Case Study: Unmasking the 120 BTC Telegram Fraudster

Demonstrating advanced Open Source Intelligence (OSINT) techniques to convert digital breadcrumbs into actionable legal intelligence. This investigation transformed an anonymous threat actor into a fully identifiable perpetrator within 96 hours.

The Challenge: A Digital Ghost Story

A British Virgin Islands-based client approached our team through partner counsel after falling victim to a sophisticated Telegram-based fraud scheme. Criminals orchestrated a carefully crafted deception, resulting in the theft of 120 Bitcoin, an asset loss valued at approximately £4.5 million at the time of the investigation.

The perpetrators operated behind layers of digital anonymity, employing disposable infrastructure and encrypted communications. The victim possessed only fragmented identifiers: a single email address, an anonymous Telegram handle, and an untraceable phone number.

The Investigation: Four Days to Identity

Our lead investigator, Ovi, deployed a systematic OSINT methodology designed to pivot from anonymous digital footprints to verified real-world identities. The operation leveraged global breach databases, social engineering patterns, and specialised access to Russian business registries.

The Data Breach Pivot

Cross-referenced initial leads against global leaked databases, identifying a crucial match where the email, Telegram handle, and phone number appeared together in breaches from VK (Vkontakte) and CDEK courier services.

Deconstructing the Alias

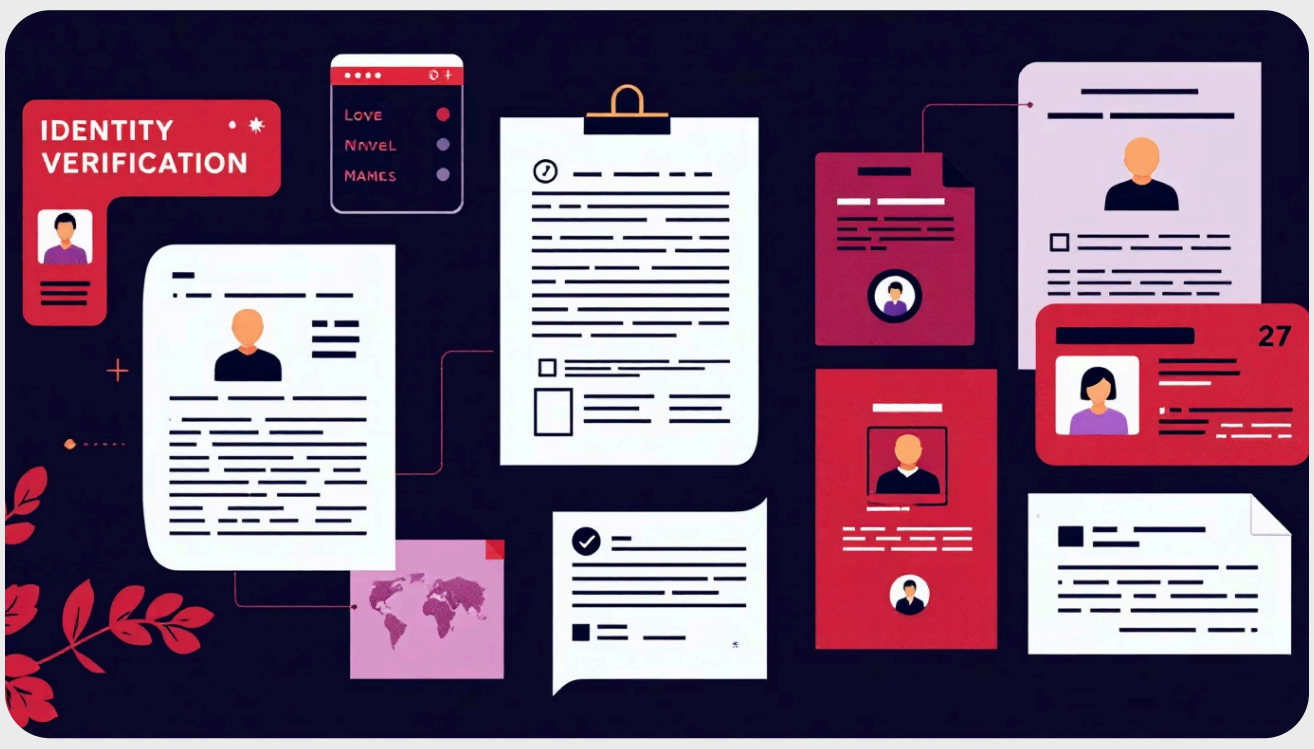
Analysed username "ShonMs" as a structured alias, successfully decoding: Shon = Shony, M = Mahamed, s = Suri, revealing full identity components.

Official Documentation

Leveraged specialised access to Russian business registries and public records, locating a registered entrepreneur matching the decoded name establishing a legal anchor connecting digital persona to physical, tax-paying entity.

The Outcome: Full Exposure

Within 96 hours, the investigation established a comprehensive profile of the perpetrator, transforming a cold case into actionable legal pursuit.



Intelligence Category

Attacker Identity: Shony Mahamed-Suri (Born 1994)

Physical Location: Grozny, Chechen Republic, Russia

Legal Status: Registered Entrepreneur in Russian registries

The investigation yielded evidence showing familial links to anti-terrorism financing watchlists and social media photos confirming university affiliation in Ukraine.

Conclusion

This case demonstrates that even seemingly anonymous attackers leave digital trails that can be reconstructed through systematic OSINT methodology. By unmasking the perpetrator and establishing verifiable identity, physical location, and legal status, we provided the legal team with actionable intelligence for civil recovery and potential criminal referral. The case proves that cryptocurrency anonymity is often an illusion.

Key takeaway: Specialised access to regional business registries and understanding of naming conventions can pivot anonymous handles to verified identities in under 120 hours.

Book a Meeting