silo
BY AUTHENTIC8

2021 HANDBOOK

Surface and dark web research: tips and techniques

How to access and analyze suspicious or malicious content without exposing your resources or your identity

Table of Contents

Secure, anonymous access to the surface, deep and dark web

Silo for Research is an online investigation solution with secure, anonymous and centralized access to the surface, deep and dark web. Built on Authentic8's patented, cloud-based Silo Web Isolation Platform, it provides 100-percent protection from all web-borne threats and complete oversight of all research activity.

Investigative teams can accomplish their goals without introducing risk to the organization or revealing intent. And all web activity is logged and encrypted to ensure and monitor compliance.

See how Silo for Research can give analysts the access they need without risk — visit our Experience Center now.

Full isolation:
All web code is executed on Silo servers, not end-user devices

Cloud-based:
Turn-key, cloud-hosted solution that creates a clean instance every time

Managed attribution:
Configure the browser fingerprint and egress location

Access surface, deep or dark web:
One-click access to any destination without tainting your environment

Workflow enhancements:
Integrated tools for content capture, analysis and storage

Complete audit oversight:
Encrypted audit logs of all web activity are captured in one place and easily exported

Investigating surface websites' ownership and history

Analysts collecting publicly available information (PAI) encounter various sites and services with valuable information. While this information is of intelligence value, there are biases, agendas, and different reasons for the dissemination of such information.

To identify these reasons, analysts have to find information on the individuals/organizations behind the site/service which hosted, maintained, and funded them.

This information is commonly obfuscated, but accessible with proper research tools and tradecraft.

Resources used for site ownership research

Analysts can leverage the following sites and services:

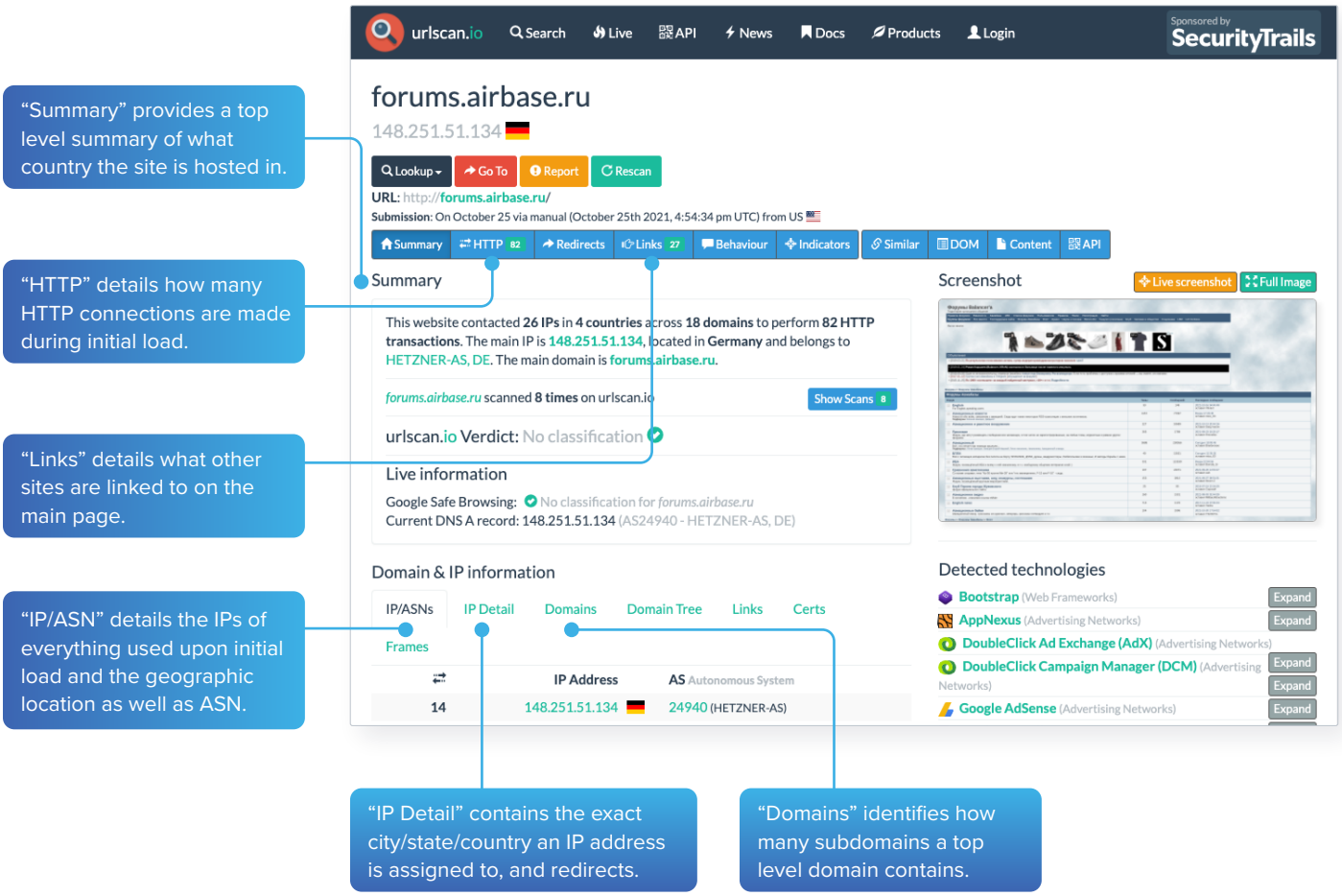
- **WHOIS records:** WHOIS records provide top level domain (e.g., russianmilitaryblog.com) information such as exact dates of registration, addresses, names, and phone numbers associated with the domain. In addition, it provides web host information.
  - URL Scan: https://urlscan.io
- **Advanced search engine use:** Using advanced search engines and search engine parameters on uniquely identifying information found on the site or WHOIS records (i.e., emails, names, mail servers, other IP addresses, etc.) can provide additional information on the site or service administrator/s.
  - Carbon Date: http://carbondate.cs.odu.edu
  - Google Dorking: https://www.google.com

On the following pages we describe how to use these tools and give examples of information that can be gleaned from them.

For more information please contact osint@authentic8.com.

WHOIS record analysis: URLscan.io

URLscan.io conducts analysis of a domain, providing the end user with information on all HTTP connections made during the site's retrieval, outbound links from the page, as well as detailed IP address information.



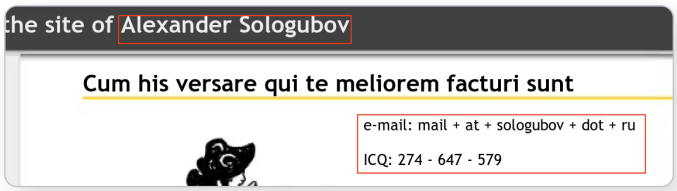
Example analysis of result panels

Forums.airbase.ru, a russian military forum, uses hosting primarily in Germany, which is likely due to Germany's strict data privacy laws. From the HTTP panel, the site uses Google Analytics for user tracking and also uses Yandex.ru for email. From the Links panel, a live "Telegram" chat is also available for users.

Example analysis of the result panel

Only one other IP aside from the current German IP has been used for hosting forums.airbase.ru.

This IP is 95.31.43.16, which also is used by a range of other domains — one of which, sologubov.ru has personal information on the individual behind forums.airbase.ru. This reveals the web host's full name, email, and ICQ number for further targeting.

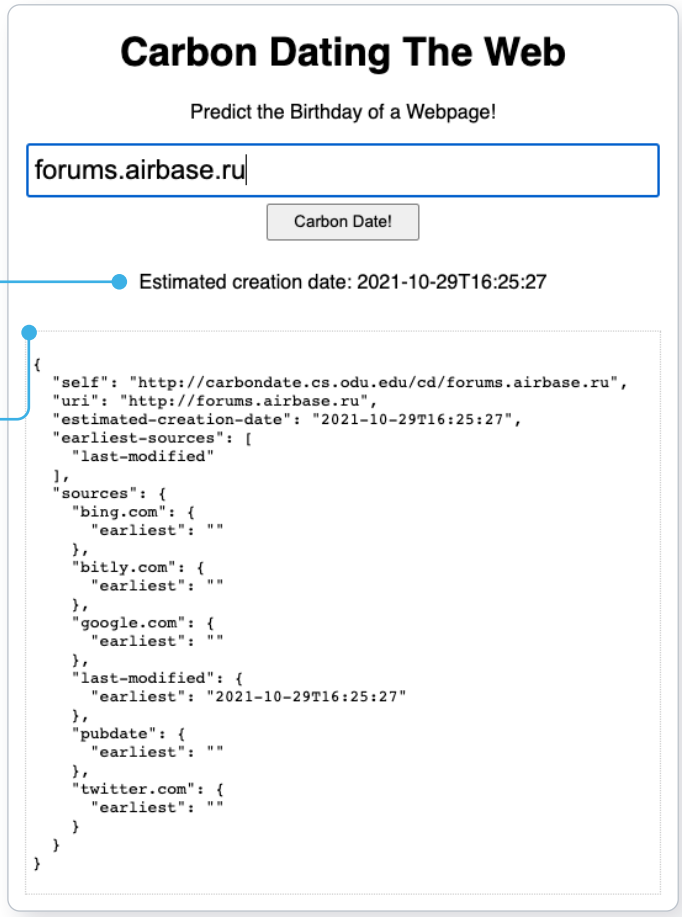


Advanced search engine: Carbon Date

This advanced search engine automates advanced searches against web.archive.org, archive.md, Bing, bit.ly, Google, and Twitter to identify the earliest scrape/index or mention of a website on the web.

"Estimated creation date" pulls the earliest date from the result set.

The result set shows the results from each source searched, and when available, a URL to the direct source itself.



Example analysis of the results panel

The earliest mention of forums.airbase.ru was in October of 2003. To view the first ever scrape of this site by web.archive.org, use the URL in the "uri-m" field.

Advanced search engine: Google Dorking

Advanced Google search parameters and features are used in a technique called "Google Dorking."

Users must combine various search parameters to effectively search and filter down results of interest to them.

The most commonly used Google Dorks are:

- **Intitle:** identifies any mention of search text in the web page title
- **Allintitle:** only identifies pages with all of the search text in the web page title
- **Inurl:** identifies any mention of search text in the web page URL
- **Intext:** only identifies pages with all of the search text in the web page URL
- **Site:** limits results to the specified file type
- **Filetype:** limits results to only the specified file type
- **Cache:** shows the most recent cache of a site specified
- **Around (X):** searches for two different words within X words of one another

The most commonly used Boolean logic search operators are:

- **AND:** searches for content mentioning two phrases anywhere
- **OR:** used in multi-part search, searches for content mentioning any combination of the first search term and two unique second search variables
- *** :** the asterisk acts as a wildcard and searches for any word or phrase
- **– :** the dash excludes any specific word or phrase (if using brackets or quotation marks)
- **( ) :** the parenthesis group specific terms or search operators together

Example analysis using advanced Google Search parameters

`site:sologubov.ru ICQ OR email`
This search will find mentions of ICQ or email on a site of interest, resulting in an ICQ number and email previously unknown to an analyst.

`site:forums.airbase.ru contact OR admin OR mod OR moderator OR donation`
This search will find uniquely identifying information that can be linked to a person, such as mentions of a moderator, a contact page, or a donation page (such as Paypal, Bitcoin, etc), resulting in multiple pages with mentions of the moderator and a donation page for their health bills.

`“95.31.43.16”`
This search will find exact mentions of forums.airbase.ru, resulting in mentions on another forum of Russian censorship of the servers IP address.

Conclusion

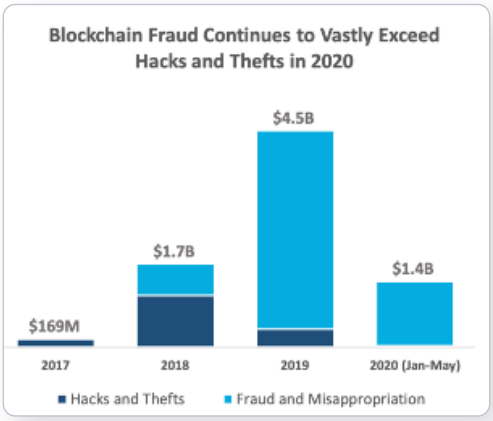
This workflow covers how to investigate the ownership and hosting information related to a site/service of interest. Results from the analysis include key identifiers such as server IPs, other related domains, and the webhost’s email address/name/ICQ number that can then be incorporated further into a finished intelligence product.

For more information please contact osint@authentic8.com.

Crypto money laundering on the rise

Since Bitcoin's historic rise, the number of users participating in the cryptocurrency ecosystem has surpassed 100 million. This increase in active cryptocurrency users has also led to a surge of cryptocurrencies being used to launder money. According to the United Nations Office on Drugs and Crime, money laundering costs the global economy between $800 billion and $2 trillion per year — that's two to five percent of the world's gross domestic product.

As the use of cryptocurrency continues to rise, so will its use in money laundering, especially with multiple types of available crypto coins and a good amount of anonymity for traders to hide their true identities. Add the dark web, and you have a murky, constantly changing and decentralized environment that creates many additional challenges for investigators.



Source: CipherTrace Cryptocurrency Intelligence

FinCEN warns of threats posed by virtual currency misuse

Criminals continue to exploit virtual currency to support illegal activity, money laundering and other behavior endangering U.S. national security. To help financial institutions, law enforcement and regulators who work with convertible virtual currencies (CVCs), the Financial Crimes Enforcement Network (FinCEN) offers guidance to assist organizations in identifying and reporting suspicious activity. The advisory highlights the risks associated with dark web marketplaces, peer-to-peer (P2P) exchangers, unregistered money services businesses and CVC kiosks. It also gives organizations a set of tools to help identify unregistered financial activity and suspicious virtual currency purchases, transfers and transactions.

The need for effective AML programs

The FinCEN regulatory framework mandates that businesses develop, implement, and maintain an effective anti-money laundering program ("AML program") that is designed to prevent organizations from being used to facilitate money laundering and the financing of terrorist activities.

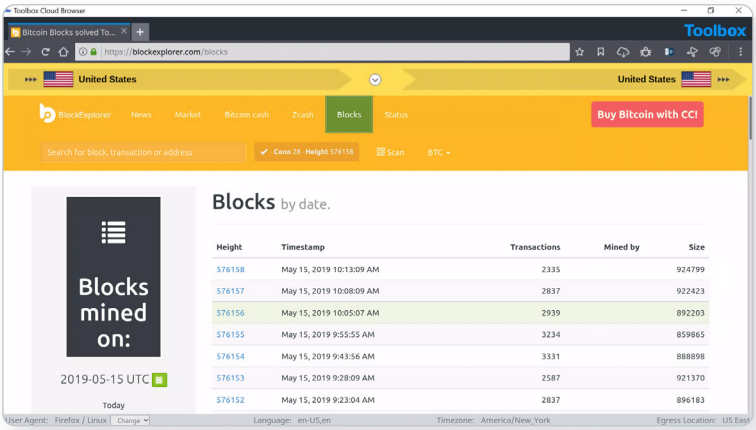
The minimum set of requirements for an AML program include:

- Establishment of policies, procedures, and internal controls designed to assure ongoing compliance (including verifying customer identification, filing reports, creating and retaining records and responding to law enforcement requests
- Designation of individuals responsible to assure day-to-day compliance with the program
- Training for appropriate personnel, including training in the detection of suspicious transactions
- Ongoing independent reviews to monitor and maintain an adequate program

> Without sufficient controls in place, financial institutions cannot reasonably assess and mitigate the potential risks posed by a customer's source of funds, and criminals can exploit the U.S. financial system by engaging in illicit transactions. Individuals engaged in illicit activity will continue to exploit these vulnerabilities as long as the perceived risk of detection is less than that of using traditional financial institutions.

Tracking cryptocurrencies

How can CVC transactions be tracked? One popular way is using blockchain technology. Blockchain is an open, decentralized ledger that records transactions between two parties in a permanent way without needing third-party authentication. For example, every transaction involving a Bitcoin address is stored forever in the blockchain; however, Bitcoin addresses are pseudonyms, meaning that the identity of the address owner (i.e., who receives bitcoin at that address) is generally unknown.



Bitcoin blockchains from blockexplorer.com

If a user's address is ever linked to their identity, every transaction will be linked to that user. Below are examples of OSINT tools that allow investigators to search by block number, address, block hash, transaction hash or public key to find out more information on bitcoin transactions.

- https://www.blockchain.com/explorer
- https://www.chainalysis.com/
- https://bitcoinwhoswho.com/

To prevent tracking on their transactions, money launderers have begun to use a system known as cryptocurrency tumblers. Cryptocurrency tumblers mix potentially identifiable currency with untraceable currency to make it harder to track.

Some addresses can be grouped by their ownership, using behavior patterns and publicly available information from off-chain sources. The challenge for forensic investigators, as usual, is to identify the persons behind the keyboard, which may be accomplished through a mixture of traditional investigative and digital forensic techniques.

Bitcoin address reports

Once a Bitcoin address is identified, it can be run through a blockchain tracking tool. Using bitcoinwhoswho.com, investigators can generate a report for bitcoin address 1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tHJ.

BTC Address	1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tH	**# Website Appearances**	9
Wallet Name	000a027d20045b7d	**Last Transaction IP**	47.254.169.156, 52.60.49.56, 148.251.139.241
Current Balance	112.11330270	**Total Received**	161472.17413649
# Transactions	13121	**# Output Transactions**	Loading...
First Transaction	13 Jun 16	**Last Transaction**	16 May 19
Last Known Input	Loading... Loading...	**Last Known Output**	1BMjmWXy7h... 16 May 19
Repeated Inputs From (50 most recent transactions)	... 37	**Repeated Outputs To** (50 most recent transactions)	1BMjmWXy7h... 13 1PqU8hFVgy... 9 1NSUvXCtWw... 4

Bitcoin address report from bitcoinwhoswho.com

Probable fields of interest:

- **Current balance/total received:** This data point allows analysts to hypothesize which type of address they're dealing with. Due to the high volume of transactions, this wallet likely belongs to a bitcoin miner.
- **Last transaction IP:** Analysts can view the last known IP to relay an output transaction involving a selected address. Repeated use of an IP can be used as a unique identifier.
- **Website appearances:** Provides a view of any site where this exact bitcoin address appeared, which could be of value for identifying reputation/type of transactions.
- **Repeated inputs from/repeated outputs to:** This data point allows analysts to view the 50 most recent Bitcoin addresses involved with incoming and outbound transactions associated with this address. By looking at the transaction history and frequently interacted-with wallets, investigators can engage in network and link analysis to identify patterns and possible relationships between the disparate Bitcoin addresses.

Tracking online drug dealers

Drug dealers use social media to sell illegal narcotics

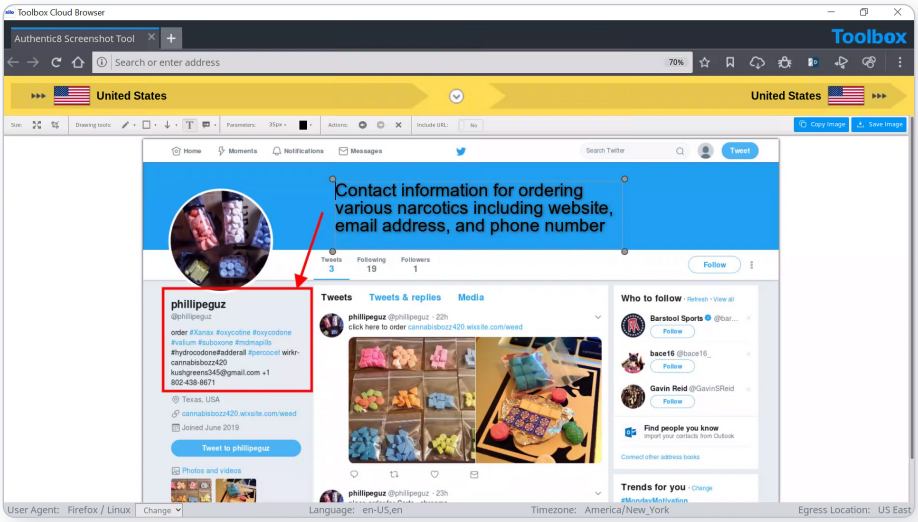
The continued rise of social media over the past ten years has led to drug dealers using various social media platforms to sell illegal narcotics on the surface web. Investigators need a safe and anonymous browsing and research framework that allows them to investigate social media drug dealers without the risk of being identified or infecting their endpoint with malicious web code. This workflow will cover how the Silo Web Isolation Platform and managed attribution solution can be utilized to identify and investigate social media drug dealers anonymously.

Identifying and investigating drug dealers on social media with Silo for Research

The first step when conducting an investigation using Silo for Research is to select a regionally appropriate egress location and a user agent string that matches regional norms. (For the sake of this workflow, we will use the U.S. and Google Chrome running on a Windows 10 machine as the user agent string.) This process allows investigators to blend in as locals of that area.

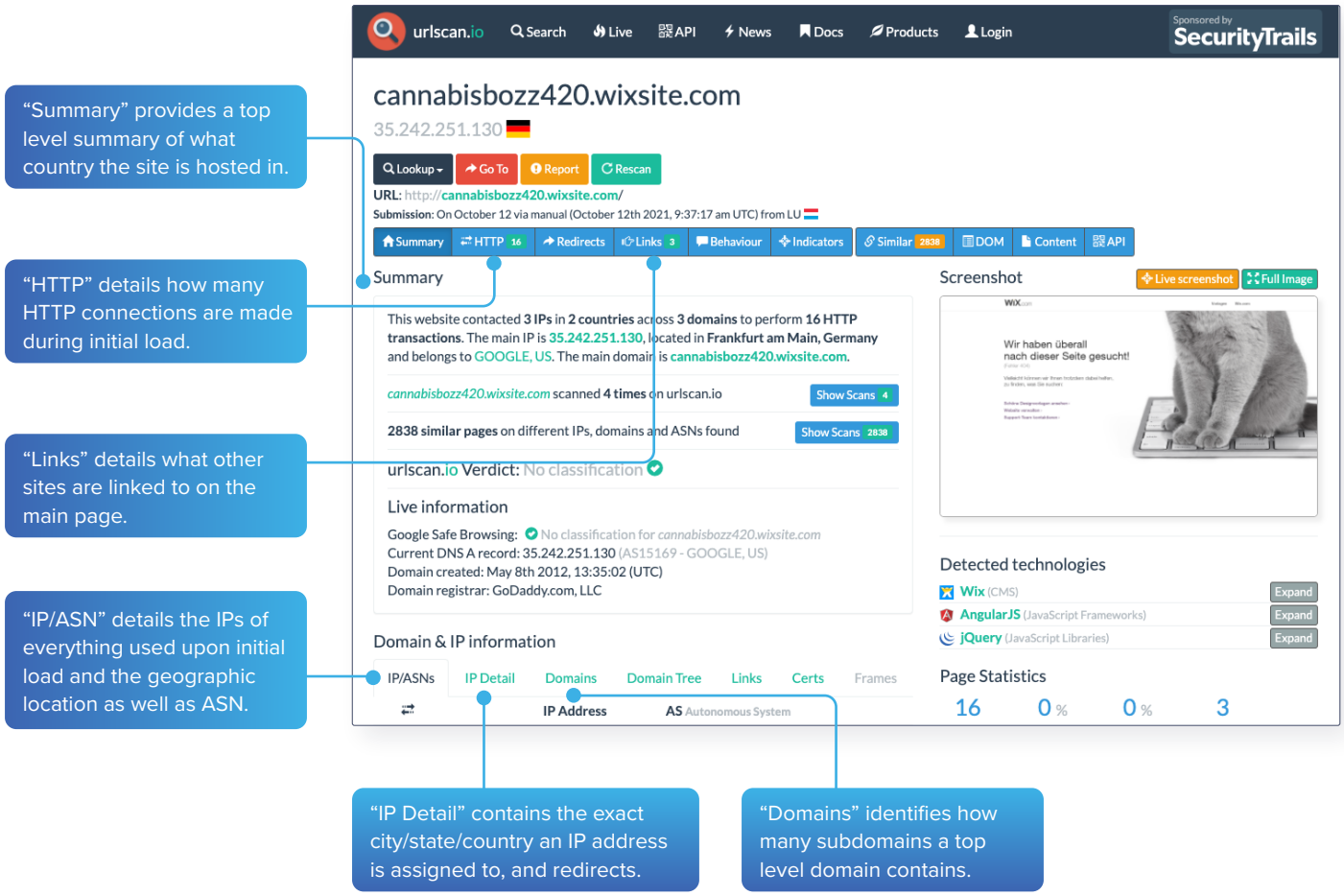
When conducting research on social media, there are various data capture tools included with Silo for Research that can be used for gathering intelligence. This first is a video download tool that allows investigators to simply download any video currently playing on their screen to save as evidence. The second is a screenshot tool that gives investigators the ability to take a screenshot of an entire page. The screenshot tool also gives investigators the ability to edit the screenshot by including boxes, arrows and text to highlight important information, as well as the ability to include the URL of where the screenshot was taken. This allows investigators to easily return to that page to gather additional intelligence.

By conducting a search on Twitter for #xanax, the Twitter user @phillipeguz was identified as an account using Twitter to market and sell illegal narcotics. Shown on this profile is information on how to place an order, including a website, email address and phone number. This information can now be run through additional search engines to possibly identify the owner of the account.



Resources for site ownership research

WHOIS records provide top-level domain information such as exact dates of registration, addresses, names and phone numbers associated with the domain. Additionally, it provides web host information. @phillipeguz posted the website cannabisbozz420 dot wixsite dot com on their Twitter feed as a location to purchase the illegal narcotics. Using https://urlscan.io/, a report was generated for this site.

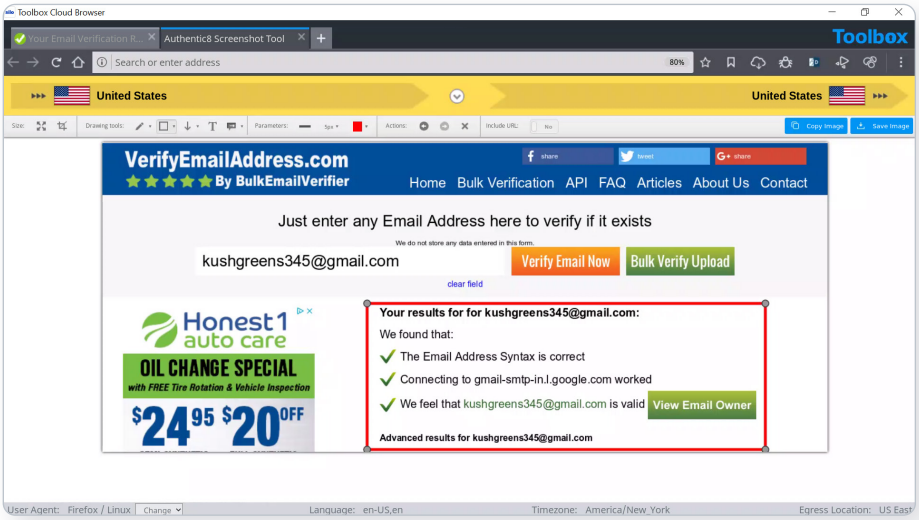


Example analysis of result panels

According to the generated report, cannabisbozz420 dot wixsite dot com/weed/about uses hosting primarily in the United States but also has hosting in Germany. This means that the distribution could also include locations outside the United States. On the website, the site owners also listed packaging locations in the United States, Germany, Australia, New Zealand, Switzerland, Sweden, Ireland and Poland. The following screenshot from their website depicts their packaging locations around the world. It appears that the domain was registered by godaddy.com. This information could be used to send out a subpoena or court order to godaddy.com to find out who registered the domain with them.

Phone number reverse lookup

The phone number +1-802-438-8671 was also listed as contact information for ordering narcotics from this Twitter page. Having this number available is extremely valuable for the investigation. The number can be run through a reverse phone number search engine to identify the subscriber information. The following screenshot is from a report generated by https://www.whitepages.com/phone/1-802-438-8671 for the listed phone number.



Example analysis of result panels

Although there is no identity listed for the number and the number is associated with a voice over internet protocol (VoIP), there is some valuable information that can be pulled from the report. Seeing that the number has a Rutland, Vermont, area code is telling: due to the website listing a packaging location on the East Coast, it is possible that the East Coast is their shipping headquarters.

Searching for additional social media profiles by email

The third piece of contact information listed on this Twitter page is the email address kushgreens345 at gmail dot com.

What is exif data?

When a digital image is captured, metadata specific to that image is stored. This information is called exchangeable image file format" — "exif" for short — data. Some examples of exif data are date, time and file size. This information can be extremely useful when conducting image analysis. Analysts can exploit exif data to find the location of the image, camera make and model, and other information that is valuable to the intelligence production cycle.

Incorporating exif data

To find exif data, an analyst can use a number of different tools. FotoForensics is the service used for the workflow described here. In the example in this report, we've taken an image of a cargo ship from a ship-spotting forum (see figure 1) and uploaded it to FotoForensics to analyst the exif data.

User-uploaded images in forums will likely have their exif data intact. However, if the analyst tries to pull exif data from an image on social media, there will likely be little to no data present. Social media platforms have begun to strip exif data off of user images to protect user privacy.

Once on FotoForensics, the analyst will have two options for image analysis. The analyst can paste an image URL or upload a file for analysis (see figure 2).

For this workflow, the analyst can save the above image of the cargo ship, and then upload the .jpg file into FotoForensics.

When the upload is complete the analyst should select the metadata field from the "Analysis" dropdown list (see figure 3). The analyst can then scroll down and begin to review information pertinent to the investigation.

Figure 1 | Image from shipspotting.com

Figure 2 | FotoForensics user interface

Figure 3 | FotoForensics post image upload with metadata analysis selected

After reviewing the exif data collected by FotoForensics, a few pieces of information stand out. The analyst can glean what type of device was used to capture the image (see figure 4). This information can be useful when investigating a party of interest that may have a standard issue camera for reconnaissance.

FotoForensics also provides the analyst with an approximate latitude and longitude coordinate (see figure 5). This coordinate can be further incorporated into a targeting packet or reconnaissance mission.

Overall, the information captured from exif data can greatly enhance a unit's analytic ability. The exploitation of images, whether of an adversarial object or person or of a location, can help the analyst to further understand their battlespace or objective.

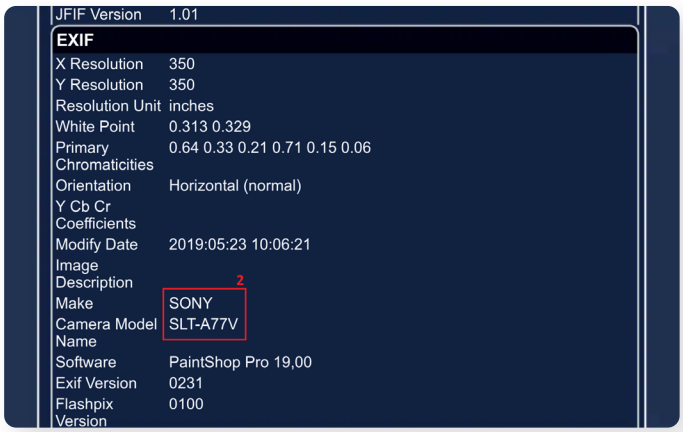


Figure 4 | FotoForensics exif data results including camera model

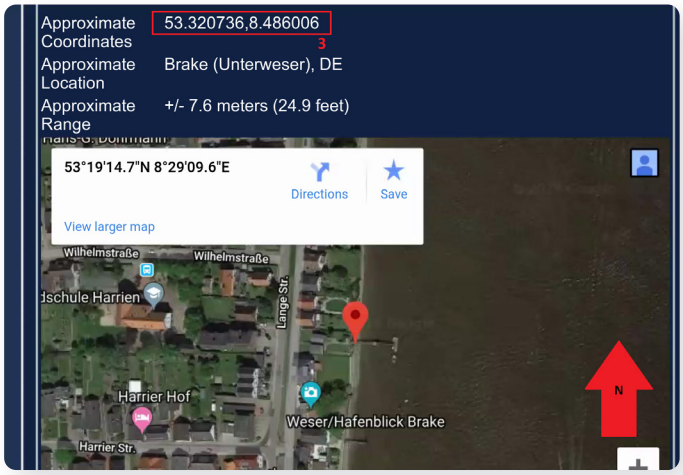


Figure 5 | FotoForensics exif data results including geographic coordinates.

Conclusion

This workflow covers how to extract and incorporate exif data into the intelligence product. The analyst found a .jpg file of a cargo ship and leveraged FotoForensics to conduct exif data analysis. Results from the analysis included key identifiers such as equipment used and location data that can then be incorporated further into a finished intelligence product.

For more information please contact osint@authentic8.com.

What is Shodan?

According to GitHub, Shodan is “the world’s largest search engine for internet-connected devices”. But what exactly does this mean?

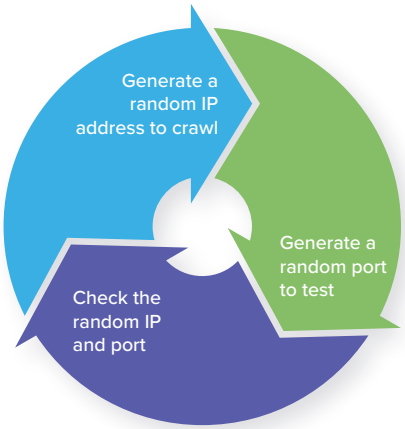
Most search engines are text indexes, meaning they allow search for content based on keywords. However, the task of scanning, indexing the ports and services running, and then searching for internet-connected devices at the scope and scale of the internet has been largely impossible to do.

With Shodan, it is now possible to identify nearly any internet-connected device, such as industrial control systems running specific software, internet-of-things devices like smart TVs, FTP servers with sensitive information and even very small aperture terminals (VSATs) on naval vessels.

How Shodan works

Shodan maintains servers across the globe that scan the internet-connected devices and harvest the banner of whatever is running on the server.

The diagram at right shows how these servers crawl.



These internet-connected devices return different banners depending on the different service running on it.

Example search returns

Two examples are below, one for an IP camera and one for an FTP server (FTP runs on port 21):

Document Error: Unauthorized
62.112.117.205
OAO MGTS
Added on 2019-05-07 10:56:51 GMT
Russian Federation, Odintsovo
Technologies: **IIS\;confidence:50**

```
HTTP/1.1 401 Unauthorized
Server: Cam-Webs
Date: Tue May  7 13:20:55 2019
WWW-Authenticate: Basic realm="Megapixel_IP_Camera"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
```

188.225.26.71
vds-olgafirsova.timeweb.ru
hosting & vds
Added on 2019-05-28 17:02:17 GMT
Russian Federation

```
220 (vsFTPd 3.0.2)
230 Login successful.
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD...
```

Basic Shodan searches and filters

Shodan allows for advanced search using filters. Filters are entered in a simple format: a filter, a colon and the search value, with no spaces between these three components.

Filter format	`filtername:value`
Filter example	`City:Moscow`

If searching a value that includes a space, double quotes must be used.

Filter example	`City:"Saint Petersburg"`

Examples of Shodan's most useful geographic filters

Country using two-letter geocode	`country:XX`
City using city name	`city:cityname`
Geographic coordinates in a bounding box	`geo:top-left-lat,top-left-long, top-right-lat,top-right-long`
Region	`region:region-name-or-state`

These filters are useful when attempting to identify something of interest in a specific AOR.

For example, a search for webcam `City:Incirlik` would find webcams, with some hopefully located near Incirlik Air Base.

Examples of software-focused filters

Firewall port	`port:XX`
Product name	`product:XX`
Product version	`version:XX`
Product vulnerability CVE	`vuln:XX`

These filters are useful when searching for a particular technology, like a database, a file server or vulnerable software.

For example, a search for `port:21 country:"RU" "login successful"` would find file transfer protocol (FTP) servers in Russia that do not require logins. This could yield valuable unsecured information if found in a location of interest, or can be used as a non-attributable temporary data transfer point.

Examples of organization-focused filters

Device hostname	`hostnames:XX`
Organization assignment	`org:XX`
Network CIDR range	`net:XX`

Examples of Shodan's temporal filters

Results before a given date	`before:00/00/0000`
Results after a given date	`after:00/00/0000`

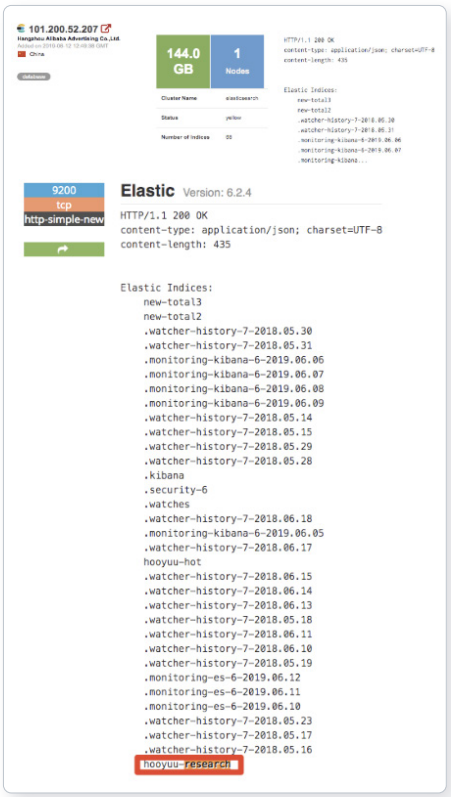
Finding open databases

A few databases openly list their indices: MongoDB, ElasticSearch and CouchDB.

Below are the baseline searches that allow you to quickly identify open databases with potentially valuable information sources.

Example database searches

Elasticsearch databases	`product:elastic port:9200`
MongoDB databases	`product:MongoDB`
CouchDB databases	`product:couchdb`
Kibana visualization of Elasticsearch	`kibana content-length: 217`
Gitlab software repos	`http.favicon.hash:1278323681`
Rsync utilities	`product:rsyncd`
Jenkins software automation	`jenkins 200 ok`



Combining these search filters and other key phrases allows analysts to identify high value and unsecured information.

Example search for Elasticsearch databases in China mentioning "research":

`product:elastic port:9200 country:cn research`

This results in identifying an IP address hosting an open elasticsearch index with mentions of research. In this case, the research is about "Hooyuu," a Chinese social media site.

The others range from what looks like security research, notifications and some form of alerting.

For more information please contact osint@authentic8.com.

silo
BY AUTHENTIC8

DATA SHEET

Silo for Research

Safe and anonymous access to all areas of the web

Silo for Research embeds security, identity and data policies directly into the browser, eliminating the risk of the web, and protecting your applications and data from exploits and misuse.

Silo for Research is a purpose-built solution for conducting online research without exposing analysts' digital fingerprint. Safely pursue investigations across the surface, deep or dark web through an isolated, cloud-based browsing interface while controlling how you appear online.

Protect your identity and your investigation

Adversaries exploit tracking mechanisms in traditional browsers to uncover analysts' identity and intent — and spoil the investigation or retaliate against them. Silo for Research manages the details they see, so analysts don't arouse suspicion.

Manage attribution

Blend in with the crowd while conducting sensitive online investigations. Silo for Research equips investigators with dozens of options to spoof their geolocation, utilizing Authentic8's global network of internet egress nodes.

But building a complete "location narrative" requires more than just changing egress. Investigators using Silo for Research can control a range of details including:

- **Browser fingerprint:** time zone, language, keyboard, operating system, device type, web browser
- **Network address:** physical location, internet provider, subscriber information
- **Data transfer and protection:** isolated browsing session, one-time-use browser (no persistent tracking), policy control to restrict upload/download, copy/paste, etc.

Isolate browsing

Ensure 100% segregation between your device — including the apps and data it holds — and all that's encountered during online investigations — like trackers, malware and more — across the surface, deep and dark web.

HOW THE BROWSER BETRAYS YOU

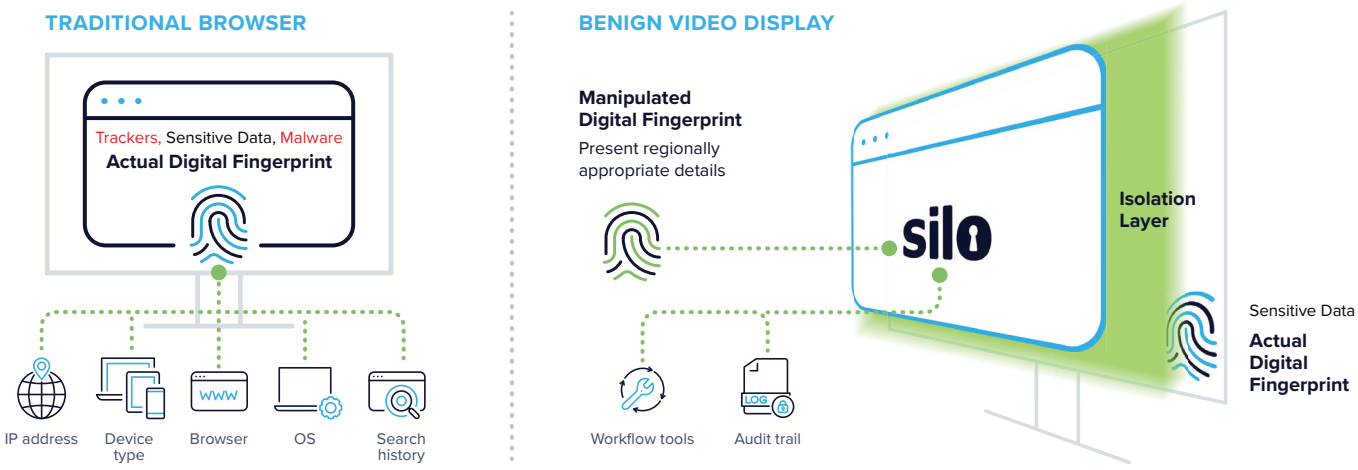
Traditional browsers disclose a range of information about you to the websites you visit.

- Passed by your browser: device type, OS, software/plugins installed, time zone, audio/video devices
- Stored in your browser by websites: cookies, HTML5 local storage
- Derived from content displayed: HTML5 canvas fingerprinting, audio

By combining these details, the subjects of your investigation can get a highly unique picture of who you are. Once they realize they're under investigation, they could hide, feed you disinformation or retaliate — online or in real life.

Silo for Research is built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that's managed by policy. All web activity is logged and encrypted so compliance teams can be sure that the tools are being used appropriately.

And, each session is launched as a one-time-use browser, ensuring cookies and supercookies don't follow investigators, even between sessions.



Improve efficiency

Purpose-built tools and third-party integrations give investigators the workflow tools they need to move through their caseload effectively. Built-in features for translation, capture and annotation simplify the data collection and analysis process. Authentic8 Secure Storage also makes it easy to save and collaborate safely on information, while adhering to policy.

Additional features are available to automate analysts' tasks, including for collection and multi-search workflows, while adhering to tradecraft best practices.

More than 500 of the world's most at-risk enterprises and government agencies rely on Silo for Research to conduct secure and anonymous online investigations, including for:

- Trust and safety
- Intelligence and evidence gathering
- Security intelligence
- Fraud and brand misuse
- Corporate research and protection
- Financial crime and compliance

To learn more about Silo for Research, request a demo or contact a sales representative.

silo BY AUTHENTIC8

INFOGRAPHIC

Top 5 Social Media Research Tools for Online Investigations

Instagram search apps

1 BILLION users on Instagram

Google reverse image search

www.google.com/imghp?hl=en&tab=ri&ogbl

- Paste or upload images to find similar images as well as other websites where that exact image has appeared. Great for finding additional social media pages for a subject

Twitter search apps

330 MILLION users on Twitter

Tweet Beaver

tweetbeaver.com

- Receive a complete analysis on an individual's Twitter profile, including tweets, replies, retweets, hashtags used, sources of tweets (Android, iPhone, online) and geotagged tweets

SocialBearing

socialbearing.com

- Comprehensive suite of searching options. Make links across variables

Reddit search apps

542 MILLION users on Reddit

Track Reddit

www.trackreddit.com

- Receive notifications on keyword searches to identify who is discussing certain topics

Reddit Insight

www.redditinsight.com

- Search by Reddit username to receive a complete overview of that username, including when the account was created, email address, posts and most common subreddits where the account has posted