"
```

What else can we learn about these sites?

OSINT PARTY!!


```
from:              "response_body"
identifier_type:   "email_address"
identifier:        "webmaster@fcrdp3t6ngxkscjcth7cmajhcubgpp72w45rwmo3hn5nz66odx2to6qd.onion"
created_at:        "2021-03-26T01:03:04.000000Z"
```

```
from:              "response_body"
identifier_type:   "html_meta"
identifier:        "generator: WordPress 5.7.1"
created_at:        "2021-05-12T00:03:40.000000Z"
```

```
from:              "response_body"
identifier_type:   "btc_address"
identifier:        "1FWrm3Z1g2W4kEQXgsUyHXEk2S9dTVK54P"
created_at:        "2021-06-21T17:30:13.000000Z"
```

```
status:            1
code:              200
created_at:        "2021-02-26T11:12:12.000000Z"
```


All credit for this tool goes to:

Data Breach for the Investigator

What you don't know can still hurt you

- Using Data breach details for additional pivot points
  - Some departments or agencies are not going to be able to use this information
  - Data Breach records allow discovery and notification
  - What was breached is as important as the names in the breach

QOMPLX:CYBER

https://tools.epieos.com/email.php

DeepPaste

Order

Anon, April 11, 2021 - 12:13 pm UTC

```
Human Trafficking Since 2008.
f001@SECMAIL.PRO
(Postcode and house number):
```

Trafficking and Kidnapping services

Anon, February 10, 2021 - 6:51 am UTC

```
For Human(child)  trafficking and Kidnapping services, contact Dang147@protonmail.com, Wickr @ Dang147.
```

Email Used

protonmail / Date, time of the creation 2017-11-23 00:54:46

discord

Email Used

protonmail / Date, time of the creation 2020-10-13 08:04:19

```
CONTACT DETAILS

Email:Bestvendor2002@protonmail.com

Wickr:Bestvendor2002

Telegram:Bestvendor2002

WhatsApp:+1(765)560-5168
```

Email:Darknetmarket1@protonmail.com

WhatsApp +1(765)560-5168

Telegram Darkwebvendor

Wickr Darkwebvendor20

CALLER NAME Slickamann Wickr	OWNER LOCATION Indiana, United States	CARRIER Bandwidth.com
PHONE TYPE Landline	AREA CODE LOCATION Bringhurst, IN	

International-Passports

Buy
REGISTER,CERTIFICATES,DOCUMENTS,IELTS,ESOL,TOEIC/TOEFL,DIPLOMAS,DEGREE,PASSPORTS,VISA,DRIVING,LICENSE,ID,CARDS..CONTACT WHATSAPP..+1(443) 267-2974 See less

http://james-travel.ru/usa.html

More Pivoting from Pastesite to Clearweb/social media

---TRAFFICKING ORGANIZATION---
pedocaria, March 24, 2021 - 4:30 pm UTC

```
----------------------
Referral CODE : AMELIA123
----------------------
------WHATSAPP------
+1 (443) 267-2974
------TELEGRAM------
+1 (443) 267-2974
```

Education Ambassador
James Travel · Full-time
Feb 1973 – Present · 48 yrs 5 mos
United States

Immigration Specialist
Immigration, Refugees and Citizenship Canada / Immigration, Réfugiés et Citoyenneté Canada · Full-time
Apr 1972 – Feb 1973 · 11 mos
Toronto, Canada Area

USA, Canada, Europe Immigration officer I have over the years

QOMPLX:CYBER

Apple ID: izak.oa3@list.ru
Password: Zako3313
ID by VK, collected by Le Hoang Giap

```
1  📌 Apple 🆔 :jilavyanlavrent22@mail.ru
2  📌 Password 🔐 :Click789
3
4  ID by VK, collected by Le Hoang Giap
```

Email : giapnework@gmail.com

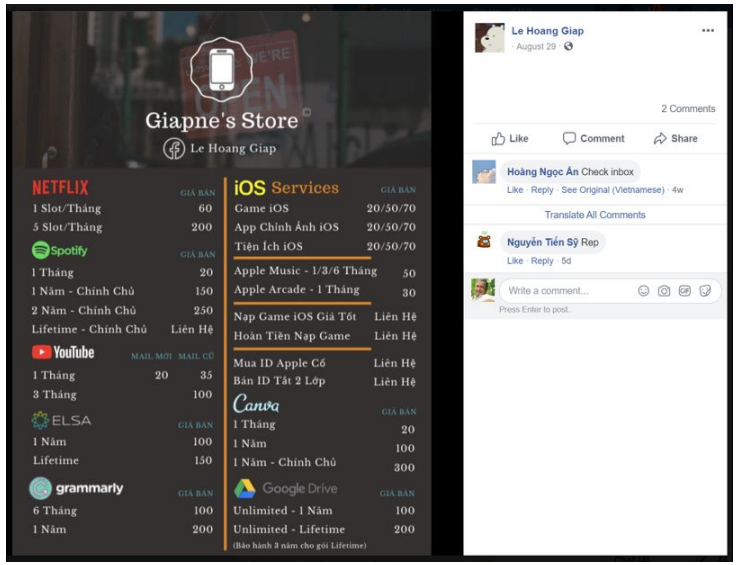
Name : Hoang Giap

GoogleID : 111491471471724557847

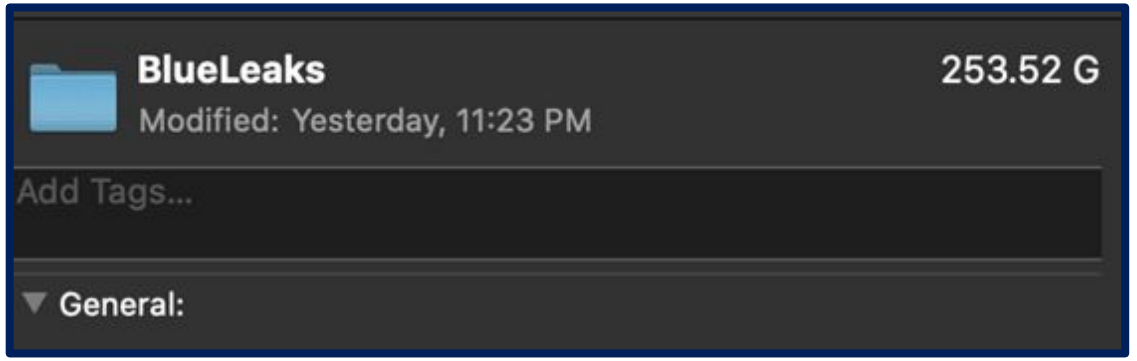
Last Update : 2020-08-20 07:52:24

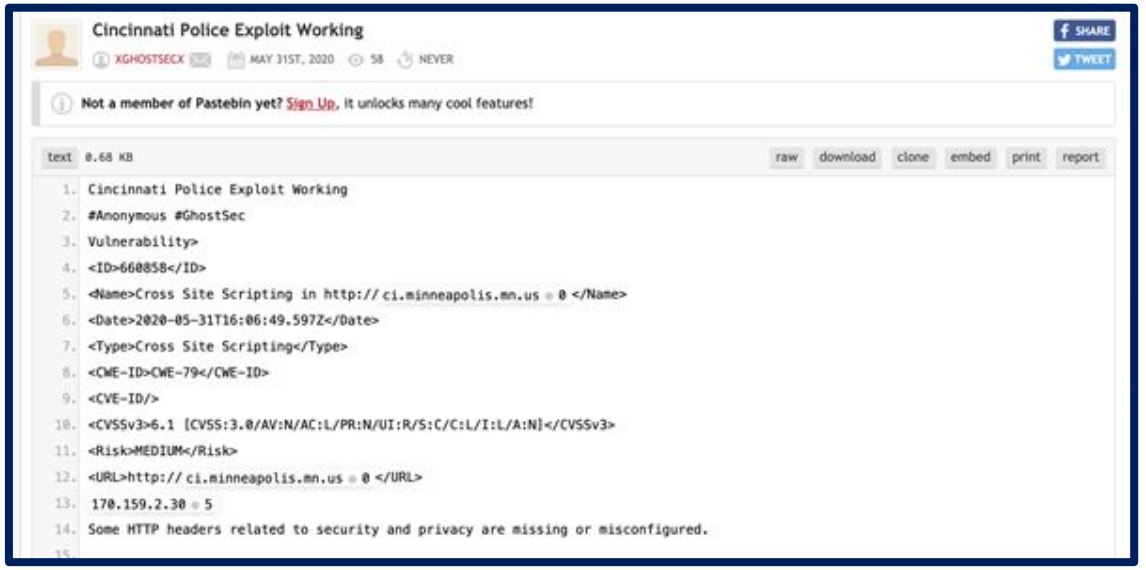
Maps
https://www.google.com/maps/contrib/111491471471724557847

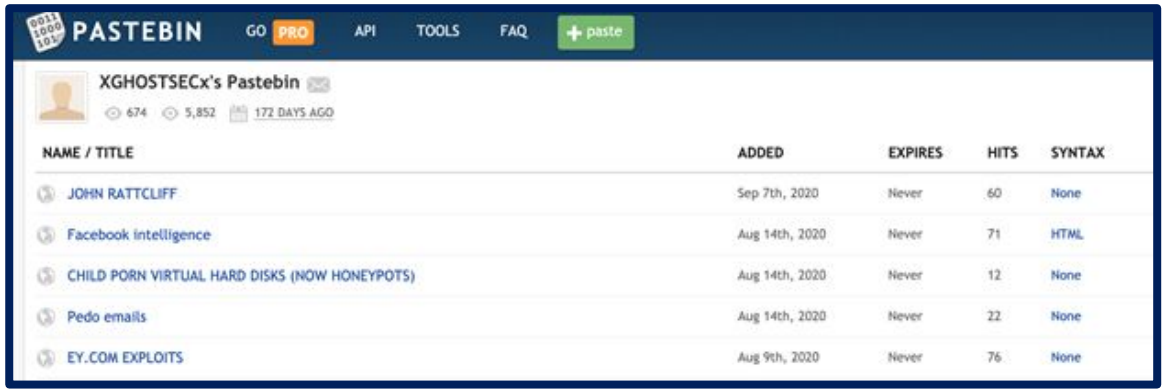
Photos
https://get.google.com/albumarchive/111491471471724557847



When you're browsing the dark web and see yourself on sale for $500





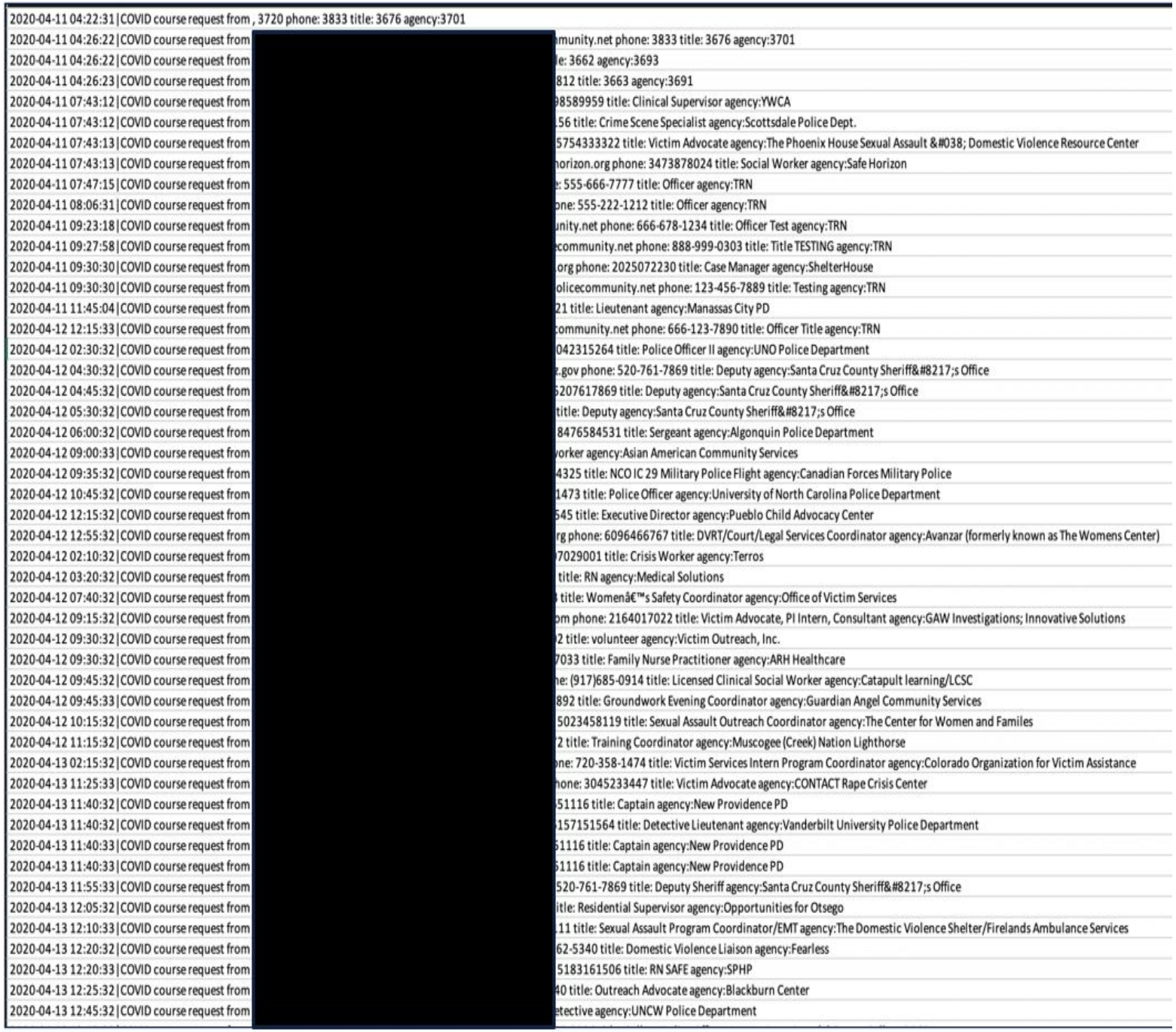


QOMPLX:CYBER

Beware of 3rd Party Vendors with Trusted access

Using Personal Emails for Department business is a bad idea

Use Email systems that are not connected to your personal information



Any Questions?

Slides & Resources

https://github.com/qomplx/ncptf2021