OSINT x UCCU
Open Source Intelligence

miaoski @ UCCU

2017.11.18

TREND MICRO™

Securing Your Journey to the Cloud

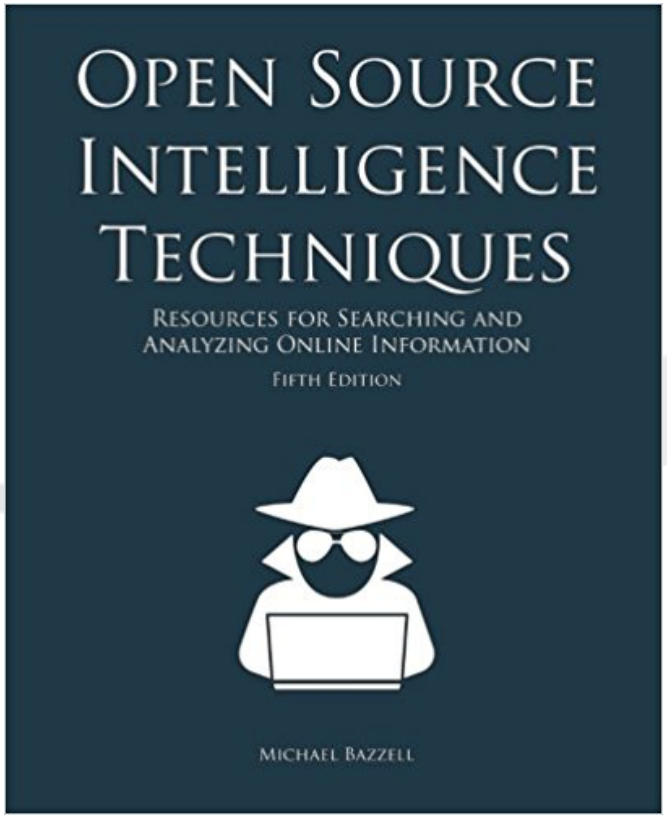
miaoski

- Senior threat researcher in Trend Micro
- Threat intelligence
- Smart City
- SDR
- Arduino, RPi, embedded

Outline

- Module 1: What is OSINT?
- Module 2: Using Search Engine
- Module 3: Social Media Profiling
- Module 4: Domain / IP Profiling

References



Michael Bazzell 5/e

林豐裕、李鎮宇、黃健誠、張佩嫈 編譯 4/e

https://inteltechniques.com/menu.html

Disclaimer

1. Sponsored by UCCU + ITRI
2. Respect privacy and laws
3. Make sure you know what you're doing
4. Be responsible

Before we start

- Download VirtualBox
- Download Tails or Buscador

- https://inteltechniques.com/buscador/index.html
- https://tails.boum.org/

Module 1
What is OSINT?

What is OSINT?

- 主體是人
- Reconnaissance of intelligence
- From publicly available information
- To address a specific intelligence requirement
- Newspaper, blog, search engine ...
- Government documents

- Often undervalued though significant

Why OSINT?

- New employee
- Criminal investigation
- Missing children / Runaway children
- Human trafficking
- Vandalism
- Stealing
- **NOT** to ~~manhunt~~ or SJW on Dcard / PTT / ...

正義魔人可以去
reddit.com/r/rbi

肉搜請洽
lionbug

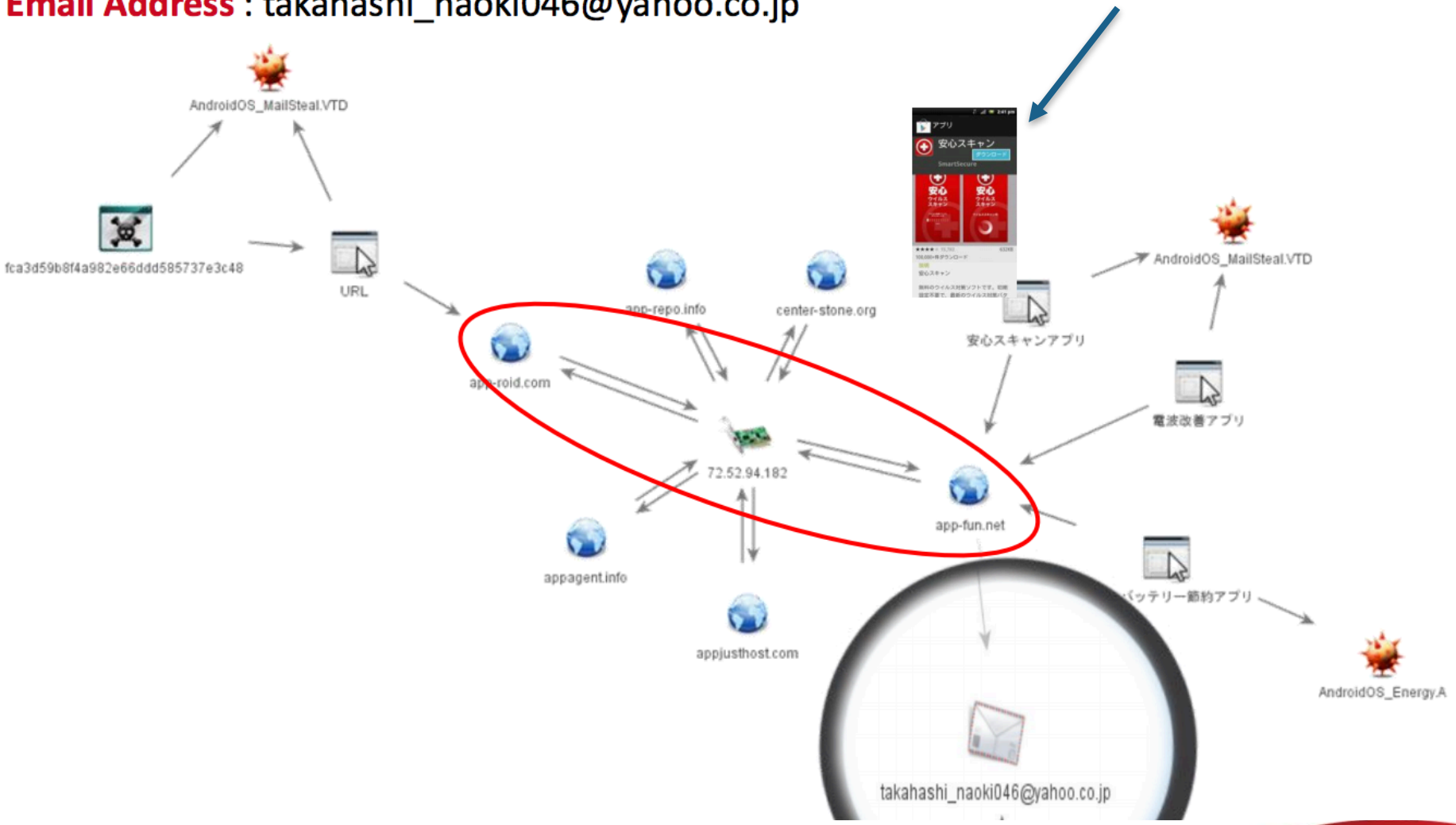
Dcard 請洽
lionbug

OSINT Includes but Not Limited to

- Location
- Real Name
- Online ID / group / community
- Phone number
- Email
- Credit card number / Bank account
- Date / Time
- Documents
- Domain / IP address
- URL

Example: Android Malware

Email Address : takahashi_naoki046@yahoo.co.jp



Example: Keylogger

حول المبرمج

Name : Ebrahim Said El-Sharawy

Work : Computer Programmer

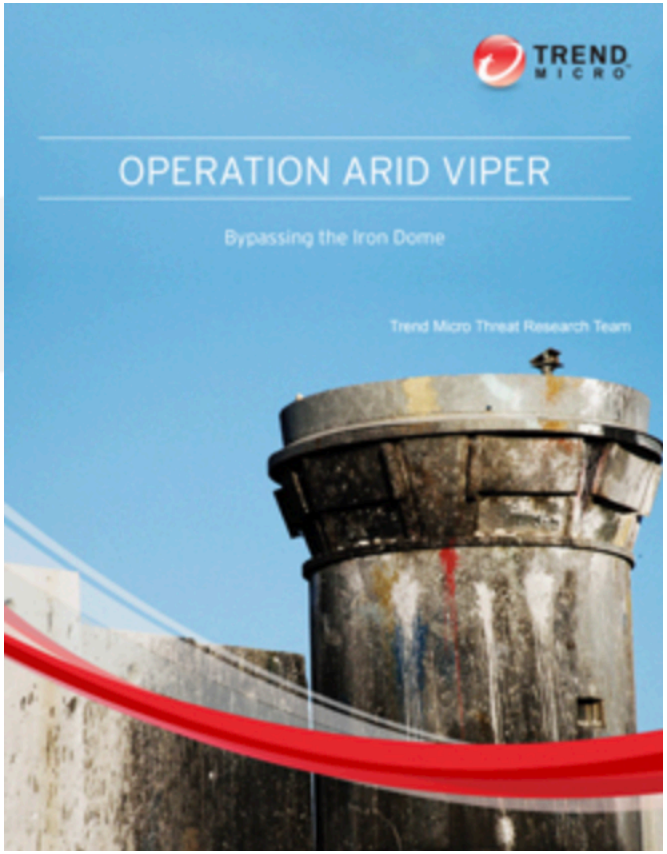
Date of Birth: July 23,1994

Mobile: +201285381220

E-mail: dev_hima@yahoo.com

Facebook: facebook.com/devhima

Twitter: twitter.com/dev_hima



Dev.Spy

الآن يمكنك حماية أبنائك من إستخدام المواقع الضارة

ومتابعة حاسوبك ومراقبته فى ذلك ... كل ذلك يتيحه لك برنامجنا الجديد المجاني

DevSpy !

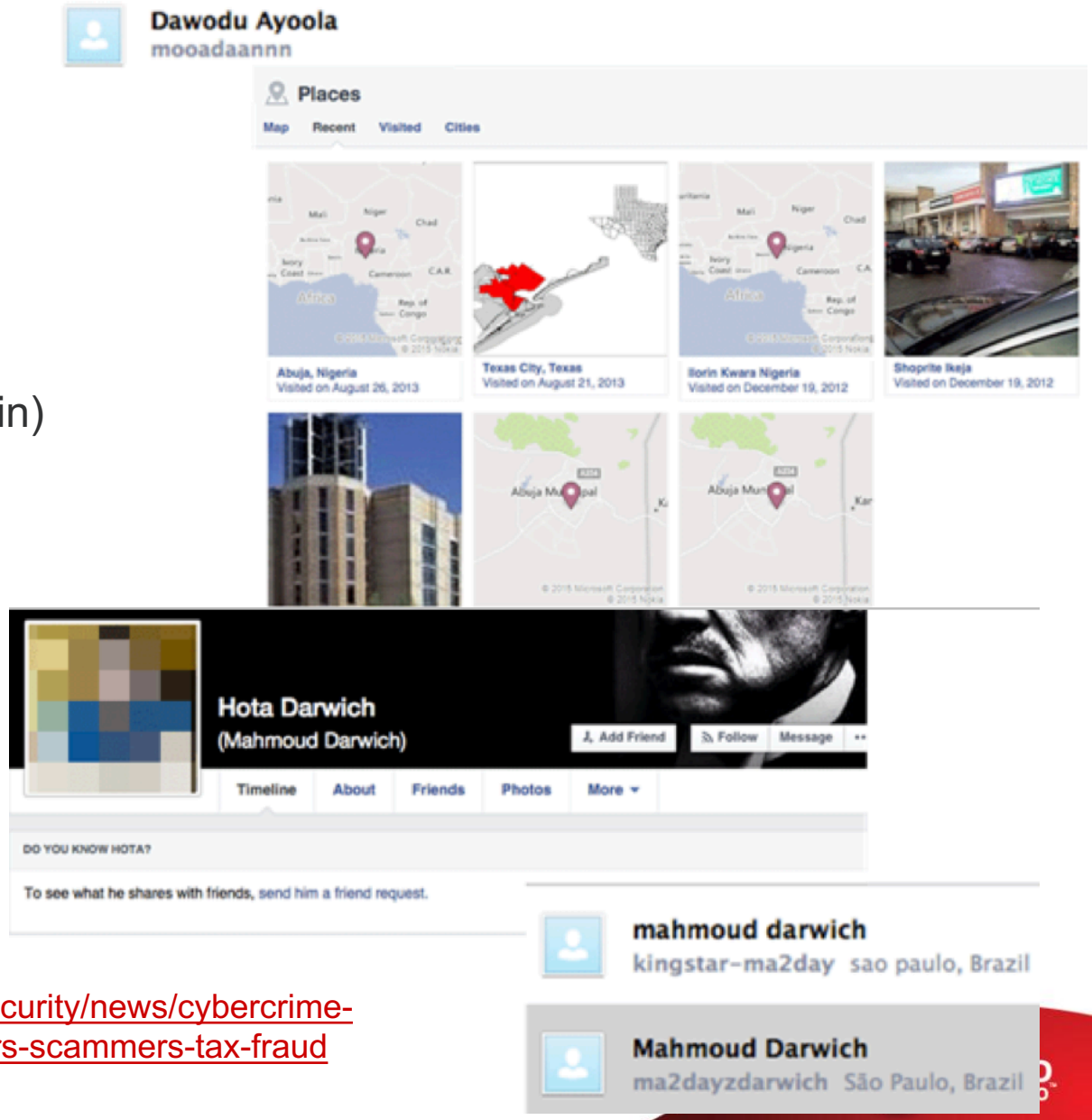
... نتمنى أن ينال إعجابكم

للتحميل

إضغط هنا

Example: from a Mutex

- Mutex: awdaw2214a
- ayool2day[.]biz
- born in 1984
- Lives in KL
- ma2dayzs[.]com (domain)



http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/staying-safe-from-irs-scammers-tax-fraud

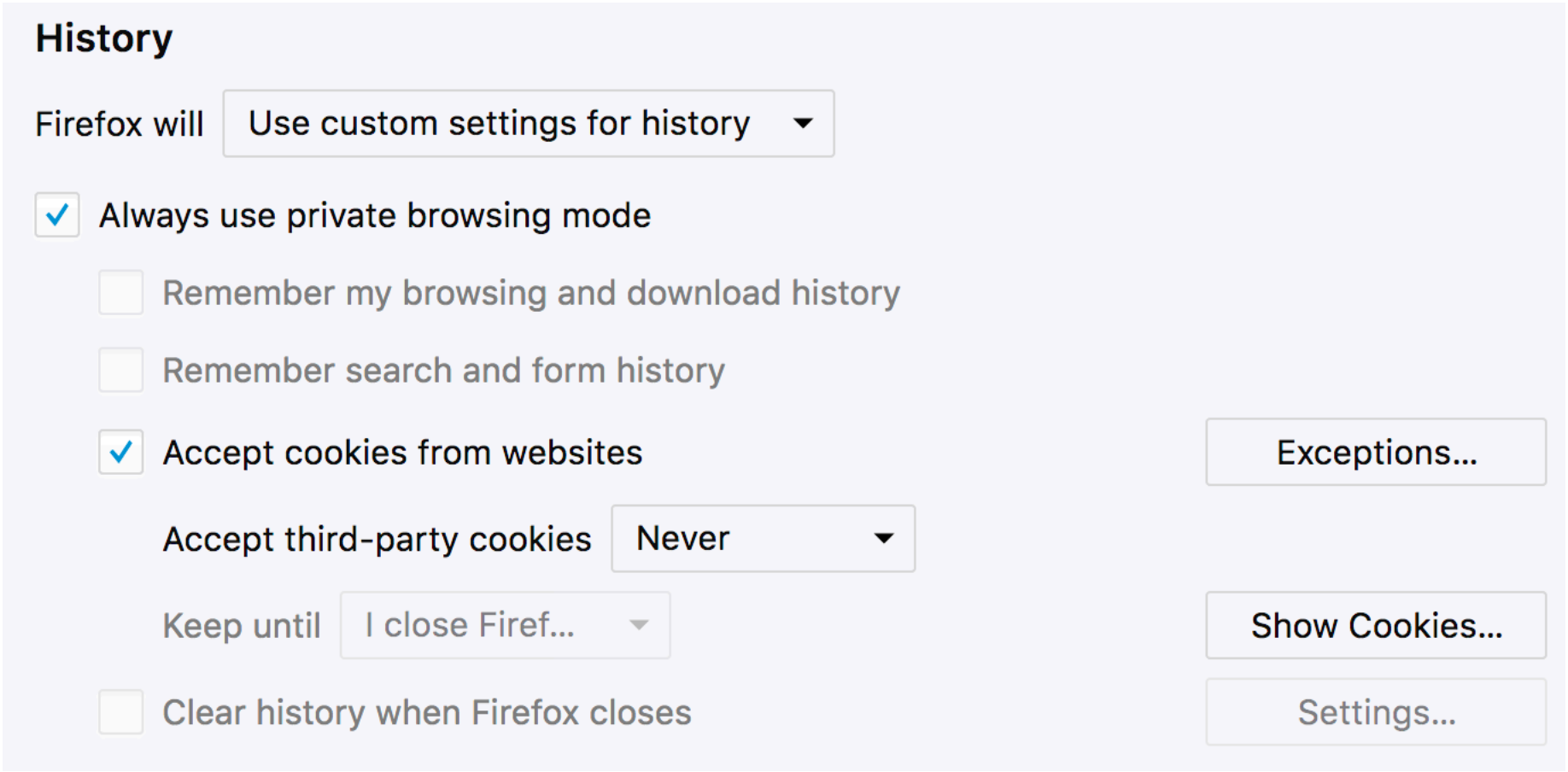
Protect Yourself! (1)

- Firefox plugins
- LiveUSB
- VM
  - Buscador
  - Tails
- VPN and/or Tor
  - PIA
  - NordVPN
  - ~~Hola!VPN~~

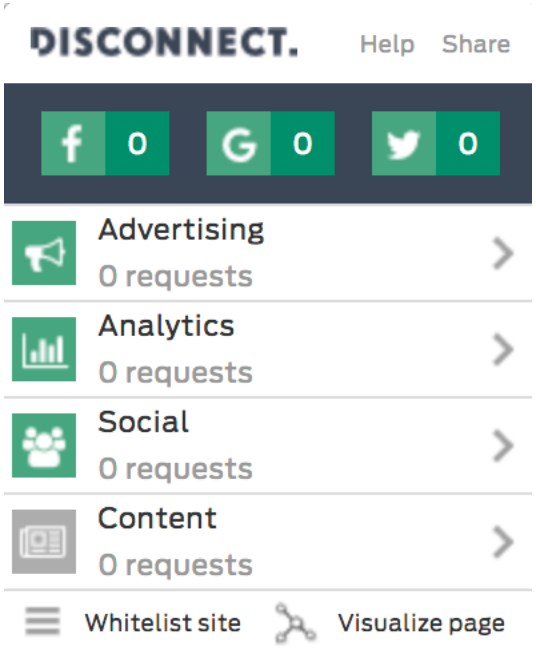
Protect Yourself! (2)

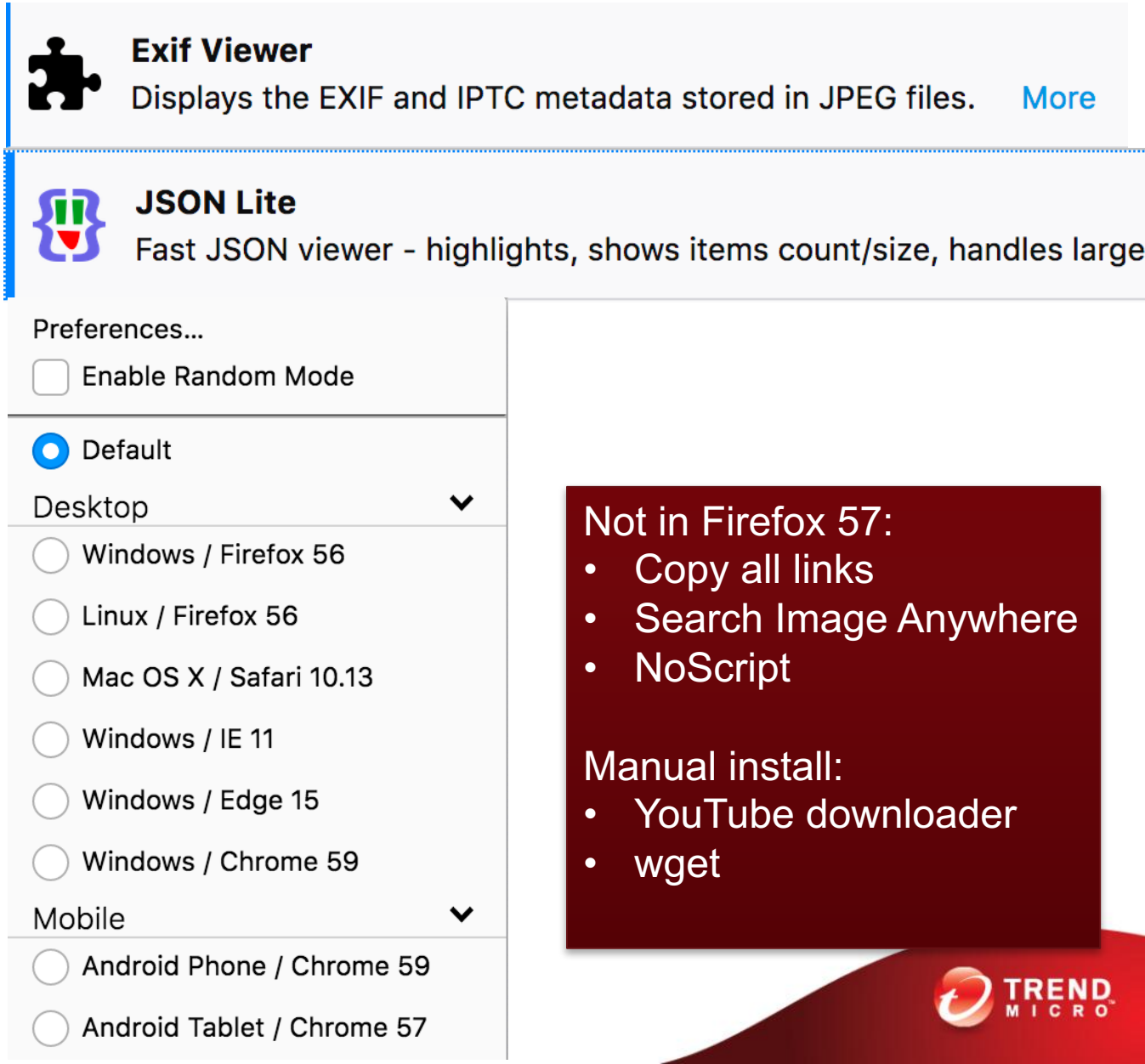
- New email
- New Facebook account
- New Twitter
- New cell phone
- New laptop

Firefox (1)


History
Firefox will
Use custom settings for history
Always use private browsing mode
Remember my browsing and download history
Remember search and form history
Accept cookies from websites
Exceptions...
Accept third-party cookies
Never
Keep until
I close Firef...
Show Cookies...
Clear history when Firefox closes
Settings...

Firefox (2)



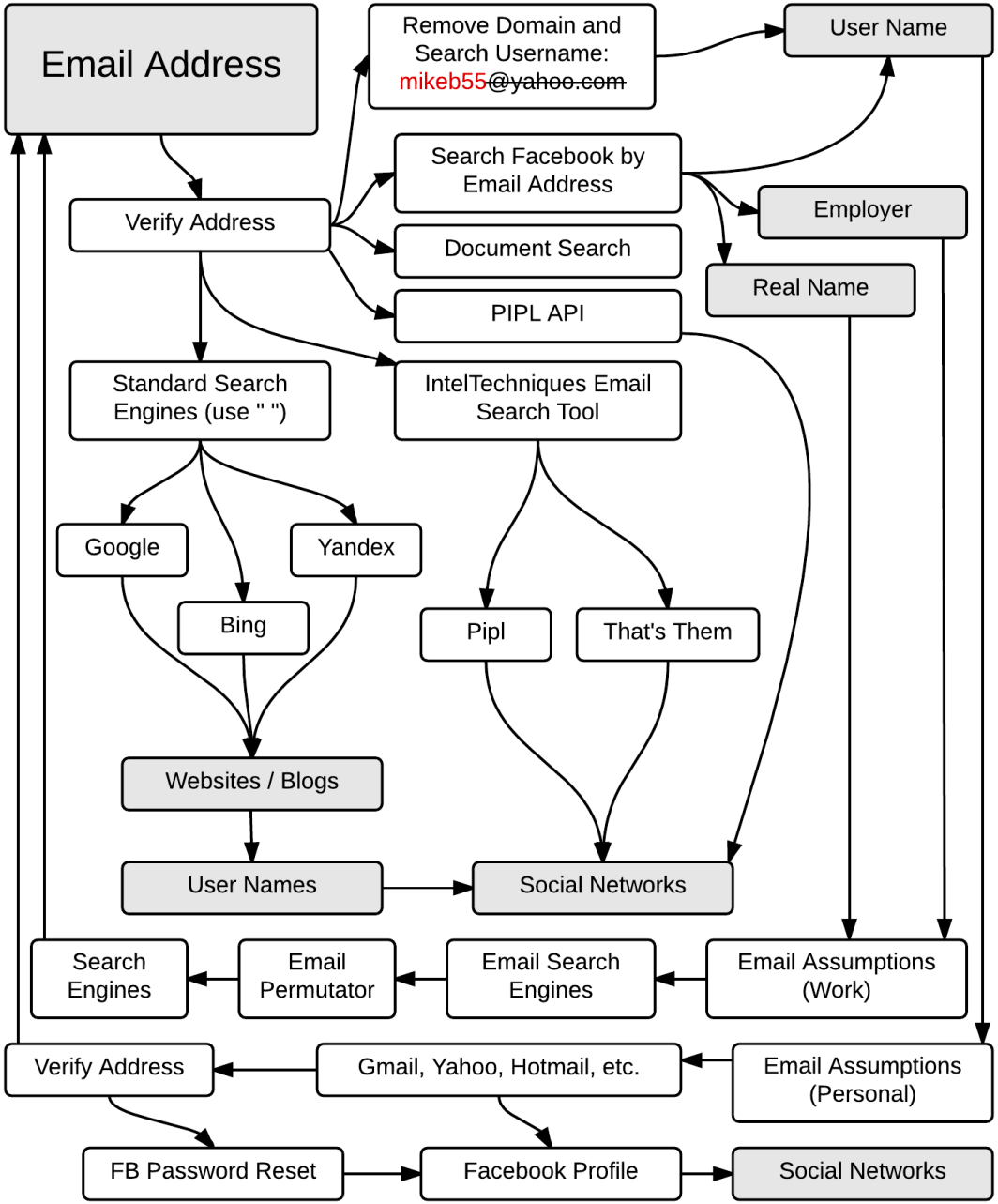


Not in Firefox 57:

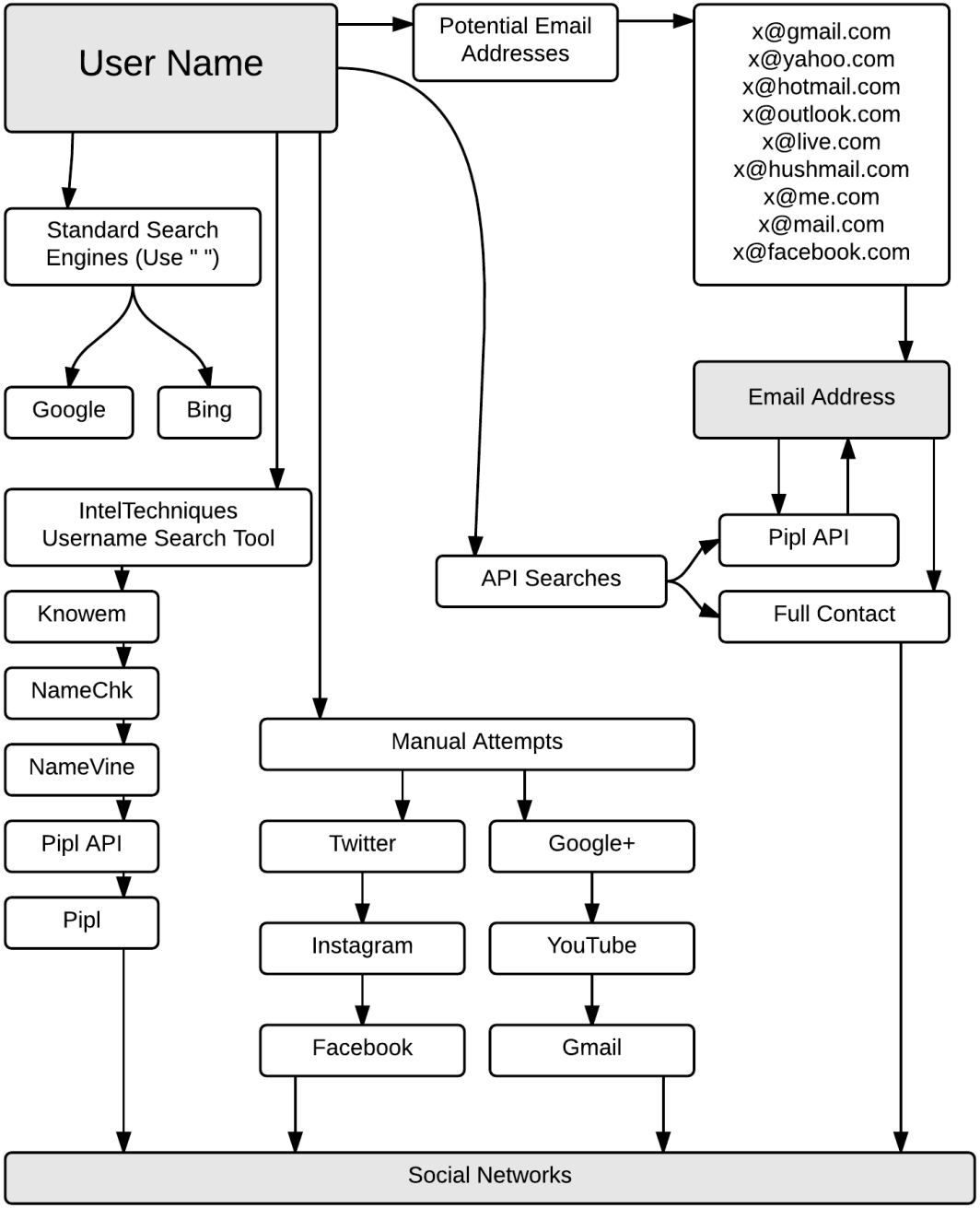
- Copy all links
- Search Image Anywhere
- NoScript

Manual install:

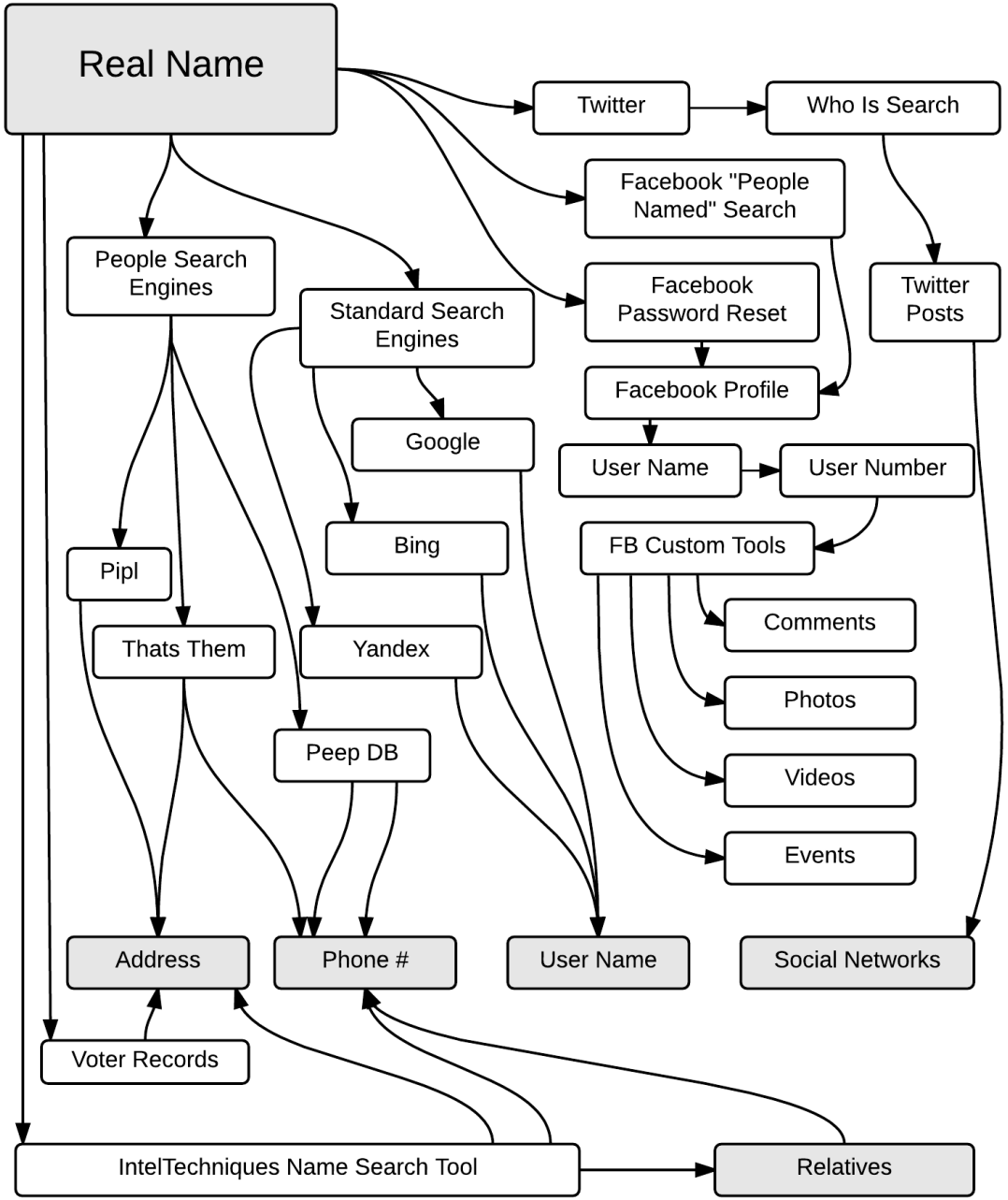
- YouTube downloader
- wget



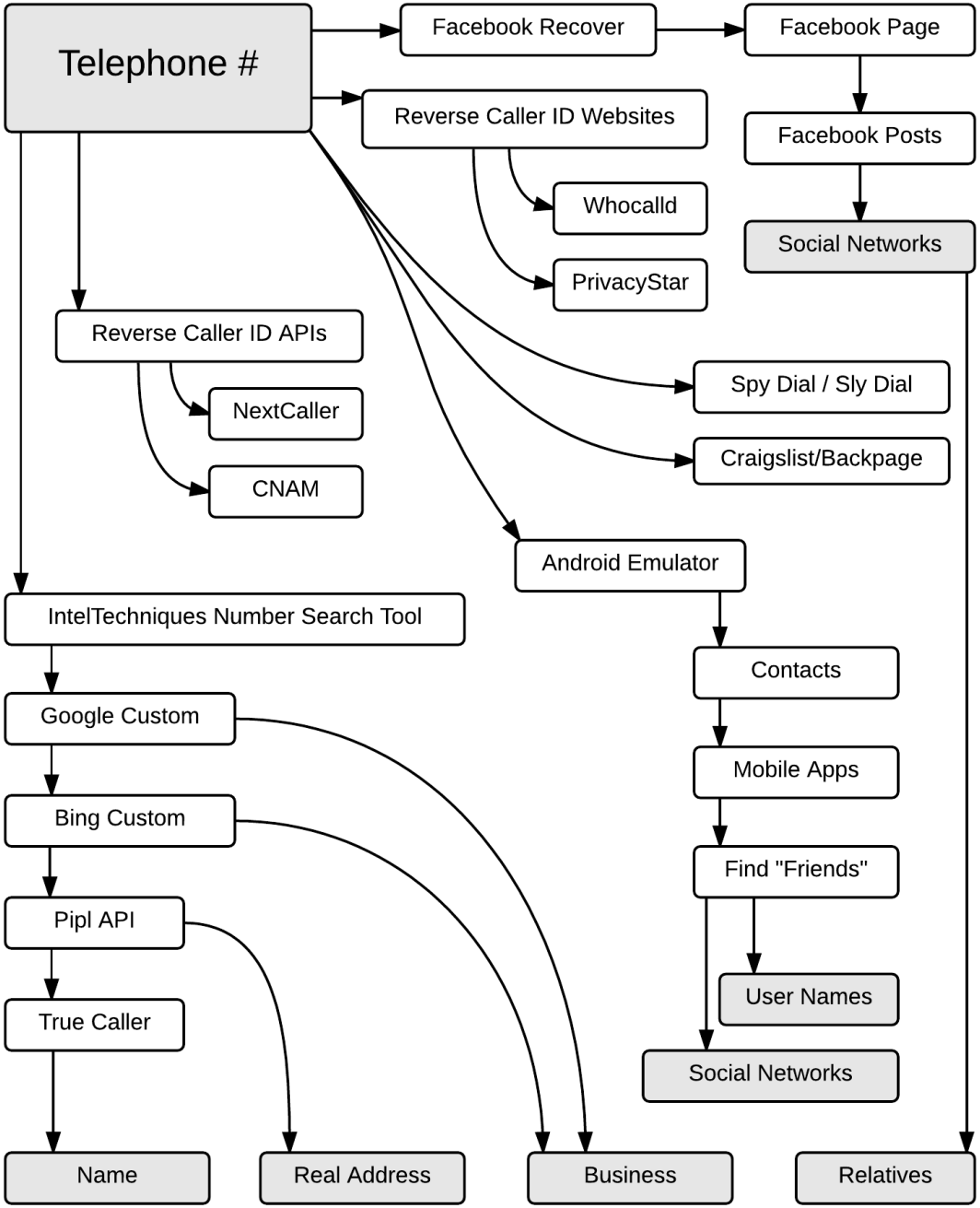
IntelTechniques.com OSINT Workflow Chart: Email Address



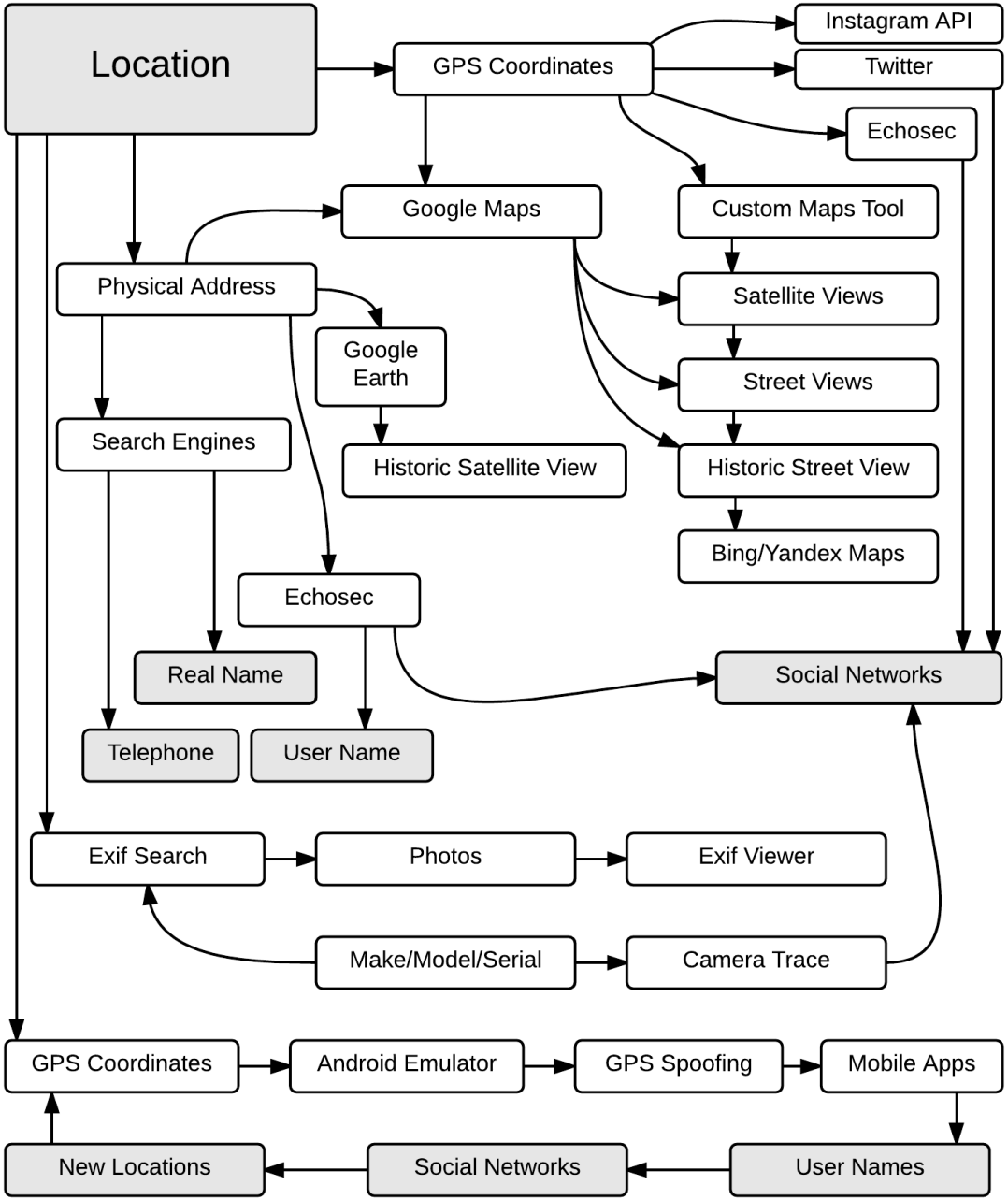
IntelTechniques.com OSINT Workflow Chart: User Name



IntelTechniques.com OSINT Workflow Chart: Real Name



IntelTechniques.com OSINT Workflow Chart: Telephone #



IntelTechniques.com OSINT Workflow Chart: Location

Module 2
Search Engines

In this Module ...

- Google dorks
- Email recon (X)
- Middle name (X)
- Education
- Genealogy
- Real estate or rent-a-car
- Tax records

Google Dorks (1)

- **"**someone@gmail.com**"**
- **site:**ntu.edu.tw "Some Document"
- Cisco **filetype:**pptx
- bazzell **-**fbi **-**osint **-**amazon **-**books **-**intelligence
- **inurl:**ftp -inurl:**(**http**|**https**)** filetype:pdf osint
- **intitle:**osint
- "osint * training"
- "osint * training" "2015**..**2017”
- **ext:pdf** trendmicro

Google Dorks (2)

- https://www.google.com.tw/search?q=osint+tools&tbs=cdr:1,cd_min:1/1/0

- https://www.google.com/inputtools/try/
- Google image reverse search

Google Dorks (3)

- site:newspaperarchive.com "this archive is hosted by"
- google.com/search?q=nsa&tbm=nws&tbs=nrt:b

ブログ ▾　新着 ▾　関連度順 ▾　リセット

NSA hacking code lifted from a personal computer in US: Kaspersky

CISO MAG (blog) - 2017/10/29

Moscow-based multinational cybersecurity firm Kaspersky Lab on October 25 said that it obtained suspected National Security Agency (**NSA**) hacking code from a personal computer in the U.S. During the review of file's ...

Kaspersky Says Its Hand Was in the Cookie Jar, But …

Security Boulevard (press release) (blog) - 2017/10/29

すべて表示

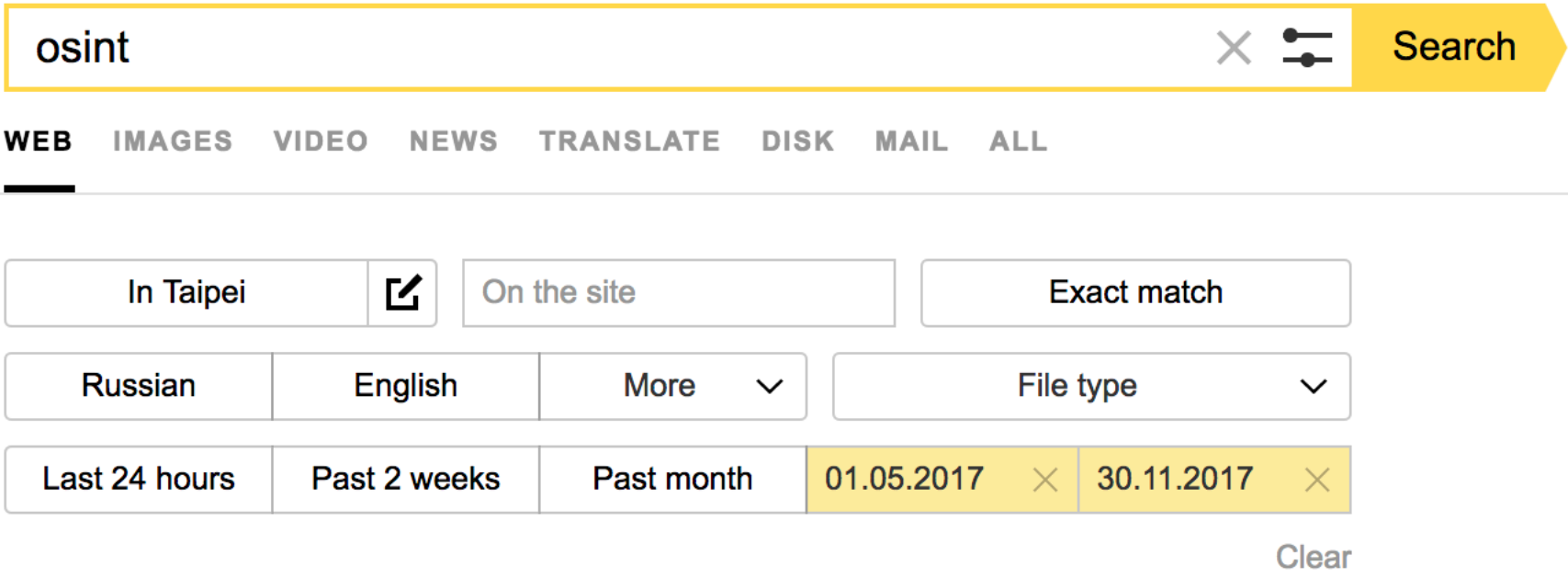
Second **NSA** Groundbreaker contract gets hit with protest

Washington Technology (blog) - 2017/10/18

In this case, we know the **NSA** cannot begin transitioning work to AT&T until the DXC protest is resolved. ... However, that is probably a moot point because even if the **NSA** cannot move the work to the new CSRA contract, ...

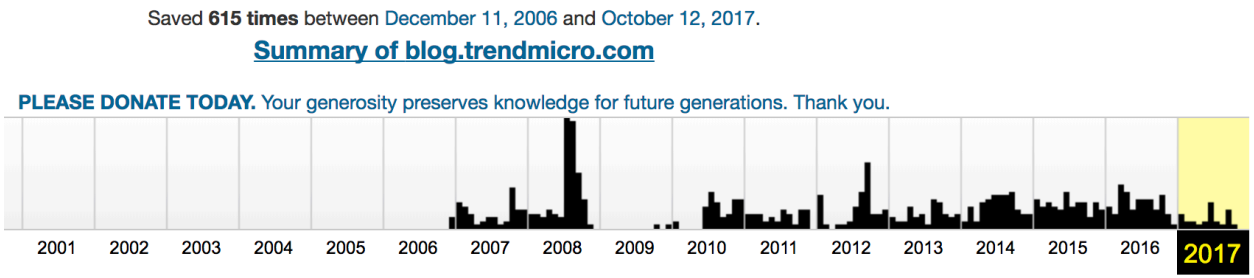
Bing / Yandex

- **linkfromdomain:**trendmicro.com
- **contains:**ppt site:trendmicro.com



Cache

- Google
- Bing
- Yandex
- Baidu
- Archive.is
- Coralcdn.org (?)
- Archive.org



Other Search Engines

- duckduckgo
- keywordtool.io
- carrot2.org
- millionshort.com
- globalfilesearch.com
- mmnt.ru (?)

👉 https://inteltechniques.com/menu.html

Phone / Name

- opencnam.com
- Calleridservice ➔ Free API key
- next caller ➔ Need to contact sales
- Truecaller ➔ like Whoscall 👍
- Spokeo
- Genealogy

Exercise

- Google First! **Donald J Trump Jr.**
- 1977.12.31 (Wikipedia)
- Tips: Need phone numbers to exercise? Search backpage or craiglist.

Example – Spokeo

Biography †

Donald Trump, Jr.'s personal information overview.

BIRTHDAY
31 December 1977

HOME TOWN
Manhattan

← Birth place

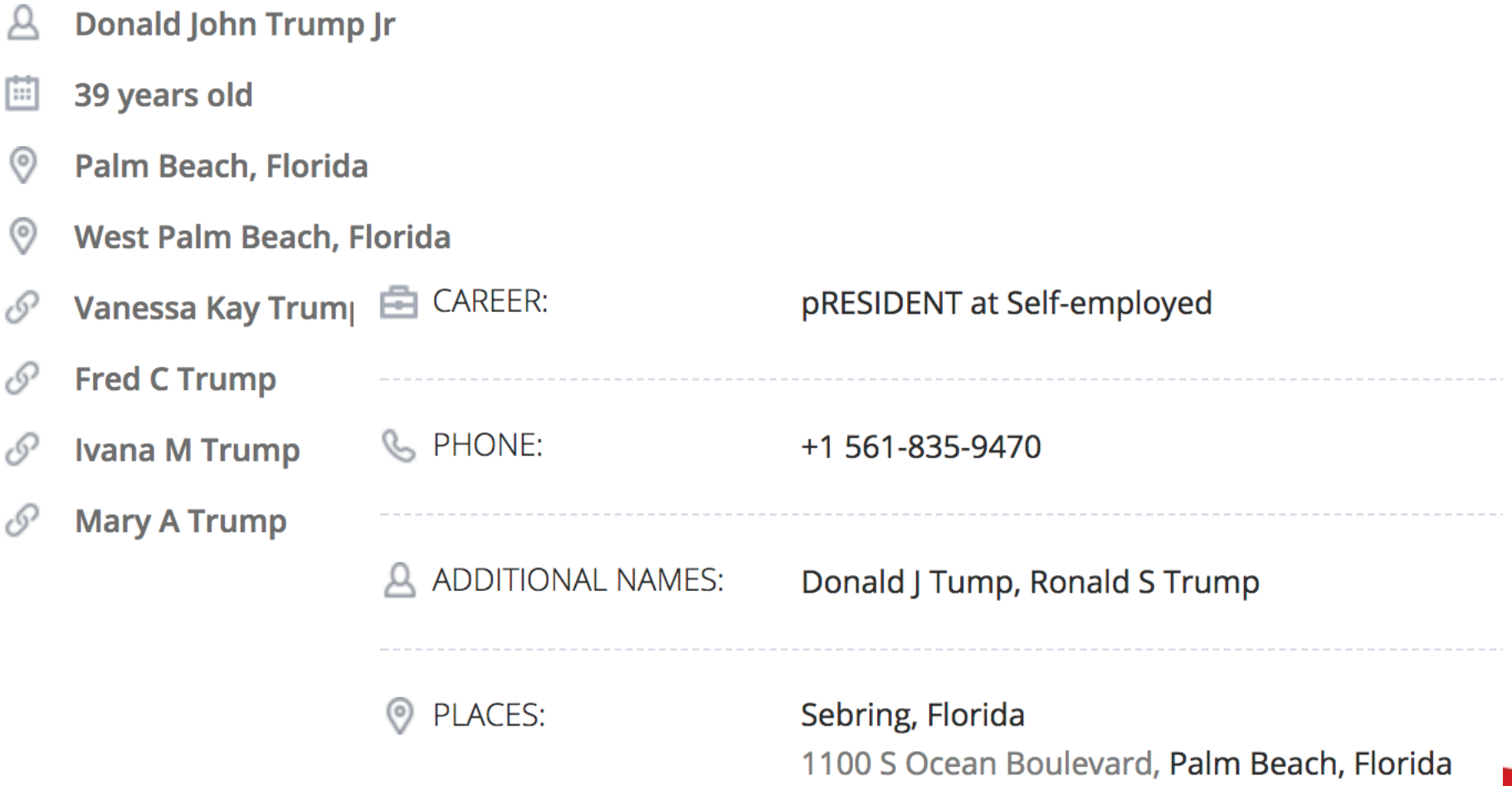
Donald Trump, Jr.

American businessman

Donald "Don" John Trump, Jr. is an American businessman who is the first child of real estate developer Donald J. Trump and Ivana Trump. He currently works along with his sister Ivanka Trump and brother Eric Trump in the position of Executive Vice President at The Trump Organization. He is also ambassador for Operation Smile.

Example – Pipl

- (Optional) Register for API trial key



Example – Ancestry

- www.ancestry.com ➔ 14-day free trial

Results 1-20 of 1,925

RECOR

Matching Person (from family trees)

Donald 'Don' John Jr Trump

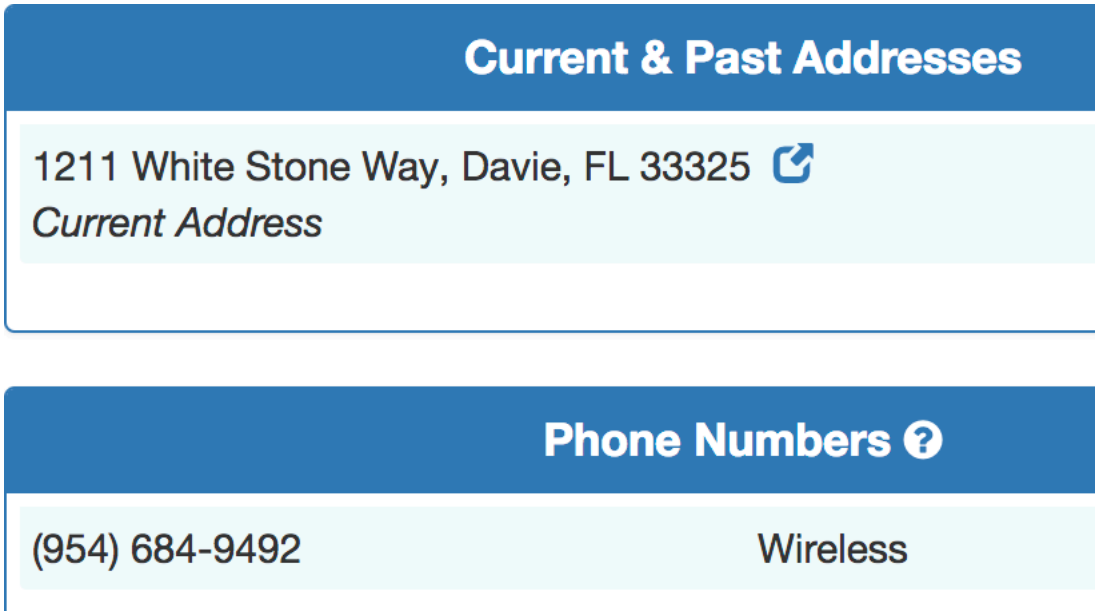
*Teller-Hamilton",O'Brien, Sheridan, Hogarty, Bracken, Michelsen-Pedersen, Presidents, Royals, God, Waldron-Benson-Schaaff

Birth: date date 1977 Kings, USA

Matching Records

Example – True People

- Family Tree Now (?)
- True People (X)



Example – ZabaSearch

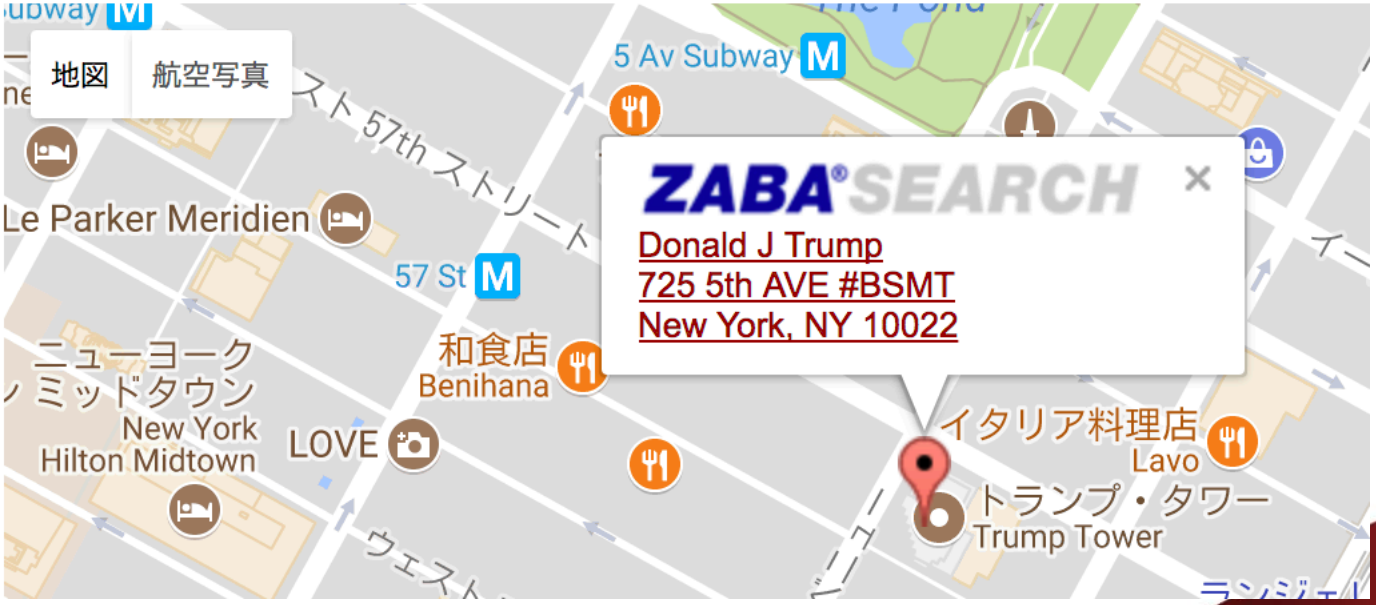
Donald J Trump
725 5th AVE #BSMT New York, NY 10022

View full profile »

More information for Donald J Trump

Other Phone Lookup
Background Check
Public Records
Property Records
Maps & Driving Directions

Donald J Trump Get the Dirt Check for Email Address
725 5th AVE #BSMT
New York, NY 10022 Confirm Current Phone & Address
Background Check on Donald J Trump



Example – Others

ADDRESS

425 East 58th St,

WPNumbers

PERSON	ADDRESS	LOCATION	PHONE
Trump donald J Chief Executive at Trump Hotels and Casino Resorts; Inc.	725 5th Avenue	NEW YORK - NY	8642929070 / 2124217136

Donald John Trump
New York ,NY
Palm Beach ,FL
Sacramento ,CA
Sebring ,FL

Phone Number	Location	Connection
+1 212-832-2000	New York, NY	work
+1 212-247-7000	New York, NY	work
+1 916-920-4631	Sacramento, CA	unset

Donald John Trump

1977-12-31

New York, NY

+1 916-920-4631

donald@trumporg.com

Quanki

Example – Make a Table

(212) 421-7136		
(561) 835-9470	Donald Trump	1110 S Ocean Blvd, Palm Beach FL.
(864) 292-9070	David Hanna	109 E 50th St NY 10022
		IP Address 208.99.198.79
	David I Hanna	
(916) 920-4631	Teresa Blake	Scrm North, CA
	Teresa A Blake	
(954) 684-9492	Hanh Pham	
	DonaldTrump	1211 White Stone Way, Davie FL.
		IP Address 134.170.109.165

Previous Addresses

5166 Connecticut Dr #2
Sacramento, CA 95841-3934
(Feb 2010 - Oct 2016)

369 Bush St
Salinas, CA 93907-2029
(Jan 2009 - Jan 2016)

822 Carro Dr #4
Sacramento, CA 95825-4443
(Mar 2012 - Dec 2015)

(916) 920-4631 might have nothing to do with Donald J Trump Jr.

Visit zillow.com for real-estate

TREND MICRO
Securing Your Journey to the Cloud

Tea Time 

Module 3
Social Media Profiling

Social Media

- Facebook
- Instagram
- VK
- Twitter
- Dating
  - OkCupid / Match / Plenty Of Fish / eHarmony / Ashley Madison
- 中國特色
  - 人人 / QQ / 淘寶 / 微博 / 陌陌

Create New Accounts

1. KeePassX
2. Email account #1 ➔ Google
3. Email account #2 ProtonMail 

4. Phone ➔ TextNow, Google Hangout
5. Twitter*
6. Instagram
7. Facebook**

*Don’t associate with a phone number.

** Virgin account is not as precious.

Facebook ...


基本データ
この人が友達とシェアしているコンテンツを閲覧するには、友達リクエストを送信しましょう。
友達になる
概要
職歴と学歴
住んだことがある場所
連絡先と基本データ
家族と交際ステータス
[redacted]さんの情報
ライフイベント
表示する勤務先がありません
表示する学校がありません
表示するスポットがありません
表示する交際情報がありません
https://www.linkedin.com/in/[redacted]

Facebook Dorks

- https://inteltechniques.com/menu.html
- users-named
- pages-named/employees/present
- users-born
- Location
- Likes
- Education
- ~~Search by email~~
- ~~Search by phone number~~*
- It doesn't tell what's not public anymore ☹

Facebook Graph API

- Before you start – **Use yourself as the target**

- Use or switch to English (US)
- https://inteltechniques.com/menu.html
- Get userid
- Populate all
- Check all the details

Twitter

- twitter.com/search-advanced
- twitter.com/#!/who_to_follow
- Twitter Deck
- moz.com/**followerwonk**/bio
- ctrlq.org/first/
- sleepingtime.org
- twiscy.com
- Google Dork ➔ site:twitter.com/username

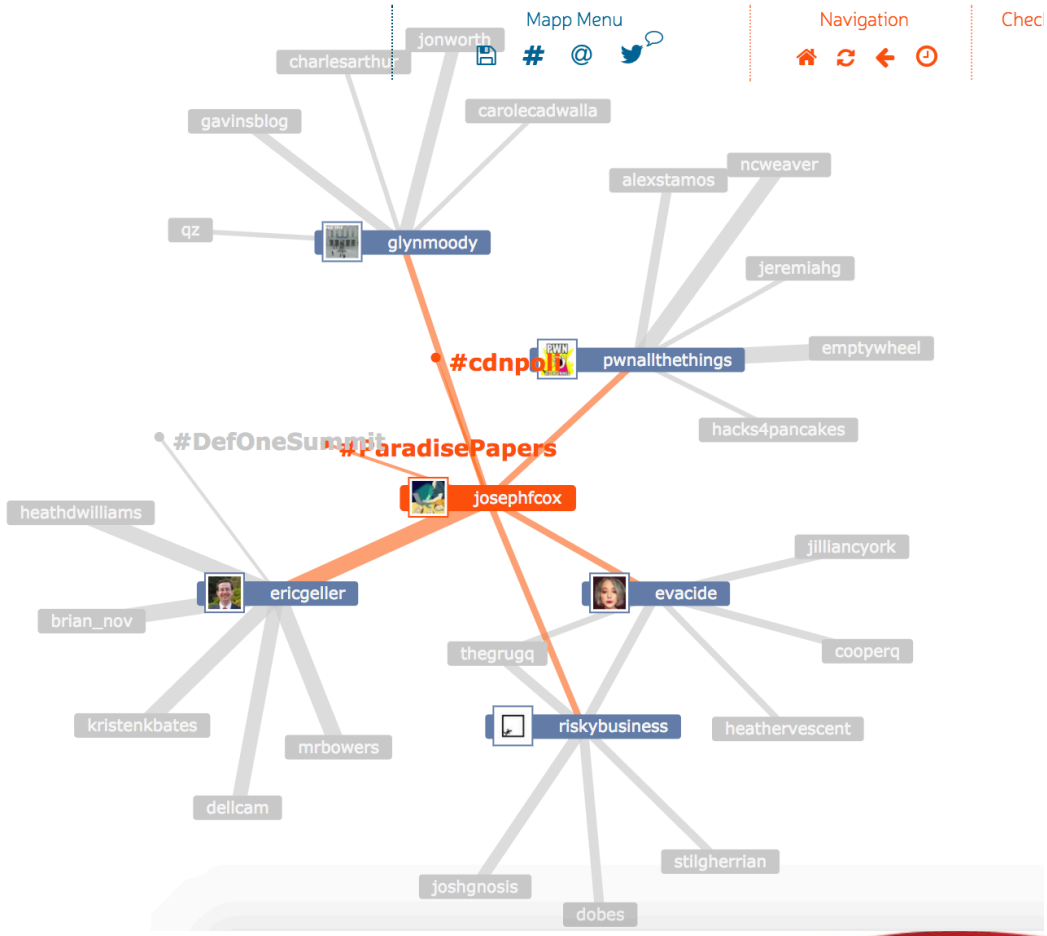
- Last 2 digits of cellphone !!!

Twitter – GPS

- tweetpaths.com
- mapd.com/demos/tweetmap
- https://twitter.com/search?q=geocode%3A25.0220839%2C121.5471991%2C2km&src=typd
- https://pbs.twimg.com/media/DOW91xRW0AAEjSO.jpg**:orig**

Twitter – Ecosystem

- fakers.statuspeople.com
- trendsmap.com
- twitonomy.com
- mentionmapp.com



Instagram

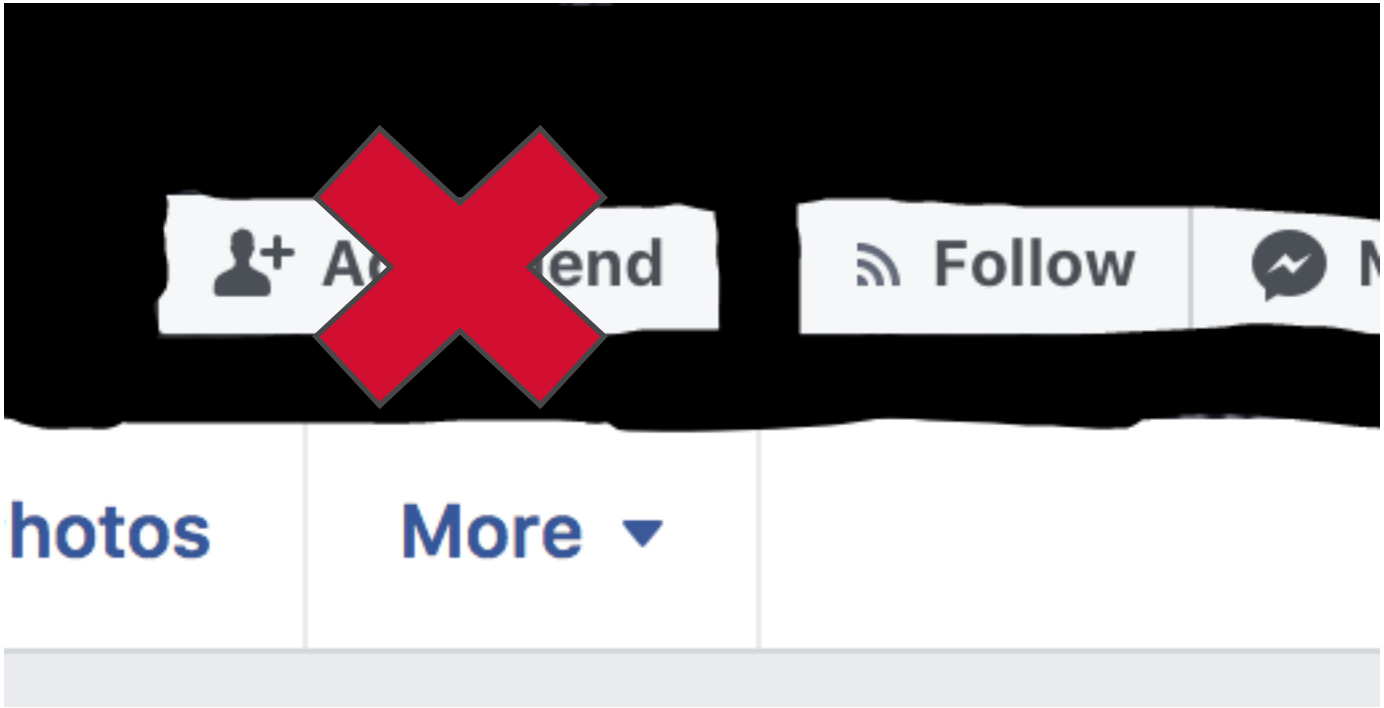
- 4K Stogram or DownloadGram
- Strips EXIF data
  - Facebook / Instagram / Twitter strip EXIF data.
- Not much we can do ☹

Tools and Sites

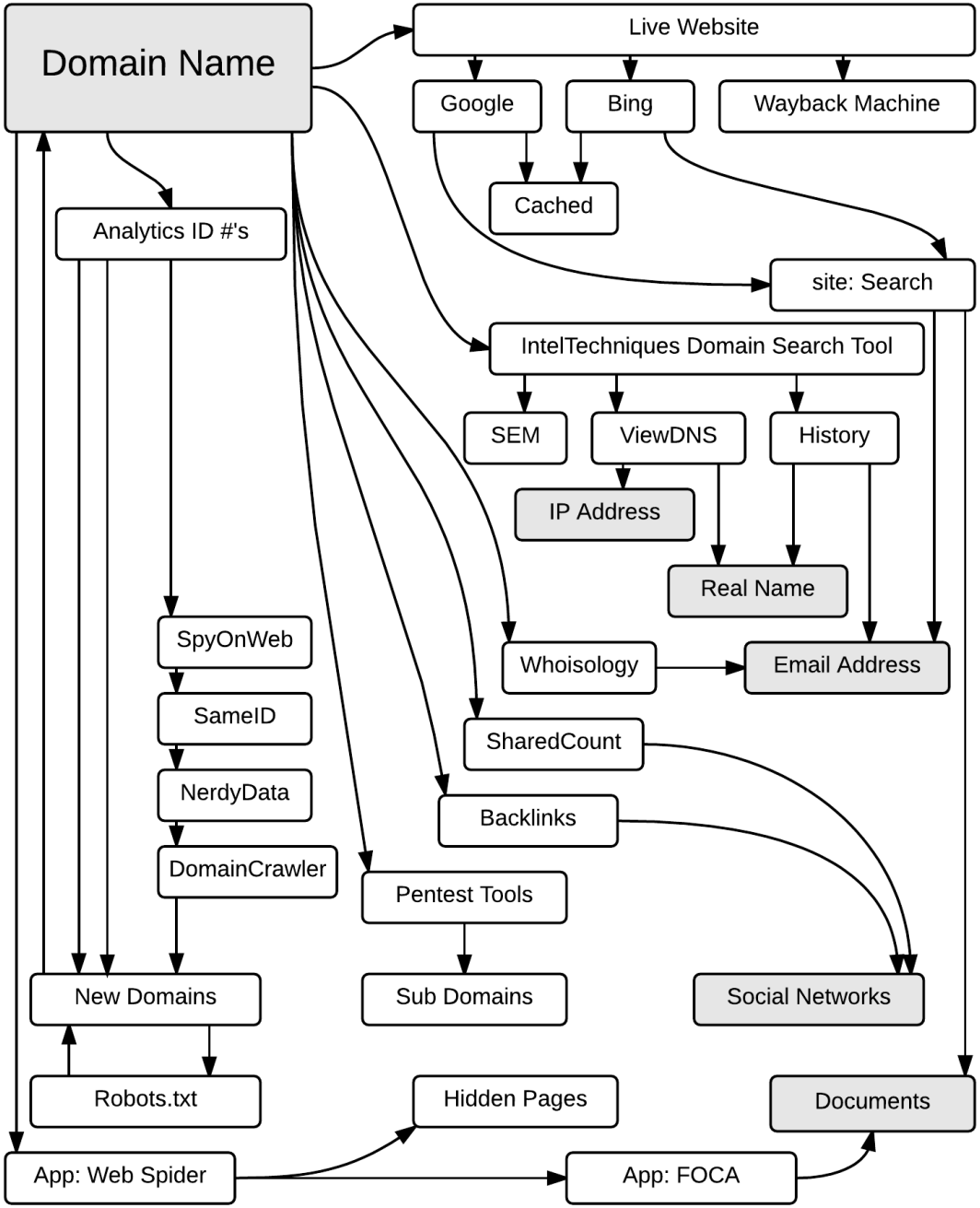
- social-searcher.com
- del.icio.us
- Flickr map search
- mypicsmap.com
- www.topix.com/pick-local
- craigslist.org

”Add Friend” Does Not Help You

- Don’t believe in “Add Friend” and cancel. Facebook has removed the feature.



Module 4
Domain / IP Profiling



IntelTechniques.com OSINT Workflow Chart: Domain Name

Common Sites

- Whois
- viewdns.info
- VirusTotal
- PassiveTotal (RiskIQ)
- MaxMind GeoIP2
- Bing IP

- ~~sameid.net~~
- ~~NerdyData~~

Whois

- Again, check https://inteltechniques.com/menu.html
- whois swiftco.net / host DOMAIN / host IP

```
Domain Name: SWIFTCO.NET
Registry Domain ID: 86102216_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.directnic.com
Registrar URL: http://www.directnic.com
Updated Date: 2017-04-28T20:30:16Z
Creation Date: 2002-04-30T05:38:15Z
Registry Expiry Date: 2018-04-30T05:38:15Z
Registrar: DNC Holdings, Inc.
Registrar IANA ID: 291
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS1.SWIFTCO.NET
Name Server: NS2.SWIFTCO.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Historical Whois Data

Registrant Name: **Henry Goss**
Registrant Organization: swift communications
Registrant Street: **2001 6th avenue Suite #3020**
Registrant City: **Seattle**
Registrant State/Province: WA
Registrant Postal Code: 98121
Registrant Country: US
Registrant Phone: **+2067282736**

DomainTools or DomainHistory.net

Reverse Whois

- viewdns.info or DomainTools

Domain Name	Creation Date	Registrar
amazinstyle.com	2015-06-04	1 API GMBH
henrygossarchitects.com	2011-07-15	ENOM, INC.
henrygossrealestate.com	2015-02-25	TUCOWS DOMAINS INC.
riceprojects.co.uk	2016-02-02	TUCOWS INC T/A TUCOWS [TAG = TUCOWS-CA]

```
Registry Registrant ID:
Registrant Name: Henry Goss
Registrant Organization: Henry Goss
Registrant Street: 900 North 185th St
Registrant City: Shoreline
Registrant State/Province: WA
Registrant Postal Code: 98133
Registrant Country: US
Registrant Phone: +1.2066500519
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: hgoss@windermere.com
```

Historical IP of 216.9.6.248

Domain	Last Resolved Date
aerospacetacomapierce.com	2017-11-05
aerospacetacomapierce.org	2017-11-10
aniota.com	2017-11-05
becomenala.com	2017-11-05
cannonconstructioninc.com	2017-11-05
capitolhillarts.org	2017-11-10

IP Address	Location	IP Address Owner	Last seen on this IP
216.9.6.248	Issaquah - United States	Isomedia, Inc.	2017-11-11
216.18.231.36	Seattle - United States	ALLHOSTSHOP.COM	2017-08-02
74.117.221.144	Cayman Islands	DirectNIC, Ltd.	2016-05-03
216.18.231.36	Seattle - United States	ALLHOSTSHOP.COM	2016-05-01
216.18.231.20	Seattle - United States	ALLHOSTSHOP.COM	2013-06-16
216.18.231.36	Seattle - United States	ALLHOSTSHOP.COM	2013-05-28
216.18.231.20	Seattle - United States	ALLHOSTSHOP.COM	2013-05-19
204.13.167.6	Seattle - United States	SWIFT VENTURES Inc	2011-11-07

Lookup Domain from IP

Domain	Last Resolved Date
chrisandhyeyoung.com	2016-02-01
lordofthepipe.com	2016-02-01
swiftco.org	2017-11-10
traffictrader.net	2017-11-06

City: Seattle
Zip Code: 98138
Region Code: WA
Region Name: Washington
Country Code: US
Country Name: United States
Latitude: 47.6062
Longitude: -122.332

Spyonweb + DomainTools

Domain name:	**swiftco.net** (whois)
IP Address:	216.9.6.248 (whois)
Analytics Id:	UA-4075801
Alexa Rank:	**n/a** (details)
Page Rank:	**?**/10
Last Seen:	15.10.2017
JSON API:	Sign in

Email	dnsadmin@trendmicro.com is associated with ~220 domains domains@trendmicro.com is associated with ~83 domains abuse@web.com is associated with ~9,656,906 domains	Reverse Whois ▾

Censys + Shodan

Basic Information

OS Unix

Network 25700 - SWIFT VENTURES Inc (US)

Routing 204.13.167.0/24 via AS7922 , AS11404 , AS18530 , AS18530 , AS25700

80
tcp
http

Apache httpd Version: 1.3.42

```
HTTP/1.1 200 OK
Date: Sun, 12 Nov 2017 04:27:55 GMT
Server: Apache/1.3.42 (Unix) PHP/4.3.2 mod_perl/1.27
Last-Modified: Fri, 07 Jul 2017 17:52:03 GMT
ETag: "55006e-2fda-595fca43"
Accept-Ranges: bytes
Content-Length: 12250
Content-Type: text/html
```

3306
tcp
mysql

MySQL Version: 3.23

```
3.23.55
```

VirusTotal

Passive DNS Replication

Date resolved	Domain
2017-11-09	mail.acornprop.net
2017-11-05	systemoptical.net
2017-10-06	capitolhillarts.org
2017-06-10	evansartworks.com
2017-05-24	mail.vazquezco.com
2017-05-21	mail.aniota.com
2017-05-19	cannonconstructioninc.com
2017-05-19	mail.chevychasebeachcabins.com
2017-05-19	mail.experienceplumbing.net
2017-05-19	mail.jkbcpa.com

VirusTotal – Subdomains

```
$ curl -s 'https://www.virustotal.com/ui/domains/swiftco.net/subdomains?limit=10' | grep self | awk -F/ '{print $6}' | awk -F¥" '{print $1}'
```

rwhois.swiftco.net
mail.swiftco.net
kb.swiftco.net
vh2.swiftco.net
tim.swiftco.net
support.swiftco.net
prvtrc.swiftco.net
klaus.vh.swiftco.net
games.swiftco.net
blog.swiftco.net
swiftco.net

PassiveTotal (RiskIQ)

Show : 25 1-25 of 110 Sort : Last Seen Descending

Resolve	First	Last	Source	Tags
systemsoptical.com	2016-06-03	2017-11-12	riskiq, virustotal	Registered
aerospacetacomapierce.com	2016-08-31	2017-11-12	riskiq, virustotal	Registered
twincommander.com	2016-01-13	2017-11-11	kaspersky, riskiq, virustotal	Registered
mail.swiftdesk.com	2017-03-25	2017-11-11	riskiq, virustotal	Registered
nalapaper.com	2017-07-09	2017-11-11	riskiq	Registered
experienceplumbing.net	2016-04-05	2017-11-11	riskiq	Registered
terrieannquilts.com	201			
systemsoptical.net	20			

Hostname	First	Last	Name	Domain
216.9.6.248	2016-12-02	2017-11-10	cwGeoData	mukilteoyachtclub.com
216.9.6.248	2016-12-02	2017-11-10	e028d6e31c87a0f22cf8294b9db1f515	mukilteoyachtclub.com
216.9.6.248	2017-01-12	2017-07-22	_gat	libertybankbuilding.org
216.9.6.248	2017-07-22	2017-07-22	_gid	libertybankbuilding.org
216.9.6.248	2017-01-12	2017-07-22	_ga	libertybankbuilding.org
216.9.6.248	2017-06-08	2017-06-08	cookietest	twincommander.com

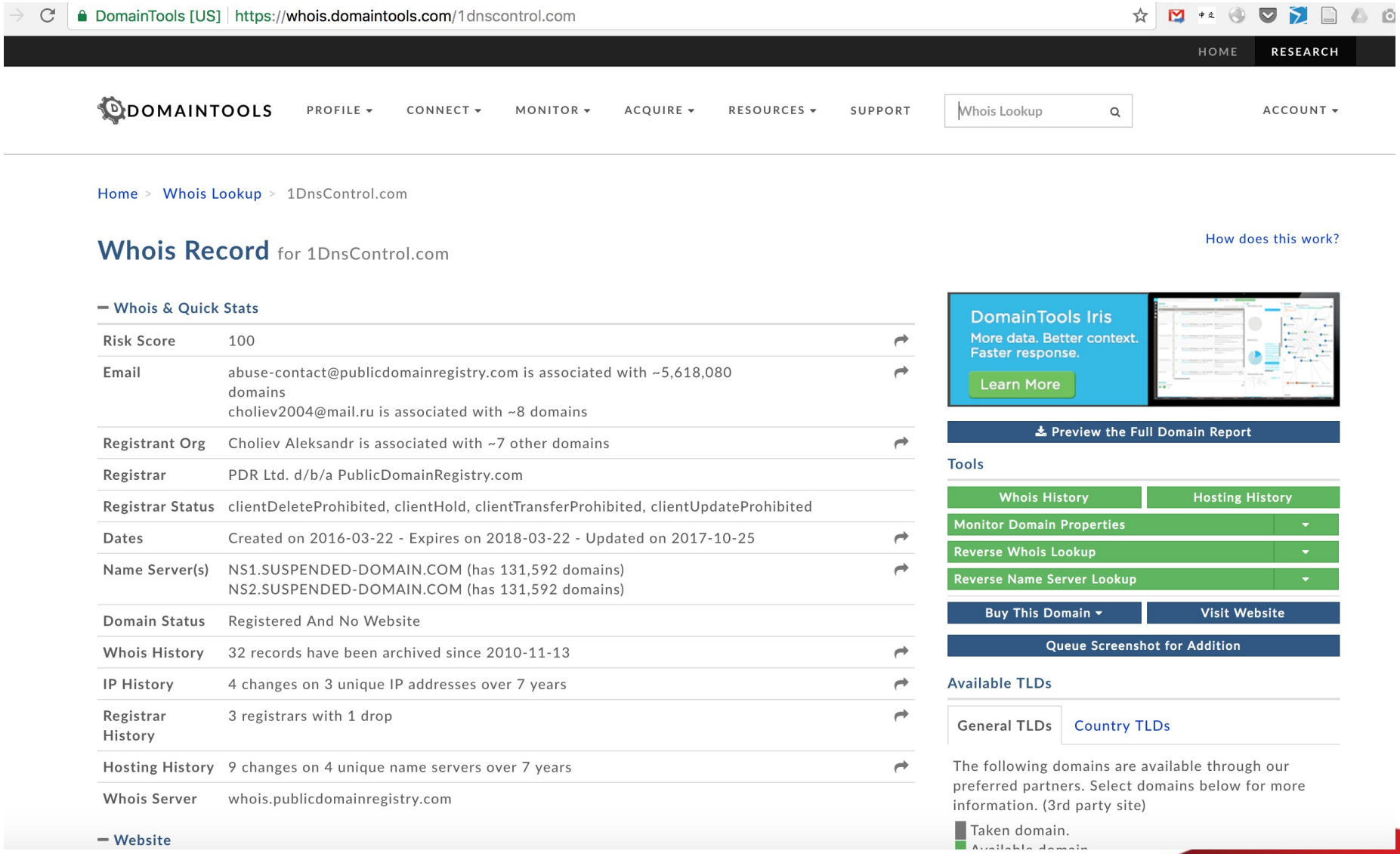
GeoIP2

- https://www.maxmind.com/ja/geoip-demo

GeoIP2 City 結果

IP アドレス	国コード	場所	郵便コード	近似座標*	精度範囲	ISP	組織	ドメイン	大都市コード
134.170.109.165	US	アメリカ合衆国, 北アメリカ		37.751, -97.822	1000	Microsoft Corporation	Microsoft Corporation		

DomainTools (Not Free) (1)



DomainTools (Not Free) (2)

Narrow Your Search

Search

Download Report

Displaying results: 1 - 8 of 8 *Prev* *Next*

Domain Name	Create Date	Registrar
1dnscontrol.com	2016-03-22	PDR Ltd. d/b/a PublicDomainRegistry.com
approvedpharmacyvnx-secured.com	2016-02-25	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
buycialisovernightdeliverybct.accountant	2017-02-06	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
cheap-trusted-pharmacy.org	2017-03-06	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
onlinepharmacydpn-secured.com	2015-12-11	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
secure-check.host	2017-03-04	--
trustedpharmacydlt.com	2016-04-26	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
webcheck01.net	2016-12-06	PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM

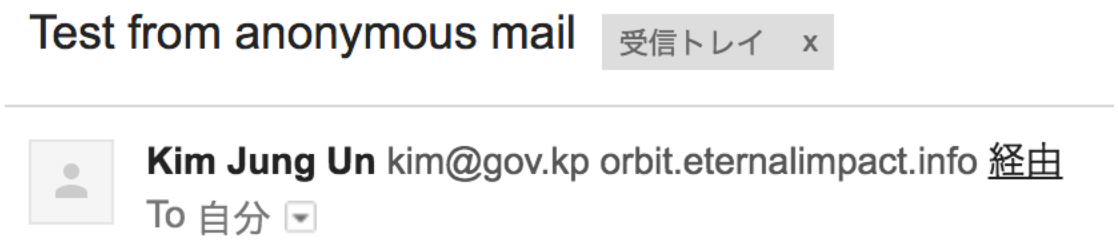
Download Report

Displaying results: 1 - 8 of 8 *Prev* *Next*

Miscllaneous

Miscellaneous Tools

- nsfwyoutube.com
- anonymousmail.me



- Social Traffic on IntelTechniques
- karmadecay.com
- wigle.net

Epilogue

- API will change
- Paywall will be built
- Webpage will disappear

- Not covered ...
  - Radio monitoring
  - Localization
  - Government documents
  - DMV data
  - Reverse video searching
  - Etc.

Be Responsible!

Contact: @miaoski