Leveraging Open-Source Intelligence to Combat Cryptocurrency Investment Scams

Johnny Botha[1], Abraham Berkman[2] and Louise Leenen[3]
[1]Council for Scientific and Industrial Research, Pretoria, South Africa
[2]Breadcrumbs, Singapore
[3]University of Western Cape and CAIR, Cape Town, South Africa

jbotha1@csir.co.za
avi@breadcrumbs.app
lleenen@uwc.ac.za

Abstract: This paper presents a follow-up study to earlier research on cryptocurrency crime, again drawing on the case of an elderly woman defrauded by an online platform known as RSI-Platform. Whereas the initial study focused mainly on on-chain analysis within the blockchain environment, the present work shifts attention to off-chain approaches, applying open-source intelligence (OSINT) techniques to deepen investigations into crypto-related fraud. By systematically examining diverse input data—such as names, phone numbers, email addresses, and URLs—this study conducts link analysis and aims to build detailed profiles of potential suspects, thereby advancing understanding of the strategies and methods used in cryptocurrency scams. The analysis aims not only to trace the scammers' digital footprints but also to reveal networks and connections to other fraudulent platforms that support these activities. Moreover, this research seeks to raise public awareness about the scale and operation of fake online investment schemes in the crypto sector. By exposing the vulnerabilities exploited by offenders and illustrating how OSINT can be used to detect and disrupt such scams, the paper adds to ongoing discussions on cybersecurity and consumer protection in the fast-changing field of digital finance. Additionally, the findings are intended to offer practical insights for law enforcement agencies, policymakers, and the wider public, encouraging a more informed and proactive response to the threats posed by crypto-related fraud.

Keywords: Cybercrime, Cybercrime investigations, Cryptocurrency scams, Fake investments, OSINT

1. Introduction

Botha et al. (Botha, Singh, & Leenen, 2026) examined a fraudulent cryptocurrency investment and trading scheme by applying an investigative process introduced in earlier work (Botha, Singh, & Leenen, 2025). The previous study focused more heavily on on-chain analysis conducted directly on the blockchain, while giving relatively less consideration to off-chain analysis. The on-chain analysis was conducted using the tool Breadcrumbs, a cryptocurrency investigation tool that offers a transaction tracing platform for digital assets.

In contrast, this investigation study concentrates mainly on the off-chain analysis, which incorporates a range of OSINT methods and techniques. OSINT involves gathering, processing, and correlating information that is publicly accessible from open data sources like social media, forums, blogs, public government data, publications, or commercial data. OSINT methodologies begin with initial input data and employ advanced collection and analysis techniques to progressively enhance understanding about a target individual or organisation. As each new piece of information is discovered, analysts move closer to their ultimate objective (Pastor-Galindo, Nespoli, Gómez Mármol, & Martínez Pérez, 2020). Two types of OSINT exist, passive and active. Passive OSINT is the process of gathering information from publicly available sources, as described above, and similar open data repositories (Kolenbrander, 2025). In the case of an investigation, passive OSINT analysis aims to collect personal data about a target without any direct interaction with them. This method utilises various tools to find specific details, aimed at constructing a profile of the target individual (Botha, Singh, & Leenen, 2025). Active OSINT typically involves the use of a program or script to collect data and leaves a log behind (Kolenbrander, 2025). Active OSINT analysis also entails interacting with a target person under deceptive circumstances, such as using a fake or undercover profile, to persuade them into disclosing personal information. This approach, however, carries a higher likelihood of the target discovering the tactic used by the investigator, potentially resulting in them changing their behaviour. This also raises legal and ethical issues, including the risk of violating the policies of legitimate platforms (such as social media) and concerns about possible entrapment. What strategies are allowed can differ significantly between jurisdictions. For this investigation, no active OSINT methods were utilised. Active OSINT can also considered hacking. For example, if it is possible to manipulate a messaging application's metadata to expose the IP of the other party on the chat, it is considered hacking (Berkman, 2026; Hwang, Lee, Kim, Lee, & Kim, 2022; Hwang, Lee, Kim, Lee, & Kim, 2022).

This paper discusses the strategies and tools employed in this study, the theories investigated and the ultimate conclusions reached based on facts and evidence found. The authors first outline the case study's background

and context, followed by an off-chain analysis of the incident. The off-chain analysis employs several OSINT techniques and methods. After sufficient intelligence has been collected to profile the target entity, a link analysis is performed. The final stage addresses the associated law enforcement procedures. The expanded OSINT sections are intended to serve as a proposal for refining the process suggested in (Botha, Singh, & Leenen, 2026). The final section concludes the paper's main findings.

2. Case Background

The previous study proposed a theory that the ex-son-in-law (referred to as 'Mr-X' in this paper) could have been collaborating with the scammers. Note that investigators tend to use the term theory and not hypothesis in their investigations. For this paper the term "theory" will be used and refers to a "working theory" or "hypothesis". It is quite common for fraudsters to use local individuals to attract potential victims. These intermediaries are typically given some type of compensation for identifying and attracting victims. The particular scam platform under examination is called RSI-Platform and was ran out of the website 'https://rsi-platform.io' (note that the web domain is not active anymore since the scammers must have taken it down). The victim, an elderly woman, was persuaded to invest in the platform, which was portrayed to be a global online trading entity based in the United Kingdom (UK), integrating traditional investments with crypto-based funding and trading mechanisms. More details on the background can be found in the previous study, (Botha, Singh, & Leenen, 2026).

This study pursues two primary objectives:

- Collect online, off-chain information to attempt to identify the suspect, and
- To investigate and substantiate the hypothesis that 'Mr-X' is involved with the scammers.

The first author of this paper contacted TCG Forensics (TCG Forensics, 2026) and Breadcrumbs (Breadcrumbs, 2023) for support with the OSINT techniques, and both companies agreed to help. Craig Pederson, the CEO of TCG Forensics, contributed by attempting to identify the scammer and by gathering as much online information as possible. Abraham Berkman, Head of Intelligence at Breadcrumbs and the second author of this paper, also assisted by collecting data to determine the scammer's identity and to either confirm or dismiss the hypothesis that Mr-X was involved with the scammers, or whether he was in fact a genuine victim. Both Pederson and Berkman have backgrounds in OSINT and cybercrime investigations.

The indicators point to the involvement of both offshore and local parties, which aligns with a syndicated operation. In these cases, funds are transferred directly into crypto-exchange accounts using a specific reference number that routes the funds to the actor's wallet. This process circumvents many fraud prevention measures and enables money laundering by avoiding traditional banking channels. Once the credit reflects in their crypto-exchange account, the actor is then able to transfer the funds onwards.

3. Investigation Process

Similarly to the previous study, this analysis also follows the investigative process proposed by (Botha, Singh, & Leenen, 2025). The process has five phases, namely:

1. Data collection
2. Analysis
3. Theory development and validation
4. Suspect identification and reasonable grounds
5. Legal action

3.1 Data Collection

This section provides an overview of the collected data (evidence) from the victim. This paper focuses exclusively on the off-chain data that was gathered. The victim provided the following inputs *(names and contact information are redacted)*:

- *Suspect website domain*
- www.rsi-platform.io
- Screenshots of the suspicious domain.
- *Cryptocurrency addresses linked to the suspect domain. The preliminary tracking of these crypto transactions is documented in the earlier study (Botha, Singh, & Leenen, 2026)*
- *Names*

- List of names linked to the suspect domain – contacts communicating via WhatsApp and phone calls (numerous persons and names, which are likely all aliases).
- *Phone Numbers*
- List of numbers in connection to the suspect domain from which calls to the victim were made (SA and UK numbers)
- *Email Addresses*
- s#####e@cryptodotcom.info
- List of scammer names@###-platform.io
- *Physical Address*
- # B### St, London E## #BG, UK

3.2 Analysis

The analysis employed three basic steps in iteration, based on advice from an OSINT expert from Hawk Eyes OSINT and Breadcrumbs (Hawk Eyes, 2026) (Berkman, 2026):

- **Evidence Overview**: An examination of the evidence at hand to gain an understanding of the case, identification of areas for evidence enrichment and development, and affirmation or refutation of theories.
- **Evidence Enrichment**: Based on the evidence at hand, various tools and investigation methods were employed to process and further enrich the evidence base. This can also be done from a completely objective outlook or an effort to affirm or refute a running theory.
- **Theory Development (see Section 2.3)**: Based on the evidence overview, theories regarding the case were developed and those theories had to be affirmed or refuted by further evidence enrichment.

Typically, a case starts with preliminary evidence supplied by a client or victim (see Data Collection in Section 3.1). This initial evidence must be analysed so that a working theory can be formed, or so that potential ways to enrich the evidence can be identified. When such opportunities are found, the evidence should be enriched and then re-examined until a theory is developed. All new information that appears to be connected to the suspect should be incorporated into a link analysis diagram, (see section 4, Figure 4). After a theory has been developed, additional evidence must be collected and repeatedly reviewed until the theory is either supported or disproved. If the theory is disproved, the investigator must reassess the evidence and formulate a new theory. This iterative process continues until a theory is confirmed and the case can be closed. See Figure 1, which illustrates this process.

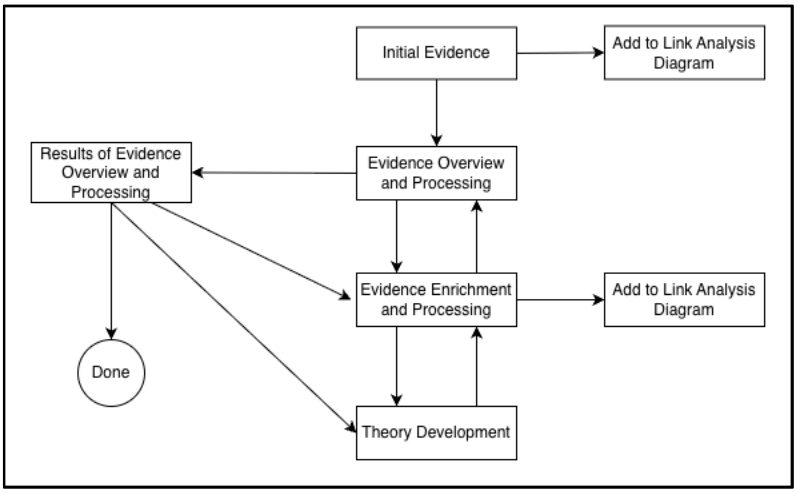

Figure 1: OSINT Investigation Process

In this segment of the analysis, OSINT methods are used to attempt to reveal the suspect's identity, based on the inputs and details provided by the victim. The proposed process by (Botha, Singh, & Leenen, 2025) does not give enough details on steps to be followed in the off-chain analysis, specifically with respect to the OSINT techniques. The steps seen in Figure 1 are added to the analysis phase in this investigation.

3.2.1 Evidence overview and processing

The client provided evidence as listed in Section 3.1. This section goes through all evidence and process them to gain more insights.

Domain Name

Because the scam originated from the website at the domain "https://rsi-platform.io", the initial step was to collect any further information associated with that domain. As the site is currently offline, the WayBackMachine (WaybackMachine, 2026) was used to retrieve historical data about its structure. The aim was to determine whether a comparable website run by the same offenders was still online, which would allow for network monitoring and a more detailed understanding of how the scam operated. Only a single screenshot from October 2022 was available on Wayback Machine (see Figure 2). This suggests that the site operated with limited capacity, received little traffic, and was active only for a short period. By using Chrome's 'inspect' tool, the screenshot revealed the site's HTML, CSS, and links to portions of its JavaScript. Distinctive code fragments were then extracted and searched on NerdyData (NerdyData, 2026) to identify other websites that might be using the same snippets. A further goal was to identify any extra information that might be obtained from the website's front end, such as additional phone numbers or email addresses. Ultimately, no further information could be collected.

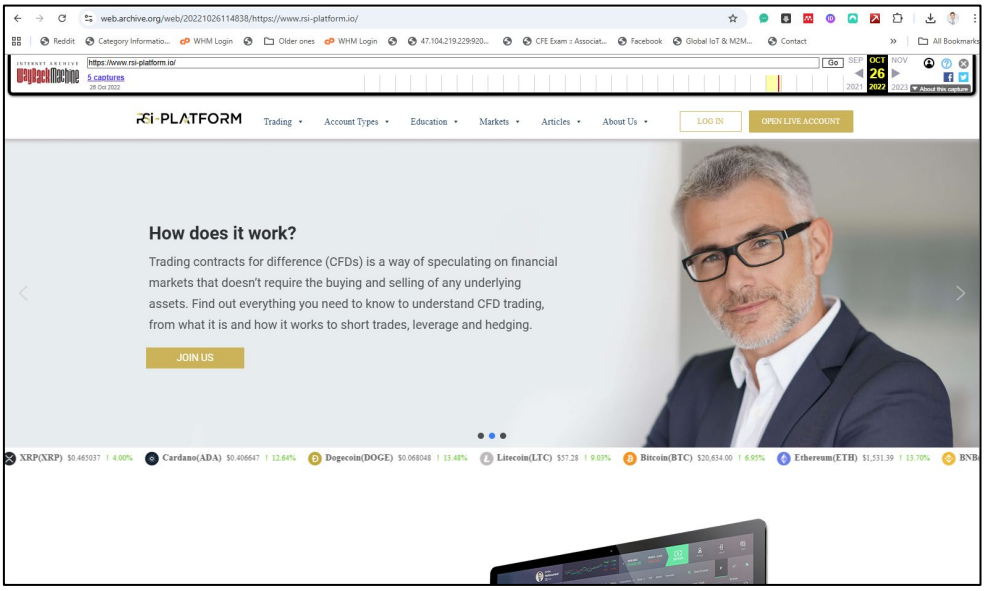

Figure 2: RSI-Platform - Home Page

WHOXY (WHOXY, 2026) reported that there is currently no active hosting on the domain. It does, however, provide information on the most recent registrar, as illustrated in Figure 3. Additional registrar data for the 2022 period may be obtainable directly from the registrar upon request. Particular focus should be given to the payment method used to acquire the domain in 2022.

MX Toolbox (MXToolbox, 2026) shows that there are currently no functioning mail routes, redirects, or traceable records linked to the domain. Opencorporates (opencorporates, 2026) further indicates that the supposed 'company' called 'vestpro', which the website claims is registered in the Seychelles, appears not to exist. There is no matching company registration or recognised legal entity connected to the site. Taken together, this strongly supports the conclusion that the rsi-platform.io website was precisely what it seems to be: just a small collection of pages created to lure in and reassure prospective victims. None of the claims or information displayed on the rsi-platform.io site can be verified against any reliable, factual sources.

The website scam detector (scam-detector.com, 2025) provides original information, reporting, reviews and analysis on websites, domains and e-commerce platforms, and advises if these are legitimately, safe and trustworthy. The www.rsi-platform.io web domain received a score of 40.7% from scam detector which signals risk and red flags. The domain was created on 23 June 2022, and the victim was scammed starting in December 2022. Shortly after the domain was created, scam detector also indicated it has a proximity to suspicious websites of 73% and a phishing score of 78%. The website's meta data was poorly configured which would not

help its online presence and resulted in a loss of credibility. The domain was active for 1 year, 11 months before it became inactive.

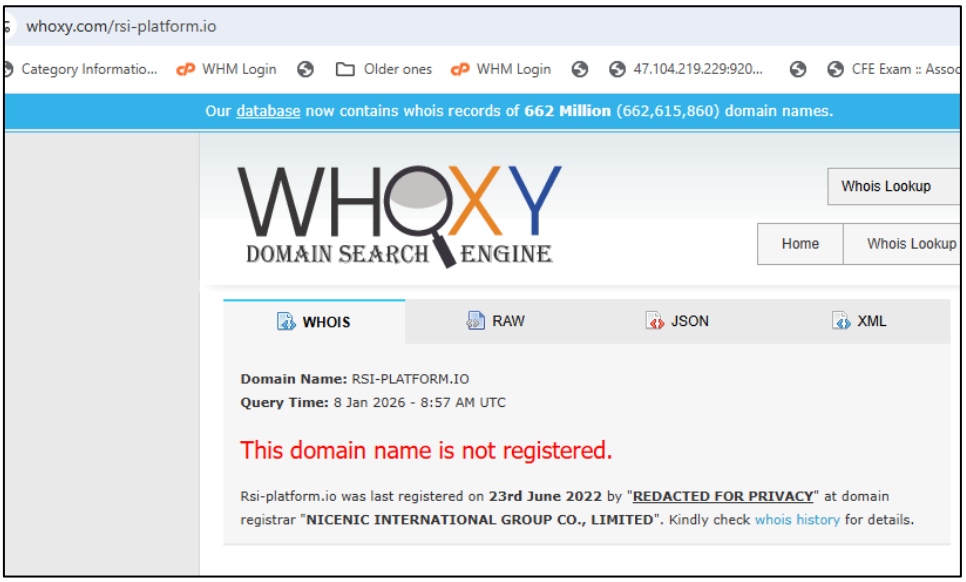

Figure 3: WHOXY Domain Search Engine

Another search result from Google pointed to the website www.55brokers.com, which suggests that RSI-platform appears to operate as a UK-based entity, with the authority to provide services in the UK. Nonetheless, its regulation is solely in St. Vincent and the Grenadines, classifying it as offshore. Therefore, this is typically indicative of a scam (55BROKERS, 2025).

Names and Contact Information

The victim provided a list that included names and phone numbers from South Africa (SA) and the UK. Through Truecaller (Truecaller, 2025), it was discovered that the SA numbers are linked to the RSI-platform ZA Office and that these numbers are Voice-over-IP (VoIP).

Regarding the list of email addresses all belonging to the domain RSI-platform.io, various user complaints were found on websites like ScamAdviser and Trustpilot (Trustpilot, 2023), involving unsolicited emails promoting 'guaranteed' investment opportunities or recovery services for lost funds. The platform has been reported as 'pig butchering' or advance-fee scams, where scammers build trust via email or chat, then request deposits or personal information. Pig butchering is an investment scam where fraudsters gain the trust of victims of time and then deceive them into investing in fake investment platforms (often fake cryptocurrency investment platforms) (DFPI, 2025).

No reliable business or professional profiles associated with any of these email names could be connected to the email addresses in recognised directories such as LinkedIn or official corporate registries.

3.2.2 Evidence Enrichment

Domain Name

A lookup of the domain in BigDomainData (BigDomainData, 2026) showed that it was registered via the Hong Kong–based registrar Nicenic International Group Co. by an individual named 'Tyron Cantrell' from 'Gwynedd County, Nigeria'. Gwynedd County is located in Wales, and no corresponding Gwynedd County could be identified in Nigeria. A review of the hosting provider, NiceNic, revealed that the platform operated without any KYC (Know your Customer) procedures and accepted payments through several methods, including cryptocurrency. This setup made it possible for clients to submit false registration details and pay in a pseudo-anonymous manner using cryptocurrency. Linking this information to the cryptocurrency addresses tied to the scammers could move the investigation forward, effectively bringing together OSINT and blockchain analysis. NiceNic's website also contained links to the platform's social media (SM) accounts on Facebook, X (formerly Twitter), and Pinterest. NiceNic cryptocurrency payment addresses included, but not limited to:

- 0xEd…61B8 - CircleCoin(USDC)

- 0x5E…2297 - USD_Tether (USDT)
- Bc1q…4mfa – Bitcoin (BTC)

By combining the on-chain and off-chain analysis, it also shows how Web2 (OSINT) and Web3 (on-chain or blockchain) investigations complement each other and are not mutually exclusive. In Web2, people depend on centralised services—such as social networks, online banking, and search engines. Web3 introduces a new model built on decentralised infrastructure and applications, such as the BTC blockchain (Lacity & Carmel, 2024). For example, in this case, discovering that the hosting company of the scammers domain accepts payment in crypto and discovering the payment addresses via OSINT, provided a new channel to trace via WEB3 (blockchain) (Berkman, 2026).

Names and Contact Information

Based on the findings from the domain investigation, it was evident that the perpetrators of the scam took deliberate steps to evade detection by using false information to conceal their identities. This conclusion was reinforced by the OSINT industry (OSINT Industries, 2026) reports, which showed multiple names associated with the same phone number, as well as the generic names given to the victims. As a result, attempting to investigate the names and contact details through traditional means would likely generate numerous false positives and consume valuable investigative time. The priority, therefore, shifted to identifying links between the contact information and other websites and/or members of the victims' families.

Using Maltego transforms, the transforms for Cyber Threat Intelligence (CTI), Corporate Intelligence, WhoisXML and Social Links were run on all the provided phone numbers and email addresses. Maltego is a cyber investigation and link analysis tool (Maltego, 2026). Additional searches were made on several of the phone numbers and email addresses using IntelTechniques (IntelTechniques, 2026), Breach Directory (Breach Directory, 2026), Non-Nonsense (NO-NONSENSE, 2026), FreeCarrierLookup (FreeCarrierLookup.com, 2026) with no results.

XDS (XDS, 2026) was used to conduct searches on telephone and/or mobile numbers. These searches returned the names, surnames and identity (ID) numbers linked to each queried number. Numbers identified as South African were subsequently verified against the CRDB Porting database (Porting, 2026) to establish the network provider for identification purposes and potential further investigation via a subpoena process. The numbers were confirmed as ported and still active on the networks of Vodacom, Telkom Mobile and SVSGNP (Saicom Voice Services).

Google searches were carried out on the names associated with the RSI platform that were supplied by the victim, and each of these names appeared in connection with negative reviews on hellopeter.com and Trustpilot. One positive review was identified on HelloPeter (hellopeter.com, 2025), but it is most likely a self-authored post made during the early phase of the scam. In the absence of a precise chronology of events, it cannot be conclusively established that this review is a self-review. Additional potentially relevant information might be available and could be obtained from HelloPeter through a subpoena. Should the review ultimately be classified as a self-review intended to bolster the scam's legitimacy, this would align with a common syndicated pattern. Although the names provided are not genuine names but rather aliases used to interact with victims, their full forms will not be disclosed in this paper. It can be noted, however, that the names are characteristic of white, English-speaking South African men and could just as plausibly be typical UK names.

WhatsApp chat logs between the victim and the suspects were recovered and imported into Maltego. However, these conversations did not reveal any additional information about the scammers' real identities beyond the aliases they used.

The provided email address, s######s@cryptodotcom.info, was subjected to various verification tools, revealing that the email account does not exist.

Mr-X

In addition, searches were made for the SM accounts of Mr-X. The searches focused on the subject's personal gmail address, the subsequent username and variations of the subject's name. A use of the service 'WhatsMyName' (WhatsMyName, 2026) revealed a Pinterest account, Roblox account and Facebook account using the target username. The Pinterest account contained a profile picture common amongst military men, this being consistent with the known military background of the subject. A reverse image search of the subject's Pinterest profile image revealed a YouTube account using the username and containing the exact same profile

image of the Pinterest account. A Google Dorks search, using the query 'person:(('name') 'surname') AND site:linkedin' while using a VPN set to SA (the home country of the target) revealed the target LinkedIn in profile.

3.3 Theory Development and Validation

Over the span of this investigation, three distinct theories were formulated and subsequently tested and validated.

3.3.1 Theory 1 – Mr-X is a victim

SA law enforcement reported that they suspect a group from the country of Georgia of being responsible for the scam that targeted the victims. It was initially believed that Mr-X had first fallen prey to the scam and, before realising it was fraudulent, had encouraged his wife and mother-in-law to use the platform, resulting in them being scammed as well. In this scenario, Mr-X would be considered a victim, along with the complainant.

By comparing the timeline of the WhatsApp conversations between the ex-husband and the RSI brokers with the victim's testimony, it was observed that a coherent pattern of interaction between Mr-X and RSI leading up to his recommendation that the victim invest in the platform. However, because the WhatsApp record is so extensive, the precise nature of these interactions remains unclear, making it difficult to draw firm conclusions.

3.3.2 Theory 2 – Mr-X worked with RSI-platform

Since it was Mr-X who introduced the victim to the platform and urged her to invest funds in it, the question arises as to what Mr-X knew about the platform's legitimacy at the time he involved his family. Moreover, the fact that Mr-X did not file a police report after it became clear that they had been defrauded supports the suspicion that Mr-X may have been part of the group operating the scam.

According to the victim's testimony, it was reported that Mr-X encouraged the victim to invest in the platform. After the scam was uncovered, Mr-X and his wife divorced, and Mr-X chose not to file a complaint with the Police. Furthermore, it was reported that efforts to obtain further information and evidence from Mr-X about the scam were met with reluctance. These circumstances led to the theory that Mr-X may have been complicit in the scam.

Because it was suspected that the target domain had been registered using cryptocurrency to pay the hosting provider, investigators initially attempted to identify links between the hosting provider's cryptocurrency payment addresses and the one used by Mr-X on VALR (ref to the initial study in (Botha, Singh, & Leenen, 2026)). This line of inquiry proved unproductive, however, as a closer review of the victim's testimony and the WhatsApp conversations strongly indicated that the RSI brokers themselves had access to their victims' VALR accounts. The victim repeatedly stated that she had deposited funds into her VALR account and then observed those funds reflected in her RSI account, despite not having initiated the transfer herself. She further testified that she had shared her VALR password with both the RSI brokers and her family. In addition, Mr-X stated in his chats with the RSI brokers that he had deposited money into his VALR account and was waiting for confirmation from them that the funds had appeared in his RSI account. This indicates that it was the brokers who transferred the funds from the VALR account to the RSI account. Given the brokers' level of access to Mr-X's VALR account, it is not possible to determine whether any outgoing funds were moved at Mr-X's instruction or even with his knowledge.

Mr-X's social media profiles were examined to identify any indications of communication or links between the Mr-X and the suspects, or with the domain hosting provider. This review covered Mr-X's YouTube content as well as his LinkedIn and Pinterest accounts. No clear associations were identified. Additional searches for any other online activity by Mr-X did not yield further information.

Refutation of the theory: A detailed review of the WhatsApp conversations between Mr-X and the RSI brokers revealed that Mr-X registered on and began investing through the platform in May 2022, and did not recommend it to the victim until August 2022.

3.3.3 Theory 3 – Mr-X hid money from his ex-wife

Evidence uncovered during the investigation indicates that Mr-X incurred debts to finance his investments in the suspect platform. One theory that emerged is that Mr-X was genuinely misled by the suspects.

Although it seems improbable that Mr-X was directly collaborating with the suspects, the fact that he failed to file a report with law enforcement remains suspicious. WhatsApp chat records indicate that Mr-X took out loans with high interest rates in order to finance his investment activities. Furthermore, when Mr-X started to incur

losses on the platform, he was instructed to deposit additional funds to keep his account balance up and avoid closing losing positions. It is very likely that Mr-X had built up a substantial level of debt before it became apparent that his money had been stolen. Since Mr-X and his wife divorced soon after the scam was uncovered, it is plausible that both the debt he accumulated and the naivety with which he lost his own and his family's money contributed to their decision to divorce.

There is also indication that a degree of financial mistrust existed between Mr-X and his wife. This inference is drawn from Mr-X's statements in the WhatsApp messages, where he expresses an intention to set up a separate trading account for his wife. This implies that, at that time, both he and his wife preserved a certain level of financial independence from one another.

Given the presumed extent of his financial autonomy and the monetary issues thought to be central to the couple's divorce, it is hypothesised that Mr-X had an incentive to conceal assets or liabilities from his wife in order to avoid weakening his position in the divorce settlement. Lodging a complaint with law enforcement would have opened his financial records to scrutiny, records that may otherwise have remained inaccessible to his ex-wife. This provides a plausible explanation for the target's refusal to cooperate with both law enforcement and private investigators, and it aligns with the available evidence in the case. As of the time of this revision, this remains the predominant working theory. Substantiating this theory would require a focused inquiry into Mr-X and his financial documentation. Such steps fell outside the remit of this investigation.

3.4 Suspect Identification and Reasonable Grounds

The first step in attempting to identify the suspects behind the scam was to analyse the names and phone numbers provided by the client. An examination of the evidence revealed multiple names connected to phone numbers. The phone number, +27-8##-6#6-### was shown as being connected to three names by an export file from OSINT Industries. This suggests that the suspects were using a text message one time code receiving service to open WhatsApp accounts and other necessary online presents. Any information found relating to this provided data would likely be fabricated and not lead to the guilty suspects.

The second attempt to identify the suspect was through the domain registration of the target domain, 'https://rsi-platform.io'. The discovered evidence showed that this too contained fabricated registration data. It was found, however, that the suspects likely paid for the domain registration with cryptocurrency This discovery led to a third strategy in identifying the suspects. By tracing the transactions from the suspects cryptocurrency addresses provided by the victim to a KYC compliant cryptocurrency exchange would allow law-enforcement to subpoena the exchange for the profile details behind the account. This strategy had already been carried out by law enforcement and they had successfully traced the transactions to the cryptocurrency exchange, Kyrrex, and sent a request for information. At the time of writing this paper, law enforcement had not received a response from Kyrrex. This remains the most likely route of gaining actionable information that could lead to the identity of the suspects.

3.5 Law Enforcement Function

This segment of the investigation is part of the legal action phase and is conducted by legal authorities to locate and prosecute the suspect, initiating the process of charging, arresting, imposing sanctions, recovering assets, and seizing funds. Refer to (Botha, Singh, & Leenen, 2025) for the detailed description of the entire process.

In this study, no legal measures were taken. It is advised that subpoenas be served on multiple mobile network operators, including Vodacom, MTN, and Telkom Mobile, to obtain IMEI information as well as any associated call and location records for the identified numbers. The subpoena should also reference any other SIM cards used in the same device(s) in order to build a complete picture of the activities. It is further recommended to subpoena the websites HelloPeter.com and Trustpilot in order to obtain the contact details of additional victims who filed complaints against the website rsi-platform.io and indicated that they were also defrauded by this scheme. Moreover, the contact information associated with the positive review, which appears to be a self-authored review by the perpetrators, may provide further data connected to the suspect.

Unfortunately, the scammers' identities are still unknown, and this stage cannot be fully carried out without adequate intelligence and supporting evidence. The perpetrators are highly skilled at concealing their tracks. The most viable approach is to trace the flow of funds on the blockchain and perform further on-chain analysis, in the hope that the scammers slip up and reveal information that can later be used in off-chain investigations. Every new detail uncovered and added to the link analysis brings us one step closer to identifying the scammers. The ultimate objective is to determine who they are and ensure they are brought to justice.

4. Link Analysis

Link analysis is the identification of relationships and connections between two entities such as individuals, organisations, etc. (Holzer, Dietz, & Yang, 2016). This technique visually represents interconnected entities as nodes and links, facilitating a clearer understanding of the data and its underlying structure (Cambridge Intelligence, 2025). The link analysis allowed for a visual representation of the relationships between the suspect and all other entities identified as being connected to them. These entities encompass all information provided by the victim, as well as any further links uncovered through the use of OSINT tools. The identified entities include mobile phone numbers, email addresses, physical addresses, names provided by the victim, names associated with mobile numbers as revealed by specific OSINT tools, mobile service providers, domain details, registrar information, and similar data points (refer to Figure 4). Although multiple linked entities could be discovered, the data is not enough to successfully identify a target suspect. When collecting information on a target, a case management strategy is needed to keep track and make sense of the findings. For this case, the link analysis and case management tool used was Maltego.

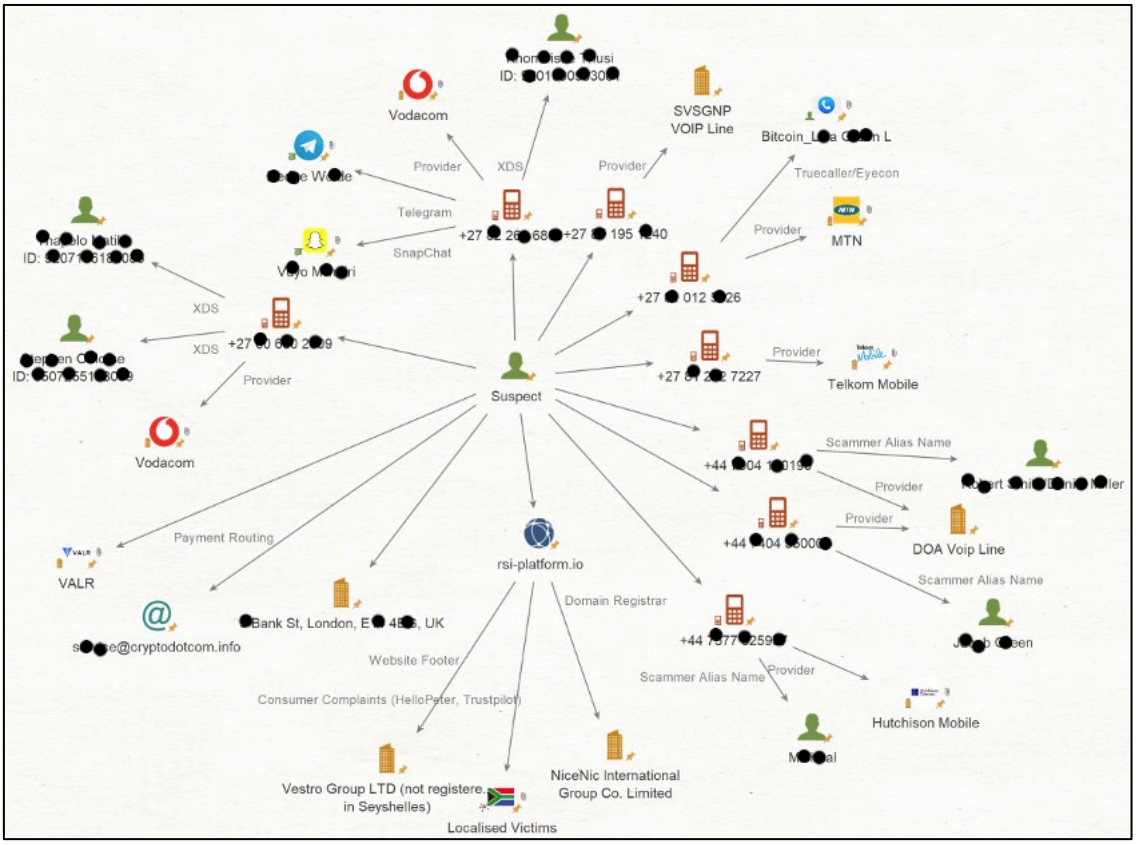

Figure 4: Link Analysis

5. Conclusion

This paper extends an earlier study that examined a particular instance of a fraudulent cryptocurrency investment scheme. While the previous work focused on on-chain (blockchain-based) analysis, the present study concentrates on off-chain investigation. It provides practical guidance by implementing a structured investigative framework previously proposed by the authors, aimed at law enforcement, regulators, investigators, analysts, and researchers. In this study, that framework is modestly refined by adding additional steps to the OSINT analytical phase and it illustrates the practical implementation steps. The author engaged two OSINT specialists to support the case analysis.

The first objective of the investigation was to identify the individuals behind the scam operated via the domain 'rsi-platform.io'. Both law enforcement and the client had already identified a promising route to uncovering the suspects—namely, the accounts they had opened on the Kyrrex cryptocurrency exchange. However, Kyrrex's lack of cooperation, combined with law enforcement's view that the offenders are likely outside SA's jurisdiction, underscores the challenges of maintaining law and order in a digital, transnational crime environment. When

victim and offender reside in different jurisdictions, and the amount stolen is too small to prompt action from international bodies yet large enough to financially devastate a household, victims are frequently left without any effective recourse.

The second objective was to validate the prevailing theory that the ex-son-in-law had been intentionally induced to incur an excessively large debt in order to trade on the RSI platform. Believing he was successful and hoping to increase overall profits, he then persuaded his wife and her family to invest as well. Once it became clear that the operators of the RSI platform were in fact criminals who had misappropriated their funds, serious domestic conflict arose, ultimately resulting in divorce. Seeking to conceal the magnitude of his debt and to improve his position in the divorce proceedings, the ex-son-in-law chose not to file a report with law enforcement in order to avoid disclosing his financial records.

As blockchain technology becomes more widely used, crimes and scams involving cryptocurrencies are also on the rise. Online fraud remains a serious global issue, largely because there is a lack of uniform, official regulation. Moreover, the borderless nature of cryptocurrency transactions has contributed to an increase in such scams within both financial and cybercrime domains. This paper also seeks to raise awareness of fake investment schemes and fraudulent cryptocurrency investment platforms.

Ethics declaration: Ethical clearance was not needed for this research.

AI declaration: The academic AI tool Writefull was used to improve language usage and grammar .

References

55BROKERS. (2025, Oct 20). *Is RSI-FX a scam or legit?* Retrieved from www.55brokers.com: https://55brokers.com/trader-inquiry/mr-51

Berkman, A. (2026, Feb 14). *OSINT Consultant & Tool Developer*. Retrieved from LinkedIn Profile: https://www.linkedin.com/in/abhawk

BigDomainData. (2026, Feb 13). *The Largest WHOIS Database in the World*. Retrieved from BigDomainData: https://www.bigdomaindata.com

Botha, J., Singh, K., & Leenen, L. (2025, Feb 3). A Proposed Bitcoin Blockchain Investigation Methodology: Based on a Case Study Approach. *Journal of Information Warfare, 24*(1), 1-18. Retrieved Feb 10, 2025, from https://www.jinfowar.com/journal/volume-24-issue-1/proposed-bitcoin-blockchain-investigation-methodology-based-case-study-approach

Botha, J., Singh, K., & Leenen, L. (2026). Evaluating an Investigative Process for Cryptocurrency-Related Crimes. *nternational Conference on Cyber Warfare and Security.* Wilmington, North Carolina, USA.

Breach Directory. (2026, Feb 16). *Breach Directory Home Page*. Retrieved from https://breachdirectory.org

Breadcrumbs. (2023, Oct 11). *Breadcrumbs Investigation*. Retrieved from https://www.breadcrumbs.app/: https://www.breadcrumbs.app/home

Cambridge Intelligence. (2025, Feb 10). *Link analysis*. Retrieved from www.cambridge-intelligence.com: https://cambridge-intelligence.com/why-link-analysis

DFPI. (2025, Oct 31). *Pig butchering – how to spot and report the scam*. Retrieved from Department of Financial Protection & Innovation (DFPI): https://dfpi.ca.gov/news/insights/pig-butchering-how-to-spot-and-report-the-scam

FreeCarrierLookup.com. (2026, Feb 16). *Home Page*. Retrieved from https://www.freecarrierlookup.com

hellopeter.com. (2025, Oct 12). Retrieved from hellopeter.com: https://www.hellopeter.com/rsi-platform-daniel-miller

Hawk Eyes. (2026, Feb 14). *Advanced Cyber Intelligence*. Retrieved from Hawk Eyes - OSINT Tools and Services: https://www.hawk-eyes.io

Holzer, C., Dietz, J., & Yang, B. (2016). Employing Link Analysis for the Improvement of Threat Intelligence Regarding Advanced Persistent Threats. *5th IAJC/ISAM International Conference* (p. 11). Orlando, Florida: International Association of Journals & Conferences (IAJC).

HTX. (2025, Oct 23). *Home Page*. Retrieved from HTX: https://www.htx.com

Hwang, Y., Lee, I., Kim, H., Lee, H., & Kim, D. (2022). Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing* (p. 1290129). Yan Huo.

IntelTechniques. (2026, Feb 16). *Tools*. Retrieved from IntelTechniques: https://inteltechniques.com/tools/index.html

Kolenbrander, J. (2025). Privacy Research using Active OSINT Techniques. 32. Virgina: Ph.D. thesis, Virgina Tech.

Lacity, M., & Carmel, E. (2024). Web2 Versus Web3 Information Privacy: An Information Systems Discipline Perspective. In M. Lacity, & L. Coon, *Human Privacy in Virtual and Physical Worlds* (pp. 111-140). Technology, Work and Globalization. Palgrave Macmillan, Cham.

Maltego. (2026, Feb 10). *Maltego*. Retrieved from www.maltego.com: www.maltego.com

MXToolbox. (2026, Jan 8). *Home Page*. Retrieved from MXToolbox: https://mxtoolbox.com

NerdyData. (2026, Feb 13). *Steal your competitor's customer list*. Retrieved from NerdyData: https://www.nerdydata.com

NO-NONSENSE. (2026, Feb 16). *Phone Variant Search*. Retrieved from https://www.no-nonsense-intel.com/phone-variant-search

opencorporates. (2026, Feb 13). *Home Page*. Retrieved from opencorporates: https://opencorporates.com

OSINT Industries. (2026, Feb 10). *app.osint.industries*. Retrieved from www.osint.industries: https://app.osint.industries
Porting. (2026, Feb 10). *Public Number Query*. Retrieved from CRDB Centralised Reference Database: https://www.porting.co.za/PublicWebsiteApp/#/number-inquiry
Pastor-Galindo, J., Nespoli, P., Gómez Mármol, F., & Martínez Pérez, G. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access, 8*, 10282-10304.
SCAMADVISER. (2025, Oct 26). *SCAMADVISER*. Retrieved from https://www.scamadviser.com/check-website/rsi-platform.io
scam-detector.com. (2025, Oct 10). *Scam Detector Validator*. Retrieved from scam-detector.com: https://www.scam-detector.com/validator/rsi-platform-io-review
TCG Forensics. (2026, Feb 10). *Home Page*. Retrieved from TCG Forensics: https://tcgforensics.co.za
TransFi. (2025, Feb 13). *What is On-Chain Analysis in Blockchain and How Do You Use It?* Retrieved from www.transfi.com: https://www.transfi.com/blog/on-chain-analysis-in-blockchain
Truecaller. (2025, Feb 10). *Number Search Results Page*. Retrieved from www.truecaller.com: https://www.truecaller.com/
Trustpilot. (2023, Oct 18). *RSI-Platform.io Review*. Retrieved from Trustpilot: https://www.trustpilot.com/review/rsi-platform.io
WaybackMachine. (2026, Feb 10). *Home Page*. Retrieved from WaybackMachine: https://web.archive.org
WhatsMyName. (2026, Feb 16). *Home Page*. Retrieved from https://whatsmyname.me
WHOXY. (2026, Jan 8). *WHOIS Domain Search*. Retrieved from WHOXY Domain Search Engine: https://www.whoxy.com/rsi-platform.io
XDS. (2026, Feb 10). *XDS Home Page*. Retrieved from XDS: https://www.xds.co.za