

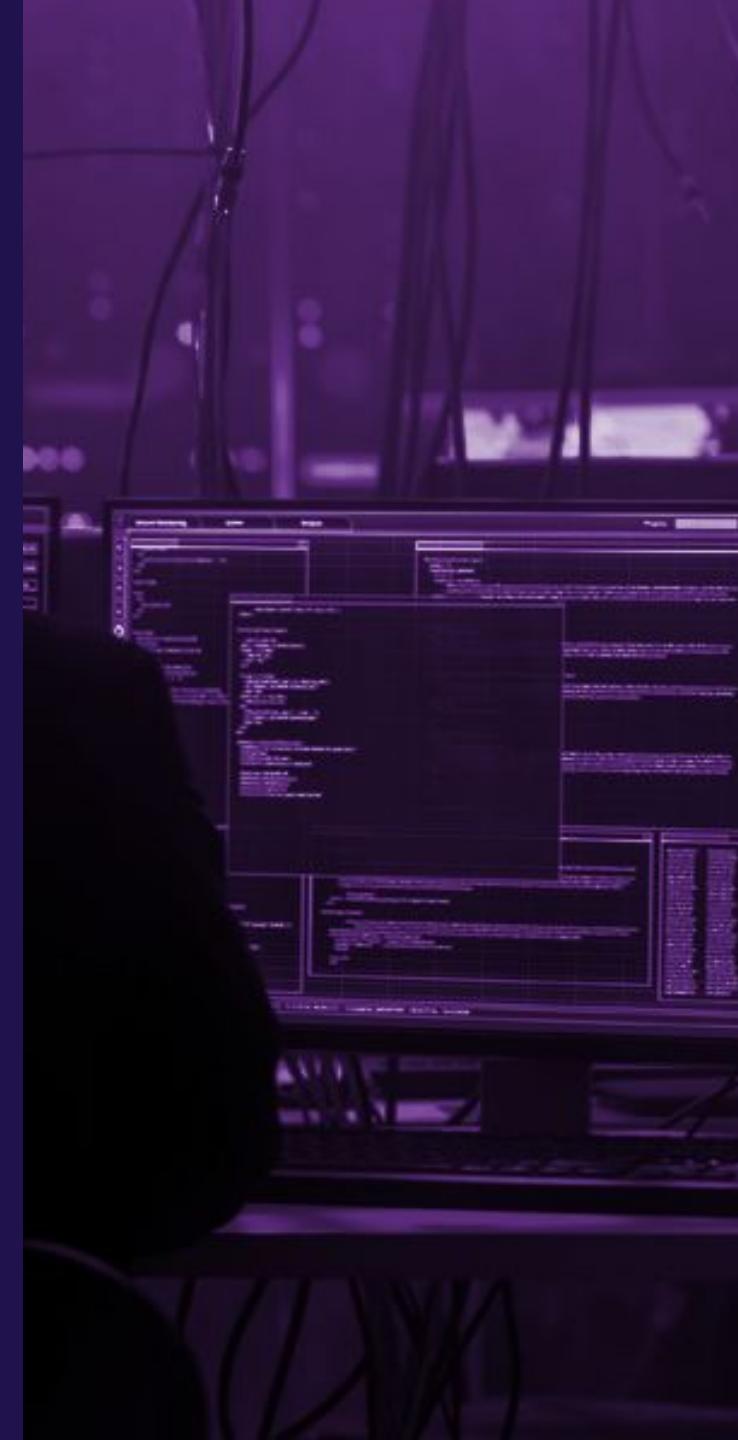
QOMPLX:CYBER

What you don't know can hurt

Archiving, social media and data breach for investigation

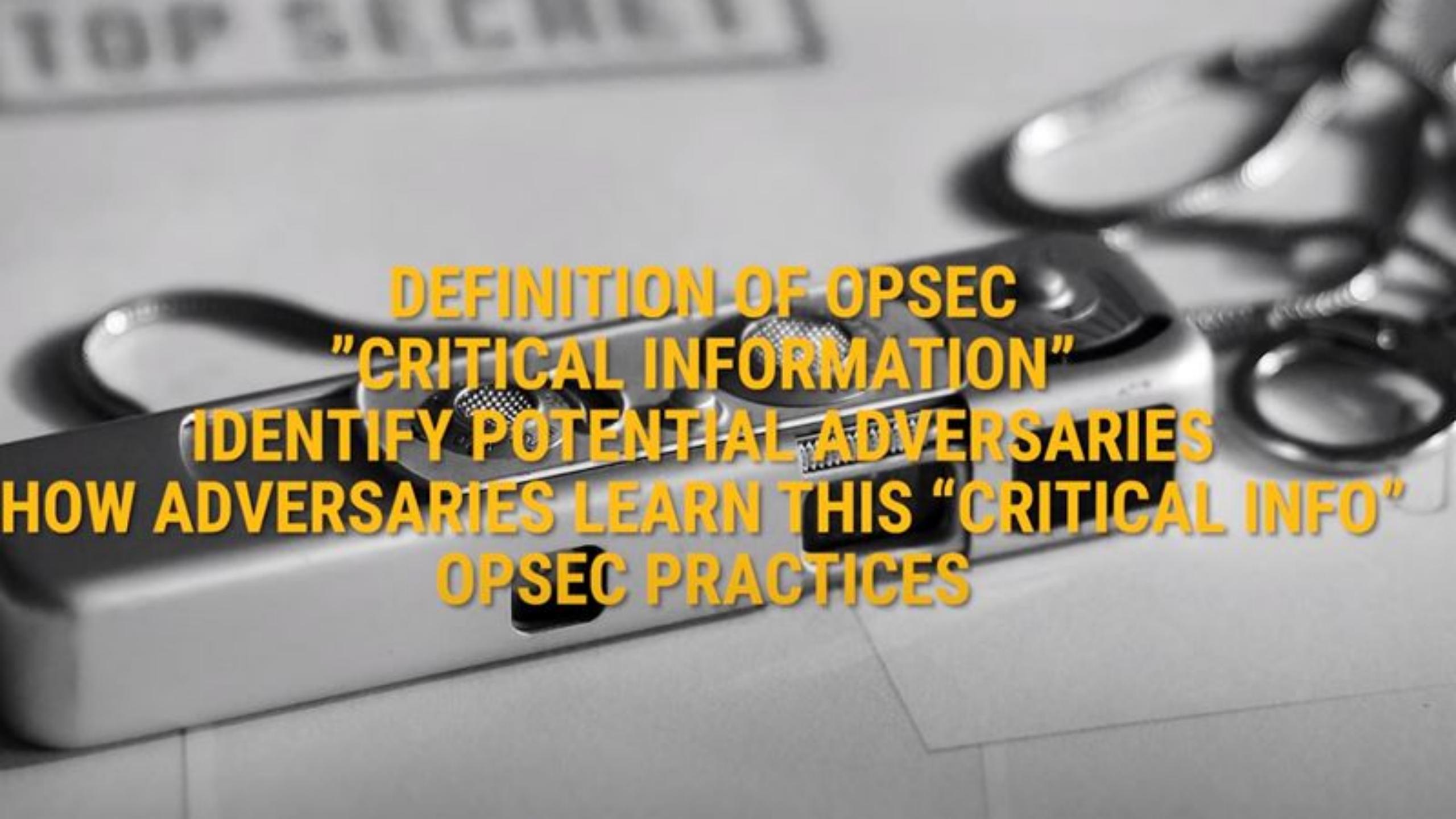
QOMPLX:CYBER

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?



YouTube - The OSINT Curious Project

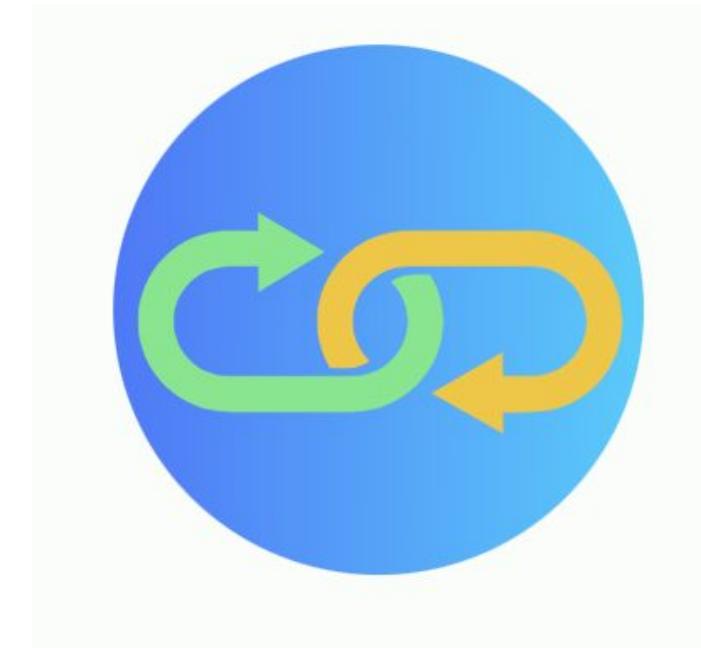
17		10 Minute Tip: Using robots.txt Files for OSINT	The OSINT Curious Project
18		10 Minute OSINT Tip: How To Use APIs to Reveal Hidden Open Source Information	The OSINT Curious Project
19		10 Minute OSINT Tip: What Can We Learn From XHR, and JSON During an OSINT Investigation?	The OSINT Curious Project
20		10 Minute Tip: OSINT and Web Analytics Codes and Tags	The OSINT Curious Project
21		10 Minute Tip: Certificates: OSINT and HTML Source Code	The OSINT Curious Project

Browser Extensions

SingleFile



Webrecorder.net



SingleFile

The screenshot shows the QOMPLX website homepage. At the top, there's a navigation bar with links for About, Products, Newsroom, Blog, Resources, Request A Meeting (which is highlighted in blue), and Sign In. Below the navigation is a dark blue banner with the text "Concerned by a potential breach? Call +1-571-416-6111". The main content area features a large image of a smartphone displaying a document. To the left of the phone, text reads: "Dun & Bradstreet and QOMPLX join forces to provide cybersecurity certification tools for defense contractors". Below this is a "Learn More" button. To the right, there's a section titled "dun&bradstreet PARTNERSHIP QOMPLX:". Further down, there's a section titled "QOMPLX Risk Cloud" with a description of their risk analytics capabilities. To the right of the text is a circular diagram representing a network or cloud architecture, composed of various icons like servers, databases, and clouds connected by lines.

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

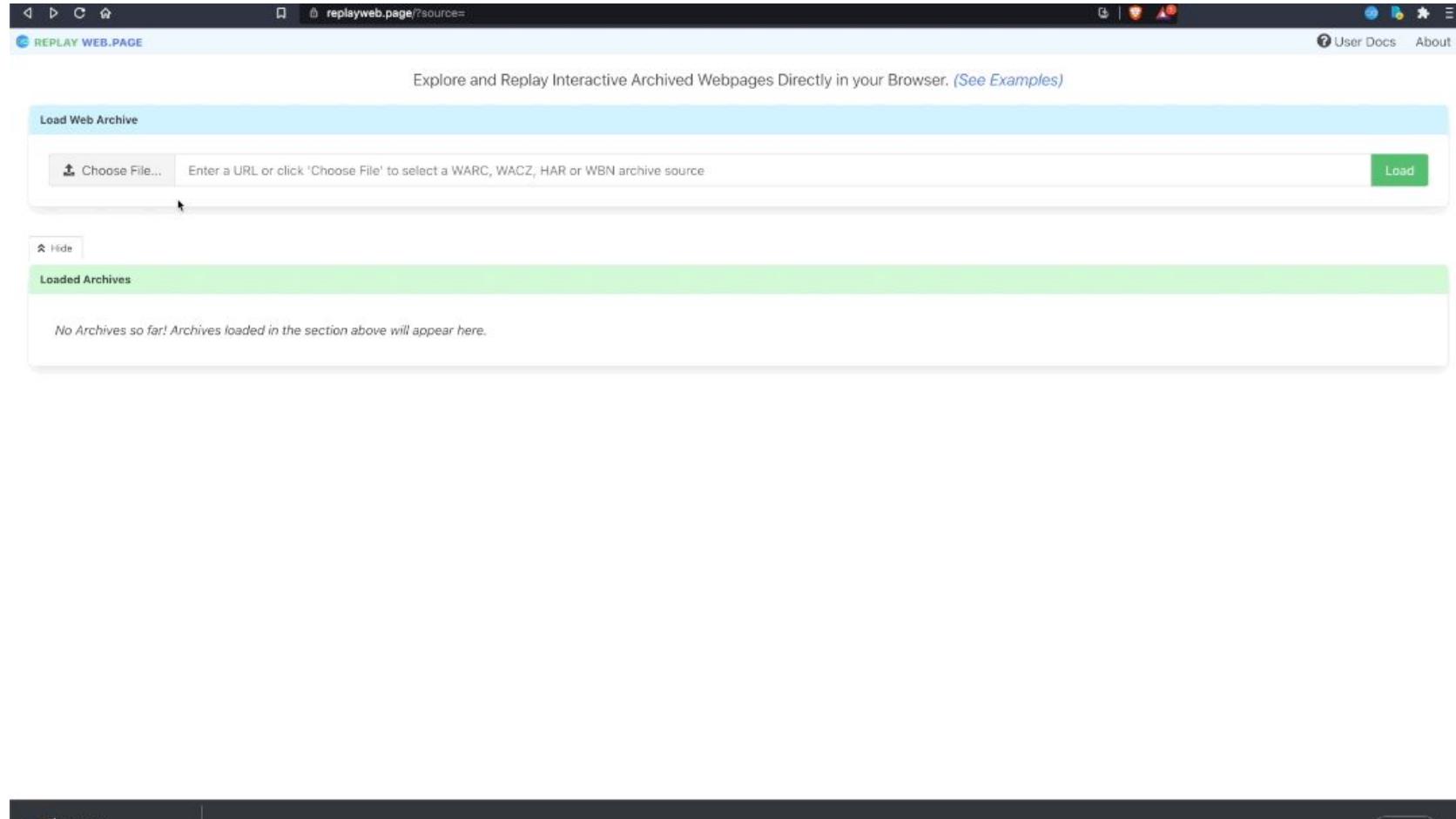
QOMPLX is a cloud-native leader in risk analytics. Our customers rapidly ingest, transform, and contextualize large, complex, and disparate data sources using our data factory in order to better quantify, model, and predict risks. We help organizations develop more informed risk strategies and decisions for Cyber Security, Insurance, and Finance.

```
graph TD; Center(( )); Center --- Node1(( )); Center --- Node2(( )); Center --- Node3(( )); Center --- Node4(( )); Center --- Node5(( )); Center --- Node6(( )); Center --- Node7(( )); Center --- Node8(( )); Center --- Node9(( )); Center --- Node10(( )); Center --- Node11(( )); Center --- Node12(( )); Center --- Node13(( )); Center --- Node14(( )); Center --- Node15(( )); Center --- Node16(( )); Center --- Node17(( )); Center --- Node18(( )); Center --- Node19(( )); Center --- Node20(( )); Center --- Node21(( )); Center --- Node22(( )); Center --- Node23(( )); Center --- Node24(( )); Center --- Node25(( )); Center --- Node26(( )); Center --- Node27(( )); Center --- Node28(( )); Center --- Node29(( )); Center --- Node30(( )); Center --- Node31(( )); Center --- Node32(( )); Center --- Node33(( )); Center --- Node34(( )); Center --- Node35(( )); Center --- Node36(( )); Center --- Node37(( )); Center --- Node38(( )); Center --- Node39(( )); Center --- Node40(( )); Center --- Node41(( )); Center --- Node42(( )); Center --- Node43(( )); Center --- Node44(( )); Center --- Node45(( )); Center --- Node46(( )); Center --- Node47(( )); Center --- Node48(( )); Center --- Node49(( )); Center --- Node50(( )); Center --- Node51(( )); Center --- Node52(( )); Center --- Node53(( )); Center --- Node54(( )); Center --- Node55(( )); Center --- Node56(( )); Center --- Node57(( )); Center --- Node58(( )); Center --- Node59(( )); Center --- Node60(( )); Center --- Node61(( )); Center --- Node62(( )); Center --- Node63(( )); Center --- Node64(( )); Center --- Node65(( )); Center --- Node66(( )); Center --- Node67(( )); Center --- Node68(( )); Center --- Node69(( )); Center --- Node70(( )); Center --- Node71(( )); Center --- Node72(( )); Center --- Node73(( )); Center --- Node74(( )); Center --- Node75(( )); Center --- Node76(( )); Center --- Node77(( )); Center --- Node78(( )); Center --- Node79(( )); Center --- Node80(( )); Center --- Node81(( )); Center --- Node82(( )); Center --- Node83(( )); Center --- Node84(( )); Center --- Node85(( )); Center --- Node86(( )); Center --- Node87(( )); Center --- Node88(( )); Center --- Node89(( )); Center --- Node90(( )); Center --- Node91(( )); Center --- Node92(( )); Center --- Node93(( )); Center --- Node94(( )); Center --- Node95(( )); Center --- Node96(( )); Center --- Node97(( )); Center --- Node98(( )); Center --- Node99(( )); Center --- Node100(( ));
```

WebRecorder Project - ArchiveWeb

The screenshot shows the QOMPLX website homepage. At the top, there's a navigation bar with links for About, Products, Newsroom, Blog, Resources, Request A Meeting (which is highlighted in blue), and Sign In. Below the navigation is a dark blue header bar with the text "Concerned by a potential breach? Call +1-571-416-6111". The main content area features a large image of a tablet displaying a document titled "QOMPLX: Repelling Ransomware". The document cover includes a padlock icon and some descriptive text. To the left of the tablet, there's a section with the heading "How Prepared Are You For a Ransomware Outbreak?" and a "Learn More" button. At the bottom left, there's a section titled "QOMPLX Risk Cloud" with a brief description of their services. On the right side of the main content area, there's a circular diagram representing a network or cloud architecture, composed of various icons like servers, databases, and clouds connected by lines.

WebRecorder Project - ReplayWeb



Online Archives



<https://archive.today>



<https://archive.org>

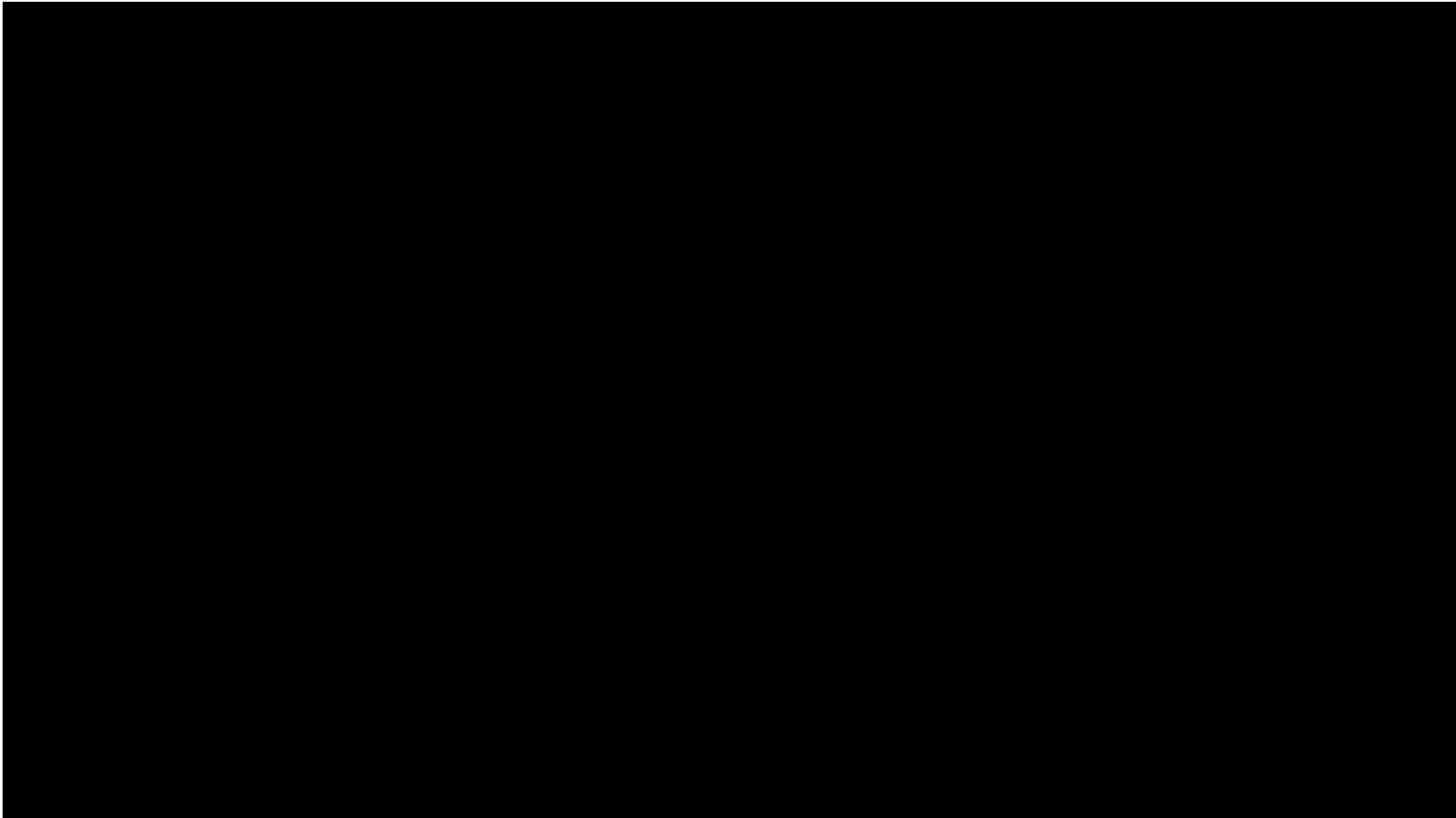


<https://perma.cc>

QOMPLX:CYBER

Archiving for Investigators

ArchiveBox.io



Standalone Tools



<https://hunch.ly>



<https://vortimo.com>



[https://calluna-software.com \(NCollector\)](https://calluna-software.com)



<https://httrack.com>

Mobile Device Capture

<https://hunch.ly>

Online investigations.
Now pocket sized.

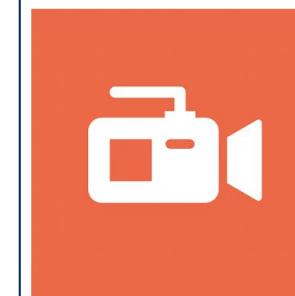
Digital evidence collection for
investigators, witnesses, and
victims

Hunchly Mobile is now available for free on iOS and
Android



 GitHub SCNCOPY

<https://github.com/Genymobile/scncpy>



AZ Screen Recorder - Video
Recorder, Livestream

AZ Screen Recorder Video Players & Editors

★★★★★ 1,471,084

E Everyone

Contains ads · Offers in-app purchases

⚠ You don't have any devices

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?

The screenshot shows the 'Add URLs' page of the ArchiveBox web application. At the top, there's a navigation bar with links for 'ADD + / SNAPSHOTS / USERS / OLD UI / DOCS', 'USER SQUASH', and 'CHANGE PASSWORD / LOG OUT'. Below the navigation is a breadcrumb trail 'Home > Add URLs'. The main content area has a heading 'Add new URLs to your archive' and a large text input field labeled 'URLs (in any format, CSV, XML, HTML, JSON, MD, TXT, etc.)'. In the bottom right corner of this input field, there's a small green circular icon with a white letter 'G'. Below the input field, there's a section titled 'Archive depth:' with two radio button options:

- depth = 0 (archive just these URLs)
- depth = 1 (archive these URLs and all URLs one hop away)

A large yellow button at the bottom right contains the text 'Add URLs and archive +'.

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

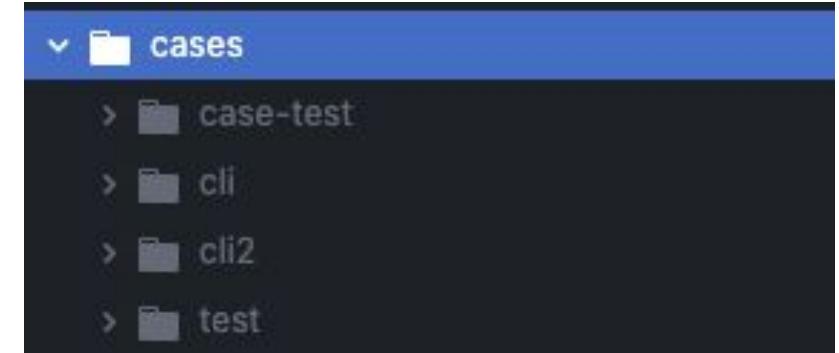
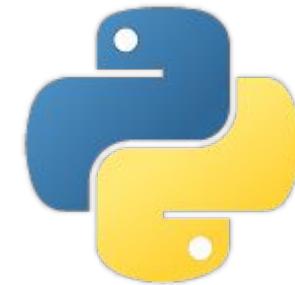
How do you fix that?

The screenshot shows the ArchiveBox web interface. At the top, there's a navigation bar with links for 'ADD + / SNAPSHOTS / USERS / OLD UI / DOCS', 'USER SQUASH', 'CHANGE PASSWORD / LOG OUT', and 'Home > Add URLs'. The main content area has a heading 'Add new URLs to your archive' and a text input field labeled 'URLs (in any format, CSV, XML, HTML, JSON, MD, TXT, etc.)'. Below the input field is a section titled 'Archive depth:' with two radio button options: 'depth = 0 (archive just these URLs)' (which is selected) and 'depth = 1 (archive these URLs and all URLs one hop away)'. At the bottom right is a yellow button labeled 'Add URLs and archive +'.

Archiving Tool for the Investigator

Archiving websites (ArchiveBox)

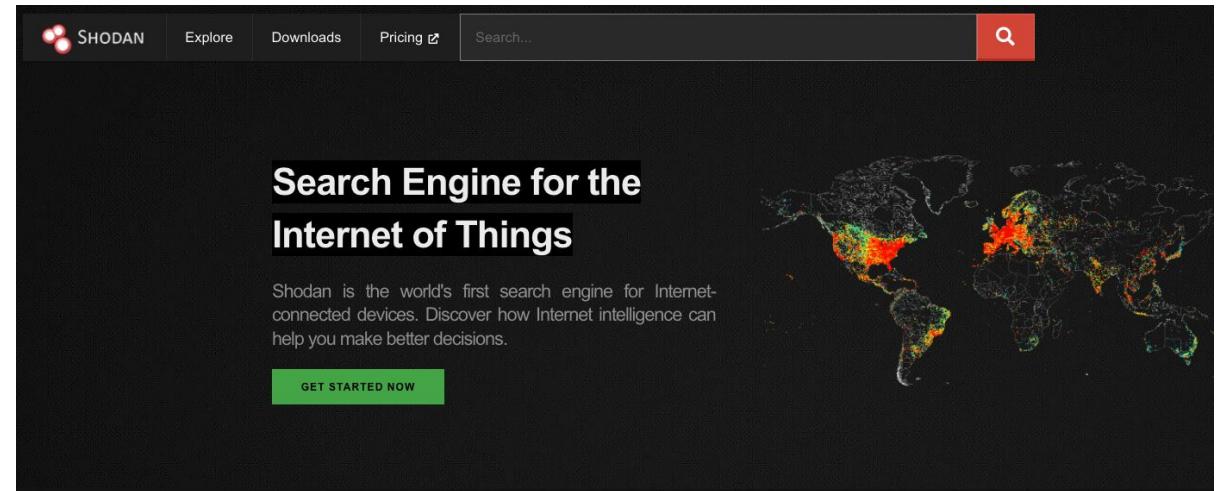
- Scripting (Python 3)
- Separate Archive Databases Into different Cases
- Lets you run databases per operations



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: arkscraper.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

```
$ python3 arksrape.py --init
Name for Archive Folder: talk-test
== ARCHIVE SETUP ==
[i] [2021-06-16 19:13:04] ArchiveBox v0.6.2: archivebox init --setup
> /Users/nathaniel.johnson/arksrape/cases/talk-test

[+] Initializing a new ArchiveBox v0.6.2 collection...
-----
[+] Building archive folder structure...
+ ./archive, ./sources, ./logs...
+ ./ArchiveBox.conf...

[+] Building main SQL index and running initial migrations...
Operations to perform:
  Apply all migrations: admin, auth, contenttypes, core, sessions
Running migrations:
  Applying contenttypes.0001_initial... OK
  Applying auth.0001_initial... OK
```

Archiving Tool for the Investigator

Using our tool

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

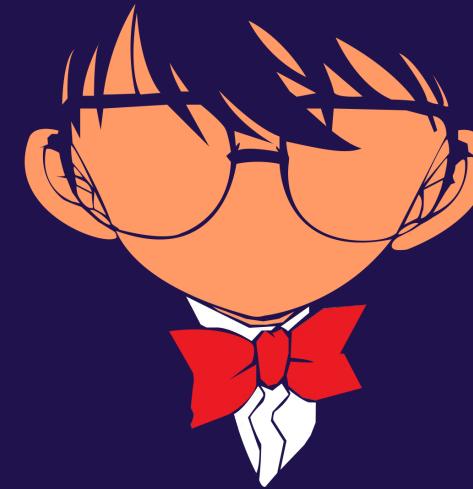
QOMPLX:CYBER

Where The kids Hangout



Salah
OSINT Specialist
QOMPLX Intelligence Unit

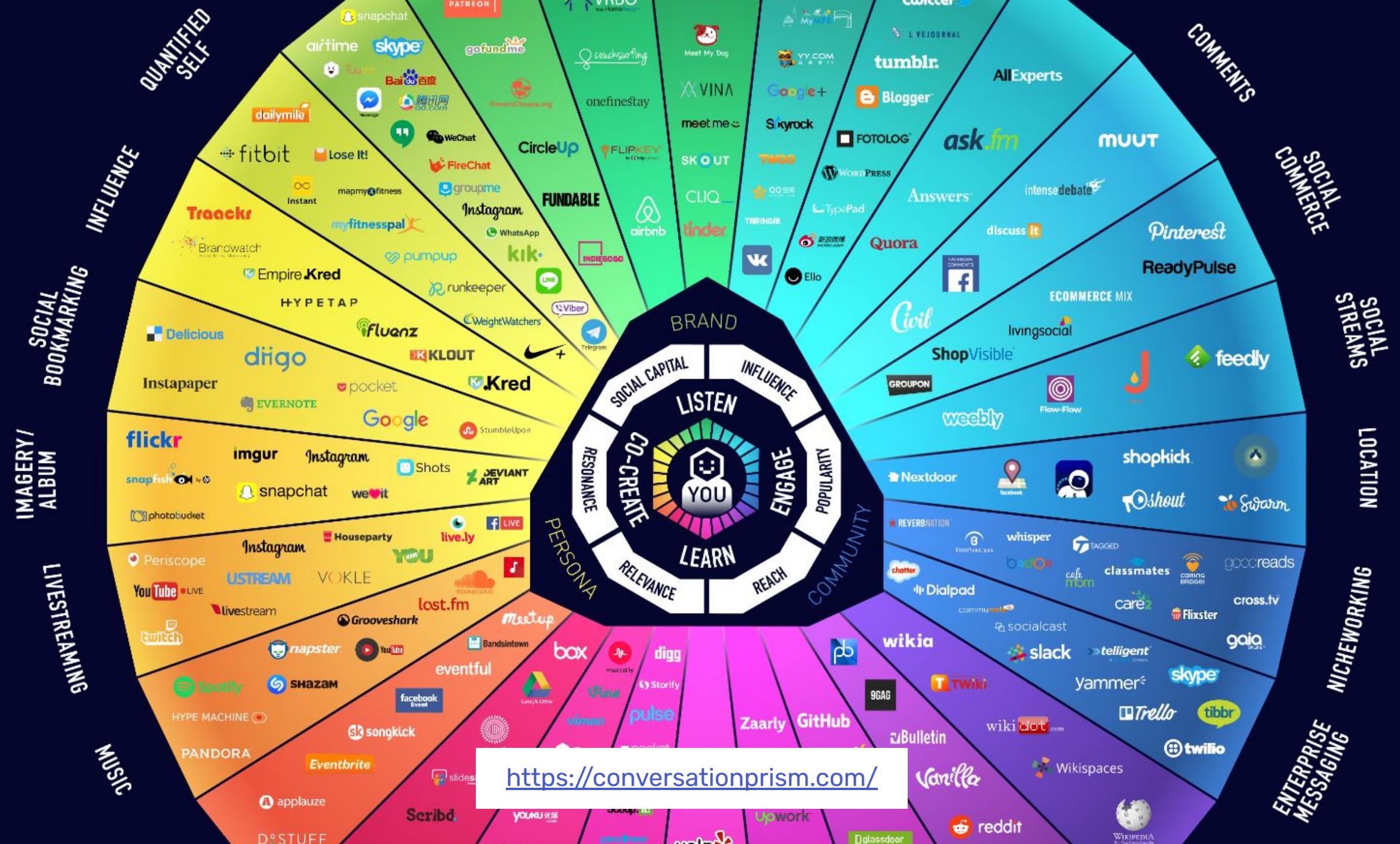
 @Salaheldinaz



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



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





2

What They Finding Online !



What They Finding Online !

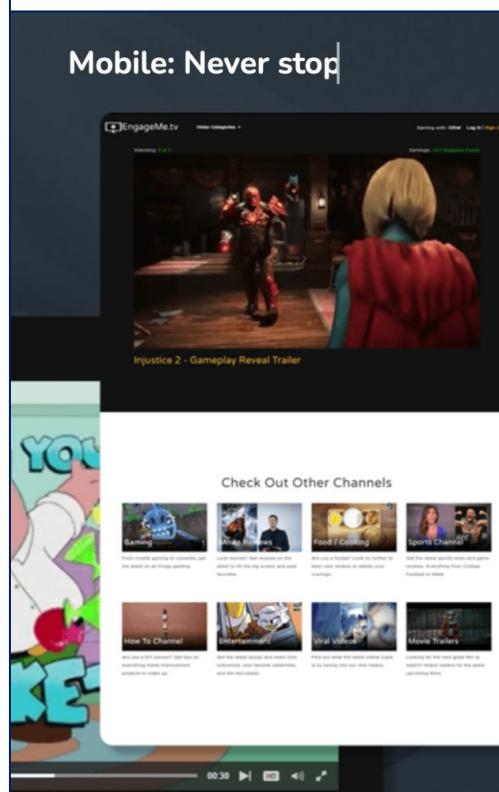
OnlyFans  @onlyfans Jun 5

It's the king of #dippydippy himself 😇 Comedian and food reviewer @upperfeast aka Anthony O'Connell is back with tips on how to keep your audience hungry for more! 🍔Anthony highlights why it's important to be yourself, be authentic, and get "all up in them stats!" 📈 So head over and join him at: onlyfans.com/upperfeast



@UPPERFEAST

Mobile: Never stop



Get paid to watch videos! Free bitcoins for watching short videos, paid instantly to your [FaucetHub](#) address.

Earn 2X Payouts

OR

Earn 1X Payouts

Instant payments via
FaucetHUB



What They Finding Online !

killme says Friends ::

I can't believe that until now after about 3 years of being friends with them, they're the only ones who had stayed. The same ones who I had spent a long time not talking to, yet they're still here for me. Why haven't I noticed sooner? Now I'm scared to lose them more than ever.

⌚ 4h 🗣 0 🎨 5

Anonymous says Friends ::

Sometimes I want friends, but then I actually get to know people and I'm cured.

⌚ 5h 🗣 0 🎨 6

Anonymous says Friends ::

Waited like 3 hours for my friend to come get food i was gonna give her. So frustrated because it took so long. Like

Teen Chat 🙄🙄🙄

Anely
Truee
I am also not good at engaging conversation

Scroll up for more messages

Teen Chat 🙄🙄🙄

Welcome to teen chat. 13-19 Only

JOIN CHAT ⓘ

LGBTQ [Social Cause]

Official LGBTQ chat room on Y99 🌈

JOIN CHAT ⓘ

Filipino room

Official room for users from the Philippines.

Topic - 🥰

JOIN CHAT ⓘ

🔎 ⏮

- E** Edward60 Curious older than 6...
- O** Oliverr. ...
- C** CathyH Hey guys i'm 5'5",11...
- Sherlin123** Hey! I'm Sherlin 95...
- DragonSlayer3.0** ...
- Joelflash_** ...
- Adrian1616** Hey I'm Adrian and I...
- Aphy** Taken by 95...
- _Ben** Busy Painting with a...
- Perside0013** Bi 13yo girl...



What They Finding Online !

The screenshot shows a typical Omegle chat session. On the left, there's a small video thumbnail of a young girl with dark hair and a hoodie, with the Omegle logo overlaid. On the right, there's a larger video thumbnail of another user, a young woman with glasses and a grey hoodie, smiling. The main text area shows a conversation:

You're now chatting with a random stranger. Say hi!
You both like japan, asian, korea, and kpop.

Stranger: hey
You: Hii
Stranger: youre cute
You: how've you been?
You: it's christal
Stranger: can you show me your tummy?
Stranger: please?

At the bottom, there are input fields with "Really?" and "Send" buttons, and a "Mouseover for options" link.

What They Finding Online !





3

Finding The Unknown

Finding The Unknown

1

Using
search
engines

Free Online Chat Room for Kids & Teens | Teen Chat Room

👉 <https://www.kidzworld.com/chat>

Perfect for after school, on weekends, or in your spare time, our online chatroom is a fantastic opportunity to make new friends and have fun with kids like you. Teens and kids chat online and ...

Kids Chat Rooms no Registration

👉 <https://yesichat.com/best-kids-chat-free-online-chat-room>

Yahoo chat rooms 2017 is a quite popular search term in google search results. Yahoo chat rooms were Marvelous and indeed a great time killer chat app. Recently people have been looking for yahoo chat rooms all over the web. Yahoo chat rooms are wonderful and

Anonymous chat school



visit from time to time; which ones you will constantly participate in (and which ones you should avoid altogether);

Kids Chat - Free Online Chat Rooms for Youths

Finding The Unknown

2 Lists, Collections



Finding The Unknown

3 Mobile Apps Stores



Apple



Google



Huawei



Amazon



Microsoft

Finding The Unknown

The screenshot shows the Google Play Store interface. The left sidebar is open, showing options like 'My apps', 'Shop' (which is selected), 'Games', 'Kids', 'Editors' Choice', 'Account', 'Payment methods', 'My subscriptions', 'Redeem', 'Buy gift card', 'My wishlist', 'My Play activity', and 'Parent Guide'. The main content area displays the 'Top free apps' section with six rows of icons. Each row contains two app cards. The visible apps include: Row 1: Voilà AI Artist - Photo Wemagine.AI (5 stars), TikTok (5 stars), Google Pay: A safe Google LLC (5 stars). Row 2: Snapchat (5 stars), ZOOM Cloud Meeti zoom.us (5 stars), Cash App Square, Inc. (5 stars). Row 3: HBO max (5 stars), Instagram (5 stars), WhatsApp (5 stars). Row 4: Disney+ (5 stars), Facebook Messenger (5 stars), PRENDE TV CINE-TV GRATIS (5 stars). At the bottom of the screen, there is a green bar with the URL <https://play.google.com/store/apps/top>.

Finding The Unknown

HUAWEI AppGallery

Featured Categories Top Search apps/games Download AppGallery

Categories

Apps Games

News & reading Business Cars Social Education Finance Food & drink Kids Lifestyle Entertainment
Navigation & transport Personalized themes Photo & video Shopping Sports & health Tools Travel

Social

 Teamstuff ★★★★★ Social Simplify your life - get teamstuff today; less w... Install	 BonBon ★★★★★ Social Ignite the spark with our app! Find your love a... Install
 HuaweiVR Phone ★★★★★ Social Install	 Communicate with Dogs ★★★★★ Social App that plays dog barking sounds to commu... Install

<https://appgallery.huawei.com/>

Finding The Unknown

Top Apps Overview Level Up Rankings Search for any app

Market iOS ▾ Country United States ▾ Category Overall ▾ Device iPhone ▾

Free Paid Grossing

Rank	App	Developer
1	TikTok	TikTok Pte. Ltd.
2	YouTube: Watch, Listen, Str...	Google LLC
3	Snapchat	Snap, Inc.
4	Instagram	Instagram, Inc.
1	Minecraft	Mojang
2	HotSchedules	HotSchedules
3	Heads Up!	Warner Bros.
4	Bloons TD 6	Ninjutsu Games
1	YouTube: Watch, Listen, Str...	Google LLC
2	Roblox	Roblox Corporation
3	Tinder - Dating New People	Tinder Inc.
4	Clash of Clans	Supercell

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

Finding The Unknown

Top Ranked iOS App Store Apps

Browse the top apps in every category and every country, updated every hour.

 iOS  Google Play  Amazon  Mac  Apple TV  iMessage

COUNTRY DEVICE CATEGORY

 United Kingdom ▾ iPhone ▾ Top Overall ▾

Top 1,000 Apps Updated an hour ago

Free

 1. NHS App
Free · NHS Digital >

 2. ITV Hub: TV P
... >

Paid

 1. Driving Theory Test 4 in 1 Kit
£4.99 · Focus Multimedia >

Grossing

 1. Tinder - Dating & New Friends
Free · Tinder Inc. >

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

Finding The Unknown

4 Apps Comparisons/Reviews

The screenshot shows the AlternativeTo.net homepage with a search bar at the top. Below it, there's a large logo for "AlternativeTo" with the subtitle "CROWDSOURCED SOFTWARE RECOMMENDATIONS". The main content area displays a list of alternatives to Omegle, with "Chatroulette" being the first item. The page includes navigation links like "Home", "Social & Communications", "Omegle", and "Alternatives".

The screenshot shows the Chatroulette page on AlternativeTo.net. It features a large "CR" icon with a heart count of 96. The page describes Chatroulette as an online tool for meeting new people through text, WebCam, and Mic. It includes a "Warning" section about potential risks for children. Below this, there's a comparison section titled "WeChat vs Omegle" with pros and cons, and several user comments. The WeChat logo is shown next to the comparison section.

Chatroulette Is this a good alternative? Yes No

Chatroulette is online tool that let you meet new people: the website start a chat with a random visitor and the user can communicate with him through text, WebCam and Mic.

Most users think Chatroulette is a great alternative to Omegle.

WeChat

VOIP service by Tencent that can make free video and voice calls no matter where you are.

Some users think WeChat is a great alternative to Omegle, some don't.

WeChat vs Omegle
pros, cons and recent comments

The point of Omegle is not having social networking and just talking to random strangers. WeChat is a social network and does not have an option to talk with random strangers.
Negative comment • over 3 years ago

WeChat has a function to chat with random nearby people
Positive comment • over 2 years ago

you can talk with youtubeers
Positive comment • about 3 years ago

<https://alternativeto.net/>

Finding The Unknown

5
Games
Platforms



Xbox



Nintendo



PlayStation

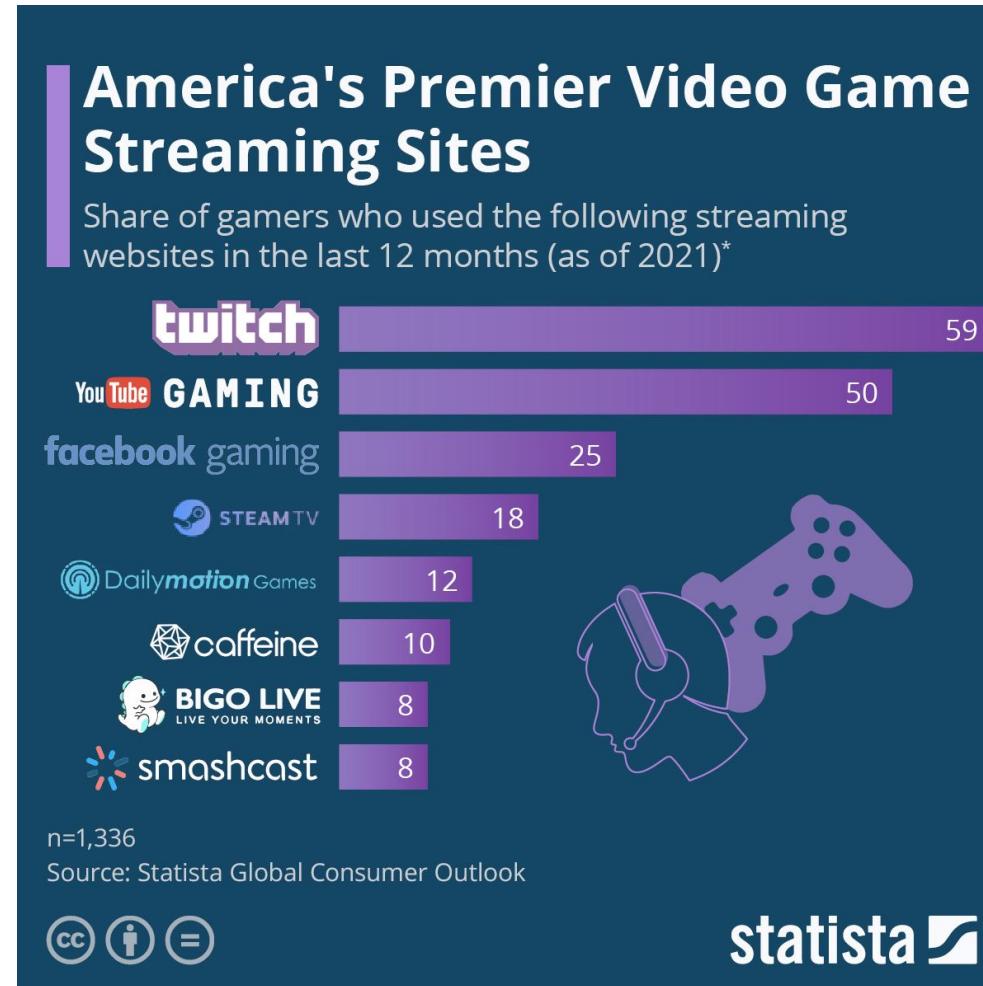


PC Gaming



6 Games Streaming

Finding The Unknown



Finding The Unknown

7 Gamers Communities

Site Name	Forum/Community URL or main URL	user URL format	user si	login t	location	birthd	join ds	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		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/											site:devfor.com/intext:username
RPG	https://forum.rpg.com/											site:forum.rpg.com/intext:username

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

The Most Interesting One



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

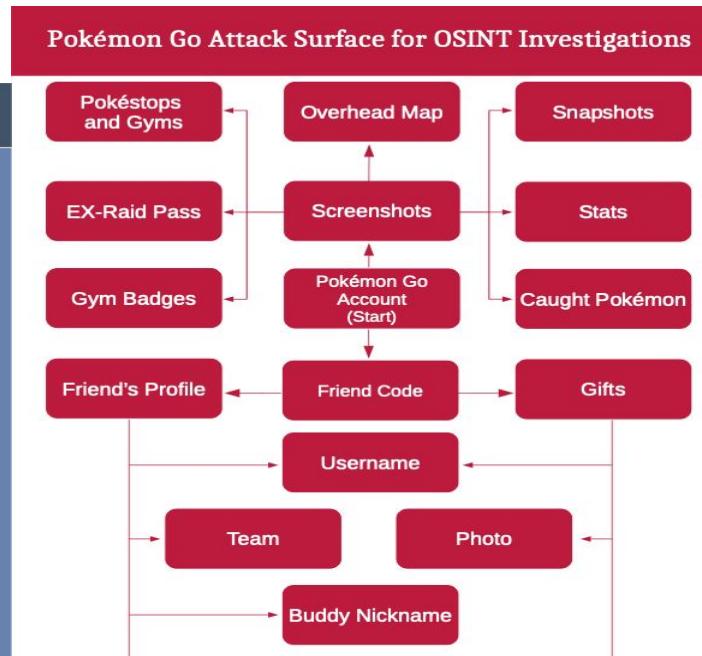
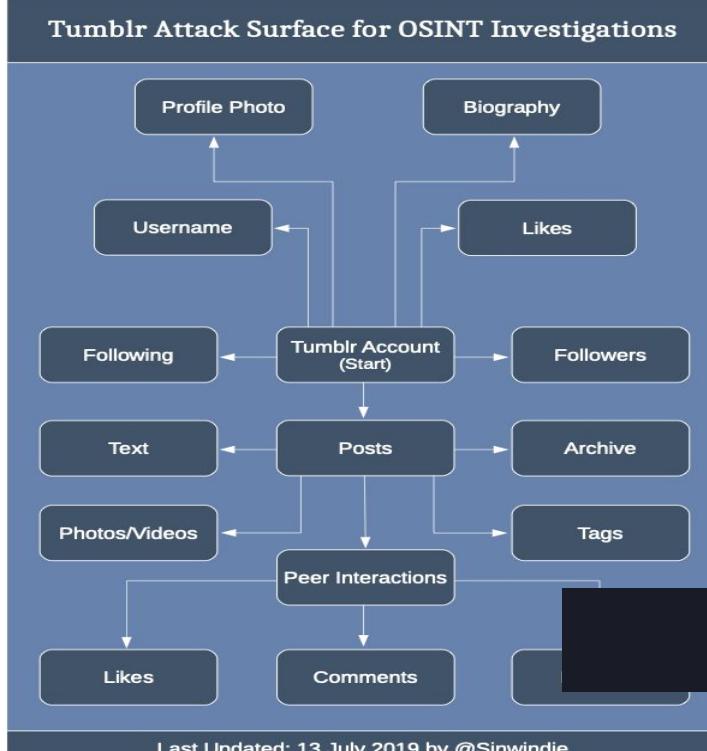
What They Share

- 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

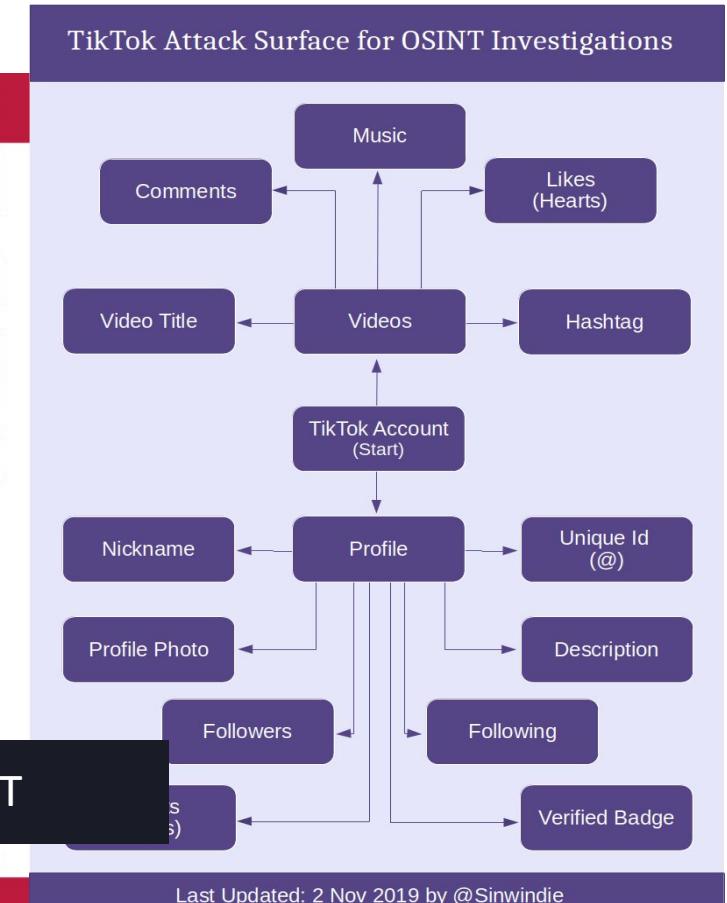
Privacy
Research

What They Share

Flowcharts



<https://github.com/sinwindie/OSINT>



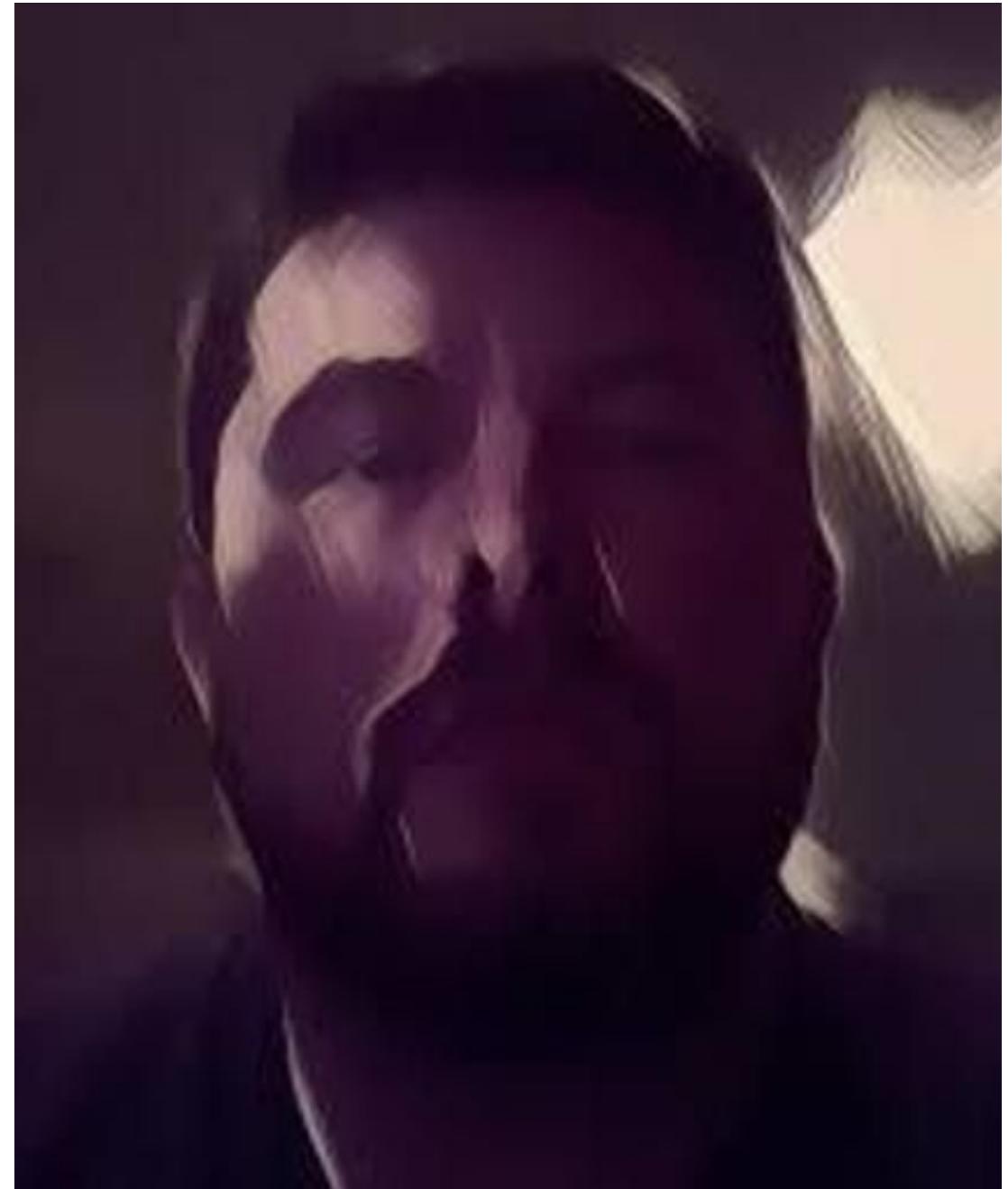
Darknet...



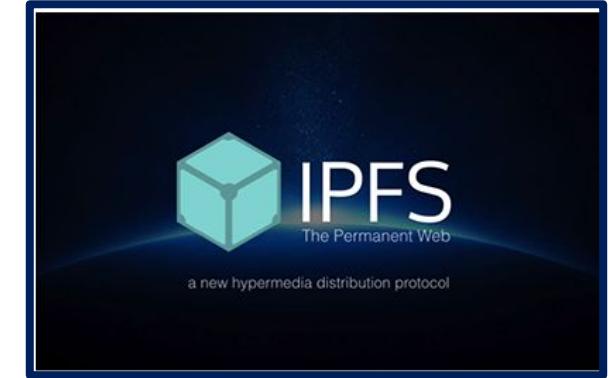
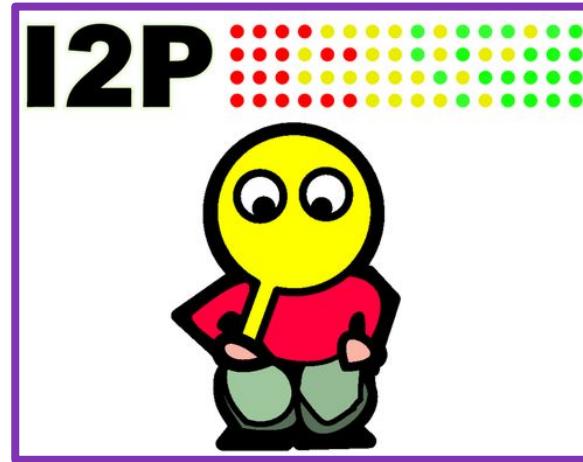
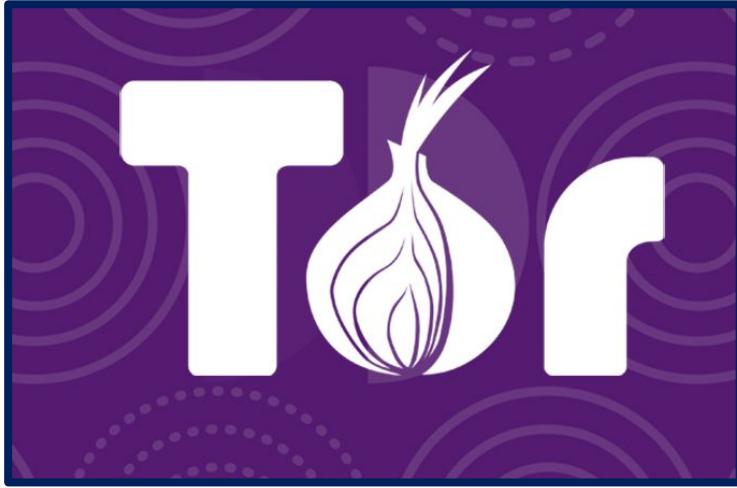
Michael James

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.onion.en	200	OnionDir
x2btcvwtemaqaoa2.onion.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
caseygd6ledkxai.onion.en	200	OnionDir
infantilefb6ovh4.onion.en	200	Infantile - No Rules Communications



HTTP ARchive format - HAR files

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

The screenshot shows the Network tab in the Chrome DevTools. It lists various JavaScript files and their URLs. A context menu is open over the entry for 'detectmobilebrowser.js', showing options like 'Copy', 'Save All As HAR', 'Resend', 'Edit and Resend', 'Block URL', 'Open in New Tab', 'Open in Debugger', 'Start Performance Analysis...', and 'Use as Fetch in Console'.

File	URL
ipvr6ydeg6t... detectmobilebrowser.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... mystickymenu.min.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... jquery.blockUI.min.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... add-to-cart.min.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... js.cookie.min.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... woocommerce.min.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... cart-fragments.min.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... skip-link-focus-fix.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... global.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... jquery.scrollTo.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... comment-reply.min.js	http://wth474sv6ct4glwiowjip
ipvr6ydeg6t... wp-embed.min.js	http://wth474sv6ct4glwiowjip

The screenshot shows the Google Admin Toolbox HAR Analyzer. It displays a timeline of network requests. A specific request is highlighted: [18:41:41.466] CASH CARDS - Hacker Financial Service - Buy Cloned Cards - Buy credit card sale - Cloned cards buy. The request details show a GET method to http://tbx3wt4fkwqr67xzuahvmuolqjsnqxvylz76kfehtasqal3qzbe4cid.onion/. The request headers include:

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.5
- Cache-Control: no-cache
- Connection: keep-alive
- Cookie: _ga=GA1.2.2142442438.1624300765; _gid=GA1.2.373317324.1624300765; RVC=1; RVCW=1624300811
- Host: tbx3wt4fkwqr67xzuahvmuolqjsnqxvylz76kfehtasqal3qzbe4cid.onion
- Pragma: no-cache
- Upgrade-Insecure-Requests: 1

QOMPLX:CYBER

```
--<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

CASH CARDS

cashcards@secmail.pro

27.01.2021 BY RREVERSII

Hello World!

Welcome to WordPress. This is your first post. Edit or delete it, then start creating!

```
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"
```

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

```
from: "response_body"
identifier_type: "btc_address"
identifier: "1FWrm3Z1g2W4kEQXgsUyHxEk2S9dTVK54P"
created_at: "2021-06-21T17:30:13.000000Z"
```

All credit for this tool goes to:



Doctor Chaos

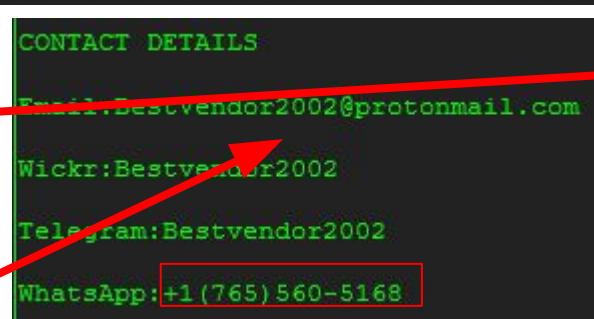
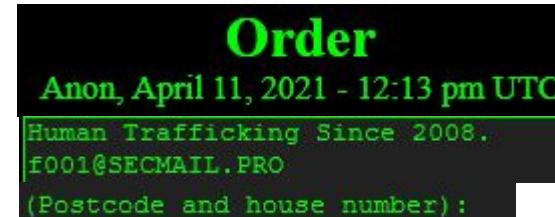
@ChaosD0c Follows you

Onion cartographer & lover of #OSINT, #HUMINT & #SIGINT

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





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 ID : jilavyanlavrent22@mail.ru
2 Password : Click789

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>

Giapne's Store

Le Hoang Giap

NETFLIX	GIA BẢN	
1 Slot/Tháng	60	
5 Slot/Tháng	200	
Spotify	GIA BẢN	
1 Tháng	20	
1 Năm - Chính Chủ	150	
2 Năm - Chính Chủ	250	
Lifetime - Chính Chủ	Liên Hệ	
YouTube	MAIL MỚI MAIL CŨ	
1 Tháng	20	35
3 Tháng	100	
ELSA	GIA BẢN	
1 Năm	100	
Lifetime	150	
grammy	GIA BẢN	
6 Tháng	100	
1 Năm	200	(bảo hành 3 năm cho gói Lifetime)

Le Hoang Giap - August 29

iOS Services

Game iOS	20/50/70
App Chính Ánh iOS	20/50/70
Tiền Ich iOS	20/50/70
Apple Music - 1/3/6 Tháng	50
Apple Arcade - 1 Tháng	30
Nạp Game iOS Giá Tốt	Liên Hệ
Hoàn Tiền Nạp Game	Liên Hệ

Mua ID Apple C6

Bán ID Tất 2 Lớp

Canva

Google Drive

Le Hoang Giap

Hoang Ngoc An Check inbox

Nguyen Tien Sy Rep

Write a comment...

Le Hoang Giap

@giapnew

Private.

facebook.com/giapnew

Archived February 2016

37 Following · 6 Followers

Not followed by anyone you're following

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



BlueLeaks Modified: Yesterday, 11:23 PM

Add Tags...

▼ General:

Cincinnati Police Exploit Working

XGHOSTSECx MAY 31ST, 2020 58 NEVER

Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

text 8.68 KB

raw download clone embed print report

```
1. Cincinnati Police Exploit Working
2. #Anonymous #GhostSec
3. Vulnerability>
4. <ID>660858</ID>
5. <Name>Cross Site Scripting in http://ci.minneapolis.mn.us </Name>
6. <Date>2020-05-31T16:06:49.597Z</Date>
7. <Type>Cross Site Scripting</Type>
8. <CWE-ID>CWE-79</CWE-ID>
9. <CVE-ID/>
10. <CVSSv3>6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]</CVSSv3>
11. <Risk>MEDIUM</Risk>
12. <URL>http://ci.minneapolis.mn.us </URL>
13. 170.159.2.38 & 5
14. Some HTTP headers related to security and privacy are missing or misconfigured.
15.
```

PASTEBIN GO PRO API TOOLS FAQ + paste

XGHOSTSECx's Pastebin

674 5,852 172 DAYS AGO

NAME / TITLE	ADDED	EXPIRES	HITS	SYNTAX
JOHN RATTCLIFF	Sep 7th, 2020	Never	60	None
Facebook intelligence	Aug 14th, 2020	Never	71	HTML
CHILD PORN VIRTUAL HARD DISKS (NOW HONEYPODS)	Aug 14th, 2020	Never	12	None
Pedo emails	Aug 14th, 2020	Never	22	None
EY.COM EXPLOITS	Aug 9th, 2020	Never	76	None

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

2020-04-11 04:22:31 COVID course request from , 3720 phone: 3833 title: 3676 agency:3701	community.net phone: 3833 title: 3676 agency:3701
2020-04-11 04:26:22 COVID course request from	3662 title: 3663 agency:3693
2020-04-11 04:26:22 COVID course request from	812 title: 3663 agency:3691
2020-04-11 04:26:23 COVID course request from	98589959 title: Clinical Supervisor agency:YWCA
2020-04-11 07:43:12 COVID course request from	56 title: Crime Scene Specialist agency:Scottsdale Police Dept.
2020-04-11 07:43:12 COVID course request from	5754333322 title: Victim Advocate agency:The Phoenix House Sexual Assault & Domestic Violence Resource Center
2020-04-11 07:43:13 COVID course request from	horizon.org phone: 3473878024 title: Social Worker agency:Safe Horizon
2020-04-11 07:43:13 COVID course request from	555-666-7777 title: Officer agency:TRN
2020-04-11 07:47:15 COVID course request from	one: 555-222-1212 title: Officer agency:TRN
2020-04-11 08:06:31 COVID course request from	unity.net phone: 666-678-1234 title: Officer Test agency:TRN
2020-04-11 09:23:18 COVID course request from	community.net phone: 888-999-0303 title: Title TESTING agency:TRN
2020-04-11 09:27:58 COVID course request from	org phone: 2025072230 title: Case Manager agency:ShelterHouse
2020-04-11 09:30:30 COVID course request from	olicecommunity.net phone: 123-456-7889 title: Testing agency:TRN
2020-04-11 09:30:30 COVID course request from	21 title: Lieutenant agency:Manassas City PD
2020-04-11 11:45:04 COVID course request from	community.net phone: 666-123-7890 title: Officer Title agency:TRN
2020-04-12 12:15:33 COVID course request from	042315264 title: Police Officer II agency:UNO Police Department
2020-04-12 02:30:32 COVID course request from	.gov phone: 520-761-7869 title: Deputy agency:Santa Cruz County Sheriff’s Office
2020-04-12 04:30:32 COVID course request from	6207617869 title: Deputy agency:Santa Cruz County Sheriff’s Office
2020-04-12 04:45:32 COVID course request from	title: Deputy agency:Santa Cruz County Sheriff’s Office
2020-04-12 05:30:32 COVID course request from	8476584531 title: Sergeant agency:Algonquin Police Department
2020-04-12 06:00:32 COVID course request from	worker agency:Asian American Community Services
2020-04-12 09:00:33 COVID course request from	4325 title: NCO IC 29 Military Police Flight agency:Canadian Forces Military Police
2020-04-12 09:35:32 COVID course request from	1473 title: Police Officer agency:University of North Carolina Police Department
2020-04-12 10:45:32 COVID course request from	645 title: Executive Director agency:Pueblo Child Advocacy Center
2020-04-12 12:15:32 COVID course request from	rg phone: 6096466767 title: DVRT/Court/Legal Services Coordinator agency:Avanzar (formerly known as The Womens Center)
2020-04-12 02:10:32 COVID course request from	7029001 title: Crisis Worker agency:Terros
2020-04-12 03:20:32 COVID course request from	title: RN agency:Medical Solutions
2020-04-12 07:40:32 COVID course request from	3 title: Womenâ€™s Safety Coordinator agency:Office of Victim Services
2020-04-12 09:15:32 COVID course request from	om phone: 2164017022 title: Victim Advocate, PI Intern, Consultant agency:GAW Investigations; Innovative Solutions
2020-04-12 09:30:32 COVID course request from	2 title: volunteer agency:Victim Outreach, Inc.
2020-04-12 09:30:32 COVID course request from	7033 title: Family Nurse Practitioner agency:ARH Healthcare
2020-04-12 09:45:32 COVID course request from	ne: (917)685-0914 title: License Clinical Social Worker agency:Catapult learning/LCSC
2020-04-12 09:45:33 COVID course request from	892 title: Groundwork Evening Coordinator agency:Guardian Angel Community Services
2020-04-12 10:15:32 COVID course request from	5023458119 title: Sexual Assault Outreach Coordinator agency:The Center for Women and Families
2020-04-12 11:15:32 COVID course request from	2 title: Training Coordinator agency:Muscogee (Creek) Nation Lighthouse
2020-04-13 02:15:32 COVID course request from	one: 720-358-1474 title: Victim Services Intern Program Coordinator agency:Colorado Organization for Victim Assistance
2020-04-13 11:25:33 COVID course request from	hone: 3045233447 title: Victim Advocate agency:CONTACT Rape Crisis Center
2020-04-13 11:40:32 COVID course request from	51116 title: Captain agency>New Providence PD
2020-04-13 11:40:32 COVID course request from	157151564 title: Detective Lieutenant agency:Vanderbilt University Police Department
2020-04-13 11:40:33 COVID course request from	61116 title: Captain agency>New Providence PD
2020-04-13 11:40:33 COVID course request from	61116 title: Captain agency>New Providence PD
2020-04-13 11:55:33 COVID course request from	520-761-7869 title: Deputy Sheriff agency:Santa Cruz County Sheriff’s Office
2020-04-13 12:05:32 COVID course request from	title: Residential Supervisor agency:Opportunities for Otsego
2020-04-13 12:10:33 COVID course request from	11 title: Sexual Assault Program Coordinator/EMT agency:The Domestic Violence Shelter/Firelands Ambulance Services
2020-04-13 12:20:32 COVID course request from	62-5340 title: Domestic Violence Liaison agency:Fearless
2020-04-13 12:20:33 COVID course request from	5183161506 title: RN SAFE agency:SPHP
2020-04-13 12:25:32 COVID course request from	40 title: Outreach Advocate agency:Blackburn Center
2020-04-13 12:45:32 COVID course request from	etective agency:UNCW Police Department



Any Questions?

Slides & Resources

<https://github.com/qomplx/ncptf2021>