

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

A black and white photograph of a computer mouse and a keyboard. In the background, a stamp with the words "TOP SECRET" is visible. Overlaid on the image is yellow text with a black outline.

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

# Darknet...



## Michael James

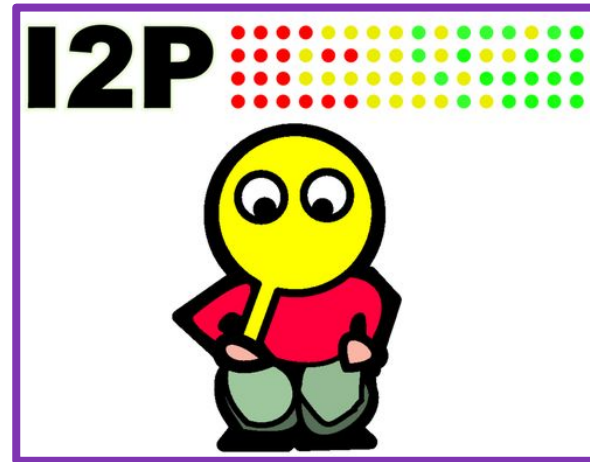
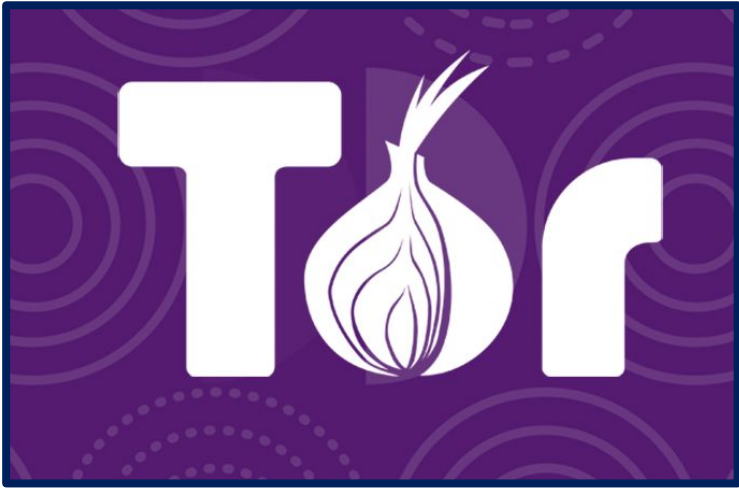
Principle OSINT Specialist  
QOMPLX Intelligence Unit

 @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

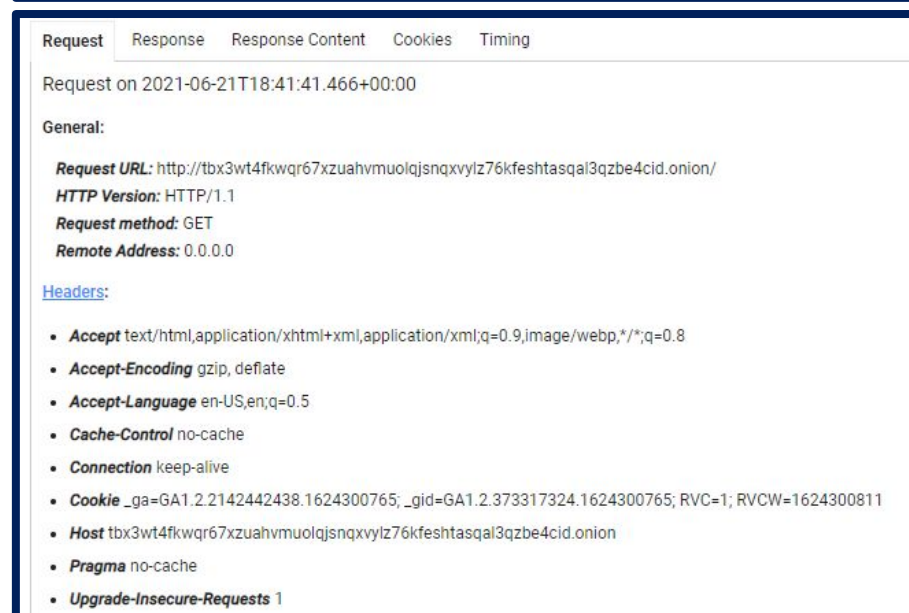
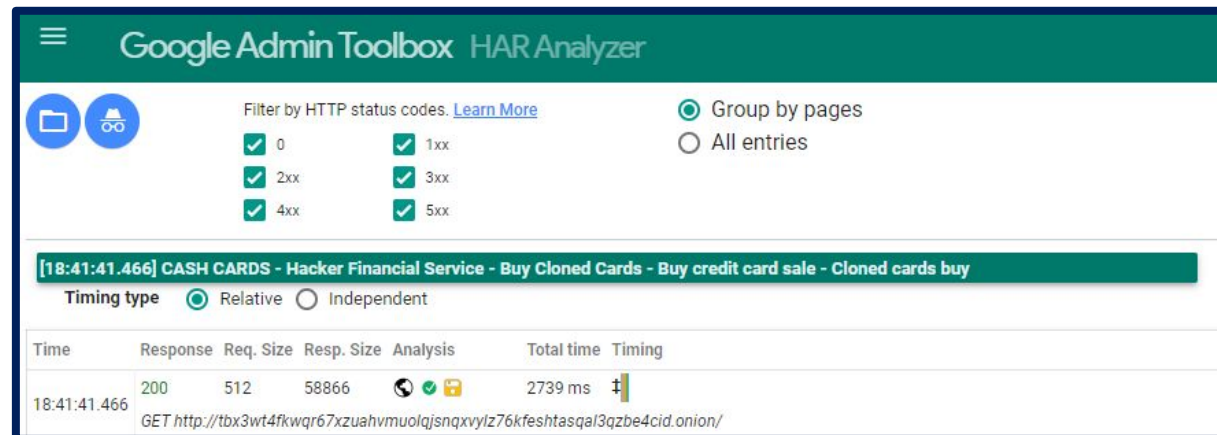
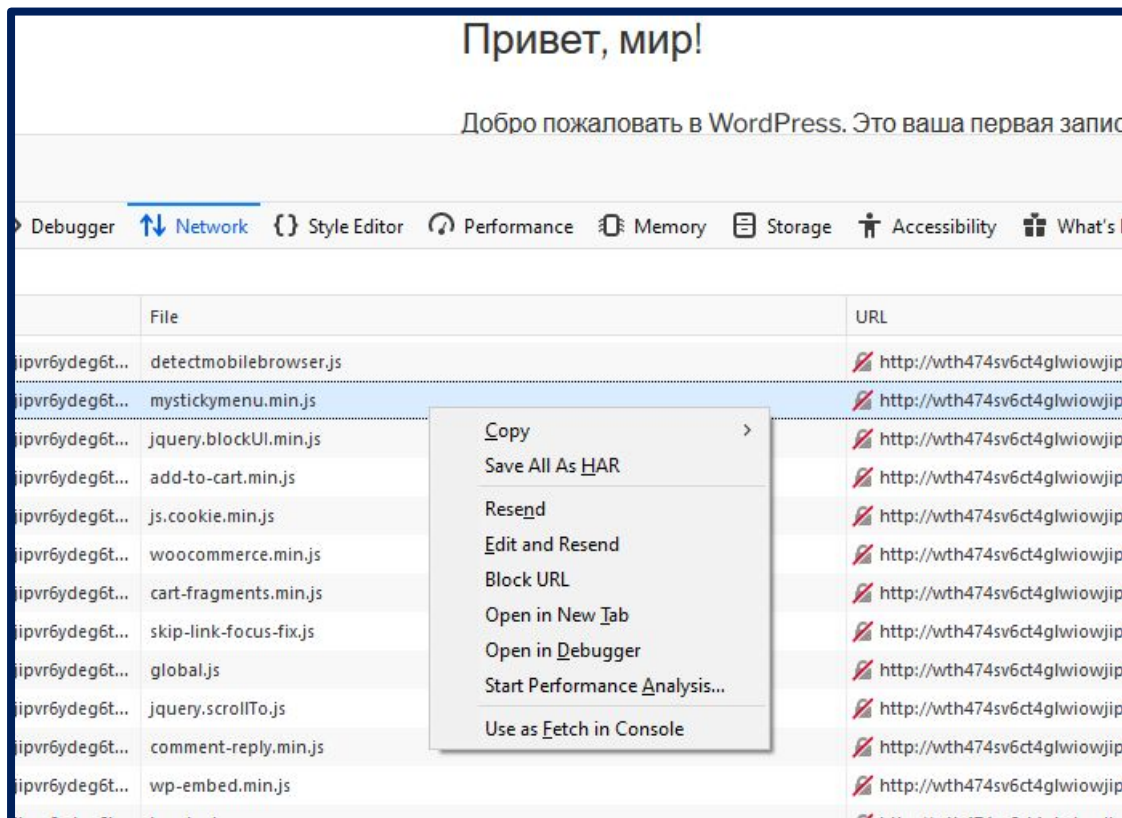
qd43byl2pgq5b7k3.onion	en	200	OnionDir
x2btcvwtemaqaoa2.onion	en	200	OnionDir - Adult
lt6ychu3k6fx3apu.onion	en	200	OnionDir
chemspain7iw2zby.onion	en	200	Store
svyagrufqojpw2ge.onion	en	200	OnionDir
7a5eaokoytoqpp6jgklwg5	en	200	Home   Towards Liberty
caseygdp6ledkxai.onion	en	200	OnionDir
infantilefb6ovh4.onion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





# HTTP ARchive format - HAR files

[https://toolbox.googleapps.com/apps/har\\_analyzer/](https://toolbox.googleapps.com/apps/har_analyzer/)



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

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

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!

# What else can we learn about these sites?

## OSINT PARTY!!

```
from: "response_body"
identifier_type: "email_address"
identifier: "webmaster@fcrdp3t6ngxksjcth7cmajhcubgpp72w45rwmo3hn5nz66odx2to6qd.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:



# 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



# 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 Dangl47@protonmail.com, Wickr @ Dangl47.

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

Bringinghurst, 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.aa3@list.ru	
Password: Zako3313	
ID by VK, collected by Le Hoang Giap	

1	🔥 Apple ID :jilavyanlavrent22@gmail.ru
2	🔥 Password 🗑️ :Click789
3	
4	ID by VK, collected by Le Hoang Giap

Email : giapnetwork@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

1 Slot/Tháng

5 Slot/Tháng

Spotify

1 Tháng

1 Năm - Chính Chủ

2 Năm - Chính Chủ

Lifetime - Chính Chủ

YouTube

1 Tháng

3 Tháng

ELSA

1 Năm

Lifetime

grammarly

6 Tháng

1 Năm

GIA BÁN

60

200

20

150

250

Liên Hệ

20

35

100

100

100

300

100

200

iOS Services

Game iOS

App Chính Ảnh iOS

Tiền Ich iOS

Apple Music - 1/3/6 Tháng

Apple Arcade - 1 Tháng

Nạp Game iOS Giá Tốt

Hoàn Tiền Nạp Game

Mua ID Apple C6

Bán ID Tất 2 Lớp

Canva

1 Tháng

1 Năm

1 Năm - Chính Chủ

Google Drive

Unlimited - 1 Năm

Unlimited - Lifetime

20/50/70

20/50/70

20/50/70

50

30

Liên Hệ

Liên Hệ

Liên Hệ

20

100

300

100

200

(Báo hành 3 năm cho gói Lifetime)

Le Hoang Giap

August 29

2 Comments

Like

Comment

Share

Hoàng Ngọc Ân Check inbox

Like · Reply · See Original (Vietnamese) · 4w

Translate All Comments

Nguyễn Tiến Sỹ Rep

Like · Reply · 5d

Write a comment...

Press Enter to post.

Le Hoang Giap

1 Tweet

Le Hoang Giap

@giapneee

Private

[tearbook.com/giapneee](https://tearbook.com/giapneee)


Joined February 2016

37 Following · 4 Followers

Not followed by anyone you're following

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





 **BlueLeaks** 253.52 G

Modified: Yesterday, 11:23 PM

Add Tags...

▼ General:


 **Cincinnati Police Exploit Working** SHARE TWEET


 XGHOSTSECX MAY 31ST, 2020 58 NEVER






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

text 0.68 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 = 0 </Name>
6. <Date>2020-05-31T16:06:49.597Z</Date>
7. <Type>Cross Site Scripting</Type>
8. <CVE-ID>CVE-79</CVE-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 = 0 </URL>
13. 170.159.2.30 = 5
14. Some HTTP headers related to security and privacy are missing or misconfigured.
```

 **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 HONEYPOTS)	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		
2020-04-11 04:26:22 COVID course request from		community.net phone: 3833 title: 3676 agency:3701
2020-04-11 04:26:22 COVID course request from		le: 3662 agency:3693
2020-04-11 04:26:23 COVID course request from		812 title: 3663 agency:3691
2020-04-11 07:43:12 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 07:43:13 COVID course request from		5754333322 title: Victim Advocate agency:The Phoenix House Sexual Assault & #038; 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 07:47:15 COVID course request from		e: 555-666-7777 title: Officer agency:TRN
2020-04-11 08:06:31 COVID course request from		one: 555-222-1212 title: Officer agency:TRN
2020-04-11 09:23:18 COVID course request from		unity.net phone: 666-678-1234 title: Officer Test agency:TRN
2020-04-11 09:27:58 COVID course request from		community.net phone: 888-999-0303 title: Title TESTING agency:TRN
2020-04-11 09:30:30 COVID course request from		org phone: 2025072230 title: Case Manager agency:ShelterHouse
2020-04-11 09:30:30 COVID course request from		policecommunity.net phone: 123-456-7889 title: Testing agency:TRN
2020-04-11 11:45:04 COVID course request from		21 title: Lieutenant agency:Manassas City PD
2020-04-12 12:15:33 COVID course request from		community.net phone: 666-123-7890 title: Officer Title agency:TRN
2020-04-12 02:30:32 COVID course request from		042315264 title: Police Officer II agency:UNO Police Department
2020-04-12 04:30:32 COVID course request from		z.gov phone: 520-761-7869 title: Deputy agency:Santa Cruz County Sheriff&#8217;s Office
2020-04-12 04:45:32 COVID course request from		5207617869 title: Deputy agency:Santa Cruz County Sheriff&#8217;s Office
2020-04-12 05:30:32 COVID course request from		title: Deputy agency:Santa Cruz County Sheriff&#8217;s Office
2020-04-12 06:00:32 COVID course request from		8476584531 title: Sergeant agency:Algonquin Police Department
2020-04-12 09:00:33 COVID course request from		orker agency:Asian American Community Services
2020-04-12 09:35:32 COVID course request from		4325 title: NCO IC 29 Military Police Flight agency:Canadian Forces Military Police
2020-04-12 10:45:32 COVID course request from		1473 title: Police Officer agency:University of North Carolina Police Department
2020-04-12 12:15:32 COVID course request from		545 title: Executive Director agency:Pueblo Child Advocacy Center
2020-04-12 12:55:32 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		1 title: Women&#8217;s Safety Coordinator agency:Office of Victim Services
2020-04-12 09:15:32 COVID course request from		pm 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: Licensed 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 Lighthorse
2020-04-13 02:15:32 COVID course request from		ne: 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		51116 title: Captain agency:New Providence PD
2020-04-13 11:40:33 COVID course request from		51116 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&#8217;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>