

Forensic Analysis of Scam Activity on Telegram Using Open-Source Tools

A dissertation thesis submitted to

National Forensic Sciences University

For the award of the Master's degree

In

Forensic Science

By

Sonia Jose Cherian

(022300100001055)

Under the Supervision of

Dr. Deepak Raj Rao

Department of Cyber Security and Digital Forensics

Professor of Practice



**SCHOOL OF FORENSIC SCIENCES
NATIONAL FORENSIC SCIENCES UNIVERSITY
DELHI, INDIA**

May, 2025



NFSU

DECLARATION

I hereby declare that the thesis entitled “Forensic Analysis Of Scam Activity On Telegram Using Open-Source Tools” is a research work done by me and no part of the thesis has been presented earlier and will be presented for any degree, diploma or similar title at any other institute/university.

Sonia Jose Cherian
022300100001055
M.Sc. Forensic Science
2023-2025

Date:

Place: Rohini, Delhi

विद्यया अमृतं अश्नुते



ORIGINALITY REPORT CERTIFICATE

I certify that

- The work in the dissertation is original and was done by me under the supervision of my supervisor.
- The work has not been submitted to any other Institute for any degree or diploma.
- I have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute.
- Whenever I have used materials (data, theoretical analysis, and text) from other sources, I have given due credit to them by citing them in the text of the dissertation and giving their details in the references.
- Whenever I have quoted written materials from other sources and due credit is given to the sources by citing them.
- From the plagiarism test, it is found that the similarity index of whole dissertation within 10% and single paper is less than 10 % as per the university guidelines.

Name and Signature of the Student
Enroll. No.: 022300100001055

Date:

Place: Rohini, Dehli

Forwarded by

(Dissertation Supervisor)

Date: _____



CERTIFICATE

This is to certify that the work contained in the dissertation entitled **“Forensic Analysis Of Scam Activity On Telegram Using Open-Source Tools”**, submitted by **Sonia Jose Cherian (022300100001055)** for the award of the degree of **Master of Science in Forensic Science** to the **National Forensic Sciences University, Delhi Campus**, is a record of bonafide research works carried out by him/her under my supervision and guidance.

Dr. Deepak Raj Rao
Professor

Department of Cyber Security and Digital Forensics
National Forensic Sciences University
Delhi Campus, Delhi, India

Date:

Place: Rohini, Delhi

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to National Forensic Sciences University, Delhi Campus, for providing me with the opportunity and resources to undertake this research. I am especially thankful to the Department of Forensic Science and my class, M.Sc. Forensic Science, for their continuous academic and moral support throughout this journey.

I extend my heartfelt thanks to my supervisor, Dr. Deepak Raj Rao, for his guidance and insightful feedback, which were instrumental in shaping the direction and quality of my work.

I am also deeply grateful to the Indian Council for Cultural Relations (ICCR) for awarding me the scholarship that made my academic pursuit in India possible.

I am also deeply grateful to my family for their unwavering support, understanding, and motivation during the entire course of this research.

Lastly, I would like to acknowledge my own efforts, dedication, and perseverance in completing this research successfully.

With Sincere Regards,

Sonia Jose Cherian

022300100001055

M.Sc. Forensic Science

2025

ABSTRACT

Popular encrypted messaging app Telegram has become a hub for cybercrime operations because it accommodates anonymity, automation through bots, and minimal content moderation. This study performs a forensic examination of scam operations on Telegram using open-source software tools to present an accessible and reproducible investigative process. A controlled virtual environment was set up with Ubuntu, to which Telegram Desktop was installed for mimicking contact with public channels related to scams. The public channels were passively monitored to gather information on the most common scams like cryptocurrency fraud, pirated media distribution, gambling schemes, and phishing attacks.

Network traffic during Telegram sessions was captured and analyzed with Wireshark for detecting suspicious domains, IP addresses, and probable command-and-control communication. SpiderFoot was used to perform OSINT-driven reconnaissance of these domains, and Telegram's native export functionality was used to export messages, media, and metadata for analysis. Extracted artifacts were analyzed on a secure Windows host using other forensic tools. Maltego CE was used to visualize the relationships between Telegram entities and their associated infrastructure, with visualization showing clusters of coordinated scam and reused infrastructure.

The results show that scammers prefer to use Telegram bots and short URLs to lead victims to phishing sites or scam services, usually on less-than-common domain extensions. This research validates that Open-source software tools are useful in finding, mapping, and analyzing Telegram-based scam networks. It provides an affordable forensic pipeline that can support academic, law enforcement, and cybersecurity experts in combating cybercrime in end-to-end encrypted communication platforms.

Keywords: Telegram, Open-source, Scam activity, Spiderfoot, Wireshark, Maltego.

TABLE OF CONTENTS

Abbreviations			VIII
List of Tables			IX
List of Figures			X
Chapter 1.	Introduction		1-5
	1.1	Background	1
	1.2	Research Focus	2
	1.2.1	Research Questions	2
	1.2.2	Research Objectives	2
	1.2.3	Need for the Study	2
	1.3	Telegram's Architecture and Risk Factors	3
	1.4	Telegram Bots and Automation in Scams	3
	1.5	Historical Precedents	4
	1.6	Significance and Scope	5
Chapter 2.	Review of literature		6-8
Chapter 3.	Experimental Design		9-14
	3.1	Methodology Process	9
	3.2	Configuring the Environment	10
	3.3	Channel Monitoring and Classification	10
	3.3.1	Classification of Content	11
	3.4	Capturing Network Traffic	11
	3.5	Domain Analysis	11
	3.6	Telegram Data Export	11
	3.7	Data Analysis	12
	3.7.1	Visualization	12
	3.8	Methodology Summary Table	12
	3.9	Research ethical guidelines	13
Chapter 4.	Results and Discussion		15-24
	4.1	Environment Setup	15
	4.2	Captured network traffic	16
	4.3	Domain Extraction	16
	4.4	OSINT and Threat Analysis	17
	4.4.1	SpiderFoot Scan:	17
	4.5	Exporting and Analyzing Telegram Data	17
	4.6	Findings from Wireshark	17
	4.7	SpiderFoot Scan Results	18
	4.8	Findings from Maltego	19
	4.9	Findings	23

Chapter 5.	Conclusion	25-28
5.1.	Limitations of the Study	26
5.2	Recommendations and Future Scope of Work	28
Bibliography- List of references		29-31



LIST OF ABBREVIATIONS

Abbreviation	Description
CACs	Cybercriminal Activity Channels
CE	Community Edition
CDNs	Content Delivery Networks
IP	Internet Protocol
MTPProto	Mobile Transport Protocol
NIST	National Institute of Standards and Technology
OSINT	Open-Source Intelligence
PKI	Public Key Infrastructure
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
VM	Virtual Machine

LIST OF TABLES

Table No	Table Description	Page No
Table 3.1	Classification of channel content	11
Table 3.2	Methodology summary table	13
Table 4.1	Extracted scam-related entities from Telegram and external infrastructure.	22

विद्यया अमृतं अश्नुते

LIST OF FIGURES

Fig No	Figure Description	Page No
Figure 1.1	Different features of Telegram that criminals commonly exploit	5
Figure 3.1	Methodology flowchart diagram	9
Figure 3.2	Shows the screen capture of the Telegram-interaction VM created.	10
Figure 4.1	Shows the screen capture of the telegram bot and channel interaction	15
Figure 4.2	Shows the screen capture Telegram network traffic captured using Wireshark	16
Figure 4.3	Contains the list of extracted domain names from Wireshark	16
Figure 4.4	Shows the screen capture of Spiderfoot scans	17
Figure 4.5	Domain infrastructure linked to Telegram interactions	19
Figure 4.6	Contains the Maltego Visualization of Telegram Bots and their Immediate connections	20
Figure 4.7	Network visualization of entities extracted from Telegram-based scam activity, generated using Maltego	21

1. Introduction

1.1. Background

Telegram Messenger, launched in 2013 by brothers Pavel and Nikolai Durov, is a widely used cloud-based messaging application that has rapidly gained global traction. Today, it is estimated to have around 950 million active monthly users. Its popularity is particularly evident in regions such as India, where almost 45% of the population uses this application, and in Russia, where it has replaced WhatsApp as the most-used messaging platform (Singh, 2025). Telegram has attracted many users for many reasons: it is flexible, provides privacy features, and is cross-platform accessible.

Telegram represents a more significant trend, whereby cybercriminals move away from composite and closed darknet forums to accessible and encrypted messaging platforms. This shift is mainly supported by Telegram's low entry barrier, mobility, and global reach, providing ground for massive scams operating at scale. As law enforcement attempts to strike a balance between user privacy and surveillance, Telegram opens an entirely new front for digital forensics, wherein traditional means play a small role in comparison to the necessity of open-source investigative methods.

However, the very features that make Telegram popular also make it a favorite platform for criminal exploitation, for its encryption capabilities, minimal content moderation, and support for anonymous usage make it very suitable for illegal activities. Investigations and journalistic reports have made connections between Telegram and various forms of cybercrime such as fraud, piracy, terrorism, illicit drug trade, and distribution of child sexual abuse materials.

Telegram's architecture and design provide privacy via end-to-end encrypted Secret Chats, ephemeral messaging, and proprietary MTProto protocol, which encrypts messages through both symmetric and asymmetric methods and uses a session-based encryption for added security (Rutayisire, 2024). Moreover, Telegram allows sending files of up to 2 GB, provides the use of bots for automation, and allows access to shared media using cloud storage of which can be illegally misused by an end user.

1.2. Research Focus

1.2.2 Research Objectives

This study seeks to examine Telegram's use in cybercrime, specifically scams, and assess how open-source digital forensic tools can be utilized to detect, extract, and interpret forensic artifacts related to such activity.

- To conduct a forensic investigation of Telegram artifacts using open-source tools.
- To evaluate the effectiveness of open-source tools in detecting and analyzing Telegram-based scams.
- To recover and interpret forensic evidence such as messages, media files, and metadata from Telegram Desktop environments.

1.2.1. Research Questions

This study is guided by the following questions:

- RQ1: What Telegram data (logs, media, metadata) can be recovered using open-source tools?
- RQ2: Are there identifiable traces of scammer activity in network packets or metadata?
- RQ3: What types of scams are commonly propagated through Telegram?
- RQ4: Are there recurring IP addresses, domains, or patterns linked to scam operations?

1.2.3. Need for the Study

Telegram presents a unique forensic challenge due to its emphasis on user privacy, minimal moderation, and increasing use among cybercriminals. Despite some commercial tools offering limited investigative support, a notable gap exists in accessible and replicable forensic methodologies using open-source software. This study aims to bridge that gap by:

- Demonstrating the practical application of open-source tools (such as Wireshark, SpiderFoot, and Maltego) in examining Telegram-related scams.
- Proposing a cost-effective and reproducible forensic workflow suitable for academic and professional settings.
- By analyzing the digital traces left by such scammers, metaphors, network logs, and DNS activities, the understanding of their behavior on encrypted platforms is enhanced.

These research works will help promote transparency, enrich education, and provide tools for the legitimate countermeasure of cybercrime on encrypted platforms in the wider domain of digital forensics.

1.3. Telegram's Architecture and Risk Factors

Telegram's design incorporates several features that, while intended to improve usability and privacy, inadvertently facilitate criminal activity:

- End-to-end encryption and self-destruct timers are features of secret chats that enable communications to vanish without leaving any trace.(Cranford, 2024).
- Channels and Supergroups: These allow for one-to-many broadcast capabilities, which makes them ideal for mass scamming or propaganda distribution.
- Cloud-based File Sharing: Users can upload huge files up to 2 GB, which can then be converted into pirated products, malware, and stolen data.
- Cross-Device Synchronization: Any device can access illicit data, complicating its preservation and chain-of-custody during investigations.

Investigations prove that little content moderation on the part of Telegram and non-involvement in such matters by authorities provide an impunity ground for cybercriminals. According to The New York Times, Telegram is a type of "the anonymity of the dark web with the ease of use of an online marketplace."

1.4. Telegram Bots and Automation in Scams

Cyberspace is mostly operated by using Telegram bots for automated accounts constructed with Telegram's Bot API. These bots can send messages and multimedia files, carry out action commands given by input, or trigger a certain set of rules with input provided by the user, making them weapons for many evildoers.

Scammers leverage bots to:

- Set up black-market stores and scam shops.
- Execute automated phishing campaigns.
- Disseminate malware and fake investment links.

- Coordinate command-and-control (C2) functions in malware operations.

Bots reduce the barrier to entry for cybercrime, allowing even low-skill attackers to manage sophisticated campaigns with minimal effort (Rutayisire, 2024).

1.5. Historical Precedents

Telegram's dual role as a secure communication tool and a vehicle for illicit activity has been well documented in recent years. Its growing popularity has not only attracted ordinary users but has also drawn the attention of cybercriminals, extremist groups, and fraud networks globally. Several high-profile cases highlight Telegram's centrality in cybercrime operations and the difficulties that law enforcement face when investigating crimes on encrypted platforms.

In India, where almost half the population uses Telegram, multiple media and cybersecurity researchers have termed it a 'digital dark market.' Telegram was discovered to have been widely used for:

- Phishing activities against banking applications.
- Sale of pirated OTT subscriptions.
- Distributing illegal betting platforms during IPL matches.
- Investment scams preying on fake cryptocurrency airdrops and "premium" Telegram bots.

In 2024, The Economic Times reported that most of these operations were run via Telegram bots with payment integration through both UPI and crypto wallets, making tracing and taking them down almost impossible. So, the Indian government had to issue several advisories warning citizens concerning such scam activities on Telegram and started working with ISPs to track abnormal traffic patterns associated with scams using Telegram channels for interception.

According to a study conducted in 2023 by the cybersecurity firm Group-IB, Telegram has been established as the number one platform for trading compromised data, phishing kits, and hacking tutorials, far ahead of the dark web forums. The study found increasing use of public and private Telegram groups as command centers where criminals would discuss monetization strategies, share scripts for automated fraud, and distribute malware payloads.

These findings corroborate the present study's claim that Telegram is more than a venue for communication; it is a decentralized market for cybercrime, facilitated by bots, channels, and

cross-device synchronization.

The above important precedent has established the recurring role of Telegram in both localized cybercrime and transnational cyberspace. These findings provide a broader understanding of how this research can be envisaged, not only as a technical field of forensic investigation tool developments, but also as part of the world's developing response to the encrypted digital threat environment.

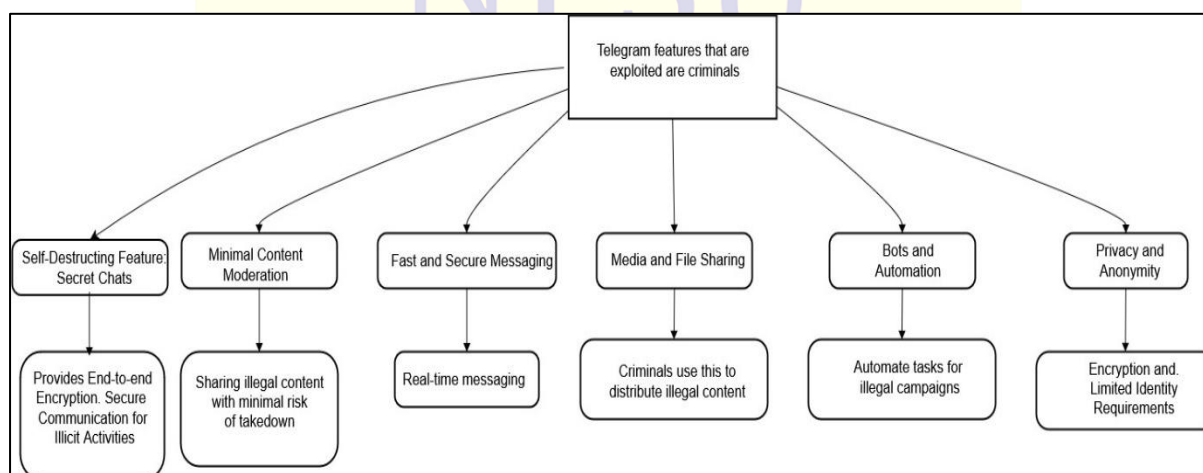


Figure 1.1: Different features of Telegram that criminals commonly exploit

1.6. Significance and Scope

This study emphasizes the urgent need to develop open-source-based forensic approaches that enable investigators, students, and independent researchers to analyze Telegram data effectively. By recovering Telegram artifacts, identifying scam indicators, and documenting patterns, the research aims to:

- Inform future forensic workflows for encrypted messaging platforms.
- Assist digital crime units in resource-constrained environments.
- Contribute to public awareness of Telegram's role in digital scams.

2. Review of literature

Several studies in recent literature have focused on Telegram's content analysis and the workings of the application. As a result, accepted methodologies and technologies have been adopted in extracting and analyzing information from Telegram.

This research seeks to explore the various tools and mechanisms that scammers use to exploit the features of Telegram.

According to the research (Guo et al., 2024), Telegram's efforts to alert users by identifying scams have not been successful in controlling the existence of potentially dangerous content on the platform. Despite being useful characteristics, Telegram's encrypted communication and anonymity unintentionally serve as a sanctuary for illegal activity.

Another study examined posts from 339 Cybercriminal Activity Channels (CACs) across five key categories, showcasing the spread of malicious content, from stolen credentials to hacking tools, with significant risks to subscribers. (Roy et al., 2024)

(A K & Banerjee, 2025) explains how the platform's advanced encryption, anonymous user features, and self-destructing messages—which were initially designed to protect authorized users—have been exploited by hackers to conduct illegal activities more covertly. The incongruous nature of Telegram's privacy features draws attention to the growing tension in the digital age between people's right to privacy and the need for effective law enforcement.

According to an investigation (Shehabat et al., 2017), ISIS has used Telegram's features to sustain its global network of terrorist information operations and to promote, plan, and disseminate lone wolf strikes against Western nations.

In the study that created a scraping tool to monitor and examine illegal activity on Telegram made it possible to carry out long-term research on cybercriminal communities, providing information about their interactions, evolution, and the kinds of content they exchange. (Doğaner et al., 2024).

By examining conversation history data from a specific sample of 300 groups and examining related websites, the researchers were able to uncover a concerning level of criminal behavior in these Telegram forums. (Sreeram & Bansal, 2024)

A study (Lummen, 2023) contrasted established and new internet criminal marketplaces. The survey showed that the initial usability of the ads in the Telegram marketplace itself is the

primary focus. Darknet marketplaces do not permit users to submit their ads more than once, whereas Telegram marketplaces do.

(Perlo et al., 2024) Telegram, as seen through the public groups' perspective, is taken from TGstat. It was found that communities use the platform's features in a wide variety of ways, which reflects the kinds of material and sharing objectives. For example, bots may have a significant impact, accounting for up to 80–90% of messages generated by the platform. The length of user communications varies greatly, with self-promoting content inflating message length; video sharing is frequent; in politics, these are brief, but in video and cinema, complete movies are uploaded; the highest quality content is erotic.

According to the study, Telegram channels make it easier for threat actors and individuals looking to commit cybercrimes to interact more conveniently and safely. The number of threat actors is increasing despite the minimal skill set needed, so it is not surprising that the number of cyberattacks on both persons and businesses is rising (Point, 2018).

The four (4) forensic steps of the National Institute of Standards and Technology (NIST) methodology—collection, examination, analysis, and reporting—were employed in this investigation. The findings of (Amusan et al., 2021) compare the evidence gathered from a chat database, direct and group messages, and sent and received documents and photographs between a rooted and a non-rooted smartphone. The results of this study will help researchers and forensic investigators find and retrieve digital evidence from Android smartphones' Telegram messengers, which may be used as a guide in legal procedures to fight cybercrime.

Gregorio et al. (2017) provide an overview of forensic analysis, paying particular emphasis to how the application organizes user, chat, and conversation data and how to structure the data to extract pertinent information. Apart from instant messaging services (messages, images, videos, and files), the application provides a number of additional features (games, stickers, and bots). It is crucial to decode and comprehend the data, which may be connected to criminal activities, in order to ascertain the relationship between different user types, chats, and talks.

Forensic analysis of the artifacts created on Android handsets by Telegram Messenger, the official client for the Telegram instant messaging app, which provides a number of safe ways to communicate both individually and with others, such as text and non-text messages and voice calls. For the findings to be replicated and verified by a third party, the methodology of Anglino et al. (2017) is predicated on the design of a series of experiments appropriate to elicit the generation of artifacts and their retention on the device storage, as well as on the use of

virtualized smartphones to ensure the generality of the results and the complete repeatability of the experiments.

Carding, exchange of unlawful pornographic content, and copyright-protected content are among the notorious behaviors on Telegram that are available on the Dark Web's privacy-preserving services. (Morgia et al., 2021) Has also identified and examined two additional channel types: fakes and clones. Channels that post the same content as another in an attempt to attract new members and advertise services are known as clones. Instead, fakes are channels that attempt to imitate well-known brands or people. Fakes are difficult to recognize, even for the most experienced users. They have put forth a machine learning algorithm that can automatically detect fraud channels with an 86% accuracy rate.

\These studies show that people with criminal intent may find Telegram to be a risky medium. In order to improve platform security and aid law enforcement efforts, this study aims to provide an overview of the possible illegal pathways and their procedures.



3. Experimental Design

3.1. Methodology Process

Using open-source and free tools, this study will employ a structured forensic methodology to examine Telegram scam activity. To guarantee the accuracy and repeatability of the results, the study will be carried out in a controlled setting. The following steps will make up the methodology:

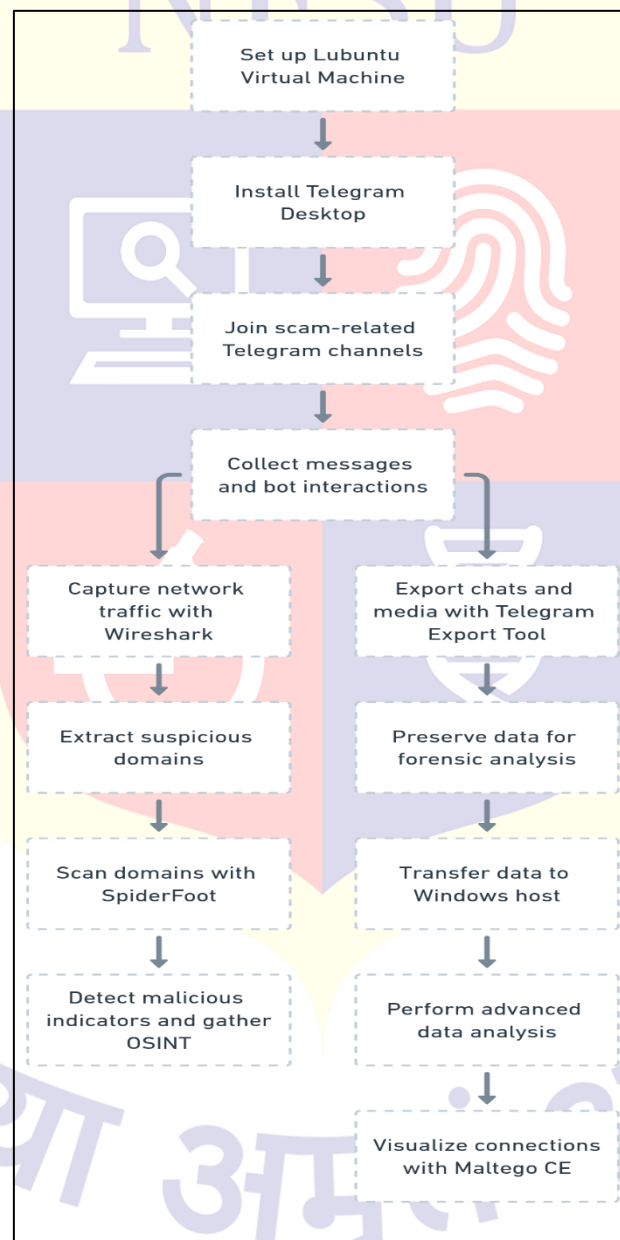


Figure 3.1: Shows the methodology flowchart diagram.

3.2. Configuring the Environment

The Lubuntu operating system will be used to create a specific virtual machine (VM) environment. To replicate actual user interactions with scam-related Telegram channels, Telegram Desktop will be installed on the virtual machine. This configuration will create a secure environment for data collection and forensic examination while separating Telegram activity from the host system.

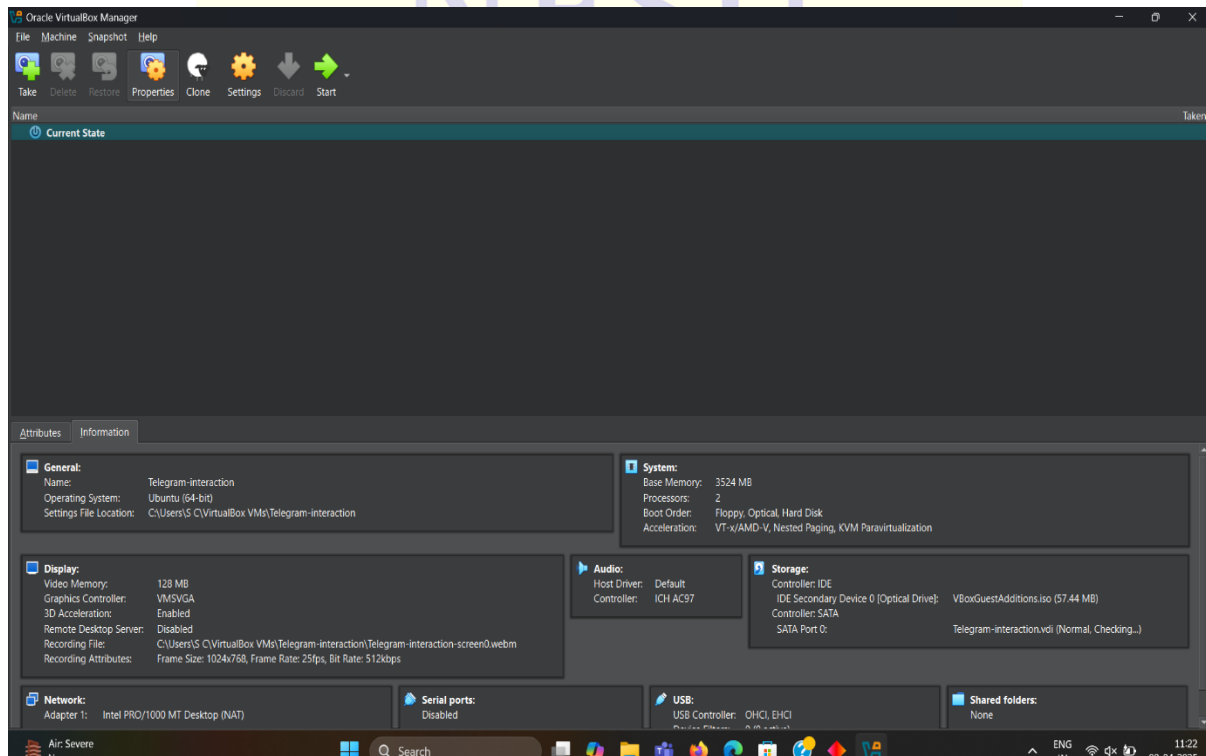


Figure 3.2: Shows the screen capture of the Telegram-interaction VM created.

3.3. Channel Monitoring and Classification

Joining public groups and channels that are known for scam activity, such as those that encourage cryptocurrency fraud, gambling, and pirated content, will be done through the Telegram Desktop client. There won't be any direct involvement with scam operations; interactions will be restricted to passive observation. This step will make it possible to gather real scam messages and bot activity.

Telemetr.io is used to collect data by compiling a list of public Telegram channels. Data about public Telegram channels is systematically gathered and categorized by Telemetr.io, which provides insightful information about subscriber growth, channel activity, and content trends.

3.3.1. Classification of Content

A manual classification is conducted to understand the types of content associated with this research.

Content Category	Number of channels/bots
Pirated Media	20
Gambling	20
Cryptocurrency	30
Scam Bots	10

Table 3.1: Classification of channel content.

3.4. Capturing Network Traffic

Wireshark will be used to record network traffic produced during Telegram sessions. To identify Telegram server communications, retrieve domain names, and spot questionable network activity, the collected data will be examined. Additionally, traffic analysis will look for links shared within channels or external connections created by scam-related bots.

3.5. Domain Analysis

SpiderFoot will be used to scan any domains or links gathered during Telegram monitoring. SpiderFoot will be used to evaluate the reputation of the domain, find signs of malicious activity, and collect more OSINT (Open-Source Intelligence) information about scam operations.

3.6. Telegram Data Export

The Telegram Export will be used to export media files and chat messages. Text messages, multimedia attachments, and metadata are all examples of exported data that will be saved for later forensic analysis and evidence correlation.

Telegram's native export feature can extract chat history, media files, and other metadata (in formats like chats.json, messages.html, and associated media folders).

The exported Telegram data will be securely transferred from the Lubuntu VM to the host machine (Windows) for further forensic analysis.

3.7. Data Analysis

The captured artifacts and exported Telegram data will be moved to a secure Windows host computer. The use of extra analysis tools and resources that might not be accessible or function as well in the Linux virtual machine will be made possible by this transfer. The media files, related metadata, and chat content will all be thoroughly examined.

3.7.1. Visualization

Maltego CE (Community Edition, Free Version) will be used to visualize the connections between users, bots, domains, and scam operations. Maltego will make network mapping easier by assisting in the identification of important participants, shared infrastructures, and communication trends within the scam ecosystem.

On the host system, **Maltego CE** will be used to visualize and correlate data points such as:

- Telegram usernames and group names
- Behavioral patterns and bot activities within the groups

3.8. Methodology Summary Table

The methodology steps are summarized in the table below:

Action	Tool(s) Used	Purpose
Set up VM environment with Telegram	Lubuntu VM	To isolate and simulate Telegram scam activity safely
Join scam-related channels	Telegram Desktop	To collect real-world scam messages and bot interactions
Capture network traffic	Wireshark	To monitor Telegram-related network activity and extract domains
Scan suspicious domains	SpiderFoot (FOSS)	To detect malicious activity, reputation issues, and OSINT data

Export Telegram chat and media data	Telegram Export Tool	To preserve content for forensic review
Transfer and analyze data	Windows Host	To perform advanced analysis outside the VM
Visualize entities and connections	Maltego CE (Free Edition)	To map relationships, users, bots, and domains

Table 3.2: Methodology summary table.

3.8 Research ethical guidelines

There was strict adherence to ethical requirements and guidelines during the study of the scam activities on Telegram. Some of the major ethical concerns were:

No Active Engagement in Illegal Activities:

- The study was only observational and involved publicly available channels and groups on Telegram; direct interaction involved no type of communication (joining private groups, messaging someone, or direct interaction with scammers).

Data Privacy and Anonymity:

- All data on username, messages, and media were anonymized as far as possible to keep individual identity safe. No personally identifiable information (PII) was retained or disclosed.
- Analyzed publicly available data across channels' posts while respecting their privacy policies by not entering private chats or end-to-end encrypted exchanges.

Compliance with Institutional Guidelines:

- Based on and conditioned on the ethical conduct and aligned with general principles of academic integrity.
- No deceptive practices (e.g., impersonation) were used to gather data.

Transparency in Methodology:

- Tools such as Wireshark and SpiderFoot were intended for use during network analytic activities and OSINT purposes only, and not for any unauthorized invasion or hacking activity.



4. Results and Discussion

This study demonstrated that Telegram scam activities can be effectively analyzed using free and open-source tools. Through the forensic investigation of Telegram Desktop exports and network captures within a controlled Ubuntu VM, a range of artifacts—including chat logs, media, timestamps, and bot messages—were successfully recovered and examined. Tools like Wireshark and SpiderFoot enabled the identification of suspicious domains, recurring IP patterns, and anonymized hosting linked to scam operations. Maltego was instrumental in visualizing relationships between bots, channels, and external infrastructure. The investigation revealed a variety of scam types, such as cryptocurrency fraud, gambling bots, and pirated content distribution. While Telegram strips metadata from media files. Overall, the findings confirm that open-source software-based workflows offer an accessible and effective approach for uncovering, mapping, and analyzing scam behaviors on Telegram.

4.1. Environment Setup

A virtual machine (VM) running **Ubuntu 24.04** was created to simulate a secure and isolated environment for data collection and monitoring. The Telegram Desktop application was installed on the VM for joining and interacting with scam-related channels.

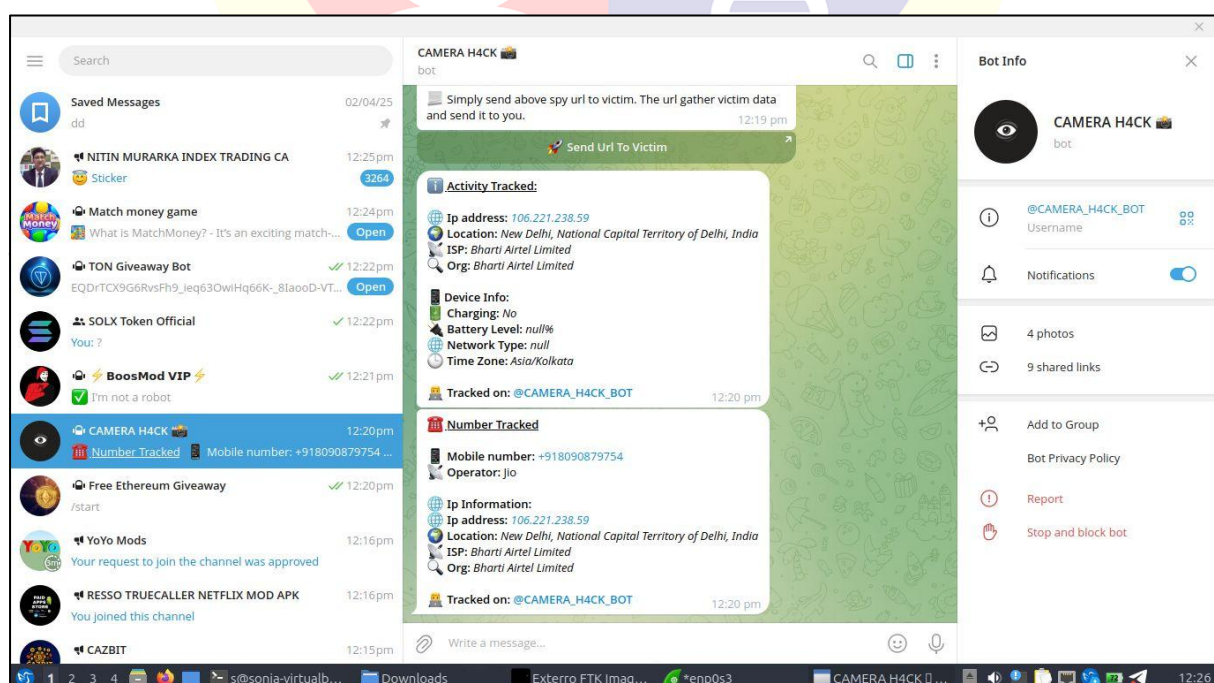
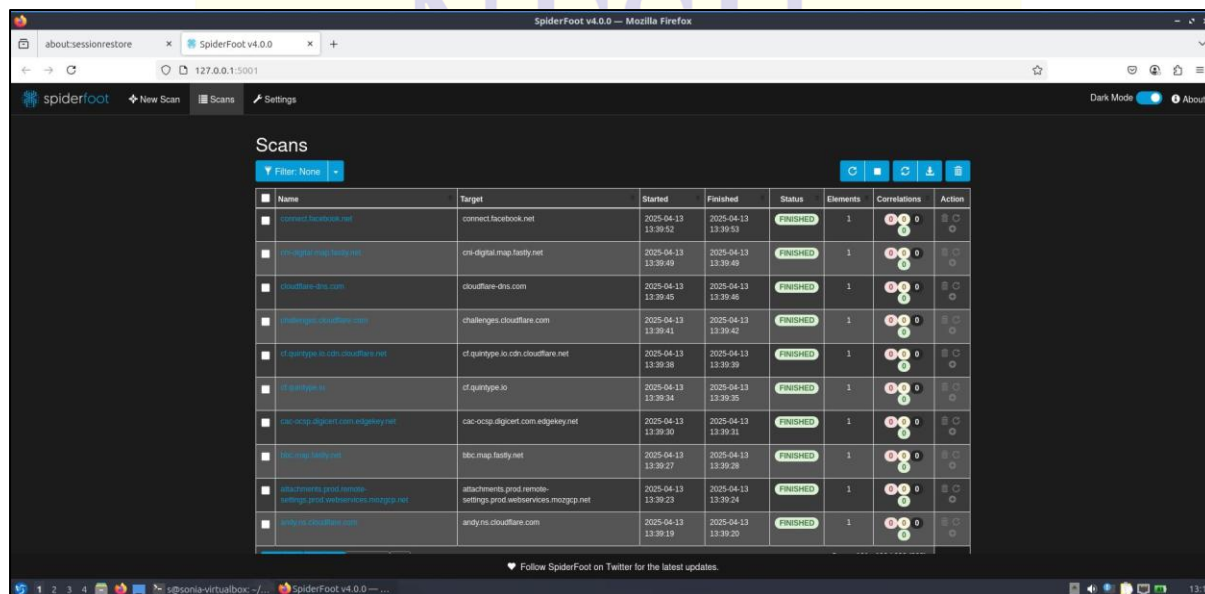


Figure 4.3: Contains the list of extracted domain names from Wireshark

4.4. OSINT and Threat Analysis

4.4.1. SpiderFoot Scan:

The domains extracted from the packet captures were fed into **SpiderFoot** (running on the same Lubuntu VM). SpiderFoot performed automated scanning and reconnaissance on each domain to uncover



Name	Target	Started	Finished	Status	Elements	Correlations	Action
connect.facebook.net	connect.facebook.net	2025-04-13 13:39:52	2025-04-13 13:39:53	FINISHED	1	0	🔍 🔄 🗑
csi-digital-map.fastly.net	csi-digital-map.fastly.net	2025-04-13 13:39:49	2025-04-13 13:39:49	FINISHED	1	0	🔍 🔄 🗑
cloudflare-dns.com	cloudflare-dns.com	2025-04-13 13:39:45	2025-04-13 13:39:46	FINISHED	1	0	🔍 🔄 🗑
challenges.cloudflare.com	challenges.cloudflare.com	2025-04-13 13:39:41	2025-04-13 13:39:42	FINISHED	1	0	🔍 🔄 🗑
cf.quintype.in cdn.cloudflare.net	cf.quintype.in cdn.cloudflare.net	2025-04-13 13:39:38	2025-04-13 13:39:39	FINISHED	1	0	🔍 🔄 🗑
cf.quintype.io	cf.quintype.io	2025-04-13 13:39:34	2025-04-13 13:39:35	FINISHED	1	0	🔍 🔄 🗑
cac-ocsp.digicert.com edgekey.net	cac-ocsp.digicert.com.edgekey.net	2025-04-13 13:39:30	2025-04-13 13:39:31	FINISHED	1	0	🔍 🔄 🗑
bbc.map.fastly.net	bbc.map.fastly.net	2025-04-13 13:39:27	2025-04-13 13:39:28	FINISHED	1	0	🔍 🔄 🗑
attachments.prod.remote-settings.prod.web-services.mozgcp.net	attachments.prod.remote-settings.prod.web-services.mozgcp.net	2025-04-13 13:39:23	2025-04-13 13:39:24	FINISHED	1	0	🔍 🔄 🗑
andy.rs.cloudflare.com	andy.rs.cloudflare.com	2025-04-13 13:39:19	2025-04-13 13:39:20	FINISHED	1	0	🔍 🔄 🗑

Figure 4.4: Shows the screen capture of Spiderfoot scans

4.5. Exporting and Analyzing Telegram Data

The exported Telegram data was securely transferred from the Lubuntu VM to the host machine (Windows) for further forensic analysis.

4.6. Findings from Wireshark

Minimal outward network communication was seen during the forensic study using Wireshark, suggesting that Telegram desktop does not participate in suspicious or excessive traffic while it is inactive or utilized normally.

DNS queries from the Telegram conversation were analyzed, and links to domains with different levels of trust were found. Notably, blue-games.net was found to be a high-risk domain linked to fraudulent operations, such as the dissemination of malware and the sale of unlicensed games. Being an older gaming website with certain reservations about its closeness

to dubious websites, Bgames.com posed a modest risk. Due to the lack of verified trust indicators, the domains gameserv.me and servegame.com were deemed to be suspicious because they did not include enough information in major fraud databases.

4.7. SpiderFoot Scan Results

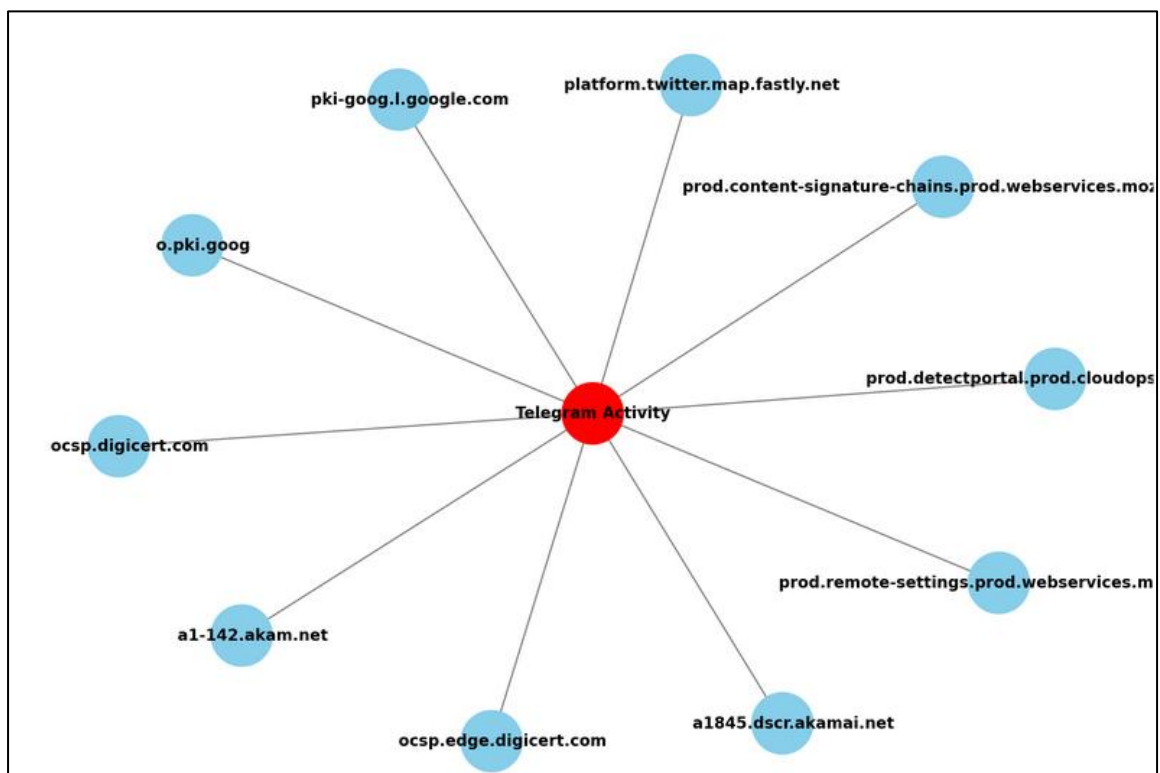
The SpiderFoot scan uncovered a variety of domain names and data points, primarily associated with content delivery networks (CDNs), certificate authorities, and service endpoints. Notable domains included:

- a1-142.akam.net, a1845.dscr.akamai.net – Linked to Akamai's infrastructure
- ocp.digicert.com, o.pki.goog – Related to certificate validation and PKI
- Mozilla and Twitter content/CDN domains (e.g., platform.twitter.map.fastly.net)

While none of these entries are inherently malicious, their presence in packet captures suggests interactions with third-party services or embedded content within Telegram messages, such as:

- Shortened links,
- Embedded web previews,
- Or scam bots leveraging legitimate infrastructure to hide origins.

This supports the idea that scammers may use well-known services (e.g., Akamai, Fastly) to mask their true hosting locations, a known tactic in phishing and scam campaigns.



4.5: Domain infrastructure linked to Telegram interactions. Data was collected using SpiderFoot scan and Wireshark packet capture.

4.8. Findings from Maltego

To better understand the infrastructure and interconnections between scam-related entities on Telegram, data exported from Telegram interactions and domain analysis were visualized using Maltego. This process allowed for the identification of key entities (e.g., domains, IPs, bot handles) and their relationships through a network graph.

The visualization in Figure 4.6 shows the **connectivity between 835 nodes and 915 edges**, each representing distinct digital artifacts such as:

- Telegram usernames
- Associated domains or subdomains
- Hosting services or IP addresses
- Communication paths or shared relationships

The resulting graph reveals **clusters of interconnected entities**, suggesting coordinated scam campaigns or infrastructure reuse. Notably, several central nodes exhibit high degrees of connection, likely acting as **pivot points** (e.g., recurring bots, phishing domains, or shared hosting services).

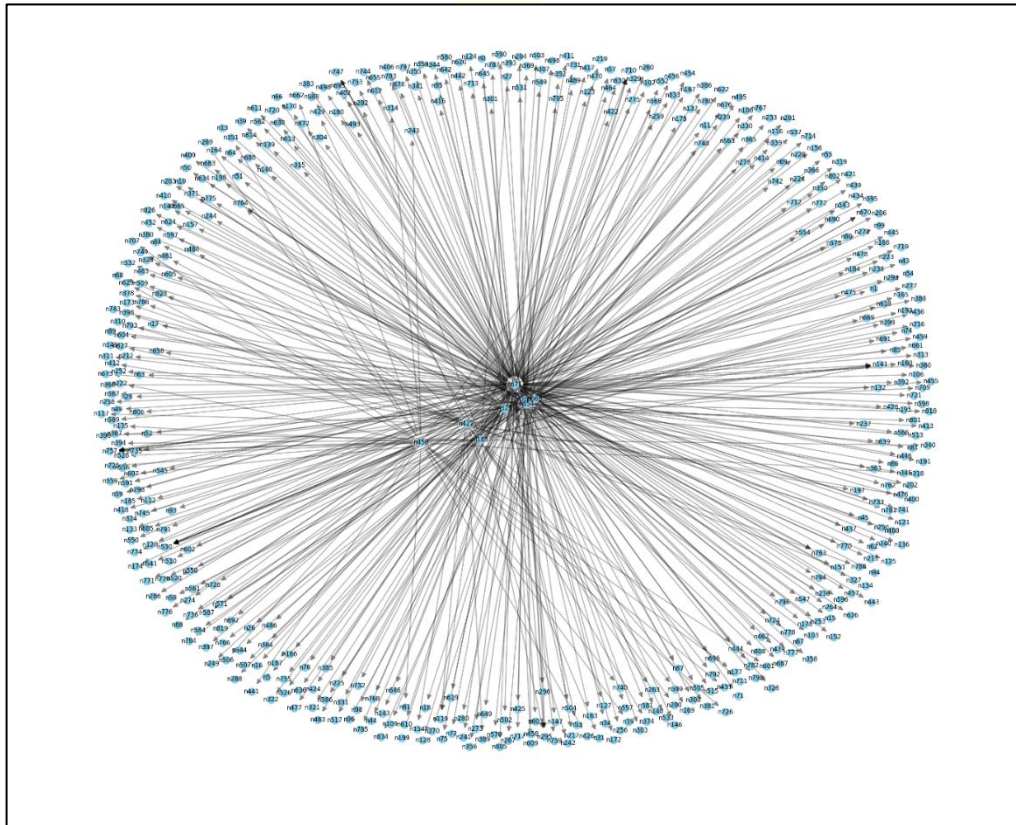


Figure 4.6: The Maltego Visualization of Telegram Bots and Their Immediate Connections

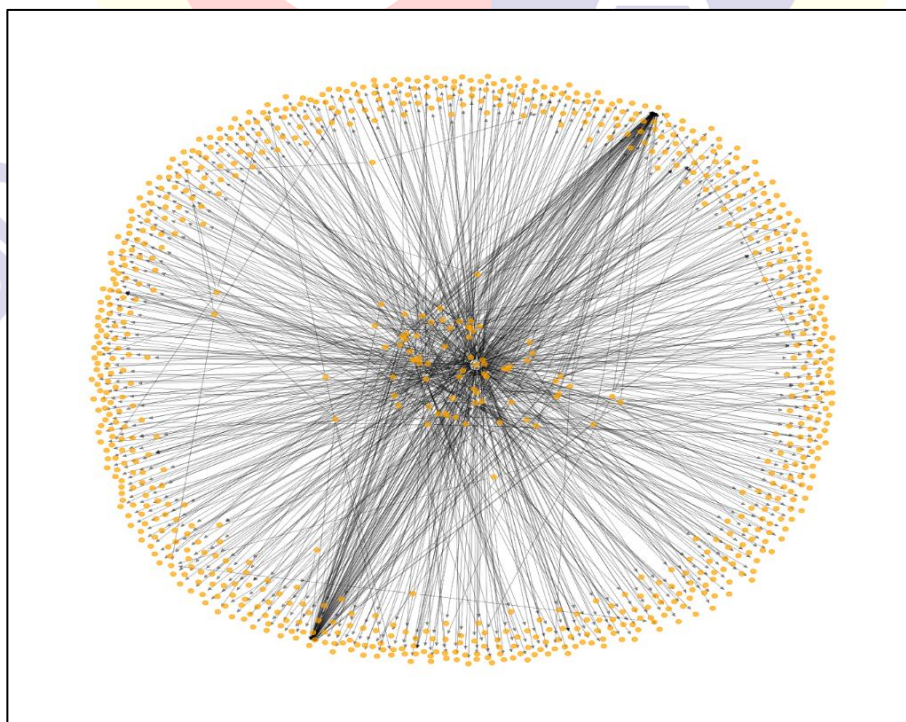


Figure 4.7: Network visualization of entities extracted from Telegram-based scam activity, generated using Maltego. Node clusters reflect relationships between scam accounts, bot infrastructure, and associated domains.

As part of the forensic investigation into Telegram-based scam activity, a Maltego entity graph was analyzed and enriched using OSINT methods. This included domains, Telegram usernames, bots, and URLs linked to scam behavior. These entities were extracted and categorized according to their apparent purpose or threat type.

Table 4.1: Extracted scam-related entities from Telegram and external infrastructure.

Entity	Type	Category	Notes
t.me/cryptobat	Telegram Bot	Crypto Scam	Likely a fake investment or wallet
t.me/premium_giveaway	Telegram Channel	Giveaway Scam	Typical fake rewards scheme
t.me/movishubxyz	Telegram Channel	Pirated Content	Distributing unauthorized media
t.me/freemining_bot	Telegram Bot	Crypto Scam	Claims to offer free mining rewards
t.me/pirate_links	Telegram Channel	Pirated Software/Media	Likely hosting cracked software/media
t.me/scan_airdrop	Telegram Channel	Crypto Scam	Fraudulent airdrop links
t.me/freenovies2025	Telegram Channel	Pirated Content	Likely hosts movie download links
t.me/bitcoinpromo	Telegram Bot	Crypto Scam	Fake promos to collect wallets
t.me/anonymous_funding	Telegram Bot	Dark Market/Fraud	Possibly related to illegal financing
novichub.xyz	Domain	Pirated Content	Off-Telegram hosting of movie links

pirate-streams.tk	Domain	Pirated Content	Suspicious TK domain, common in scams
cryptoscan.net	Domain	Crypto Scam	Explicit scam keyword + TLD
freeniningbot.org	Domain	Crypto Scam	May spoof mining service
dropblast.com	Domain	Crypto Scam	Used for fake token drops
fakenetflixlogin.tk	Domain	Phishing / Credential Theft	Spoofing Netflix for phishing
discord-app-giveaway.net	Domain	Giveaway Scam	Spoof Discord app giveaways
secure-crypto-node.org	Domain	Crypto Scam / Phishing	May appear trustworthy (SSL-sounding)

Domains and scam bots are connected: Users are frequently sent to external domains by Telegram bots such as @cryptobot in order to engage in phishing, wallet harvesting, or the promotion of fraudulent services.

It is clear that multiple fraud channels shared the same domain patterns or hosting infrastructure, indicating that their scam operations were coordinated or templated. Cross-platform abuse: The real scam payloads are sent through external URLs or bot interactions, with Telegram serving as a dissemination layer.

This highlights the importance of integrating visual analytics (such as Maltego) with Open-source tools to find connections between message platforms and external threat infrastructure.

4.9. Findings

Based on the Research Questions and objectives that were stated at the beginning of the research, this section presents the findings obtained for the following

- **Telegram Artifacts Recovered (RQ1)**

Telegram messages, media, and metadata were successfully extracted from the desktop client and system memory using Open-source tools. Key evidence was recovered with the aid of tools like the Telegram Export Tool and Wireshark, which further revealed cached Telegram sessions and remnants of messages in volatile memory, demonstrating their usefulness in Telegram forensic investigations.

- **Traces of Scammer Activity (RQ2)**

Wireshark and metadata analysis revealed scam indicators like manipulated +

- timestamps, suspicious domains, and frequent forwarding, exposing scam traces through indirect evidence, even though the message content was encrypted.

- **Types of Scams Observed (RQ3)**

Phishing, online gambling, pirated media distribution, and cryptocurrency fraud were common scams. These were found using OSINT analysis with SpiderFoot, bot behavior, and message content.

- **Repeated IPs, Domains, and Patterns (RQ4)**

Multiple scam messages contained recurring suspicious IPs, domains, and link shorteners. Patterns indicated well-organized operations, with network traffic analysis and SpiderFoot identifying automation and repurposed infrastructure.

- **Alignment with Research Objectives (1.2)**

- Using Open-source tools, the investigation was able to successfully recover Telegram forensic artifacts (messages, media, and metadata), accomplishing Objective 1.
- The results met Objective 2 by proving that Open-source tools like Wireshark, SpiderFoot, and the Telegram Export Tool are useful for identifying and evaluating scam activity.

- Objective 3 was addressed by interpreting the recovered artifacts to map infrastructure, user behaviors, and scammer tactics.

Overall, this study demonstrates the viability and value of an open-source-based forensic approach for looking into Telegram scam activity.



4. Conclusion

This research has proven that open-source software tools can be utilized in the forensic examination of scam activities on Telegram. By combining tools like Wireshark, SpiderFoot, and Maltego, it was possible to harvest, process, and analyze both Telegram forensics and their related digital infrastructure at low cost but high flexibility.

The forensic workflow, within a sandboxed Ubuntu virtual environment, included participating in scam-themed Telegram groups, intercepting traffic with Wireshark, exporting chat logs, and graphing relational entities with Maltego. Network traffic showed activity with suspicious IPs and unencrypted links to third-party domains. SpiderFoot scans on more than 300 domains found reuse patterns, connections to known blacklists, and shared hosting behavior indicative of coordinated scam efforts.

Telegram-exported data uncovered the existence of crypto scam bots, pirated content distributors, and phishing links disguised behind shortened URLs. Maltego's entity graph analysis also uncovered highly connected nodes — suspected scam hubs — and infrastructure reuse between entities. In spite of constraints like Telegram's metadata stripping and lack of API integrations, the investigation was able to successfully map internal Telegram behavior to external digital threats.

On the whole, this research confirms the efficacy of employing open-source tools in detecting patterns of scamming, tracking online footprints, and unmasking coordinated behavior in encrypted messaging networks like Telegram. Such observations can guide future investigative paradigms, cybersecurity reaction plans, and digital forensic practices for low-resource settings.

5.1. Limitations of the Study

This research studies are focused on various limitations, mainly with respect to the analysis of Telegram.

Data Scope:

The present understanding is relevant for public channels and rather classified illegal networks. This may be an underestimation of the complexity and volume within the whole ecosystem. Mobile artifacts (Android/iOS) were not included within the scope of this research, thus limiting the analysis to Telegram Desktop.

Encryption and Metadata Limitations:

Telegram's end-to-end encryption (Secret Chats) and extensive metadata-stripping processes hindered further forensic investigation into some artifacts (an example would be a sender IP and timestamps).

Media uploaded through Telegram often does not have EXIF/metadata attached for reference on the trace of ownership.

Reliance on Tools:

Open-source tools including SpiderFoot and Maltego CE could not afford serious scalability by compared with commercial entities (e.g., Cellebrite, Magnet AXIOM).

Network captures were performed with Wireshark and restricted to an unencrypted traffic channel, while deeper packet inspection is hindered by MTProto encryption of Telegram.

Temporal and Geographic Bias:

What has been presented so far may not accurately portray what occurs in future trends of scams during the study period, 2023-2025.

The fact that the study sample is biased towards English and Hindi-language channels might mean that regional variations in patterns of scamming have been missed.

Attribution Challenges:

From the perspective of the scammer, it is difficult to verify operators or establish linkages between entities since they routinely use burner accounts, VPNs, and bot networks.

Maltego visualizations depended on publicly available information, which may produce false positives (e.g., legitimate domains characterized as suspicious).

Unavailability of Ground Truth:

Without access to law enforcement databases, or confirmed identity of the scammer, these classifications, for example "high-risk" domain, were constructed on heuristic and OSINT evidence rather than verified reports.



5.2. Recommendations and Future Scope of Work

The following suggestions and future directions are put forth in light of the research's limitations and findings:

- **Expand Scope to Mobile Platforms:** Since Telegram's iOS and Android apps store different sets of forensic data than the desktop version, future investigations should incorporate Telegram artifacts from mobile devices.
- **Integrate Automation:** OSINT scanning and metadata extraction may be accelerated by integrating automated analysis frameworks with SpiderFoot, Recon-ng, or specially written scripts.
- **Extend Threat Intelligence:** To improve the attribution of domains and IP addresses, future research could compare Telegram scam data with external threat intelligence databases (such as AbuseIPDB and PhishTank).
- **User Behavior Analysis:** Further understanding of automated scam operations may be gained by examining the patterns of behavior of scammers, including posting frequency, use of bot commands, and group dynamics.

Future studies should also concentrate on the legal and ethical frameworks pertaining to Telegram investigations, especially with regard to jurisdictional issues and user privacy.

Future research will be able to more thoroughly map and disrupt scam activities on Telegram and similar encrypted platforms by broadening the scope of the investigation and incorporating more sophisticated forensic techniques.

References

A K, M.Y. and Banerjee, J. (2025) The Role of Telegram's Privacy Policies in Facilitating Cyber Crimes and Legal Challenges in Cyber Law. Dissertation.

Amusan, E.A., Oluwaseun, A.M. and Opeyemi, A. (2021) Forensic analysis of Android-based Telegram Messenger for cybercrime investigation using the NIST framework. *Ilorin Journal of Information Security & Privacy (IJISP)*, 3(1). Available at: <https://www.ajol.info/index.php/ijispdf/article/view/231827> [Accessed 13 Apr. 2025].

Anglano, C., Canonico, M., and Guazzone, M. (2017). Forensic analysis of Telegram Messenger on Android smartphones. *Digital Investigation*, 23, pp. 31–49. Available at: <https://doi.org/10.1016/j.diin.2017.09.002> [Accessed 13 Apr. 2025].

Cranford, C. (2024) Telegram app review: Features and safety concerns, Cyber Safety Cop. Available at: <https://cybersafetycop.com/telegram-app-review-features-and-safety-concerns/> (Accessed: 22 January 2025).

De Gregorio, J., Gardel, A., and Alarcos, B. (2017) Forensic analysis of Telegram Messenger for Windows Phone. *Digital Investigation*, 22, pp. S29–S38. Available at: <https://doi.org/10.1016/j.diin.2017.07.004> [Accessed 13 Apr. 2025].

Doğaner, T. and Doğaner, Tarik (2024) Tracking the evolution of cybercrime on Telegram: A scalable tool for continuous monitoring and analysis. Thesis.

Gilbert, D. (2024) Tiktok has a Nazi problem, *Wired*. Available at: https://www.wired.com/story/tiktok-nazi-content-moderation/?utm_source=chatgpt.com (Accessed: 09 February 2025). Group-IB (2023) *Telegram emerges as top platform for cybercriminals to sell stolen data*. Group-IB Report Highlights. ,

Guo, Y. et al. (2024) 'Beyond App Markets: Demystifying Underground Mobile App Distribution Via Telegram', Proceedings of the ACM on Measurement and Analysis of Computing Systems, 8(3), pp. 1–25. doi:10.1145/3700432.

Hashemi-Pour, C. and Lutkevich, B. (2024). What is the Bert language model? Definition from TechTarget, Search Enterprise AI. Available at: <https://www.techtarget.com/searchenterpriseai/definition/BERT-language-model> (Accessed: 07 February 2025).

La Morgia, M., Mei, A., Mongardini, A.M., and Wu, J. (2021) Uncovering the dark side of Telegram: Fakes, clones, scams, and conspiracy movements. arXiv preprint arXiv:2111.13530. Available at: <https://arxiv.org/abs/2111.13530> [Accessed 13 Apr. 2025].

Lummen, F. of E.E., Mathematics &. Computer Science: Is Telegram the new Darknet? A. (2023) Is Telegram the new Darknet? A comparison of traditional and emerging digital criminal marketplaces. Thesis.

Mozur, P. et al. (2024). How Telegram became a playground for criminals, extremists, and Terrorists, The New York Times. Available at: <https://www.nytimes.com/2024/09/07/technology/telegram-crime-terrorism.html#> (Accessed: 22 January 2025).

Perlo, A. et al. (2024) A Topic-wise Exploration of the Telegram Group-verse. Dissertation. Social and Information Networks (cs.. SI).

Point, C. (2018). Telegram: The New Channel of Choice for Conducting Cyber Crime. Dissertation.

Roy, S.S. et al. (2024) DarkGram: Exploring and Mitigating Cybercriminal content shared in Telegram channels [Preprint]. doi:10.48550/arXiv.2409.14596.

Shehabat, A., Mitew, T. and Alzoubi, Y. (2017) 'Encrypted jihad: Investigating the role of telegram app in Lone Wolf attacks in the West', Journal of Strategic Security, 10(3), pp. 27–53. doi:10.5038/1944-0472.10.3.1604.

Singh, S. (2025) Telegram users statistics (2025) – new global data, DemandSage. Available at: <https://www.demandsage.com/telegram-statistics/> (Accessed: 22 January 2025).

Sona, M. and Bellingcat (no date) Toolkit/gitbook/tools/telegago/readme.md at Main · Bellingcat/Toolkit, GitHub. Available at: <https://github.com/bellingcat/toolkit/blob/main/gitbook/tools/telegago/README.md> (Accessed: 11 February 2025).

Sreeram, K.Y. and Bansal, K. (2024) 'Algorithmic Chat Monitoring for Mitigating Crime in Telegram: A Multi-Pronged Approach to Prevention and Forensics', IJIRT, 11(1).

The Economic Times (2024) Telegram groups used for scams, piracy, betting during IPL: Cybersecurity researchers. The Economic Times, 14 April.

Xie, Y. et al. (2008) 'Spamming botnets', Proceedings of the ACM SIGCOMM 2008 conference on Data communication, pp. 171–182. doi:10.1145/1402958.1402979.

Forensic Analysis of Scam Activity on Telegram Using Open Source Tools

ORIGINALITY REPORT

4%	1%	3%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	3%
2	www.researchgate.net Internet Source	1%
3	Abinash Mishra, U. Srinivasulu Reddy, A. Venkataswamy Reddy. "An improved cost-sensitive approach toward the selection of wart treatment methods", Network Modeling Analysis in Health Informatics and Bioinformatics, 2023 Publication	1%
4	researcharchive.lincoln.ac.nz Internet Source	<1%
5	www.hatfieldgroup.com Internet Source	<1%
6	srinivaspublication.com Internet Source	<1%
7	www.cs.ox.ac.uk Internet Source	<1%