OSINT and Anonymity: Why Protecting Your Identity Matters During Investigations

By Elena Dollfuss, Data Researcher, ORYXLABS

Note: This blog post is the first in a series aimed at making digital security easier to understand, especially for those who don't know code. Whether you are managing a team, running a small business, or simply curious, these posts are written to help you stay informed and protected.

In the dynamic world of open-source intelligence (OSINT), the ability to uncover valuable information is paramount. Yet many overlook the first rule of OSINT: do not let anyone know you are doing it.

For any investigator, whether you’re mapping an organisation’s external assets, assessing cyber threats, or conducting corporate reconnaissance, protecting your digital trace isn’t just a best practice; it is essential for operational security and, ultimately, the quality of your analysis. If the object of your investigation becomes aware of your presence, it may adapt and even fool you.

This blog post will delve into why anonymity is non-negotiable in OSINT, examine the pervasive threat of browser fingerprinting, and equip you with the knowledge to remain invisible when conducting your investigations.

Why anonymity is essential

Every click, every page view, and every search query leaves a digital trace. Even if information is publicly available, sifting through it is akin to navigating a squeaky library cart across a quiet room.

Even when your work is entirely ethical and legal, you don’t want your activities linked back to you or your organisation.

The risks of poor anonymity during OSINT include:

- **Website logging and tracking**: Websites record visitor data such as IP addresses, device details, and activity which can be linked back to you.
- **Retargeting and profiling**: Ad networks track visitors across sites, building profiles that persist over time.
- **Browser fingerprinting**: Websites use unique browser/device traits to track you without cookies.
- **Operational security (OPSEC) mistakes:** Simple errors, like accidentally logging into a personal account or failing to isolate targets, can expose your identity.

Conducting OSINT without protecting your digital trace is equivalent to wearing a blinking neon sign and a nametag. If your data is exposed, it becomes alarmingly easy for targets or automated defence systems to recognise, track, and even block your activity.

The mechanisms of digital exposure

To protect yourself, it is crucial to understand how your identity can be compromised.

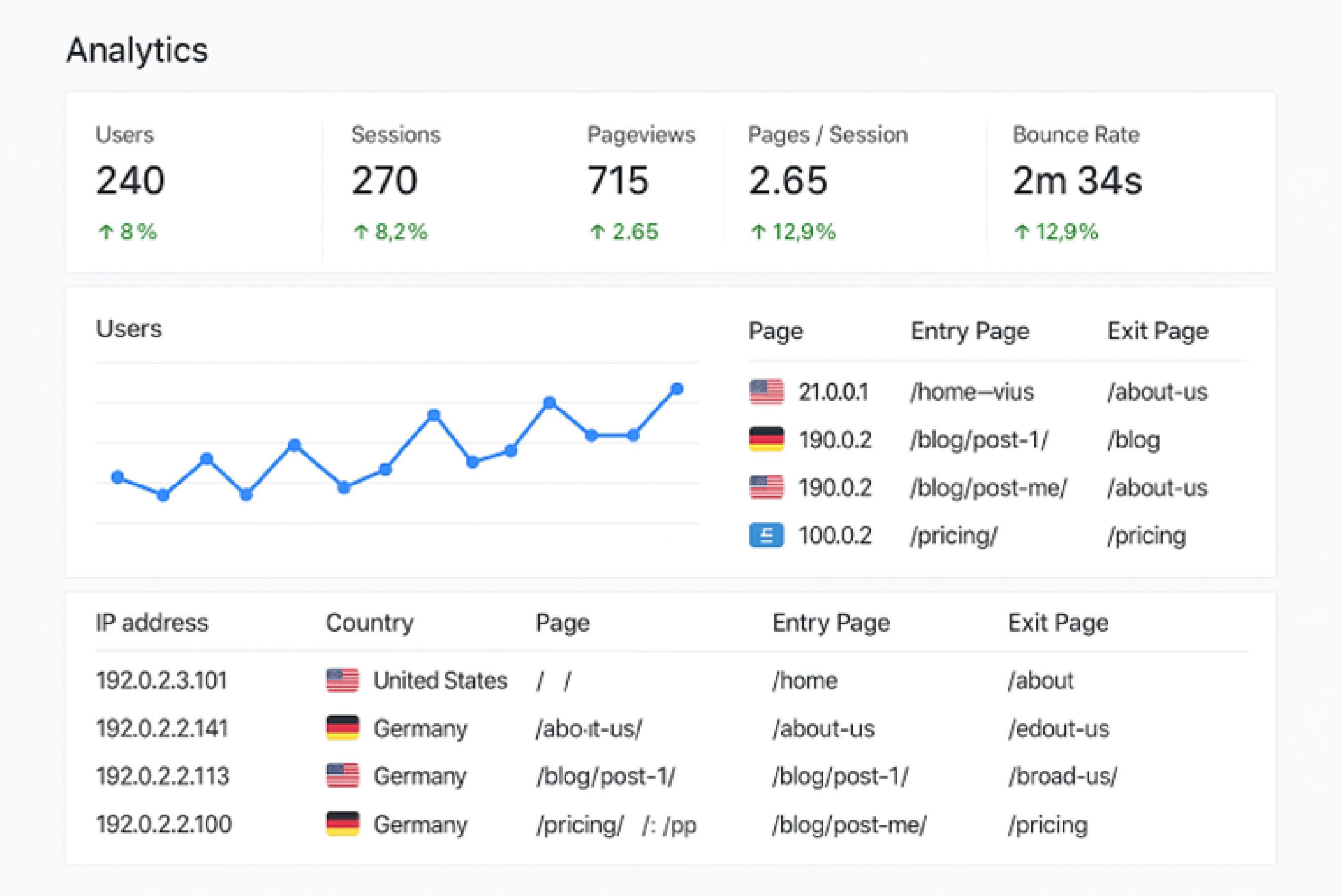
Website logging: the server’s diary

Website logging is the internet’s diary. Upon visiting a site, the server automatically records what you click and where you came from. These logs are treasure troves of information for the website owner and, potentially, for anyone trying to identify you.

Website logs include:

- IP addresses: Your approximate geographic location and ISP.
- Timestamps: Your exact date and time of access.
- HTTP headers: Your browser type and version, OS, and language settings.
- Referrer URL: The last page you visited before landing on the current site.

- Request details: Specific pages you visited, including buttons clicked, forms submitted, and files submitted.



Analytics

Users	Sessions	Pageviews	Pages / Session	Bounce Rate
240	270	715	2.65	2m 34s
↑ 8%	↑ 8,2%	↑ 2.65	↑ 12,9%	↑ 12,9%

Users

Page	Entry Page	Exit Page
21.0.0.1	/home—vius	/about-us
190.0.2	/blog/post-1/	/blog
190.0.2	/blog/post-me/	/about-us
100.0.2	/pricing/	/pricing

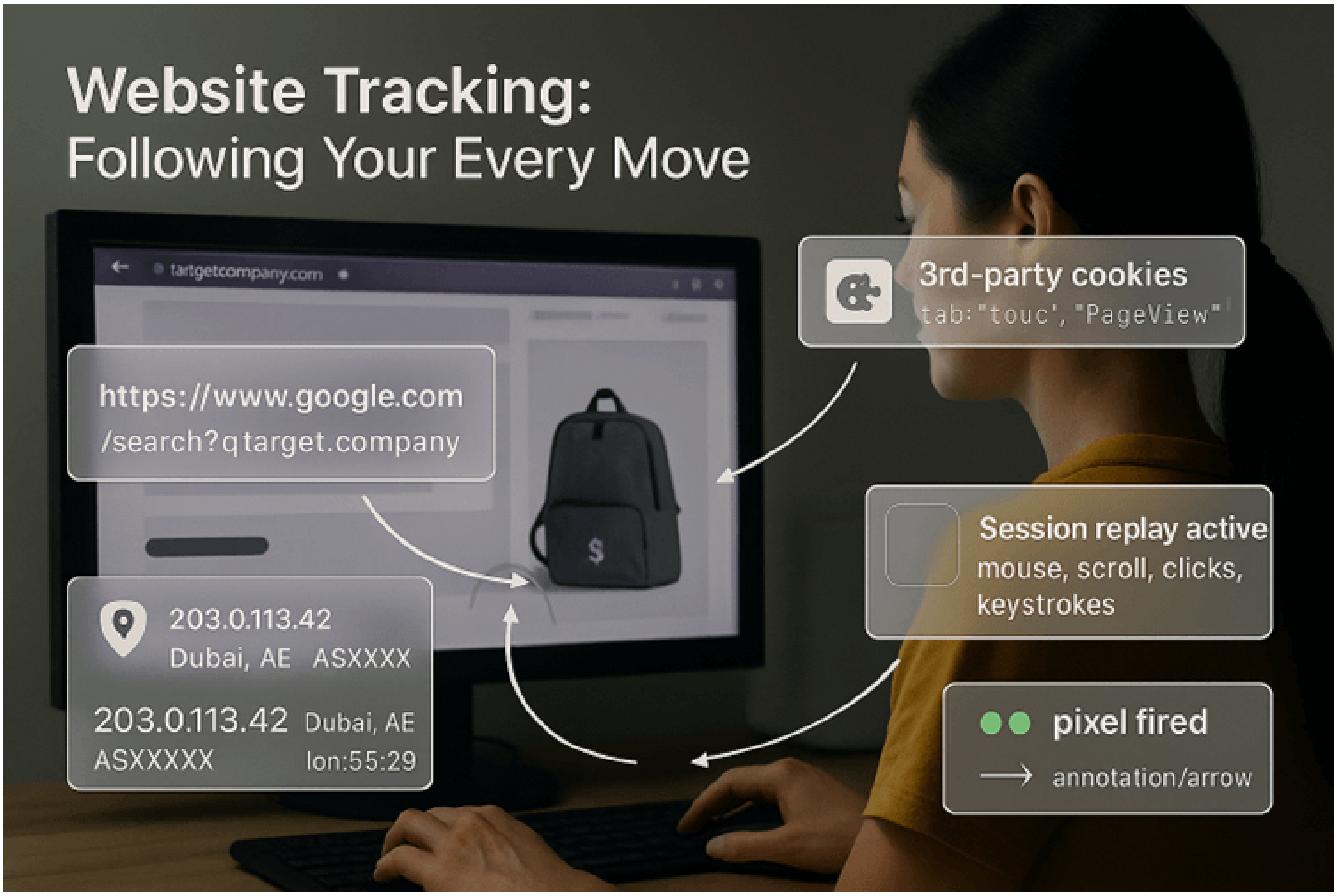
IP address	Country	Page	Entry Page	Exit Page
192.0.2.3.101	United States	/ /	/home	/about
192.0.2.2.141	Germany	/abo·ıt-us/	/about-us	/edout-us
192.0.2.2.113	Germany	/blog/post-1/	/blog/post-1/	/broad-us/
192.0.2.2.100	Germany	/pricing/ /: /pp	/blog/post-me/	/pricing

Website tracking: following your every move

Beyond passively logging your moves, website tracking can build a detailed profile of you.

Common tracking mechanisms include:

- **Cookies (session and persistent):** Small files stored in your browser. Session cookies might remember your login or shopping cart, while persistent cookies (often from ad trackers) can follow you across many sites.
- **Third-party trackers and pixels**: Tiny, invisible scripts or images that collect data on your actions as you browse.
- **Referrer tracking**: The “referrer” HTTP header which automatically tells the next site you visit where you came from.
- **Session replay scripts**: An advanced feature which allows some sites to record your mouse movements, clicks, scrolls, and even typing, offering a complete replay of your session.
- **IP and geo tracking**: An address for your approximate location, which, combined with timestamps, can identify repeat visits from the same user.



Browser fingerprinting: the ultimate identifier

Browser fingerprinting is a sophisticated method that websites use to identify visitors even without cookies.

It is the website bouncer – but does not need a photo ID to recognise you. Instead, it assesses unique markers such as screen resolution, special fonts, and graphics rendering, and combines these into a unique “fingerprint”.

Browser fingerprints are generated using:

- Screen resolution
- Installed fonts and plugins
- WebGL and Canvas rendering output (how your browser draws graphics)
- Time zone and language settings
- User-agent headers (identifying your browser and OS).

These signals combine to create a highly unique profile that can track visitors across multiple sessions or websites, even when using incognito or private browsing mode.

Browser Fingerprinting:
The Ultimate Identifier

Screen Resolution: 1920×1080

Installed Fonts: Arial, Roboto, Courier

WebGL Rendering: Enabled

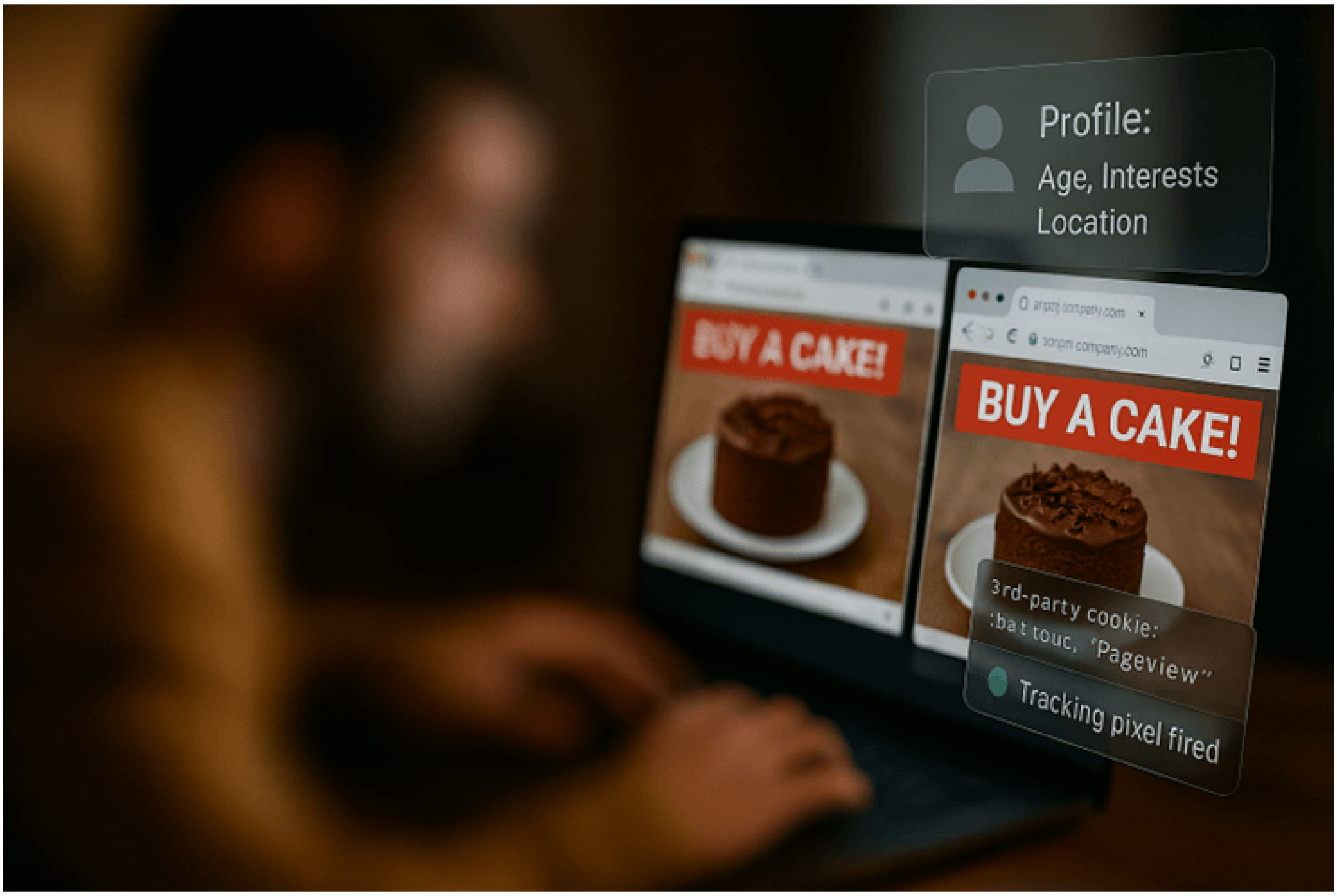
Time Zone: UTC+4 (Asia/Dubai)

User-Agent: Firefox 122.0 on Ubuntu

Retargeting and profiling: building your digital persona

Once a website has gathered your data, it may use this to influence your behaviour through retargeting and profiling:

- **Retargeting**: Used in online advertising, where ads are shown to you based on your previous behaviour or interactions with a specific website. This is a marketing technique where an individual's online behaviour, such as viewing a specific product, is used to repeatedly target them with advertisements for that same product across different websites and platforms. It uses cookies, tracking pixels, or even browser fingerprinting to "follow" you across the web.
- **Profiling**: The long-term, persistent creation of detailed behavioural, demographic, and psychographic profiles of users. Unlike short-term retargeting, profiling builds an evolving, comprehensive picture of your preferences over months or even years, based on your browsing, purchase history, and social data. It’s like the internet's own personal stalker.



Example in action: your digital trail

When visiting an e-commerce site, your digital fingerprint is immediate:

- The site logs your IP, browser details, and referrer.
- Analytics scripts start recording the pages you browse and your behaviour.
- Third-party ad trackers drop cookies for retargeting, meaning you might later see ads for those products on social media.
- The site stores your unique browser fingerprint (based on your fonts, screen size, language, etc.).

This allows the site to correlate your activity even if you clear cookies.

Conclusion

In the world of OSINT, your safety and operational security (OPSEC) are of the utmost importance. Best practices dramatically minimise the risk of being profiled, tracked, or exposed during your investigations.

Your mission is clear: gather intelligence without leaving a trace.

DISCOVERY is an external attack surface management and digital risk protection solution that provides a holistic, continuous approach to cyber situational awareness, vulnerability assessment, threat intelligence monitoring, and attack simulation at a national scale. By leveraging the principles of anonymous OSINT, **DISCOVERY** ensures that your investigations into potential threats and vulnerabilities are conducted without exposing your organisation's identity or operational security.

Stay vigilant, stay anonymous.