



The Netherlands

CHAIR: Judith de Boer
Defence Lawyer



Romania

Ovidiu Valea
CyberOps Network



Romania

David Timofte
CyberOps Network

BREAK-OUT SESSION | Cyber, Tech and AI

OSINT, Cyber Investigations and Defence Challenges

Agenda

Understanding OSINT

- What is OSINT? The Art & Science
- Definition & Legal Applications
- OSINT for Legal Professional

Digital Tracing Techniques & Live Demos

- Canary Tokens
- Metadata in files
- Google Dorking (Hacking)

Most Relevant Use Cases of OSINT

- Professional OSINT Tool Management

Preserving Evidence: Creating Your Own Chain of Custody

Challenging Digital Evidence in Court

- Challenging OSINT & IP Address Attribution
- Collection Methodology Questions
- Legal Authority Issues

Securing Lawyer-Client Communications

- Counter-Surveillance for Defense Attorneys
- OPSEC for Legal Professionals
- Protecting Your Business from Digital Threats

Q&A Session

OSINT: Definition & Legal Applications

Open-Source Intelligence (OSINT) is the discipline of collecting and analyzing data from public sources to produce actionable intelligence.

- Social media or User Generated Content (UGC) platforms
- News sources & publications
- Public records & databases
- Forums & discussion boards
- Business registries
- **It's NOT hacking.** It is the lawful use of publicly accessible information.
- **The Challenge:** The skill isn't just finding data; it's in the expert analysis, connecting disparate dots, verifying information, and understanding the context to build a coherent picture.

For Defence Lawyers, expert OSINT provides:

- Legally admissible evidence for a case
- In-depth vetting of expert witnesses
- A strategic advantage by deconstructing the prosecution's case
- Proactive protection for your practice and your clients

Remember: Our ethical obligations require transparency about investigative methods when presenting findings in court.

Open Source Intelligence for Legal Professionals

Words Matter in Digital Intelligence

OSINT

Open Source Intelligence: Actionable information specifically designed for governments, militaries, law enforcement, and corporate security teams to inform critical decision-making.

OSINF

Open Source Information: Raw, publicly accessible data that has been collected but requires analysis and verification before becoming actionable intelligence.

OSINV

Open Source Investigation: The systematic application of open source techniques to gather OSINF and conduct thorough analysis within formal investigations.

The OSINV Process



Monitoring

Continuous surveillance of digital channels and sources



Collection

Systematic gathering of relevant data and information



Analysis

Critical evaluation and verification of collected information



Investigation

Comprehensive fact-finding to establish truth

③ **Event Verification Focus:** Professional investigators establish the *who, what, when, where*, and *how* of incidents. The *why* remains extremely rare without direct witness testimony or insider access.

Digital Tracing: Canary Tokens

How can we trace the location or identity of a perpetrator?

Canary Tokens are a free, effective tool to track digital activity, demonstrating a core tracing principle.

How they work:

1. A unique "token" is generated (e.g., a URL, a PDF document).
2. This token is embedded in a message to the target.
3. When the target interacts with the token, it "triggers."
4. A notification is sent with raw data, including:
 - The IP address that triggered the token.
 - Approximate geographic location.
 - Time and date of the interaction.
 - The user agent (browser/device) used.

The Expert Step: An analyst takes this raw data and begins the real investigation—attributing the IP, correlating the data, and building a profile.



<https://canarytokens.com/nest/>

It is that easy!

canarytokens.com/nest/

Create a Canarytoken. Deploy it somewhere.

Know. When it matters. ?

All Microsoft Phishing Cloud Database Other

Search



Get an alert when an attacker visits your URL.

Web bug



Get an alert when an attacker resolves a DNS name.

DNS



Get an alert when an attacker attempts to use your credit card.

Credit Card



Get an alert when an attacker follows your QR Code.

QR code



Get an alert when an attacker loads your MySQL dump.

MySQL



Get an alert when an attacker uses your AWS API Key.

AWS keys



Get an alert when someone opens a fake app on your device.

Fake App



Get an alert when a log4j logline is vulnerable to CVE-2021-44-228.

Log4shell



Your Credit Card Canarytoken is active!

Place it on your computer and get notified when you're breached:



THINKST
CANARYTOKEN

Canarytokens.org
4367 9701 3335 8260

Expires 12/2026 CVV 137 **VISA**

Card Name
Canarytokens.org

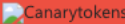
Card Number
4367 9701 3335 8260

Expires
12/2026

CVV
137

[Download Credit Card](#) [Test Credit Card](#) *Use me!*

 If the card is ever used in an authorization, the transaction will be declined, but you will be alerted.





Your Canarytoken was triggered

QR code Canarytoken has been triggered by the Source IP 84. [REDACTED]

Reminder
Test - ECBA

Source IP
84. [REDACTED]

Date	Time
2025/09/09	19:20 UTC

User agent
Mozilla/5.0 (iPhone; CPU iPhone OS 18_5_0 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko)
CriOS/140.0.7339.101 Mobile/15E148 Safari/604.1

Canarytoken ID
[REDACTED]

Alert History

Manage Alert

More info on this Canarytoken? [Click here](#)

LIVE DEMO: Tracking Digital Footprints

Canary Tokens: Digital Tripwires

Create Token

Generate a unique token at canarytokens.org and embed in document/email

Deploy

Send to target or place where subject will access

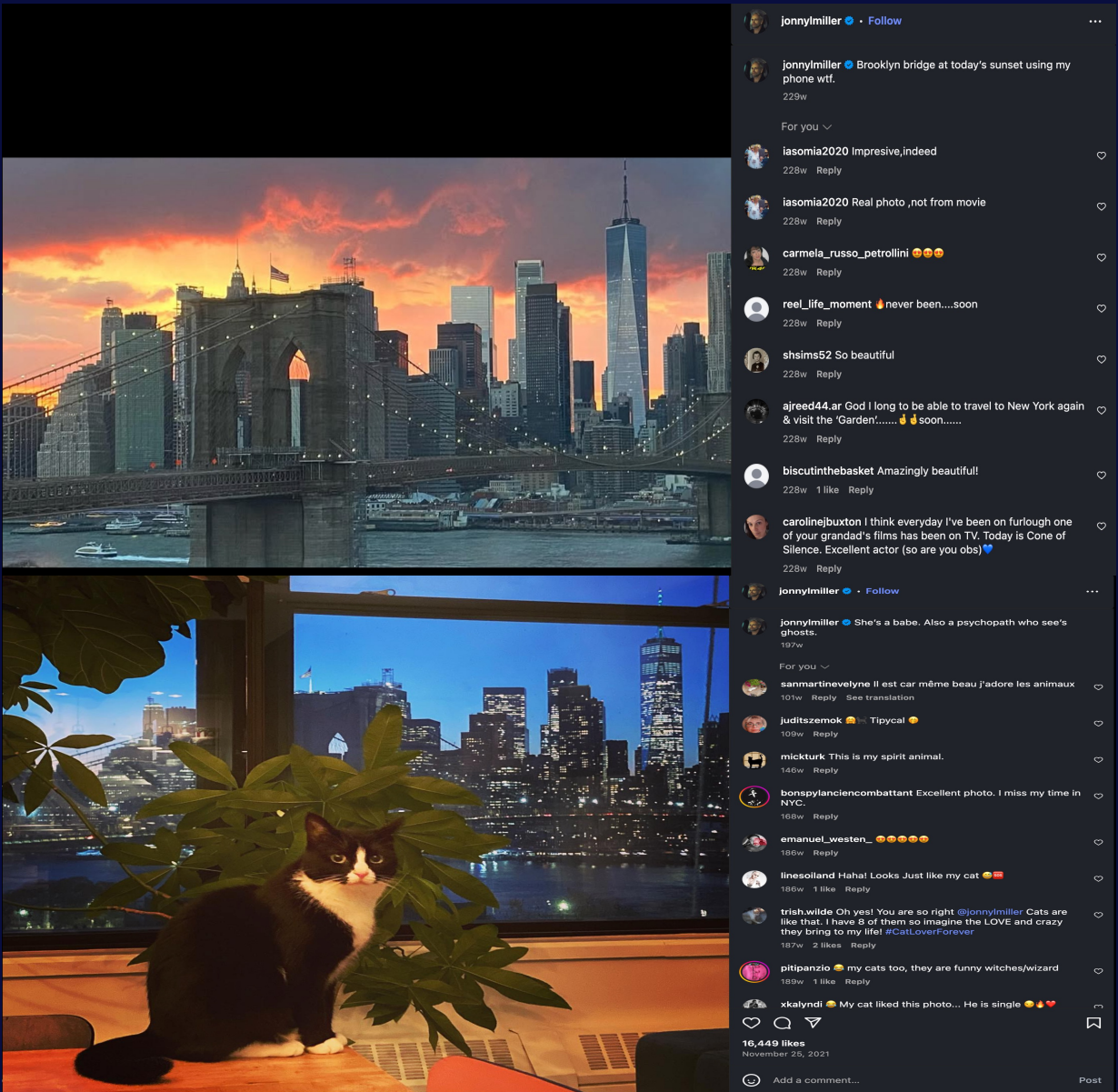
Receive Alert

Get notification with IP, timestamp, and device info when accessed

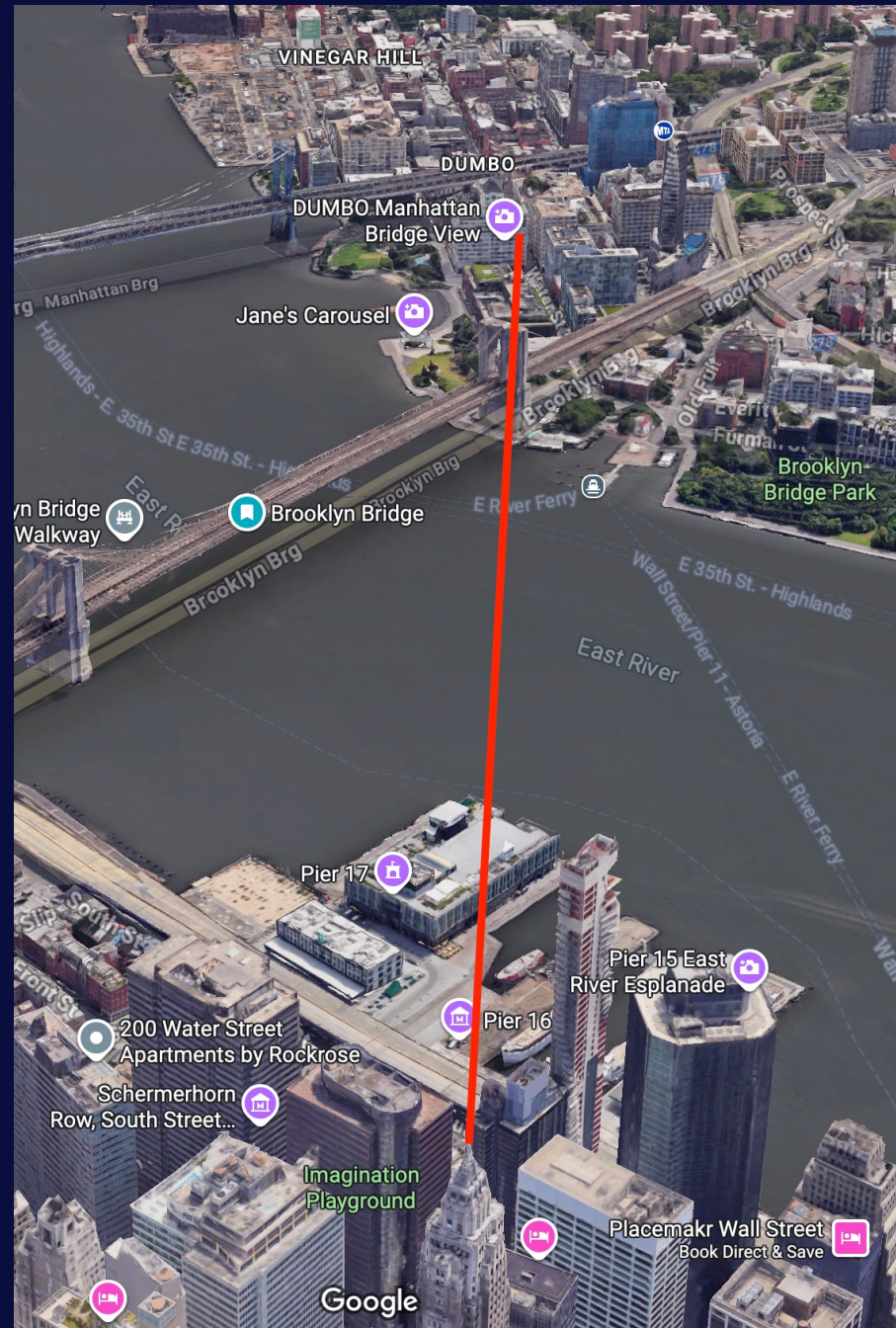
Legal consideration: Ensure deployment adheres to applicable privacy laws and disclosure requirements in your jurisdiction

Discover Angelina Jolie's ex-husband apartment using OSINT

Angelina Jolie and Jonny Lee Miller hung out in his Dumbo apartment. Using photos from his Instagram and an article from the DailyMail we're able to figure out where he lives.



Discover Angelina Jolie's ex-husband apartment using OSINT



Finding Rita Ora's London house

Rita Ora did an Archdigest video a while back and showed off her house somewhere in London. Let's find it using OSINT.



Finding Rita Ora's London house

Inside Rita Ora's Victorian-Era Sanctuary | Open Door | Architectural Digest



Arthur Rackham

35 languages

Article Talk

Read Edit View history Tools

From Wikipedia, the free encyclopedia

Arthur Rackham RWS (19 September 1867 – 6 September 1939) was an English book illustrator. He is recognised as one of the leading figures during the Golden Age of British book illustration. His work is noted for its robust pen and ink drawings, which were combined with the use of *watercolour*, a technique he developed due to his background as a journalistic illustrator.

Rackham's 51 colour pieces for the early American tale *Rip Van Winkle* became a turning point in the production of books since – through colour-separated printing – it featured the accurate reproduction of colour artwork.^[1] His best-known works also include the illustrations for *Peter Pan in Kensington Gardens*, and *Fairy Tales of the Brothers Grimm*.

Biography [edit]

Rackham was born at 210 South Lambeth Road, *Vauxhall*, London as one of 12 children. In 1884, at the age of 17, he was sent on an ocean voyage to Australia to improve his fragile health, accompanied by two aunts.^[2] At the age of 18, he worked as an insurance clerk at the Westminster Fire Office and began studying part-time at the *Lambeth School of Art*.^[3]

Arthur Rackham



Self-portrait, 1934

Born	19 September 1867 London, England
Died	6 September 1939 (aged 71) <i>Limpsfield</i> , Surrey, England
Known for	Children's literature, <i>Illustration</i>

Finding Rita Ora's London house

english-heritage.org.uk/visit/blue-plaques/

English Heritage

Visit | About us | Support us | Learn | Shop | Join |

Q

Members' Area

LONDON'S BLUE PLAQUES

London's famous blue plaques link the people of the past with the buildings of the present. Now run by English Heritage, the London blue plaques scheme was started in 1866 and is thought to be the oldest of its kind in the world.

More than 1,000 plaques across the capital, on buildings humble and grand, honour the notable women and men who have lived or worked in them. Discover some of the people commemorated with blue plaques, or search for a plaque, below.

The English Heritage London blue plaques scheme is generously supported by David Pearl and members of the public.



FIND A PLAQUE

Name or keyword

eg. Actor or Charles Dickens

London borough

All London Boroughs

▼

Category

All Categories

▼

SEARCH

>

From 1906 the family lived in Chalcot Gardens, near [Haverstock Hill](#),^[6] until moving from London to [Houghton, West Sussex](#) in 1920. In 1929, the family settled into a newly built property in [Limpsfield, Surrey](#).^[7] Ten years later, Arthur Rackham died at home of cancer.

1 RESULT FOR RACKHAM

RACKHAM, ARTHUR (1867-1939)

Painter, Illustrator

📍 16 Chalcot Gardens, Belsize Park, London, NW3 4YB, London Borough of Camden

RACKHAM, ARTHUR (1867-1939)

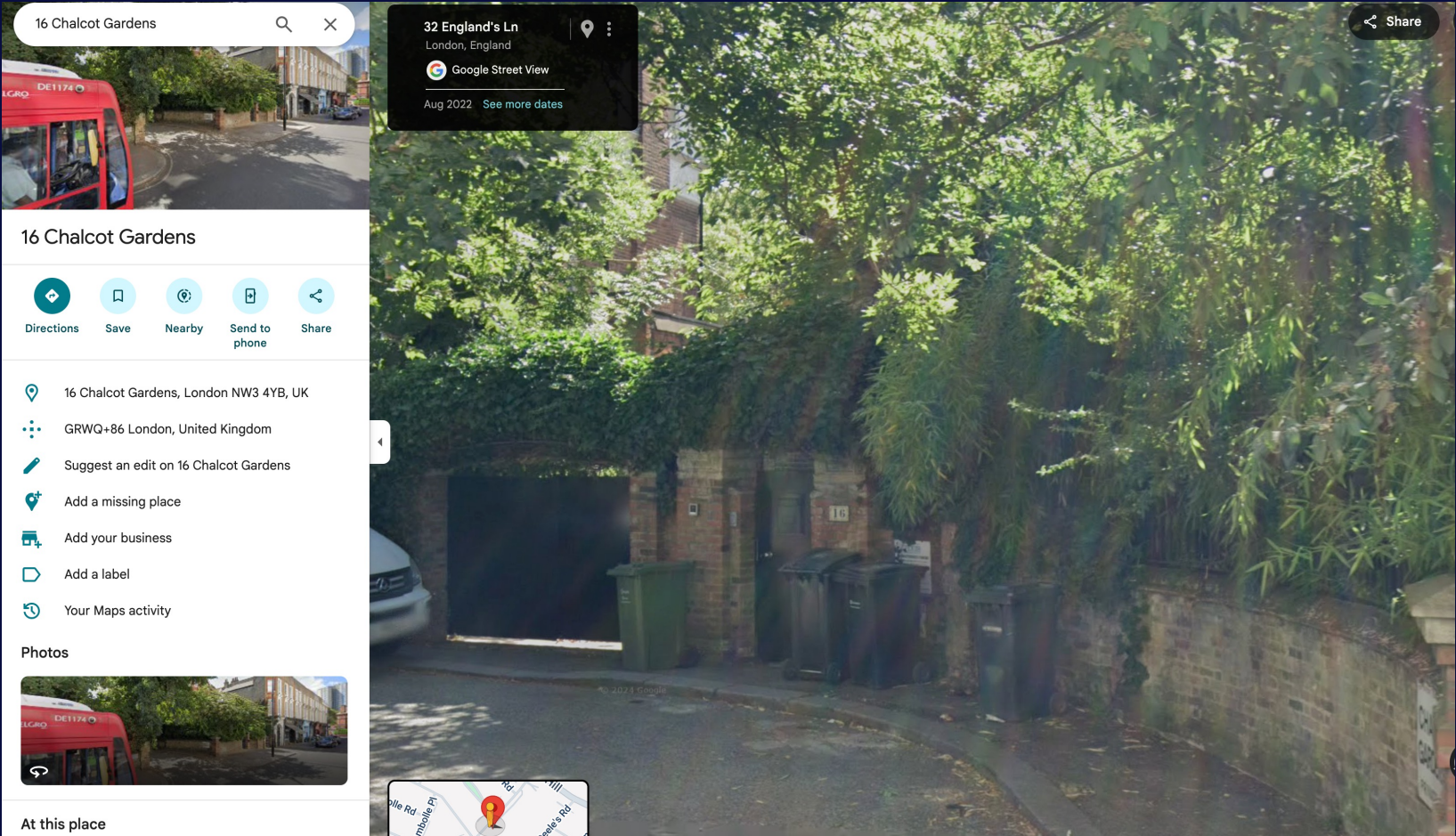
Plaque erected in 1981 by Greater London Council at 16 Chalcot Gardens, Belsize Park, London, NW3 4YB, London Borough of Camden

All images © English Heritage

Profession	Painter, Illustrator
Category	Cartoons and Illustration
Inscription	ARTHUR RACKHAM 1867-1939 Illustrator lived here
Material	Ceramic

 CYBEROPS

Finding Rita Ora's London house



The Photo's Secret (EXIF Data Extraction)

- 1. Enable Location Services:** First, ensure that the camera on your device has location services enabled. This setting allows the camera to record the GPS coordinates in the photo's metadata.
- 2. Capture the Image:** Take a digital photo of your target subject or location.
- 3. Transfer the File:** Transfer the photo file from your camera or phone to a computer. You can do this easily using a method like Airdrop, a USB cable, or by emailing the file.
- 4. Use an Online EXIF Viewer:** Open a free online EXIF viewer tool in your web browser. Popular options include **get-metadata.com** or **exif.tools**.
- 5. Extract the Data:** Drag and drop the photo file from your computer directly into the viewer's upload area. The tool will instantly read and display all the embedded EXIF data.
- 6. Pinpoint the Location:** Locate the **GPS coordinates** in the displayed data. You can often click on the coordinates to open a mapping application like Google Maps, which will show the exact location where the photo was captured.

```
dondada@Dons-MacBook-Pro ~ % exiftool Downloads/ECBA/WindowsXP_1551719014755.jpg
ExifTool Version Number      : 12.76
File Name                    : WindowsXP_1551719014755.jpg
Directory                   : Downloads/ECBA
File Size                    : 234 kB
File Modification Date/Time  : 2025:09:12 10:15:26+03:00
File Access Date/Time       : 2025:09:12 15:04:00+03:00
File Inode Change Date/Time  : 2025:09:12 10:15:29+03:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
XMP Toolkit                  : Image::ExifTool 11.27
GPS Latitude                  : 54 deg 17' 41.27" N
GPS Longitude                 : 2 deg 15' 1.33" W
Copyright                    : OWoodflint
Image Width                  : 1920
Image Height                  : 1080
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 1920x1080
Megapixels                   : 2.1
GPS Latitude Ref              : North
GPS Longitude Ref            : West
GPS Position                  : 54 deg 17' 41.27" N, 2 deg 15' 1.33" W
```

The X-Ray Vision (Google Dorking)

What is Google Dorking?

Google Dorking is a technique that uses specialized search queries to find information that is publicly available but not easily accessible through standard searches. It's not hacking; it's simply a skill that allows you to use Google's advanced operators to find files and data that organizations have accidentally left exposed to the public. This includes everything from confidential spreadsheets and internal presentations to login pages and private documents.

The Challenge

An admin endpoint (e.g., a page allowing user creation) has been left exposed on the following dummy website, designed for security testing.

URL: testphp.vulnweb.com

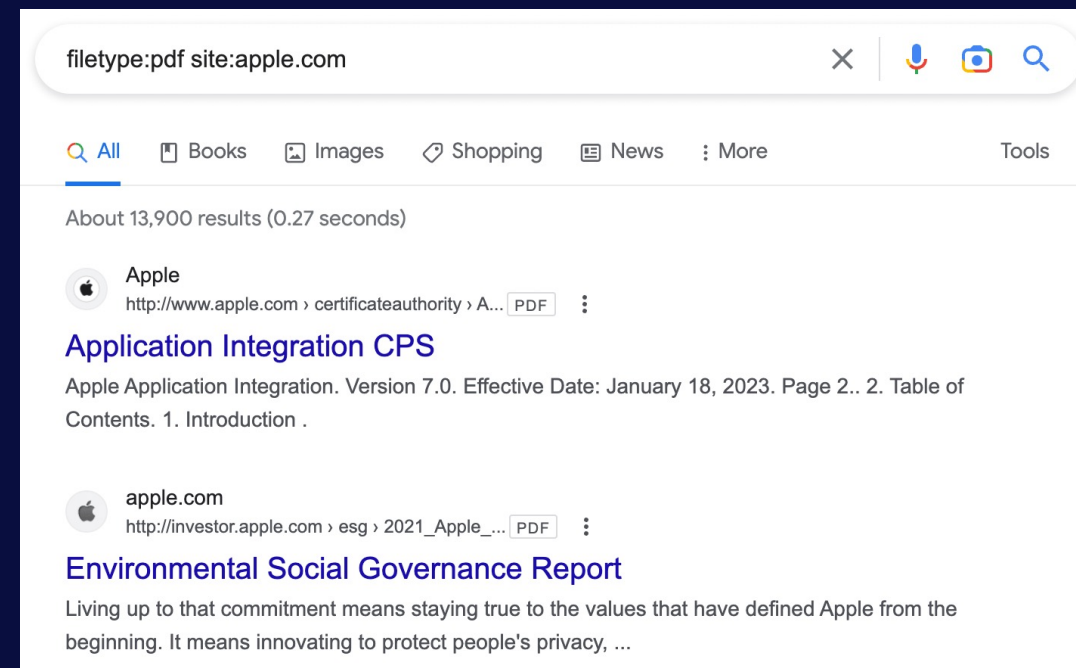
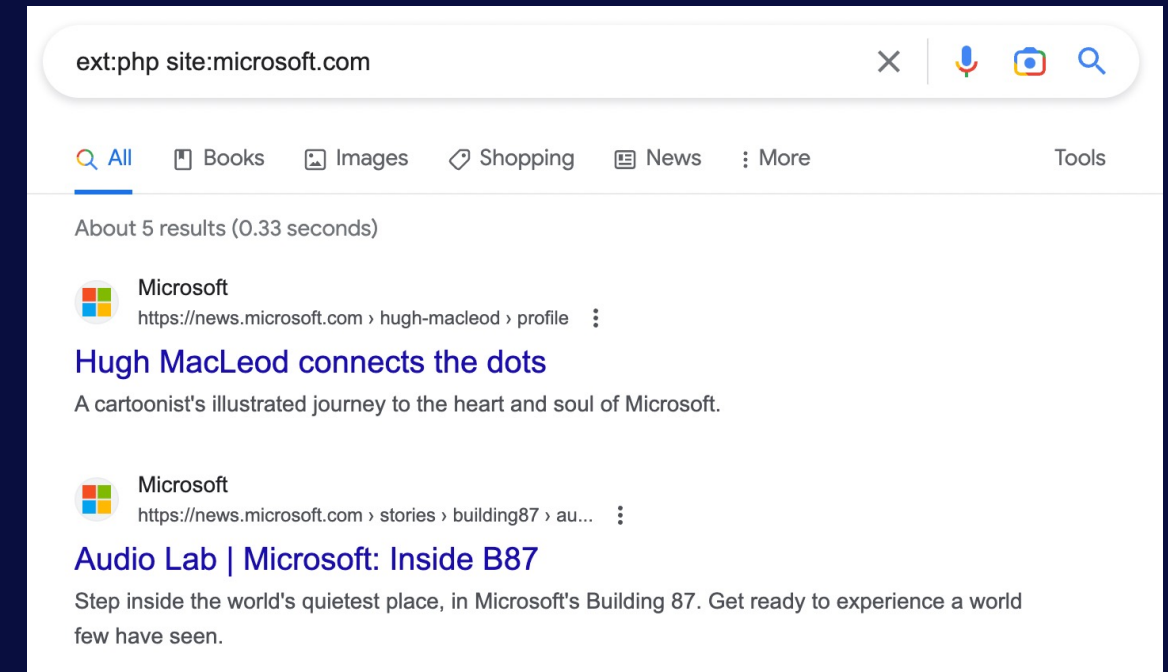
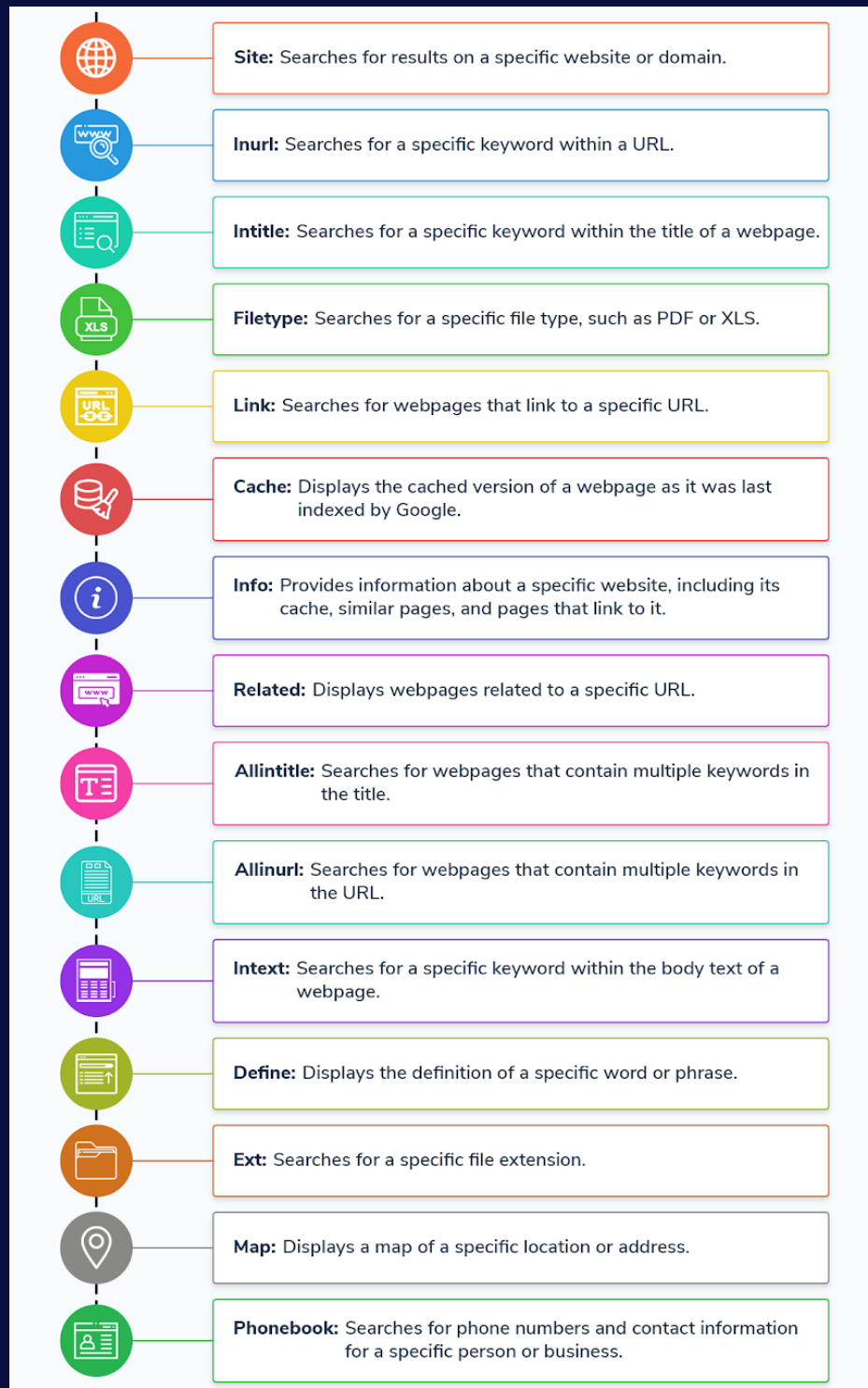
Your Mission: Use the Google search operators to find the admin endpoint and create a user without authorization.

Step-by-Step Guide

1. Open your web browser and navigate to <https://www.google.com/search?q=Google.com>.
2. In the search bar, construct your query by combining the operators. You will need to use site: to limit the search to the provided URL and quotation marks to search for the exact name of the flag.
3. Enter the complete search query and hit enter. The search results should lead you directly to the hidden file.

- Answer: **site:testphp.vulnweb.com inurl:"admin"**

Google Dorking Commands



Most Relevant Use Cases of OSINT

Due Diligence & Background Check:

Assessing individuals, companies.

Cybersecurity & Threat Intelligence:

Identifying vulnerabilities, tracking threat actors, and enhancing defenses.

Fraud Detection & Risk Management:

Uncovering deceptive practices, financial scams, and reputational risks.

Market Research & Competitor Analysis:

Gaining insights into industry trends, customer behavior, and competitor strategies.

Journalism & Investigative Reporting:

Uncovering facts, verifying information, and exposing corruption.

Geopolitical Analysis & National Security:

Monitoring global events, tracking extremist groups, and informing policy.

Professional OSINT Tool Management

Essential Online Investigation Dashboard

Modern OSINT investigations require a comprehensive suite of specialized digital tools. From social media analysis platforms to metadata extraction utilities, these tools form the backbone of professional intelligence gathering.

ALWAYS VET YOUR TOOLS!

Tool Authentication

Verify the legitimacy and security credentials of every investigation tool before deployment in sensitive cases.

Data Integrity

Ensure tools maintain chain of custody standards and provide audit trails for legal proceedings.

Privacy Compliance

Confirm that tools comply with relevant privacy regulations and professional ethical standards.

⚠️ Unvetted tools can compromise investigations, expose sensitive data, or introduce malicious code into your systems. Professional due diligence is non-negotiable.



Bellingcat



Set it on Fire Child
Github



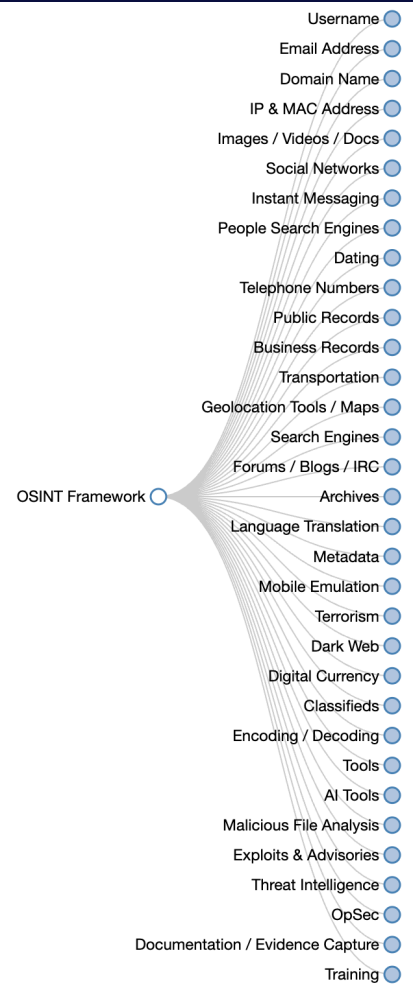
Hatless1der
Github



Cyb Detective
Github



Cyb Detective
OSINT Map



Preserving Evidence: Creating Your Own Chain of Custody

When you collect digital evidence, you must prove it hasn't been altered. This is the chain of custody.

1. Document Everything:

- Write down every step you take. What did you search for? Where did you click? What did you download? Note the date and time.

2. Record the Collection:

- The best method is a screen recording of the entire process, from logging in to saving the file. This shows every action and proves you didn't manipulate the evidence.

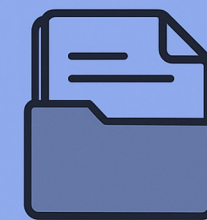
3. Create a Digital Fingerprint (Hash):

- Use a free tool to calculate the "hash" (a unique code) of the original file the moment you save it. If even one pixel is changed, this code will change completely. Record this code.

4. Use Archiving Tools:

- For websites and social media, use an archiving service like **archive.today**. It saves a copy of the page independently and gives you a link to a time-stamped, verifiable version.

CHAIN OF CUSTODY OSINT INVESTIGATION



EVIDENCE



COLLECTION



DOCUMENTATION



SECURITY



Challenging Digital Evidence in Court

IP Attribution Challenges

- Dynamic IP assignments and CGNAT complications
- Unsecured networks/public WiFi usage
- VPN/proxy/Tor usage possibilities
- Timestamp inconsistencies across devices

Collection Methodology Questions

- Chain of custody documentation
- Tool reliability and version information
- Calibration and maintenance records
- Analyst qualifications and certifications

Legal Authority Issues

- Jurisdictional questions for cross-border data
- Warrant specificity and scope limitations
- GDPR/data protection violations
- Fruit of the poisonous tree arguments

Remember: The prosecution must prove beyond reasonable doubt that their technical evidence specifically links to your client – simply the technical possibility is **insufficient**.

Defence Challenge: Questioning Authority's OSINT

Source Reliability:

How credible is the source? A random forum post? An anonymous social media account?

Chain of Custody:

How was the data collected, preserved, and presented? Was it altered?

Authenticity:

Can the prosecution definitively prove the online persona belongs to your client?

Relevance:

Is the OSINT evidence directly relevant?

Expert Testimony:

Challenge the qualifications and methodology of the state's "expert."

Remember: OSINT is useful, but it's also fragile. And fragility is exactly what you can exploit in court.

Defence Challenge: The Police's Chain of Custody

When the police present digital evidence, their chain of custody must be flawless. Ask simple, practical questions.

Who, When, Where?

Who collected the evidence?
What was the exact date and time? What was the physical location of the officer?

How?

What software or tool was used to capture the information? Was it just a screenshot? Did they record the process?

The Original Fingerprint:

Ask for the digital fingerprint (hash) of the file at the moment of collection. Does it match the fingerprint of the evidence presented in court?

Storage:

Where and how was the file stored between collection and trial? Who had access to it? Can you provide an access log?

Defence Challenge: IP Address Attribution

An IP address is not a person. An expert can prove it.

IP address attribution represents one of the most significant challenges in digital forensics. Legal professionals must understand the technical limitations and potential pitfalls when dealing with IP-based evidence.

Shared IP Networks

Entire households, office buildings, coffee shops, and public spaces often share a single public IP address through Network Address Translation (NAT), making individual attribution impossible.

Dynamic IP Assignment

Most residential and mobile IP addresses change frequently through DHCP lease renewals, meaning today's address may belong to a completely different user tomorrow.

VPNs & Proxy Services

Virtual Private Networks and proxy servers mask true locations, potentially routing traffic through servers in different continents while maintaining user anonymity.

Compromised Networks

Unsecured Wi-Fi networks allow unauthorized access by neighbors, passersby, or malicious actors, creating plausible deniability for the registered network owner.

Geolocation Limitations

IP geolocation databases typically provide city or regional accuracy at best, rarely pinpointing specific addresses, and often contain outdated or incorrect information.

Securing Lawyer-Client Communications

The Confidentiality Triad



Never discuss case details on standard cellular calls, unencrypted emails, or third-party messaging platforms lacking E2EE protection.

Counter-Surveillance for Defense Attorneys



Physical Measures

- Faraday bags for phones during sensitive meetings
- Regular sweeps for listening devices in offices
- Privacy screens for monitors/devices
- Awareness of physical surroundings during client meetings

Digital Protections

- Dedicated devices for sensitive case work
- Regular security updates on all devices
- VPN usage for all internet connectivity
- Disk encryption for all storage
- Two-factor authentication everywhere

Remember: Surveillance may be both state-sponsored AND private (opposing parties, tabloid media). Assume heightened risk in high-profile cases.

Protecting Ourselves: OPSEC for Legal Professionals

How can we use these investigative techniques to protect ourselves as professionals? Understanding OSINT capabilities is the first step toward implementing effective operational security.



Conduct a Digital Self-Audit

Perform comprehensive searches of your online presence. Google yourself using various combinations of your name, professional affiliations, and contact information to understand your digital footprint.



Practice Mindful Posting

Avoid sharing sensitive personal information, location data, travel plans, or case-related details that could compromise your safety or professional obligations.



Recognize Social Engineering

Develop skills to identify phishing attempts, pretexting, and other social engineering tactics designed to extract credentials or sensitive information.



Strengthen Privacy Settings

Review and enhance privacy configurations across all social media platforms, professional networks, and online accounts. Limit public access to personal information.



Implement Strong Authentication

Use complex, unique passwords for each account and enable Two-Factor Authentication (2FA) wherever possible to prevent unauthorized access.



Sanitize Digital Documents

Remove metadata from files before sharing externally. Document properties can reveal editing history, user names, and other sensitive details.

What is OPSEC?

Operational Security is an analytical and executional process that can be applied to any activity or operation for the purpose of denying valuable or critical information to an adversary.

"We're clean on OPSEC"

Pete Hegseth

TEAM UPDATE:

TIME NOW (1144et): Weather is FAVORABLE. Just CONFIRMED w/CENTCOM we are a GO for mission launch.

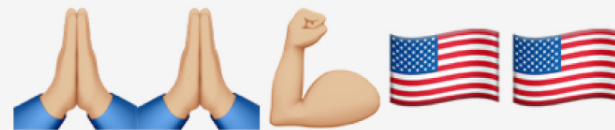
JD Vance

I will say a prayer for victory

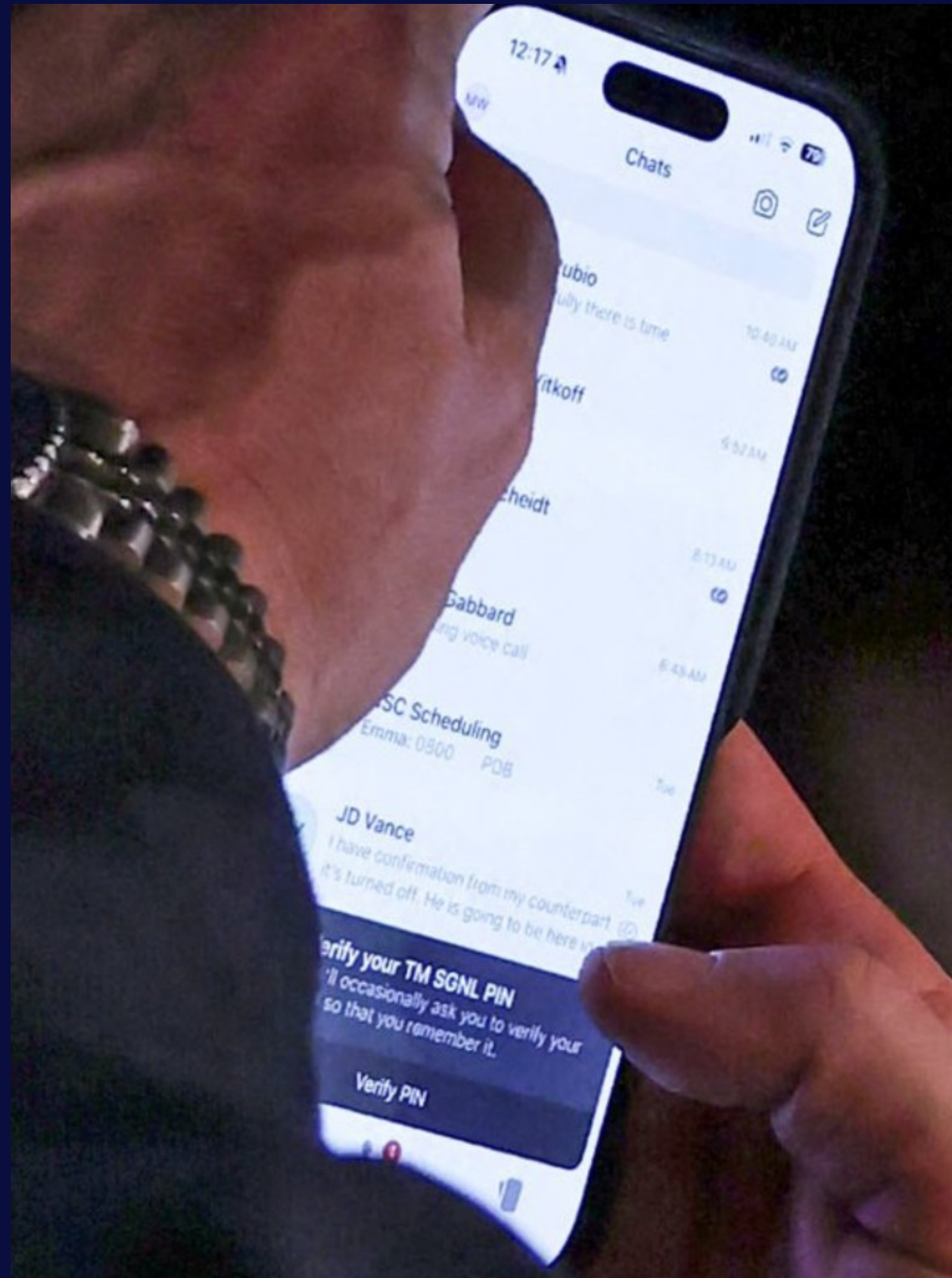
Pete Hegseth

We are currently clean on OPSEC.

Steve Witkoff



“We’re clean on OPSEC”



Business Email Compromise Defense

Business Email Compromise (BEC) attacks cost organizations billions annually. Professional email analysis and robust internal protocols form your primary defense against sophisticated fraud attempts.



Expert Email Analysis

Suspicious email headers contain detailed routing information. Forensic experts can analyze message paths, authentication records, and metadata to determine true origins and detect spoofing attempts.



Payment Verification Protocols

NEVER change payment information based solely on email requests. Always verify through independent communication channels using previously established contact methods.



Voice Confirmation Requirements

ALWAYS verbally confirm high-stakes financial requests using known, trusted phone numbers from your records—never numbers provided in suspicious emails.

ⓧ **Staff Training is Critical:** Train all employees to maintain healthy skepticism toward urgent or unusual requests, especially those involving financial transactions or sensitive information sharing.

Essential Security Mindset

When in doubt, verify through multiple independent channels. The cost of verification is always less than the cost of successful fraud.

Quiz



Real Quiz



CASE STUDY: The 120 Bitcoin Heist

The Scenario: A victim loses 120 Bitcoins in a sophisticated fraud.
The investigation begins with very limited information from authorities.

The Loss: 120 BTC

The Initial Leads (The "Digital Breadcrumbs"):

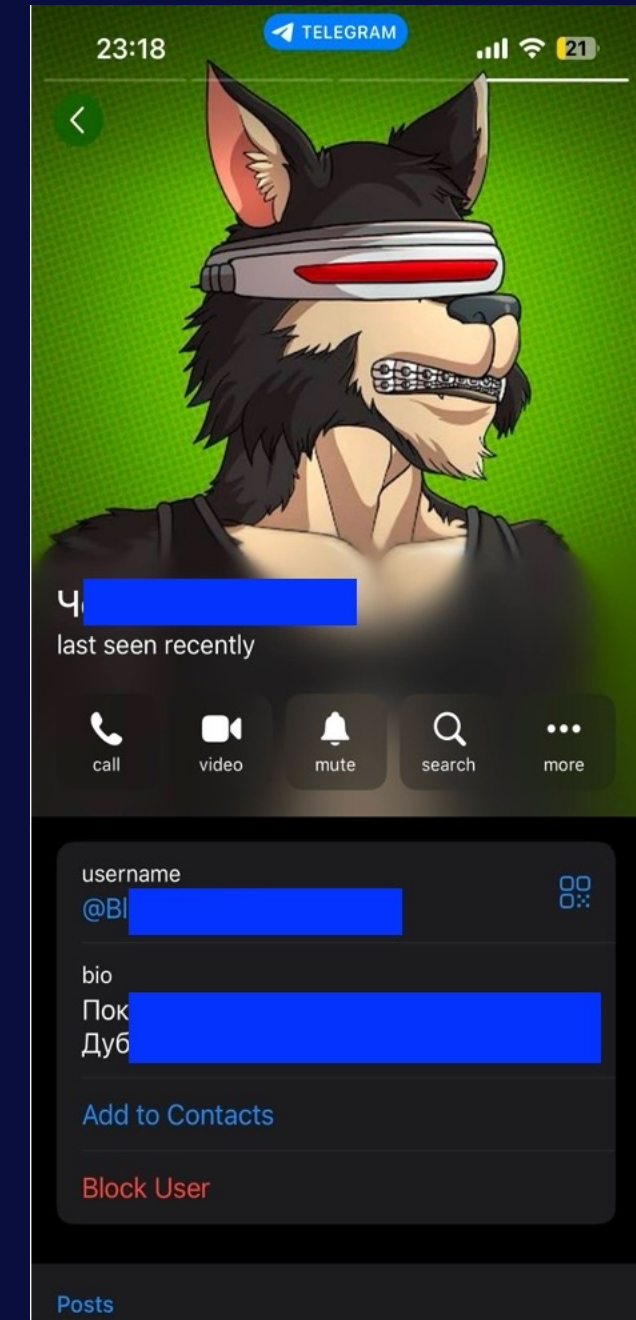
An email address: sXXXXX@mail.ru

A username: ShamMs

A Telegram handle: BlackXXXX

A phone number: +792XXXXXXX

The Objective: Can we turn these few digital clues into a real-world identity?



CASE STUDY: Connecting the Dots

The investigation focused on finding where these clues appeared together online.

Step 1: The Data Breach Pivot:

Searching leaked databases revealed that the email, phone number, and the full name Shamurzaev MagoXXX-SaXXX appeared together in multiple breaches (VK, CDEK courier). This was the key that connected the alias to a real name.

Step 2: Deconstructing the Alias:

The username ShamMs was identified as a structured alias:

Sham = Shamurzaev

M = MagoXXX

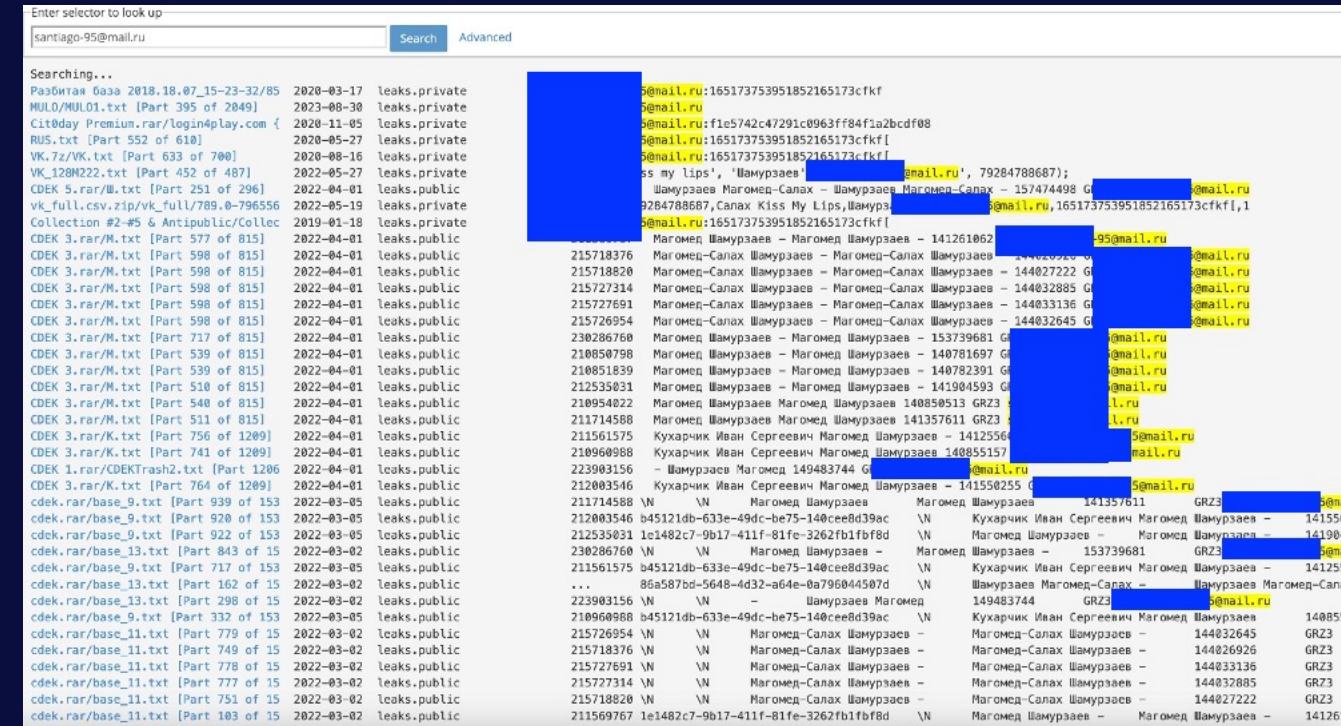
S = SaXXX

Step 3: Social Media & Public Records:

A search for the full name led to a VK (Vkontakte) profile with photos, confirming his identity.

The profile and other public data confirmed his location as Grozny, Chechnya.

Russian business registries showed he was a registered entrepreneur, providing a legal anchor to his identity.



Current plate format [edit]

Breakdown of the main elements of the Russian vehicle registration plate.

The current format uses a letter followed by 3 digits and two more letters. To improve legibility of the numbers for Russian cars abroad, only a small subset of Cyrillic characters that [look like Latin characters](#) are used (12 letters: A, B, E, K, M, H, O, P, C, T, Y, X), additionally D was issued on some very early plates.^[1] Finally, the region number (77, 97, 99, 177, 197, 199, 777, 797 and 799 for [Moscow](#); 78, 98, 178, and 198 for [Saint Petersburg](#), etc.) and the international code [RUS](#) with the 1991 to 1993 Russian flag typically to the right of it, however the flag is not mandatory, and since 2013

owners may order plates without it ^[2]

19	Republic of Khakassia
(20)^[b], 95	Chechen Republic
21	Chuvash Republic

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners may order plates without it ^[2]

owners

CASE STUDY: The Outcome

From a handful of digital clues, a complete profile was built.
The Attacker: Shamurzaev MagoXXX-SaXXX, a Russian national born in 1994.
Location: Grozny, Chechen Republic, Russia.

- Key Identifiers Confirmed:**
- Photos from social media.
 - University affiliation in Ukraine.
 - Official business registration records.

Significant Risk Factors Uncovered:
A familial name match to an individual listed under Russian anti-terrorism financing laws.
Origin in a region known for transnational criminal networks.

Conclusion: The investigation successfully unmasked a supposedly anonymous attacker, providing the legal team with a real name, face, location, and actionable intelligence.



Страна проживания: Россия
Город: Грозный
Телефон: 22861
Текущая деятельность: НТУ «ХПИ»

Отправить
сообщение



ПОДРОБНАЯ ИНФОРМАЦИЯ:

Салах Шамурзаев проживает в городе Грозный, Россия. Родной город - Чечня. Из открытых источников получены следующие сведения: информация о высшем и среднем образовании, карьере, службе в армии.

Салах пишет о себе:
Я чеченец!)

Интересы Салаха:
Сижу за компом!) Гуляю...) Кайфую от всего!)

САЛАХ ШАМУРЗАЕВ ЖИВЕТ ЗДЕСЬ:

* Фактический адрес проживания определен с точностью до города: Россия, Северо-Кавказский федеральный округ, Грозный.

Q&A and Key Takeaways

Use OSINT Defensively

Apply the same techniques authorities use to verify their claims and develop counter-narratives

Protect Yourself

Implement proper security measures to prevent business email compromise and surveillance

Secure Client Communications

Use appropriate encrypted channels and educate clients on proper security protocols

Challenge Digital Evidence

Question technical assumptions and demand proper authentication of digital forensics

Contact Information

infosec@CyberOpsNetwork.com | www.CyberOpsNetwork.com

HACKERS KNOW YOUR VULNERABILITIES
DO YOU?

Workshop time – Group 1

1. Download the following image: <https://bit.ly/ECBA-CyberOps>
2. Use only details from GitHub, Twitter(X) and the WordPress website to answer the questions from the quiz



Workshop time – Group 2

Picture 1



Picture 2

