silo
BY AUTHENTIC8

2021 HANDBOOK

Tools and Techniques for Online Law Enforcement Investigations

Table of Contents

Keep your online investigations anonymous and secure, even on social media and the dark web

Silo for Research enables law enforcement to gather intelligence and evidence securely and anonymously across the surface, deep and dark web. Built on Authentic8's patented, cloud-based Silo Web Isolation Platform, Silo for Research provides 100-percent protection from all web-borne threats and complete oversight of all research activity. Investigators can count on full online anonymity in an isolated browsing environment, and increase efficiency with an integrated suite of workflow productivity tools.

State, local and federal law enforcement agencies across the country rely on Silo for Research every day to protect their investigations. See how its managed attribution capabilities can make a powerful difference for your organization — 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

silo
BY AUTHENTIC8

Going after criminals on their own turf: the internet

How law enforcement can stay safe in online investigations

Today, nearly all criminal investigations — not just cybercrime investigations — have the potential to include online research. Law enforcement professionals routinely look up persons of interest on open-source databases, social media, online marketplaces and web forums. They scour court websites, find personal records and uncover connections through simple as well as complex web searches.

Online research is crucial to building a thorough case, but it comes with an array of challenges that could affect the outcome of the investigation or put the investigator — or their organization — at risk. With every click in a traditional web browser, law enforcement professionals are giving away important details about their identity and their mission. And if the subjects of their investigation catch wind of either, they could go into hiding, disinform or retaliate.

To protect investigations, the law enforcement professionals that conduct them and the agencies they represent, it's vital to be aware of the inherent risks of online research — and what tools and tradecraft can be used to overcome them.

Why are online investigations risky?

The cybersecurity risks of the internet are well documented in daily headlines of ransomware attacks, dangerous vulnerability exploits and massive data breaches. In July 2019, the Los Angeles Police Department was involved in a data breach that released thousands of current aspiring police officers' personal records. A year later in July 2020, the BlueLeaks archive exposed the personal information of 700,000 cops.

These and other cyberattacks show the risk law enforcement agencies are up against simply because of devices and corporate networks connecting to the internet.

But there's another risk to those conducting online investigations: attribution.

Attribution could reveal your identity and intent

Attribution refers to all the identifiable details that websites collect each time you visit. These details are passed to websites by different sources, including the device and browser you're using. Combined, attribution details create a digital fingerprint that is extremely unique and can easily be used to uncover your actual identity.

Traditional browsers like Chrome, Firefox or Safari are built to track users and obtain an array of information about their device, browsing activity and more. These functions exist to tailor browsing experiences based on your location, device settings, browsing history, browsing behavior and details of the browser itself. Most of this information is monetized and resold.

While a bit creepy, most internet users tolerate such tracking. But for law enforcement professionals using the web as a resource for their investigation, it can cause major problems.

Details of your digital fingerprint are passed to websites from different sources, including:

- **Internet address and connection:** registered owner, subscriber information
- **Browser and device type:** OS, software/plugins installed, time zone, audio/video devices, cookies, HTML5 local storage, HMTL5 canvas fingerprinting, audio rendering
- **Unique online behavior:** social media connections, shopping interests, websites visited, account activity

This information ensures compatibility with the content that will be displayed (for example, if you're requesting from a mobile device, the website will display differently than on a desktop, or the language of the displayed content will match the language setting of your device).

Separately, these components may be insignificant, but all together they can help websites — and their webmasters — track and identify who you are, who you're working for and what your interest is in a certain site.

Learn more in the guide, What's in Your Digital Fingerprint, included in this handbook

Using social media in law enforcement investigations

Social media has become one of the most robust sources of information for law enforcement investigators to quickly gain insight on persons of interest and their affiliates. However, social media brings with it another layer of risk due to the information it gathers about you. Here's an example:

Facebook receives "off-Facebook" activity; even while you're not on Facebook, it can collect information about apps you're using and sites you're visiting. So it's possible for Facebook to see you have an interest in aviation, you read Denver news, you've shopped at Galls.com (a law enforcement supplier), that you have an AT&T FirstNet account, you're interested in firearms, real estate investing and have been looking at events in the Washington D.C. area.

Take a break and disconnect your off-Facebook activity now

So even if your profile doesn't say you work for law enforcement, the details provided to Facebook could make it easy to guess that you do. This can be a problem when it comes to the friend recommendation feature.

Hazards of the friend recommendation

When a social media platform suggests a new friend, they look at your location, your mutual friends and searches you've completed. But if you're using your own profile while performing your investigation, the platform may suggest friends based on the person you've searched.

And if it's happening to you, you can bet it's happening to your subject — they see you pop up as a friend recommendation. You may also be appearing as a friend recommendation to confidential sources, putting them in jeopardy.

Learn more in the guide, Social Media's Value and Danger to Law Enforcement Investigations, included in this handbook

5 challenges of online investigations

BLOCKED ACCESS

Cybersecurity teams block untrusted websites. While this is good IT hygiene, it can mean that investigators sitting behind the firewall can't access websites that may be useful to their case. Even if you're able to get an exception from the security team, you've lost valuable time, and you're still working in an unsafe environment.

UNTRUSTED CONTENT

Investigations could involve websites that deliver malware or malicious code, enabling infections or further tracking of activity on your device. If your machine isn't properly segregated, infections could spread through your network.

CHAIN OF CUSTODY

Collecting information online is just the beginning. It must be cataloged and stored securely to meet chain of custody requirements. If you want to collaborate and share information, it adds even more complexity.

ALERTING THE SUSPECT

Most websites track visitors in some degree of detail. Also, advertisers use visitor information to serve ads and make recommendations. If these trackers can see you, your suspect can see you.

RETALIATION

Once suspects know you're watching, they can decide how to respond. They may keep things in the cyber realm and launch an attack against your device or your network. Or they can take things offline and come after you in the real world, using the details of your digital fingerprint to uncover your true identity and personal information. Other retaliatory tactics are to go dark — as in shutter a website or social media account — or disinform to spoil the investigation.

Using the dark web in law enforcement investigations

Of all internet traffic, the dark web only composes a very small amount. But to leave the information past the surface web untouched is to miss out on information that could prove to be essential.

If information on the dark web is relevant to your investigation, you'll need to use special software to access it. Tor is often the tool of choice. While it does a great job of obfuscating your IP address, Tor still has some tracking mechanisms. The Tor Project website even hedges claims of complete anonymity saying, "Tor Browser aims to make all users look the same, making it difficult for you to be fingerprinted based on your browser and device information" (italics added for emphasis).

So if you think browsing Tor is automatically anonymous, think again. Details of your digital fingerprint are still attributed to you and passed to the dark website.

The dark web is also notorious for booby-trapping websites with malware built to track activity like keystrokes. If your browsing environment isn't isolated from your device or network infrastructure, you could be risking infection from these websites — for yourself and your organization.

WHAT'S THE DIFFERENCE? SURFACE, DEEP AND DARK WEB

Surface web: the internet most of us use daily (a.k.a open web, clear web). It's the traditional format of the web, composed of open pages easily accessed by search engines on any browser.

Deep web: sites that require login or subscription services, such as court record databases.It has some barriers to accessibility while being adjacent to the surface web and is typically accessed via the same browsers.

Dark web: the area of the internet that can only be accessed by using a specific software. There are different versions available, from the most well-known (e.g., Tor/The Onion Router) to the lesser used (e.g., Freenet, I2P, ZeroNet).

Learn more: Understanding the dark web and how it can aid your investigation

Traditional safeguards no match for today's risks

Tools that used to be effective in protecting law enforcement networks and professionals are no longer working. Cracks can form in the patchwork methods that aim to provide airtight security, completely managed attribution and steadfast compliance.

Segregated network

Some organizations set up a different network exclusively for online investigations to limit organizational exposure to web-borne threats. This requires investment to set up and maintain. As it's run by people, it's also subject to human error. Investigators may find this setup cumbersome, too, as they have to switch services, machines or even locations to access the network or analyze evidence they've collected while using it.

And without lots of additional, equally resource-intensive measures, adversaries can still identify exactly who you are.

Private browsing

Most people use private browsing to keep others from seeing internet activity on that specific device. It clears cookies and data you've entered into forms. The problem is that information is still collected by supercookies and other tracking mechanisms that private browsing does nothing to prevent. Private browsing also does nothing to protect against web-borne threats.

VPN

With a VPN, you get a bit more anonymity as it changes your IP address and location, and it's still better than using your network, but there are many identifying details VPNs are helpless to disclose. And unfortunately, it still executes directly on your machine. Even if you do click on a malicious link using a VPN, you can still download malware.

Neutralizing security and attribution risks in online investigations

To protect investigations, the law enforcement professionals conducting them and the agencies they represent, you need the right tools for the job. The solutions discussed below address the security and attribution risks of online investigations, but also are built to support the tradecraft and expertise that their users exercise every day.

Cloud-based browsing to eliminate persistent tracking and maintain security

Cloud-based browsers execute all web code remotely, so it never reaches the endpoint, giving users a benign video display to interact with. Because of this isolation, cloud-based browsers can be used on any device or any network without the risks of web-borne threats.

Using a cloud-based browser not only enables law enforcement to isolate their investigative browsing from their device and network — protecting them from malicious content — it can also segregate browsing itself.

While all cloud-based browsers provide protection from malware to your device/network, not all provide anonymity during browsing investigations. Some can obfuscate connection to your organization, attributing to the cloud service provider, while others can obfuscate even that. To avoid persistent tracking between web sessions, these more advanced cloud-based browsers can provide a fresh, non-attributed browsing session every time they're launched; and paired with managed attribution, they can control tracking and attribution within a session.

Cloud-based browsers can also support multiple sessions with each executing its own virtual container and using different digital fingerprints at the same time. This can help investigators segregate and not cross-contaminate browsing sessions for different sites of interest, different investigations and different purposes (i.e., personal browsing vs. browsing for investigative purposes).

Managed attribution to conceal identity and intent

Managed attribution lets you control and customize how your digital fingerprint appears to sites that you interact with online. It gives you the ability to manipulate any number of identifiable details, such as keyboard and language preferences, time zone selections, browser and OS settings, and lots more. By matching these details to average site visitors of sites you're investigating, analysts and law enforcement professionals can blend in with the crowd and avoid tipping off investigative targets.

Managed attribution is delivered through purpose-built browsers for online investigations.

Spoofing geolocation to further change your digital fingerprint

Websites may block users coming from certain regions or IP addresses, or they may display different information to these visitors which could impact investigations.

In addition to changing digital fingerprint settings, investigators looking to manage their attribution can benefit from using a global egress network to spoof geolocation and appear as an in-region visitor.

Leveraging a network of internet egress nodes lets you adjust the location from which you appear to be visiting, showing a local IP address that doesn't refer to you or your agency. This ensures you can view and collect data as the visitor you desire to be, not the visitor you are.

Workflow tools to increase productivity

To keep up with caseloads, online investigators need tools of the trade at their fingertips. This means built-in solutions to the browser where investigations are conducted that support the key stages of research — access, analysis, capture and audit.

As described above, cloud-based browsers can simplify secure access to the web from any device or network.

In the analysis stage, built-in packet capture, source viewing and translation capabilities in the investigative browsing environment can greatly increase the efficiency. Automating multi-search workflows (preferred groups of specialized sites for different types of analysis) can also improve productivity, letting investigators run frequently used searchers across multiple sites in a single click.

When capturing data, small inefficiencies can add up. The ability to capture screenshots and videos, tag assets with URLs and timestamps, and save assets into case files from within the investigative browsing environment can save time every day. Automating data collection by scheduling recurring collections on various sites can also greatly improve efficiency; in addition, automated collections help investigators maintain tradecraft — even when they're not performing the capture themselves (due to time constraints, odd hours, etc.).

SECURE STORAGE

Data collected online must be securely stored off-network in the cloud to protect the organization from malware or similar risks. Using shared storage in the cloud also improves efficiency in collaboration, ensuring fellow analysts can properly access necessary information.

Lastly, to maintain compliance during investigations, all web activity must be logged, and all logs must be encrypted with organization-managed keys. If usage policies can be applied to a user and their cloud-based browser (rather than a device), the organization can seamlessly enforce and log investigator activity on any device or network.

For investigations that may lead to more formal reviews — by courts, regulators or internal teams — presenting evidentiary logs may be required. Presenting these logs and case materials requires centralized processes with strict custodial records. Investigators need the tools in place to track collections and monitor their workflows throughout their research.

Learn more in the guide, 13 Tools to Improve Online Law Enforcement Investigations, included in this handbook

Protecting investigations in a data-driven world

The role of online research in law enforcement investigations will only increase. The time for erecting the right strategy around secure web use and best-practice search protocol is now. This will require consideration in terms of policy as well as which tools will support investigator tradecraft and organizational security. With the right solutions, law enforcement agencies can protect their network, their personnel and the integrity of their investigations and keep their communities safer.

silo
BY AUTHENTIC8

What's in your digital fingerprint and how to control it

Your digital fingerprint — or browser fingerprint — may seem like innocuous details. But for online investigators, especially in law enforcement, they could make or break your case.

Traditional browsers such as Chrome, Firefox or Safari are built to track users and obtain an array of information about their device, browsing activity and more. Mostly innocent in intent (if not a bit creepy), these functions exist to tailor browsing experiences.

Search engines and websites may display differently based on your location, how long you spend on particular pages, the browser and device you're using, etc. These details are correlated your online behaviors across different sites to paint a more complete picture of your specific interests. Most of this information is monetized and resold; and even though it sounds a bit intrusive, most people begrudgingly agree to have their browsing habits catalogued, collated, analyzed and resold in exchange for ease and convenience.

For an online investigator, though, this type of tracking can present a serious problem — especially for law enforcement professionals conducting criminal investigations.

The same tracking mechanisms that enable personalized ads and simplify shopping experiences can be exploited by adversaries and investigative targets. All this data collected over time across sites can easily give away an investigator's identity and intent. And once adversaries know who you are and what you're up to, they can disappear, cover their tracks or even launch a retaliation campaign against you or your agency — online or the real world.

What's in a digital fingerprint?

In addition to cookies (bits of code designed specifically to gather and save information on your online sessions), there are many other types of data that websites and devices track to help profile and identify you.

Your digital fingerprint or browser fingerprint includes everything from which sites you click on (and which ones you skip) to the type of connection you use (IP address and provider), your hardware (device type, OS, video and audio cards), configurations (keyboard and language settings, time zones, etc.), installed software and plugins, and even seemingly random things like battery status. All of this information helps browsers track you across sessions.

And while millions of web users around the world have similar devices and search for the same terms, traditional browsers are capable of fingerprinting users based on small differences and distinct combinations of settings and behaviors that make your online presence incredibly unique.

It's important to understand that by simply turning off the most commonly used cookies or switching to Google's Incognito or "private browsing" mode, investigators are not fully protecting their identities or ensuring anonymity.

Learn more: **What VPN and Incognito Mode still give away in your online identity**

Every law enforcement agency needs to build a comprehensive strategy for understanding what information is being tracked, and design an approach on how to shield their analysts and protect their missions.

What's in *my* digital fingerprint?

To find out what information is in your digital fingerprint, our experts recommend starting with an assessment of what an adversary may already know about you and your online behavior. Sites like AmIUnique.org can provide basic information about your online configuration and how trackable it is, as well as offer advice on how you can tweak it to blend in more easily.

You can also get lots of helpful information on what type of data your browser is giving away on sites like Browserleaks.com.

If you're an online investigator, "unique" is the last thing that you want to be. Web-savvy and/or well-funded criminals, terrorists and fraudsters will be capable of counterintelligence and potentially retaliation — online or in the real world.

Knowing how you're tracked and understanding what you can do to minimize it can make a huge difference in the success of your investigation, not to mention the safety of yourself and your organization.

What is managed attribution and why is it important?

Managed attribution lets you control and customize how your digital fingerprint appears to sites that you interact with online. It gives you the ability to manipulate any number of identifiable details, such as keyboard and language preferences, time zone selections, browser and OS settings, and lots more. By matching these details to average site visitors of sites you're investigating, analysts and law enforcement professionals can blend in with the crowd and avoid tipping off investigative targets.

Managed attribution is delivered through purpose-built browsers for online investigations.

Spoofing geolocation to further change your digital fingerprint

Websites may block users coming from certain regions or IP addresses, or they may display different information to these visitors which could impact investigations.

In addition to changing digital fingerprint settings, investigators looking to manage their attribution can benefit from using a global egress network to spoof geolocation and appear as an in-region visitor.

Leveraging a network of internet egress nodes lets you adjust the location from which you appear to be visiting, showing a local IP address that doesn't refer to you or your agency. This ensures you can view and collect data as the visitor you desire to be, not the visitor you are.

Cloud-based browsing to eliminate persistent tracking and maintain security

Cloud-based browsers execute all web code remotely, so it never reaches the endpoint, giving users a benign video display to interact with.

Using a cloud-based browser not only enables analysts and law enforcement to isolate their investigative browsing from their device and network — protecting them from malicious content — it can also segregate browsing itself.

While all cloud-based browsers provide protection from malware to your device/network, not all provide anonymity during browsing investigations. Some can obfuscate connection to your organization, attributing to the cloud service provider, while others can obfuscate even that. To avoid persistent tracking between web sessions, these more advanced cloud-based browsers can provide a fresh, non-attributed browsing session every time they're launched; and paired with managed attribution, they can control tracking and attribution within a session.

Cloud-based browsers can also support multiple sessions with each executing its own virtual container and using different digital fingerprints at the same time. This can help investigators segregate and not cross-contaminate browsing sessions for different sites of interest, different investigations and different purposes (i.e., personal browsing vs. browsing for investigative purposes).

With so much information collected about your every move, it's hard to remain anonymous online. And while for ordinary citizens it's an annoyance at best, for online researchers, digital fingerprinting can impede their ability to do their work and compromise the integrity of their investigations. Knowing what's being tracked and having the right toolset to conceal their identity and intent can help federal, state and local law enforcement agents better use the internet to gather data on criminal individuals and organizations — and bring them to justice.

silo
BY AUTHENTIC8

13 tools to improve online law enforcement investigations

Use data aggregators to pull together info from courthouses across the country, add extensions to better utilize video and images and safely search social media.

Federal and local law enforcement agencies have whole divisions dedicated to fighting cybercrime. But the internet is an extremely valuable resource for much more than gathering intelligence on cyber terrorists or investigating computer-based fraud. Social media sites, online data aggregators and special browser plugins and extensions can help law enforcement officers:

- Quickly gather data on any person or organization
- Uncover associations between addresses, phone numbers and user personas
- Find locations where images were taken
- Connect information from different sources to paint a complete picture of someone's profile

Our experts compiled a list of various tools and sites, along with a brief explanation of their benefits and how they can help advance your investigations.

Online data tracking aggregators to jumpstart your research

Depending on what information you need, there are plenty of websites that can fast-track your initial investigation. Several open-source online investigative tools specifically look at people-centered data. They work by scanning court websites and aggregating what they find.

These sites are legal and review public documents based on the Freedom of Information Act (FOIA). They gather information, including phone numbers, possible addresses, possible family members and known associates. And they save time, so you don't have to visit individual court websites.

What's also nice about these tools is you don't have to create a persona — you can access them directly and pull down your first level of information with little risk.

Cyber Background Checks

Cyber Background Checks provides access to billions of public records about millions of adults throughout the U.S. It's sorted to isolate the information you need and organize it into a comprehensive, easy-to-interpret summary. You can find people and where they live by searching their names, discover who lives at a particular address, see who owns an email address and look up unknown phone numbers.

FamilyTreeNow

FamilyTreeNow is a free genealogy site, where you can search for family members, associates, addresses and phone numbers of any individual.

Spokeo

Spokeo has organized over 12 billion records from thousands of data sources into easy-to-understand reports that include available contact info, location history, photos, social media accounts, family members, court records, work information and much more.

OSINT Techniques

OSINT Techniques provides numerous free open-source resources for researching and analyzing data. Although the information on the website can be used for a variety of purposes, it would be most helpful to investigative roles such as analysts and researchers.

Intelius

Intelius provides public data about people and their connections to others. Investigators can check criminal records, background checks, property data and more.

Accurint

Accurint is part of LexisNexis and serves as the most widely accepted locate-and-research tool available to government, law enforcement and commercial customers. Its proprietary data-linking technology returns search results in seconds to the user's desktop.

Pipl

Pipl is the essential investigative tool used by insurance and financial institutions, government agencies and media companies. It speeds your investigation tasks by helping quickly locate persons of interest, uncover connections between people, addresses, phones and social handles, and even determine the credibility of sources, witnesses and suspects.

Exif Viewer Chrome extension

Exif Viewer is a simple tool to read the EXIF data from your JPG images. There's lots of helpful information held in image files: Some photos have GPS data and others contain the camera's shutter count, which helps identify the type of camera used to take the image. This utility lets you open a JPG image from your computer or a URL to view its EXIF data. You can also right-click on a JPG image in a browser and select "EXIF Image Info" from the context menu.

Using social media in law enforcement investigations

For online investigators, social media sites like Facebook, Snapchat, Instagram or TikTok could be a treasure trove of information. But just like traditional detectives, investigators must be extra careful to maintain anonymity and keep their identity and intent hidden while researching social media. Not only could a clumsy move spook the bad guys into going deeper undercover, it could also trigger retaliation (cyber or material), putting law enforcement agents at risk.

Tools for safely investigating persons of interest on social media

There are several specialized tools that were developed specifically to help online investigators browse social media sites without risk. They can be a helpful addition to investigators' portfolios when it comes to following suspects and persons of interest on social media platforms.

Social Searcher

Social Searcher is a real-time social media monitoring engine. It allows you to search for users, keywords, and trends across 11 different social media platforms. It searches for content in social networks in real-time and provides deep analytics data. Users can search without logging in for publicly posted information on Twitter, Google+, Facebook, YouTube, Instagram, Tumblr, Reddit, Flickr, Dailymotion, and Vimeo. Free users can also save their searches and set up email alerts. Premium features include saving social mentions history, exporting data, API integration, advanced analytics, and immediate email notifications.

Inflact

Inflact is a multi-purpose service, which includes an excellent tool for Instagram searches. Influencers, bloggers and regular users can choose tools based on their needs. It offers free and paid services for building a social media audience, managing content and communicating with clients. And it's great for investigators, too!

Twitter Advanced Search

Twitter Advanced Search is available when you're logged into twitter.com. It allows you to tailor search results to specific date ranges and people. You can also search words, phrases and hashtags; what's trending in particular locations; and then see profiles posting on the topic.

TikTok

TikTok has taken off in the last couple of years, and while it's generally just good fun and a lucrative platform for some folks to make money, TikTok is also used by criminal organizations as a platform for their propaganda, drug sales and a way to connect with potential victims. Searching TikTok is very straightforward: if you're looking for a specific profile, use TikTok.com/@ and then a username. If you're looking at a particular hashtag, enter TikTok.com/tag/ and then the keywords or phrases you're searching for. Searches on TikTok don't require a login.

Social Bearing

Social Bearing is an open search and statistics tool. It can analyze Twitter mentions, find top tweets, hashtags, trends or Twitter conversations; show most popular tweets containing specific pictures or links; uncover facts; find geolocated tweets; and analyze any user's timeline.

Browser beware

These days, it's easy to find anyone or anything online. That's important to remember in terms of what you can find out about your suspects, but also in terms of what they can find out about you. Many sites that offer you information on people and organizations are known to sell registration information, which of course is not desirable for law enforcement investigators.

Maintaining anonymity is essential for any online investigation. While performing your research on the web, law enforcement professionals need to be able to control what investigative subjects can learn about them by what their browser discloses (hint: it's a lot).

Read more: **What attributes are disclosed via your browser and device?**

Managing attribution is the definitive way to properly disguise your identity and intent — without creating a false persona, relying on a "dirty" network or using a burner device. By controlling the details of your digital fingerprint, you can blend in with the crowd and perform your investigation without tipping off your suspect or blowing the case.

silo
BY AUTHENTIC8

Social media's value and danger to law enforcement investigations

Social media is increasingly useful to law enforcement investigations. But it, along with other OSINT sources, comes with inherent risks to access.

Despite the dangers, the web is playing an increasingly important role in conducting thorough and efficient law enforcement investigations, and nowhere is that more true than on social media.

Social media has become one of the most robust sources of information for law enforcement investigators to quickly gain insight on persons of interest and their affiliates. Reports estimate that the total number of social media users is over 4 billion — that's equal to more than half the global population.

Social media profiles and activity can reveal a pattern of life that often provides a rich context of behaviors and contacts. It can reveal phone numbers, hangout locations, habits and possessions (e.g., cars, phones or clothes). With geolocation, it can even help you identify a subject's location at a specific time.

But searching social media to support law enforcement investigations carries an elevated risk — on top of the standard risks of accessing the web for OSINT collection and other research.

Web-based risks to law enforcement investigations

The "standard" risk of using the web is cyber risk. Anyone clicking a link or navigating to a site could encounter malware that downloads to their device and potentially spreads in their network.

Malware comes in all shapes and sizes, from ransomware that's increasingly targeting police departments to keyloggers that can track everything you type.

This is why browser isolation is important — particularly in investigations that will likely encounter bad actors or risky content, as in law enforcement investigations — to keep absolute separation between the browsing environment and the device.

Isolated, cloud-based browsers mean web code (and the threats that lie within it) execute in the cloud and not the local device, while the user interacts with a benign video display that looks and behaves just like the normal browsing experience.

But there's another risk particular to investigators: tipping off investigative targets simply because of how (most) browsers work.

Tracking mechanisms can spoil law enforcement investigations

Traditional browsers like Chrome, Firefox or Safari track users during — and even between — browsing sessions and obtain an array of information about their device, browsing activity and more.

Tracking exists to tailor browsing experiences based on your location, device settings, browsing history, browsing behavior and details of the browser itself. These details are not just collected by the browser, they're conveyed to the websites you visit; specifically, they include:

- **Internet address and connection:** registered owner, subscriber information
- **Browser and device type:** OS, software/plugins installed, time zone, audio/video devices, cookies, HTML5 local storage, HMTL5 canvas fingerprinting, audio rendering
- **Unique online behavior:** social media connections, shopping interests, websites visited, account activity

And this is where it becomes a problem for investigators.

Separately, these components may be insignificant, but all together they can help websites — and their webmasters — track and identify who you are, who you're working for and why you're snooping around.

Your "digital fingerprint" is highly unique. If it sticks out like a sore thumb on the site you're investigating, the webmaster may perform counter-intelligence, feed you disinformation or retaliate. They could also use it to uncover your true identity and come after you or your organization.

If your investigative target knows who you are, best case scenario: that investigation is compromised. Worst case scenario: it could get personal.

Social media is tracking on steroids

So your standard web browser is built to track you (note: this is still happening even if you're in private browsing mode). But social media takes tracking to a whole new level. Here's an example:

Facebook receives "off-Facebook" activity; even while you're not on Facebook, it can collect information about apps you're using and sites you're visiting. That means it's possible for Facebook to see you have an interest in aviation, you read Denver news, you've shopped at Galls.com (a law enforcement supplier), that you have an AT&T FirstNet account, you're interested in firearms, real estate investing and have been looking at events in the Washington D.C. area.

So even if your profile doesn't say you work for law enforcement, the details provided to Facebook could make it easy to guess that you do. This can be a problem when it comes to the friend recommendation feature.

Hazards of the friend recommendation

When a social media platform suggests a new friend, they look at your location, your mutual friends and searches you've completed. But if you're using your own profile while performing your investigation, the platform may suggest friends based on the person you've searched.

And if it's happening to you, you can bet it's happening to your subject — they see you pop up as a friend recommendation.

You may also be appearing as a friend recommendation to confidential sources, putting them in jeopardy.

Your profile can turn you into the target

Who you are offline is very similar to who you are online — and criminals know this. If the details of your digital fingerprint, including social media activity, point to law enforcement, your investigation could be compromised and you could potentially be at personal risk.

Law enforcement professionals and organizations have valuable data the bad guys can use or sell; as such, they often become targets of cyberattacks.

- The 2020 CIO Survey found cyberattacks are increasing on state and local governments, with spear-phishing and malware being the most common threat vectors.
- In July 2020, The Intercept reported on the BlueLeaks archive that exposed the personal information of 700,000 cops. The theft included 16 million rows of data, including emails, descriptions of alleged crimes, and detailed personal information.
- In July 2019, the LAPD was involved in a data breach releasing thousands of current aspiring police officers' personal records. They didn't realize the breach happened until the hacker told them.

Also, if you're conducting an investigation, your intelligence and evidence could be the target of attacks or leaks, compromising your case.

Before you create that fake persona ...

Because social media is, well, social, it's easy to get caught up in the idea of creating false personas (i.e., creating a fake name, fake email address, etc.) in order to search the platform and interact with subjects relevant to your investigation.

That isn't a best practice, and platforms are cracking down to eliminate such accounts. Instead, there are many tools provided by the social media sites or third-parties in line with platforms' policies. Explore these options thoroughly before you take any risks that would run you afoul of platform terms and conditions, policies within your organization or the law.

Control your digital fingerprint

Other OSINT sources — on the surface and dark web — aside from social media also play an important role in law enforcement investigations.

To protect the integrity of your investigation, ensure your personal safety and that of your agency, you need to control the details conveyed about you to websites you research.

This may start with location spoofing. If you think this is as simple as using a VPN, think again.

With a VPN, it's important to remember:

1. You're still using your native browser that is leaking all kinds of information about your location, as well as your browsing habits, your device, etc.
2. You will need to purchase VPN access in the various regions where you want to appear local
3. It's known that you're using a VPN (the IP address will be associated with the VPN provider) which could block you from accessing the site
4. You're not protected against malware infection

Other purpose-built solutions offer networks of internet egress nodes across the U.S. and around the globe that can give investigators the desired in-region access without appearing to originate from a VPN-associated IP address.

But it takes more than an internet egress location to thoroughly cloak your identity. In fact, if other details of your "location narrative" don't match with where you appear to be accessing from, it may raise a red flag to your investigative subject.

To complete the narrative, you need to match numerous other details to your assumed identity. Consider the following:

- What language, keyboard and timezone settings are appropriate for this egress location?
- What browser and OS (and what version) are common to users in this region? (StatCounter is a great resource to find out market share of this and other info)
- What do other device and browser details say about me (audio/video devices; installed software, plugins, fonts; battery status)?
- How could cookies and other unique identifiers (e.g., session IDs and employee number) reveal my identity or intent?
- What could adversaries or investigative targets learn from conveyed details of my local storage or cached data?

Browse with a clean slate

If you're running multiple digital fingerprints for researching different sites, you'll need to ensure your browsing sessions are isolated from one another.

Using an isolated, cloud-based browser can give you a fresh browsing experience in every session, eliminating persistent tracking mechanisms that follow you as you search — even after you close and relaunch the browser. Some such browsers will also allow you to run multiple isolated browsing sessions at the same time, so that you can conduct multiple investigations but not cross-contaminate.

Each time you launch a remote, isolated browser, you start with a clean slate. This means the search terms used, websites visited, browsing patterns, time of use, shopping preferences, etc. won't contaminate the digital fingerprint you assume to research a particular site or case.

Law enforcement investigators leveraging web research are at a heightened risk because of who they are and who they're going after. Knowing those risks and how to counteract them is of the utmost importance to ensure a successful investigation and protect those conducting it.

Tracking online drug dealers

Drug dealers use social media to sell illegal narcotics

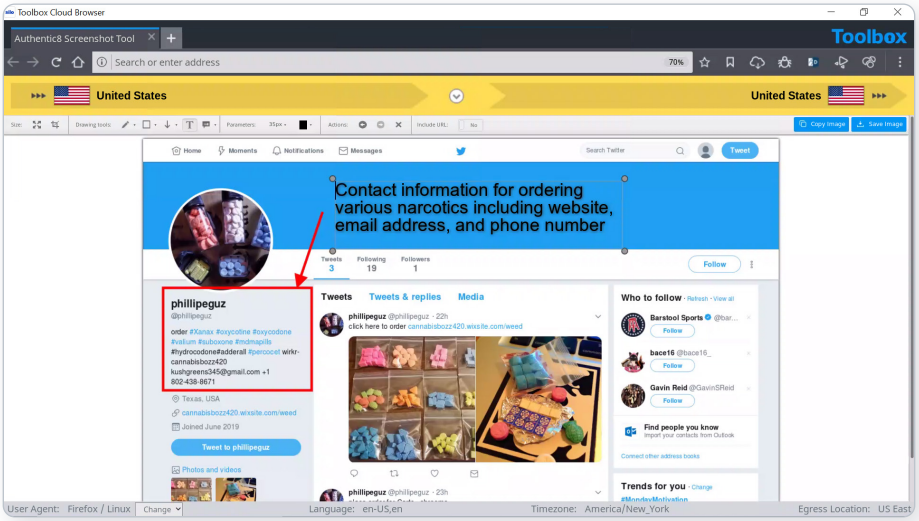
The continued rise of social media over the past ten years has led to drug dealers using various social media platforms to sell illegal narcotics on the surface web. Investigators need a safe and anonymous browsing and research framework that allows them to investigate social media drug dealers without 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.

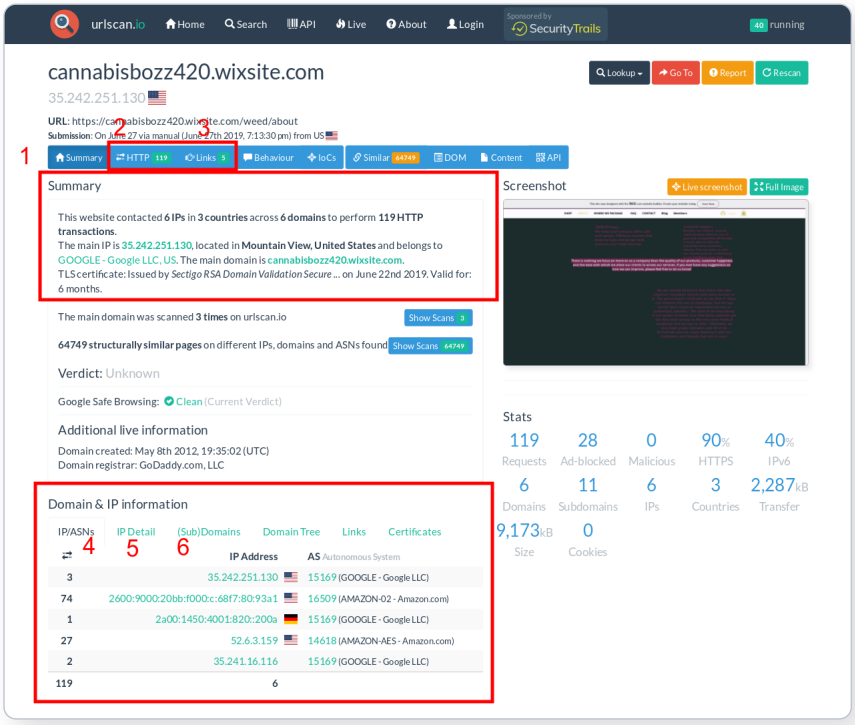
When conducting research on social media, there are various data capture tools included with Silo for Research that can be used for gathering intelligence. This first is a video download tool that allows investigators to simply download any video currently playing on their screen to save as evidence. 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.



Breakdown of URLscan.io result panels

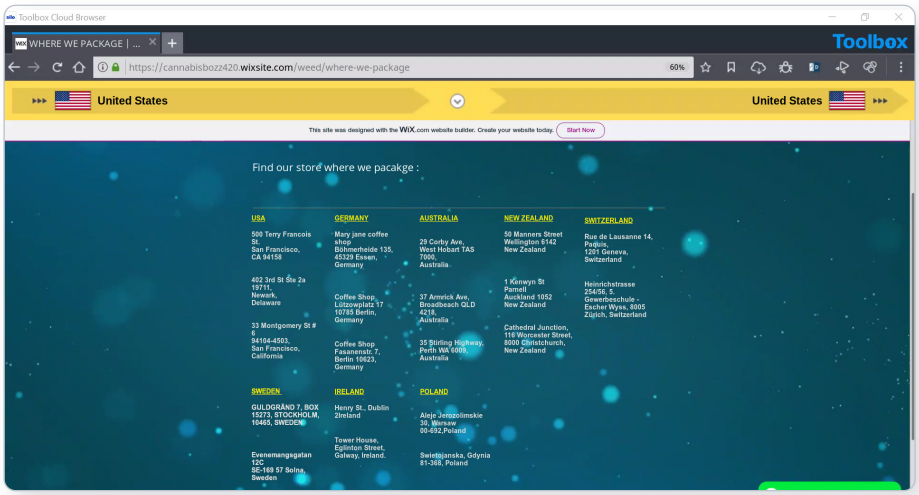
1. "Summary" provides a top-level summary of what country the site is hosted in.
2. "HTTP" details how many HTTP connections are made during initial load.
3. "Links" details what other sites are linked to on the main page.
4. "IP/ASN" details the IPs of everything used upon initial load and the geographic location as well as ASN.
5. "IP Detail" contains the exact city/state/country an IP address is assigned to, and redirects.
6. "(Sub)domains" identifies how many subdomains a top level-domain contains.

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.

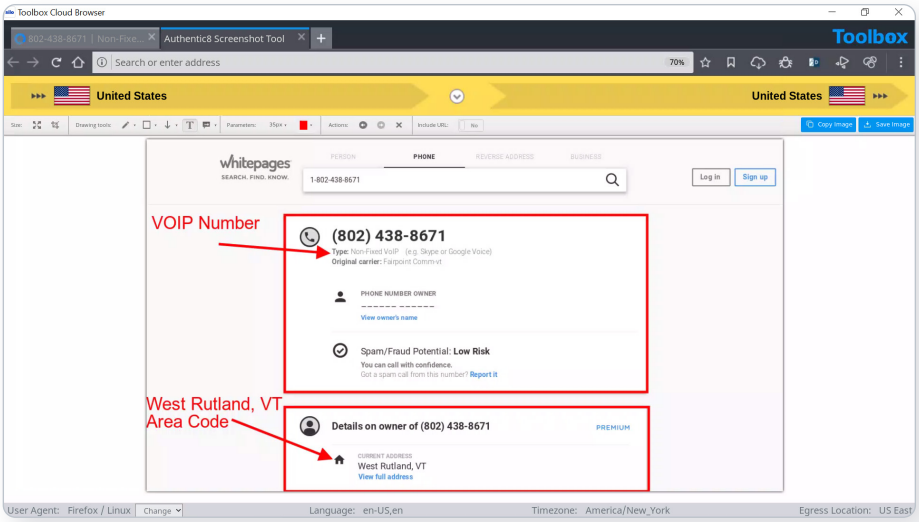
Phone number reverse lookup

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.



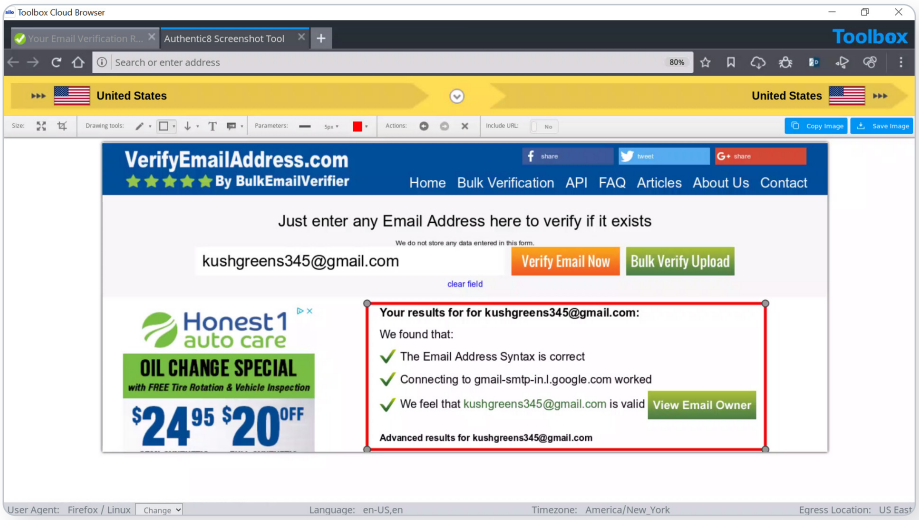
Example analysis of result panels

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. Once a possible email address is identified for a target, it can be run through https://verifyemailaddress.com to verify that it is a legitimate email address. Once an email address is verified, a subpoena or court order can be sent to the email provider to identify who owns and operates that email address. The screenshot below depicts the results from verifymyemailaddress.com for the email address kushgreens345 at gmail dot com, and it is in fact a legitimate email address.



Conclusion

With drug dealers increasingly utilizing social media to distribute illegal narcotics, investigators need a safe and anonymous method to investigate and capture social media data. This workflow covered how Silo for Research can be used by investigators to safely and anonymously investigate and capture data from social media drug dealers.

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

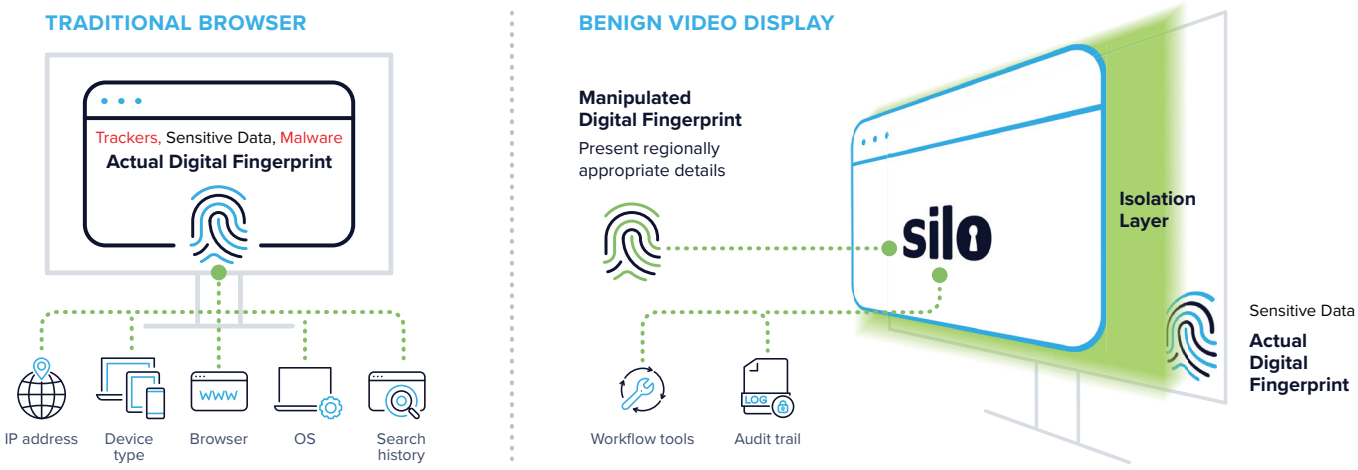
Traditional browsers disclose a range of information about you to the websites you visit.

- 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 for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It's built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

+1 877-659-6535
www.authentic8.com