



Advanced Online Research Tools

SEMCAACFE Chapter

April 5, 2018

Presented by: Lori Tesch, CFE, CFF, CPA

WAYNE STATE UNIVERSITY



Open Source Intelligence Techniques

Michael Bazzell

Inteltechniques.com

**Phone privacy app
is Sudoapp.com**

A screenshot of the IntelTechniques website. The header features the title 'INTELTECHNIQUES By Michael Bazzell' next to a photo of a man in a suit. To the right, it lists 'OSINT TRAINING', 'PRIVACY CONSULTING', and 'DIGITAL SECURITY'. A navigation bar includes links for 'Online Training', 'Live Events', 'Services', 'Tools', 'Links', 'Forum', 'Blog', 'Podcast', 'Books', and 'Contact'. The main content is divided into two sections: 'IntelTechniques Services' and 'IntelTechniques Free Resources'. The 'Services' section has icons for 'Online Training' (computer with graduation cap), 'Keynotes' (person at podium), 'Live Training' (person at whiteboard), 'Services' (shield with checkmark), and 'Books' (stack of books). The 'Free Resources' section has icons for 'Search Tools' (globe with magnifying glass), 'Book Links' (open book), 'Web Forum' (speech bubbles), 'Blog' (speech bubble with dots), and 'Podcast' (microphone). On the right, a 'NEW OSINT GUIDE!' announcement states that the sixth edition of the book is available, with a link to click for details. Below the text is an image of the book 'OPEN SOURCE INTELLIGENCE TECHNIQUES: RESOURCES FOR SEARCHING AND ANALYZING ONLINE INFORMATION, SIXTH EDITION' by Michael Bazzell.



Online Research Tool Categories

- Search Engines
- Social Media
- Online Communities
- E-Mail
- Phone #s
- Photos





Search Engines

Google

bing

Yandex





Google

Operators:

Quotation marks “John Smith”

Site:forbes.com “John Smith”

“Cisco” filetype:ppt (pptx)

Exclude “John Smith” –engineer

“Peter Smith” OR “Pete Smith”

“internet * training”

“peter smith” “1..999 comments”



Bing

Operators:

All the same as Google except the file type
“contains:ppt site:cisco.com”

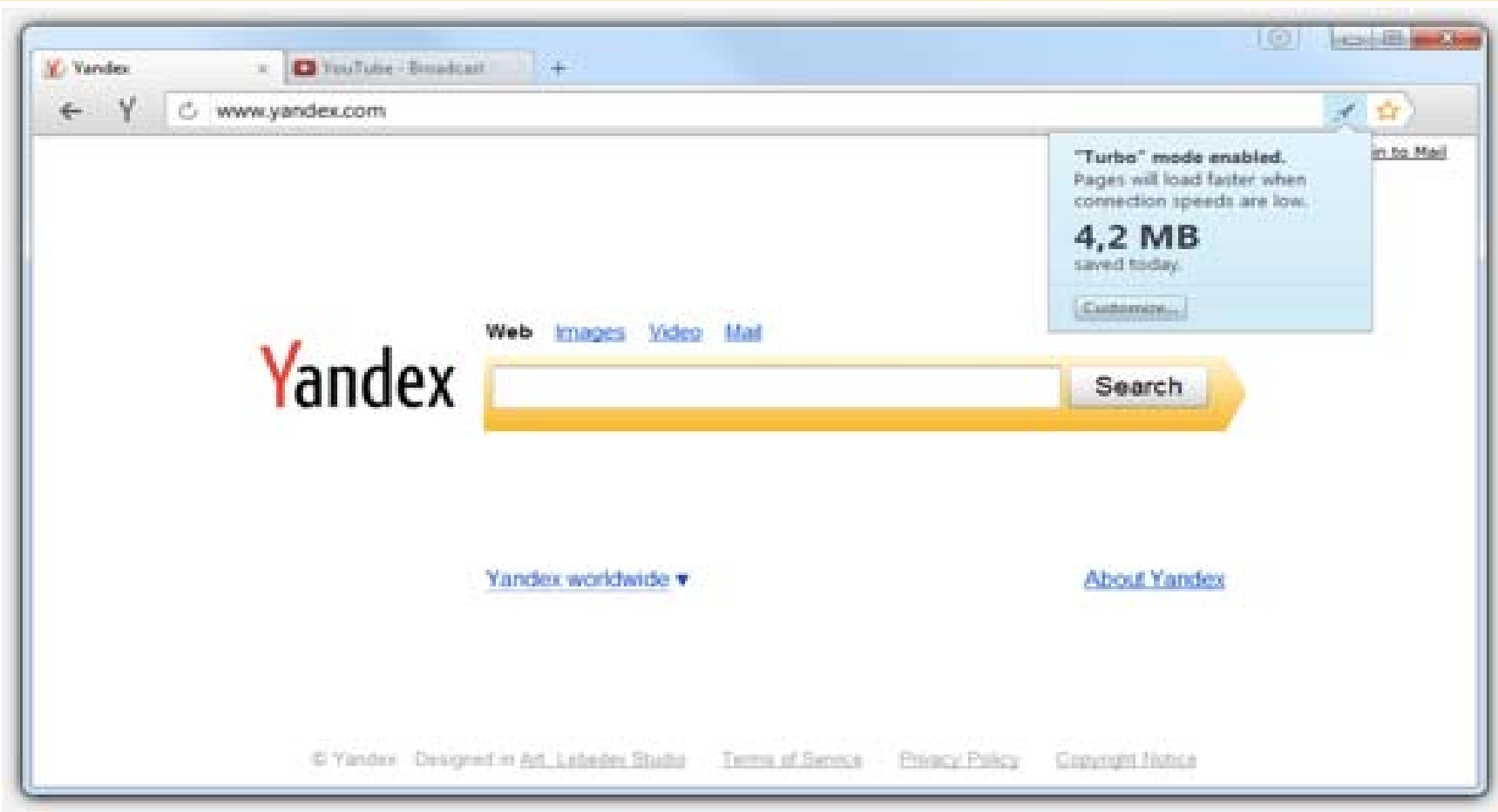


YAHOO!

YAHOO!



Yandex





Tor



Welcome to Tor Browser

You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)

SnapFiles

Search [securely](#) with [Disconnect.me](#).

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

[Tips On Staying Anonymous »](#)

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)

Don't be afraid to use Tor, just be cautious. There is a great deal of information available and you might find something about your target.




Tor

Onion Identity Services – Get your fake passport and a new identity today

Onion Identity Services – Get yo...
abbujjh5vqtq77wg.onion

Drivers Licenses



Product	Price	Quantity
Norway Drivers License	1150 EUR = 10.832 \$	<input type="text" value="1"/> X Buy now
Denmark Drivers License	1150 EUR = 10.832 \$	<input type="text" value="1"/> X Buy now
Netherlands Drivers License	1150 EUR = 10.832 \$	<input type="text" value="1"/> X Buy now
UK Drivers License	1000 EUR = 9.419 \$	<input type="text" value="1"/> X Buy now

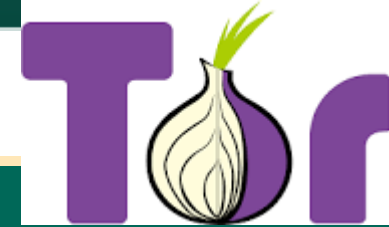


Tor

A screenshot of a Tor Browser window displaying the BlackMarket Reloaded website. The browser's address bar shows the URL `5onwnspjvuk7cwvk.onion/index.php`. The website has a dark blue header with the title "BlackMarket Reloaded" and a navigation menu including Home, Your Account, Your Purchases, Forum, Logout, and Help. A sidebar on the left lists various categories such as Drugs (2514), Services (1173), Data (621), Weapons (164), Collectables (31), Metals/Stones (39), Other (256), Software (137), Movies (31), Tobacco (170), Counterfeits (116), Alcohol (39), and eBooks (785). The main content area displays a grid of items for sale, each with a thumbnail image, a title, a description, and a price in BTC. The items include:

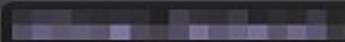
- 10z. Rascal OG (Indoor) - 2.00000 BTC
- How to Build A Laser Listening Device - 0.05926 BTC
- Platinum CC Fullz, PINS; Checker included SSN/DOB - 0.22222 BTC
- 2c-b 1000mg - 1.73693 BTC
- 10 Orange Haze Cannabis seeds - 0.10200 BTC
- Decoy package. Free shipping. - 0.03860 BTC
- Perfect quality Ray-Ban replica sunglasses Aviator - 0.22815 BTC
- Suppressors Home made, Patents etc 138 pdf files (232Mb) - 0.14474 BTC


The bottom of the screen shows a Windows taskbar with the "Screencast-O-Matic.com" watermark and several open applications including Studio 2013 and a download manager.



Tor

[Products](#) [FAQs](#) [Register](#) [Login](#)





We are a team of 3 contract killers working in the US (+Canada) and in the EU. Once you made a "purchase" we will reply to you within 1-2 days, contract will be completed within 1-3 weeks depending on target.

Only rules: no children under 16 and no top 10 politicians.

Product	Price	Quantity
We kill your target in the USA/Canada	10000 USD = 74.036 \$	<input type="text" value="1"/> X Buy now
We kill your target in the European Union	12000 USD = 88.843 \$	<input type="text" value="1"/> X Buy now




Tor

USfakeIDs

[Products](#) [FAQs](#) [Register](#) [Login](#)

US Fake Drivers Licenses - Scannable, Holograms, UV etc



Our fake drivers licenses are all scannable, contain original hologram and UV, microprint, laser engraving etc.
Shipping from the US within 48 hours!
We only sell the best quality, you wont find any better on the net.

Product	Price	Quantity
Delaware	200 USD = 0.316 ₿	<input type="text" value="1"/> X Buy now
Illinois	200 USD = 0.316 ₿	<input type="text" value="1"/> X Buy now
South Carolina	200 USD = 0.316 ₿	<input type="text" value="1"/> X Buy now
New Jersey	200 USD = 0.316 ₿	<input type="text" value="1"/> X Buy now
Colorado	200 USD = 0.316 ₿	<input type="text" value="1"/> X Buy now
Pennsylvania	200 USD = 0.316 ₿	<input type="text" value="1"/> X Buy now



Tor

AK 47

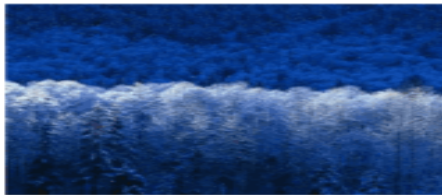


\$3.56853199 ~~\$2200.00~~

Vendor: burmtaway(2)
Ship to: USA
Ship from: USA

[VIEW DETAILS](#)

AK 47



\$12.16545010 ~~\$7500.00~~

Vendor: playdoh(1)
Ship to: usa
Ship from: ammu-nation

[VIEW DETAILS](#)

3,000,000V 18"
BATON/FLASHLIGHT STUNGUN

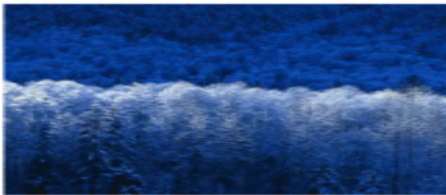


\$0.09732360 ~~\$60.00~~

Vendor: WalkThePlank(1)
Ship to: World
Ship from: USA

[VIEW DETAILS](#)

45 CARBINE



\$7.29927015 ~~\$4500.00~~

Vendor: playdoh(1)
Ship to: usa
Ship from: hhhhhh

[VIEW DETAILS](#)

AK47 KALACHNIKOV -ENVOI
DEPUIS LA FRANCE-



\$1.78970921 ~~\$1114.46~~

Vendor: acheterenfrance(2)
Ship to: European Union
Ship from: France

[VIEW DETAILS](#)



Social Media





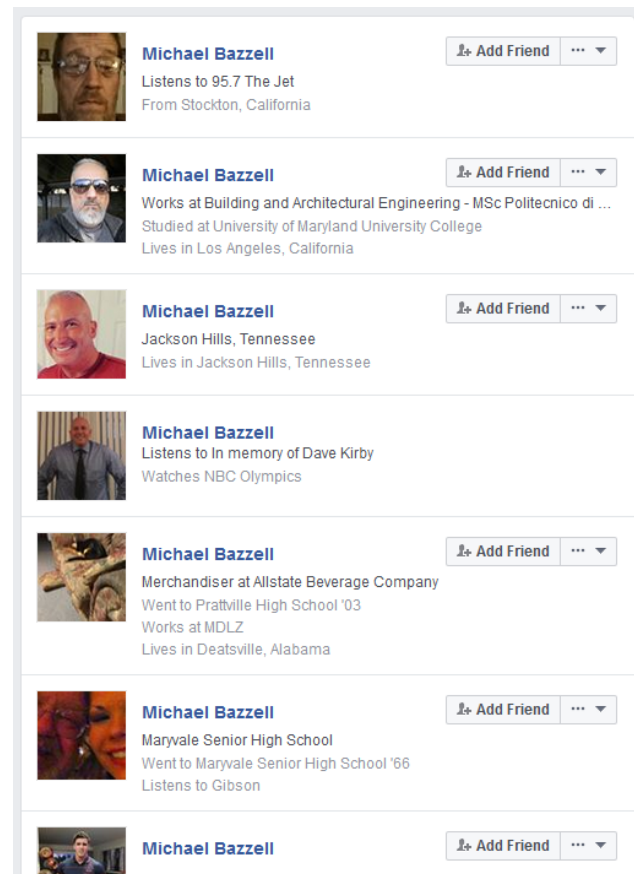
Facebook

**“Facebook says Cambridge Analytica
may have had data on 87 million
people”**



Facebook

[https://www.facebook.com
/search/str/Michael%20Ba
zzell/users-named](https://www.facebook.com/search/str/Michael%20Bazzell/users-named)





Social Media Tips

Set up an email account at GMX.com to use when creating any covert accounts.

Try to keep your identities the same across platforms.

Easy to set up covert Twitter, Instagram and LinkedIn accounts
recruitin.net



Online Communities



WAYNE STATE UNIVERSITY



Reddit



MY SUBREDDITS ▼ POPULAR · ALL · RANDOM · USERS | ASKREDDIT · WORLDNEWS · VIDEOS · FUNNY · TODAYILEARNED · PICS · GAMING · MOVIES · NEWS · GIFS · MILDLYINTERESTING · AWW · SHOWERTHOUGHTS · TELEVISION · JOKES · SCIENCE · OLDSCHOOLCOOL · MORE »

reddit hot new rising controversial top gilded wiki

Want to join? Log in or sign up in seconds. | English

Welcome to Reddit.
Where a community about your favorite things is waiting for you.

BECOME A REDDITOR and subscribe to one of thousands of communities.

trending subreddits r/WhitePeopleTwitter r/humblebrag r/pathofexile r/Pointless_Arguments r/nonononoyes 26 comments

- 14.6k Scientists in Antarctica have harvested their first crop of vegetables grown without earth, daylight or pesticides as part of a project designed to help astronauts cultivate fresh food on other planets. (apnews.com)
submitted 2 hours ago by mvea to r/space
519 comments share save hide report
- 21.7k Oklahoma governor compares teachers to 'a teenage kid that wants a better car' (cnn.com)
submitted 3 hours ago by TattooedHead to r/news
2194 comments share save hide report
- 21.5k In Assassin's Creed Origins if you spend too much time in the desert, you start hallucinating. (gfyat.com)
submitted 3 hours ago by GrandMasterSubZero to r/gaming
794 comments share save hide report
- 24.4k Czechoslovakian wolf dog. (i.redd.it)
submitted 3 hours ago by WarlockOPain77 to r/pics
538 comments share save hide report
- 10.7k TIL C&P: Thomas Jefferson used a razor to cut passages from the New Testament and literally pasted them together into what is now known as the Jefferson Bible, currently on display at the Smithsonian. He felt the focus should be on Jesus' life and moral teachings, not inexplicable miracles (americanhistory.si.edu)
submitted 3 hours ago by kissingskeletons to r/todayilearned
571 comments share save hide report
- 74.7k He waited his entire life for this moment (gfyat.com)
submitted 4 hours ago by SlimJones123 to r/funny
1749 comments share save hide report

search

username password

remember me reset password login

Submit a new link

Submit a new text post

Claim your circle

<https://www.reddit.com/user/CHRISB>

<https://api.pushshoft.io/reddit/search/comment/?author=CHRISB>



craigslist

post to classifieds

my account

search craigslist

event calendar

M	T	W	T	F	S	S
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

[help, faq, abuse, legal](#)
[avoid scams & fraud](#)
[personal safety tips](#)
[terms of use](#) new
[privacy policy](#)
[system status](#)

[about craigslist](#)
[craigslist is hiring in sf](#)
[craigslist open source](#)

[craigslist blog](#)
[best-of-craigslist](#)
[craigslist TV](#)
["craigslist joe"](#)
[craig connects](#)

detroit metro

mcb wyn okl

community

[activities](#)
[artists](#)
[childcare](#)
[classes](#)
[events](#)
[general](#)
[groups](#)
[local news](#)
[lost+found](#)
[missed](#)
[connections](#)
[musicians](#)
[pets](#)
[politics](#)
[rants & raves](#)
[rideshare](#)
[volunteers](#)

services

[automotive](#)
[beauty](#)
[cell/mobile](#)
[computer](#)
[creative](#)
[cycle](#)
[event](#)
[farm+garden](#)
[financial](#)
[household](#)
[labor/move](#)
[legal](#)
[lessons](#)
[marine](#)
[pet](#)
[real estate](#)
[skilled trade](#)
[sm biz ads](#)
[therapeutic](#)
[travel/vac](#)
[write/ed/tran](#)

discussion forums

[android](#)
[apple](#)
[arts](#)
[atheist](#)
[autos](#)
[beauty](#)
[bikes](#)
[celebs](#)
[comp](#)
[foxit](#)
[food](#)
[frugal](#)
[gaming](#)
[garden](#)
[haiku](#)
[help](#)
[history](#)
[housing](#)
[parent](#)
[pets](#)
[philos](#)
[photo](#)
[politics](#)
[psych](#)
[recover](#)
[religion](#)
[rofo](#)

housing

[apts / housing](#)
[housing swap](#)
[housing wanted](#)
[office / commercial](#)
[parking / storage](#)
[real estate for sale](#)
[rooms / shared](#)
[rooms wanted](#)
[sublets / temporary](#)
[vacation rentals](#)

for sale

[antiques](#)
[appliances](#)
[arts+crafts](#)
[atv/utv/sno](#)
[auto parts](#)
[aviation](#)
[baby+kid](#)
[barter](#)
[beauty+hlth](#)
[bikes](#)
[boats](#)
[books](#)
[business](#)
[cars+trucks](#)
[cds/dvd/vhs](#)
[cell phones](#)
[clothes+acc](#)
[collectibles](#)
[computers](#)
[electronics](#)
[farm+garden](#)
[free](#)
[furniture](#)
[garage sale](#)
[general](#)
[heavy equip](#)
[household](#)
[jewelry](#)
[materials](#)
[motorcycles](#)
[music instr](#)
[photo+video](#)
[rvs+camp](#)
[sporting](#)
[tickets](#)
[tools](#)
[toys+games](#)
[trailers](#)
[video gaming](#)
[wanted](#)

jobs

[accounting+finance](#)
[admin / office](#)
[arch / engineering](#)
[art / media / design](#)
[biotech / science](#)
[business / mgmt](#)
[customer service](#)
[education](#)
[food / bev / hosp](#)
[general labor](#)
[government](#)
[human resources](#)
[internet engineers](#)
[legal / paralegal](#)
[manufacturing](#)
[marketing / pr / ad](#)
[medical / health](#)
[nonprofit sector](#)
[real estate](#)
[retail / wholesale](#)
[sales / biz dev](#)
[salon / spa / fitness](#)
[security](#)
[skilled trade / craft](#)
[software / qa / dba](#)
[systems / network](#)
[technical support](#)
[transport](#)
[tv / film / video](#)
[web / info design](#)
[writing / editing](#)
[\[ETC\]](#)

english

nearby cl

[akron-canton](#)
[ann arbor](#)
[ashtabula](#)
[battle creek](#)
[brantford](#)
[central mi](#)
[chatham-kent](#)
[cleveland](#)
[erie](#)
[flint](#)
[fort wayne](#)
[grand rapids](#)
[jackson](#)
[kalamazoo](#)
[kitchener](#)
[lansing](#)
[lima-findlay](#)
[london](#)
[mansfield](#)
[meadville](#)
[monroe](#)
[port huron](#)
[saginaw](#)
[sandusky](#)
[sarnia](#)
[the thumb](#)
[toledo](#)
[tuscarawas co](#)
[windsor](#)
[youngstown](#)

us cities

us states

canada

cl worldwide

WAYNE STATE UNIVERSITY



Flippity.com

Goofbid.com

Fatfingers.com

Searchtempest.com



“site:amazon.com John Smith”

“site:targetwebsite.com John
Smith”

[Amazon.com/gp/registry/search](https://www.amazon.com/gp/registry/search)

WAYNE STATE UNIVERSITY



You must have an account to browse profiles.

You must have a premium account to contact anyone.

If a person uses one dating services, they more than likely use others (with the same profile info).



E-Mail

hunter.io/email-verifier

verify-email.org

tcpiputils.com/email-test

tools.verifyemailaddress.io

findanyemail.net

email-format.com

haveibeenpwned.com



Phone Numbers

[Twilio.com/lookup](https://www.twilio.com/lookup)

[Opencnam.com](https://www.opencnam.com)

[Whocalld.com](https://www.whocalld.com)

[Calleridservice.com](https://www.calleridservice.com)

[Nextcaller.com](https://www.nextcaller.com)

[Challenge.burnerapp.com](https://challenge.burnerapp.com)



Photos

images.google.com
Bing.com/images

A screenshot of the Google Images search interface. At the top is the Google logo. Below it is a search bar containing the word 'google'. To the right of the search bar are icons for a camera and a magnifying glass. Below the search bar are tabs for 'All', 'News', 'Videos', 'Maps', 'Images' (which is selected and underlined), and 'More'. To the right of these tabs are links for 'Settings' and 'Tools'. Below the tabs is a section titled 'Search by image' with a close button (X). Under this title is the text 'Search Google with an image instead of text. Try dragging an image here.' Below this text are two options: 'Paste image URL' with a question mark icon, and 'Upload an image'. Below these options is a large text input field. To the right of the input field is a blue button labeled 'Search by image'.



Photos

Tineye.com

Image.baidu.com

Imageraider.com

Pictriev.com

Twicsy.com

Twipho.net



Photos

Exif.regex.info/exif.cgi

Fotoforensics.com

Izitr.com

[Forensically \(29a.ch/photo-forensics\)](http://Forensically(29a.ch/photo-forensics))



Photos

Forensically^{Beta} Open File Help



Magnifier

Magnification

4

Enhancement

Histogram Equalizatio ▾

Clone Detection

Error Level Analysis

Noise Analysis

Level Sweep

Luminance
Gradient



Questions?

