Forensic Analysis of the Android Image

This report details a comprehensive forensic investigation into an alleged internet fraud scheme involving a fake investment website designed to lure individuals into investing in fraudulent cryptocurrency, promising exceptionally high returns on investment.

The report outlines the methodologies and tools utilized, presents key findings, and provides recommendations for future preventative measures and legal actions.

Tools used: Autopsy, 7zip, Android forensic image

Methodology: This encompassing evidence collection, examination, analysis, and reporting. An android image was extracted with 7zip extraction software, which was feed into Autopsy for analysis. The forensic investigation adhered to a rigorous, multi-phase methodology to ensure the integrity, authenticity, and admissibility of all collected digital evidence. This structured approach, adapted from established digital forensic principles, involved the following key stages:

1. collection/Acquisition:

- **Victim Device Acquisition:** Where available and permissible, forensic images of relevant storage media (e.g., the mobile phone, tablets) used by victims to interact with the fake website or communicate with
the perpetrators were acquired. Strict chain of custody protocols were maintained throughout this process, and hardware write-blockers were utilized to ensure that no data on the original media was inadvertently altered during the imaging process

- **Call logs:** various calls and phone numbers of the conspirators were recovered; this gives more insights into their deceitful act.
- **Message logs**: these were also retrieved to ascertain and monitor the trend of communication and strategies in carrying out their elicit fraud.
- **Open Source Intelligence (OSINT) Gathering:** Publicly available information was systematically collected from various online sources, including social media platforms, online forums, cryptocurrency communities, and news articles related to the scam. This intelligence helped in understanding the scam's promotion, identifying potential victims, and uncovering additional digital footprints of the perpetrators.

- **Artifacts:** web histories, web cookies, web search were also collected this helps to know the tress of web visited by this perpetrator, and the type of search conducted.

2. **Examination:** Following the secure collection of data, the examination phase involved a meticulous and systematic processing of the acquired digital evidence to identify and extract information pertinent to the investigation. This phase was characterized by:

- **Data Carving and Recovery:** Advanced data carving techniques were employed to recover deleted files or fragments of files from unallocated space on acquired disk images. This was crucial for uncovering hidden or intentionally removed evidence.
- **Targeted Keyword Searches:** Extensive keyword searches were conducted across all acquired data. Keywords included the name of the fake website, specific cryptocurrency names mentioned in the scam, known aliases of perpetrators, victim names, and terms commonly associated with investment schemes (e.g., 'ROI', 'guaranteed returns', 'withdrawal').
- **File System and Metadata Analysis:** A detailed analysis of file system metadata, including creation, modification, and access timestamps, was performed to reconstruct the chronological sequence of events. This helped in understanding when specific files were created, accessed, or altered, providing insights into the perpetrators' activities.

3. Analysis:

Message Log analysis:

2024-03-17 03:09:45 WAT

Deduced the name of the alleged suspect to be Bro Sam from the message supposedly to be from his pastor.

2024-03-17 03:19:10 WAT

A scam idea was mention to be carried out

2024-03-17 03:20:44 WAT

A fake investment crypto currency website was to be created to lure in innocent people

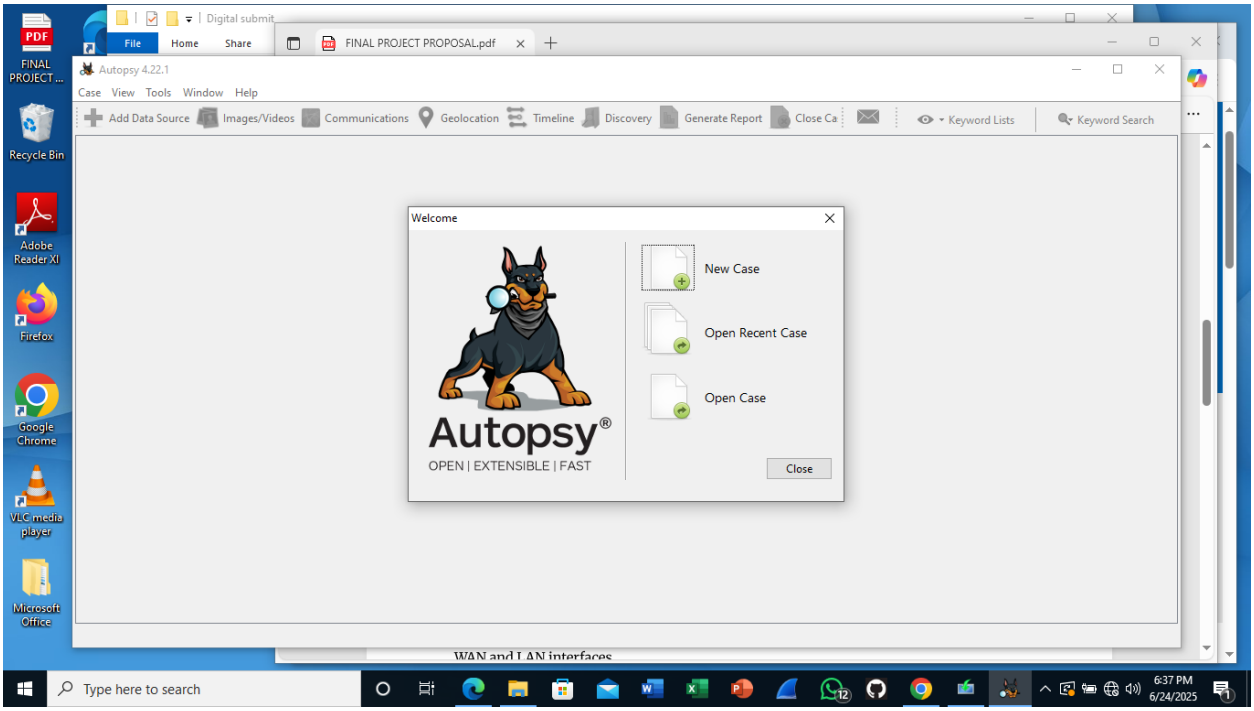
2024-03-17 03:23:45 WAT

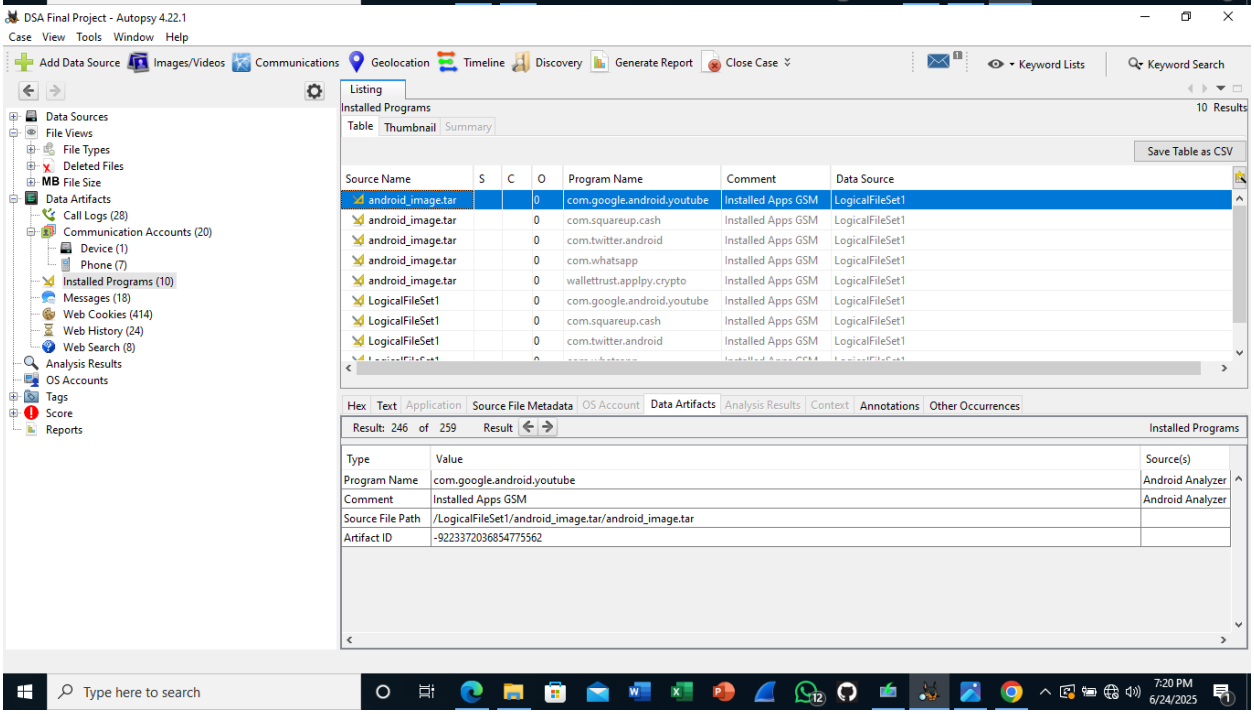
A bitcoin wallet address to be used 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn. Which actually belong to Woodberry

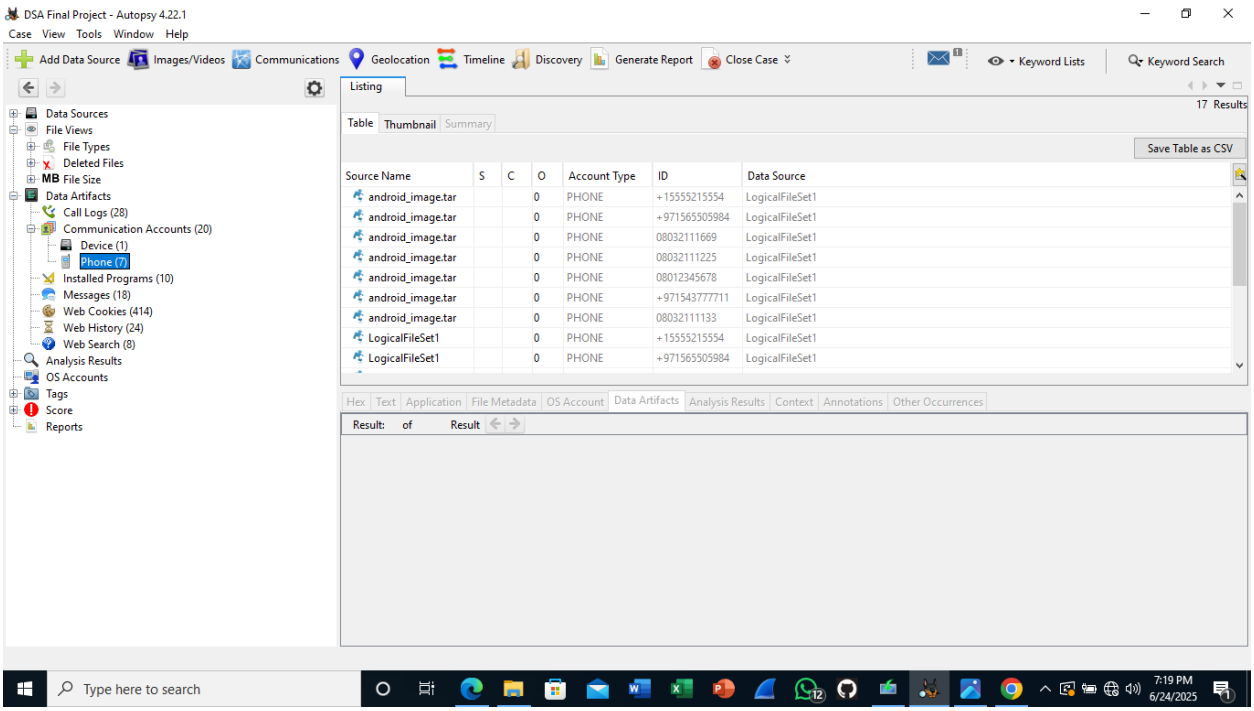
2024-03-17 04:29:40 WAT

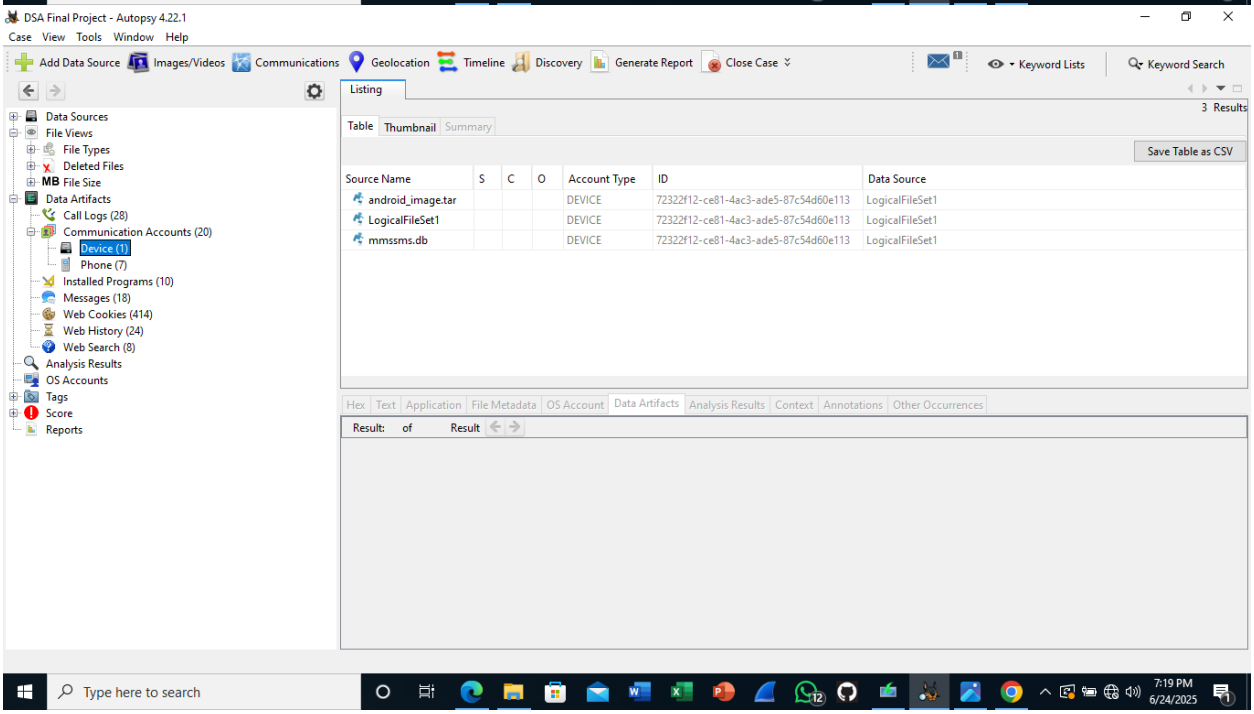
The fake investment website was actually created.

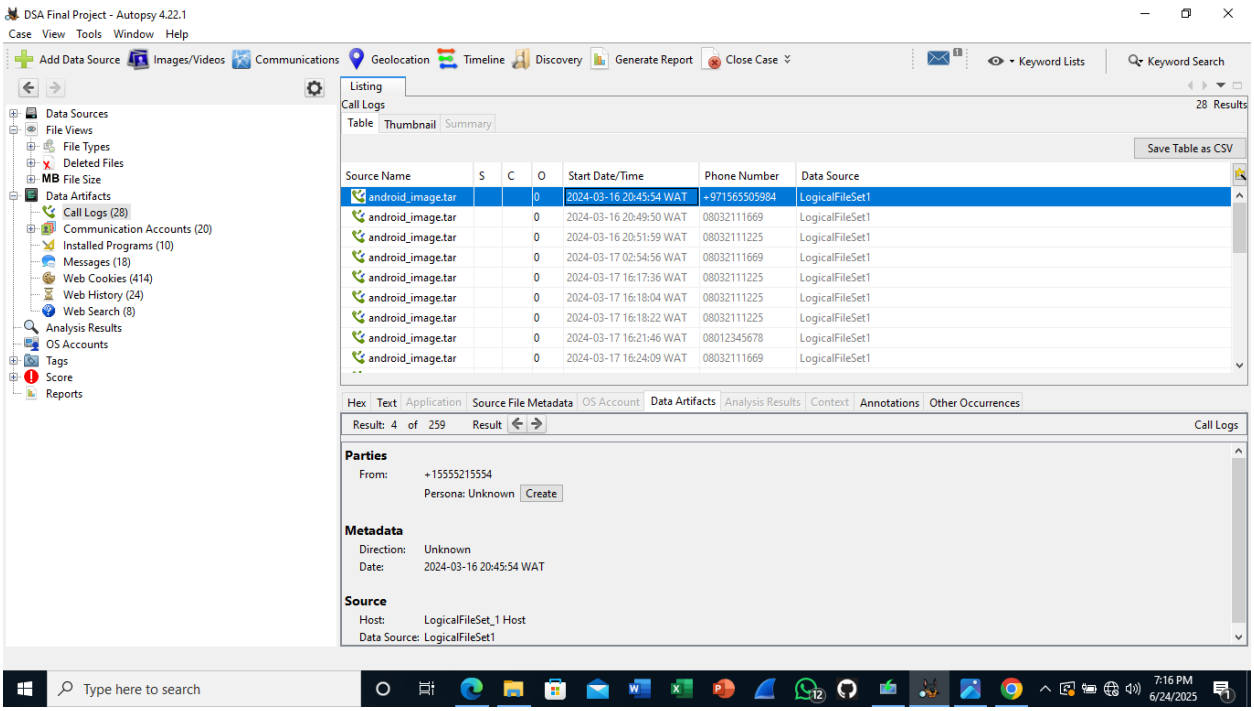
- ## Screen shorts

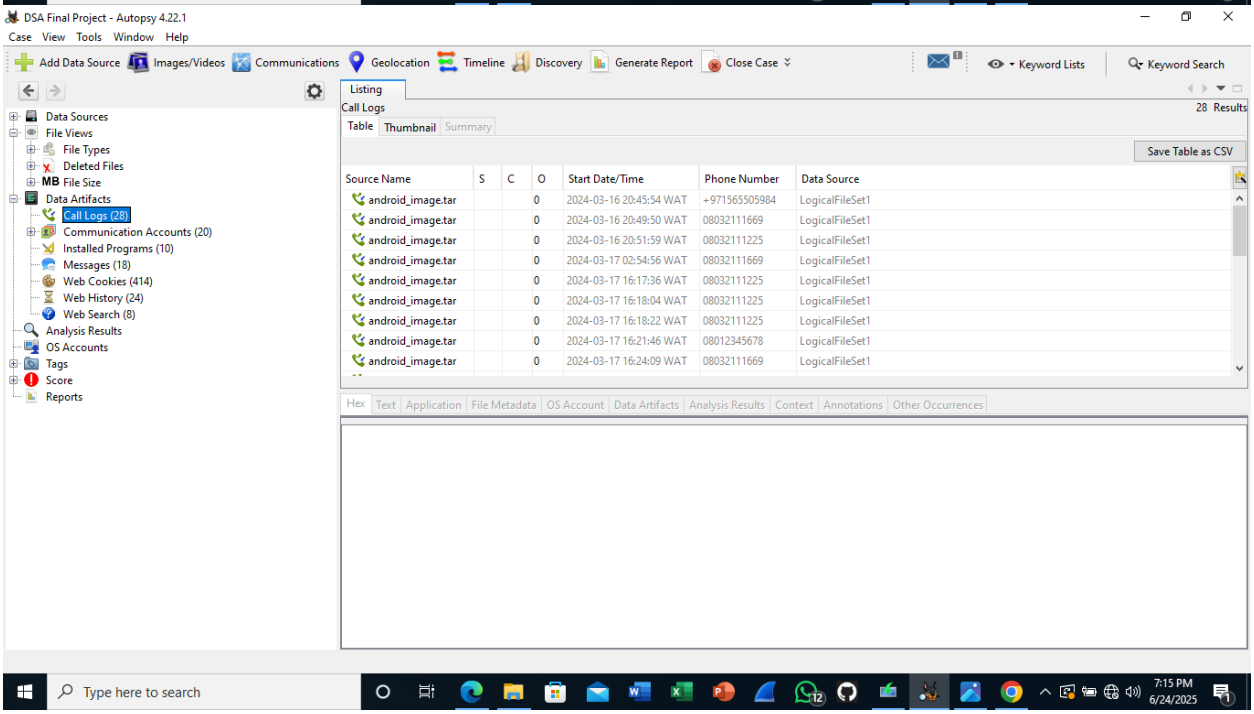

FINAL PROJECT ...
Recycle Bin
Adobe Reader XI
Firefox
Google Chrome
VLC media player
Microsoft Office
Digital submit
File
Home
Share
FINAL PROJECT PROPOSAL.pdf
Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Ca
Keyword Lists
Keyword Search
Welcome
New Case
Open Recent Case
Open Case
Autopsy®
OPEN | EXTENSIBLE | FAST
Close
WAN and LAN interfaces
Type here to search
6:37 PM
6/24/2025

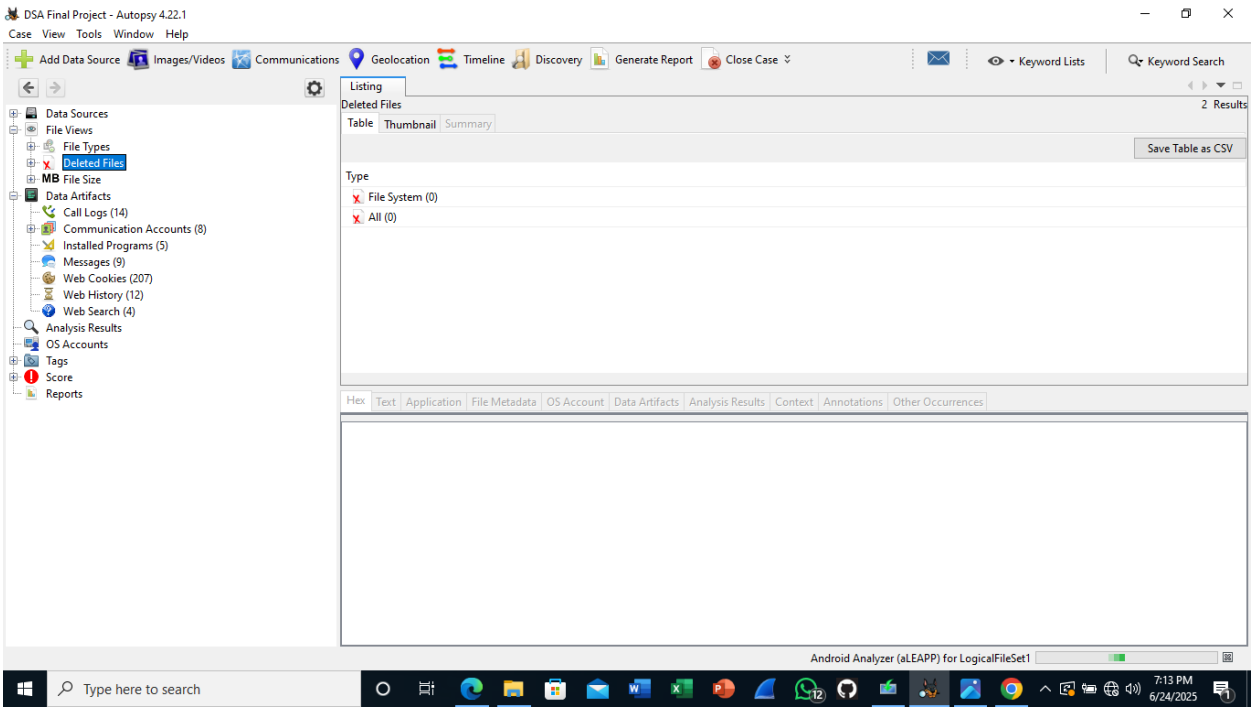

DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (28)
Communication Accounts (20)
Device (1)
Phone (7)
Installed Programs (10)
Messages (18)
Web Cookies (414)
Web History (24)
Web Search (8)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Installed Programs
10 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
Program Name
Comment
Data Source
android_image.tar 0 com.google.android.youtube Installed Apps GSM LogicalFileSet1
android_image.tar 0 com.squareup.cash Installed Apps GSM LogicalFileSet1
android_image.tar 0 com.twitter.android Installed Apps GSM LogicalFileSet1
android_image.tar 0 com.whatsapp Installed Apps GSM LogicalFileSet1
android_image.tar 0 wallettrust.applpy.crypto Installed Apps GSM LogicalFileSet1
LogicalFileSet1 0 com.google.android.youtube Installed Apps GSM LogicalFileSet1
LogicalFileSet1 0 com.squareup.cash Installed Apps GSM LogicalFileSet1
LogicalFileSet1 0 com.twitter.android Installed Apps GSM LogicalFileSet1
Hex
Text
Application
Source File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Result: 246 of 259
Result
Installed Programs
Type
Value
Source(s)
Program Name
com.google.android.youtube
Android Analyzer
Comment
Installed Apps GSM
Android Analyzer
Source File Path
/LogicalFileSet1/android_image.tar/android_image.tar
Artifact ID
-9223372036854775562
Type here to search
7:20 PM
6/24/2025

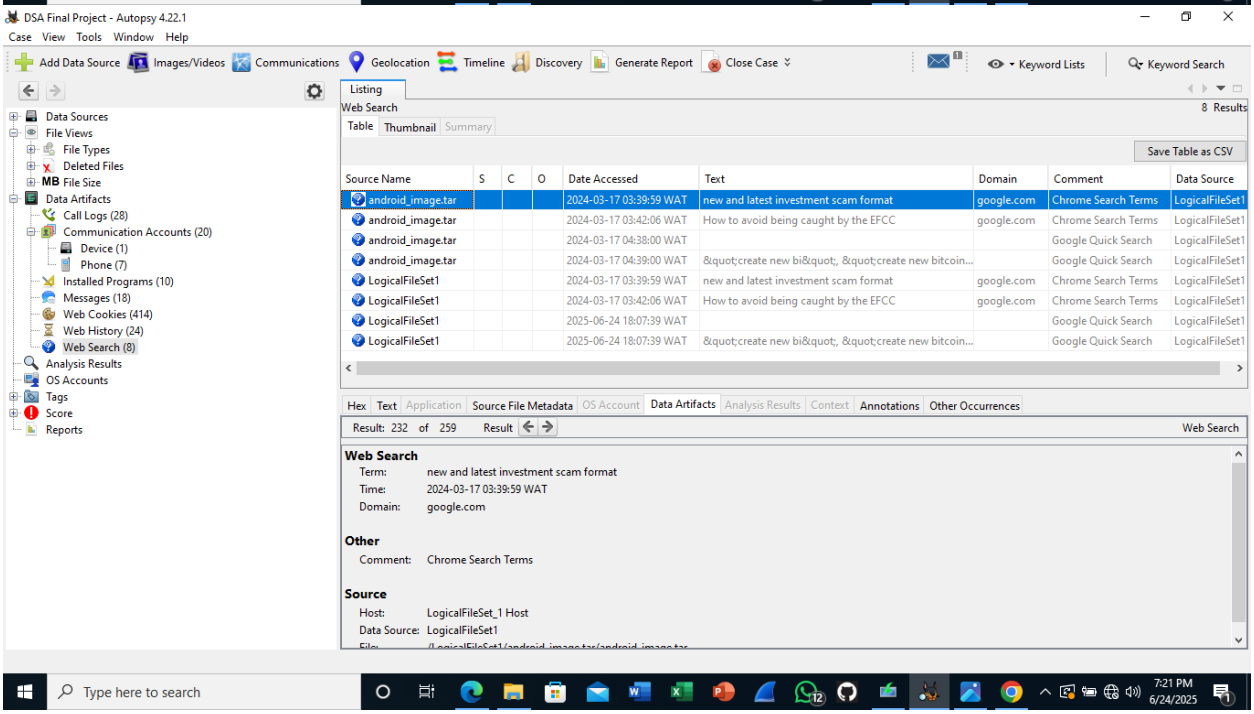

DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
17 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Account Type ID Data Source
android_image.tar 0 PHONE +15555215554 LogicalFileSet1
android_image.tar 0 PHONE +971565505984 LogicalFileSet1
android_image.tar 0 PHONE 08032111669 LogicalFileSet1
android_image.tar 0 PHONE 08032111225 LogicalFileSet1
android_image.tar 0 PHONE 08012345678 LogicalFileSet1
android_image.tar 0 PHONE +971543777711 LogicalFileSet1
android_image.tar 0 PHONE 08032111133 LogicalFileSet1
LogicalFileSet1 0 PHONE +15555215554 LogicalFileSet1
LogicalFileSet1 0 PHONE +971565505984 LogicalFileSet1
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: of Result
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (28)
Communication Accounts (20)
Device (1)
Phone (7)
Installed Programs (10)
Messages (18)
Web Cookies (414)
Web History (24)
Web Search (8)
Analysis Results
OS Accounts
Tags
Score
Reports
Type here to search
7:19 PM
6/24/2025

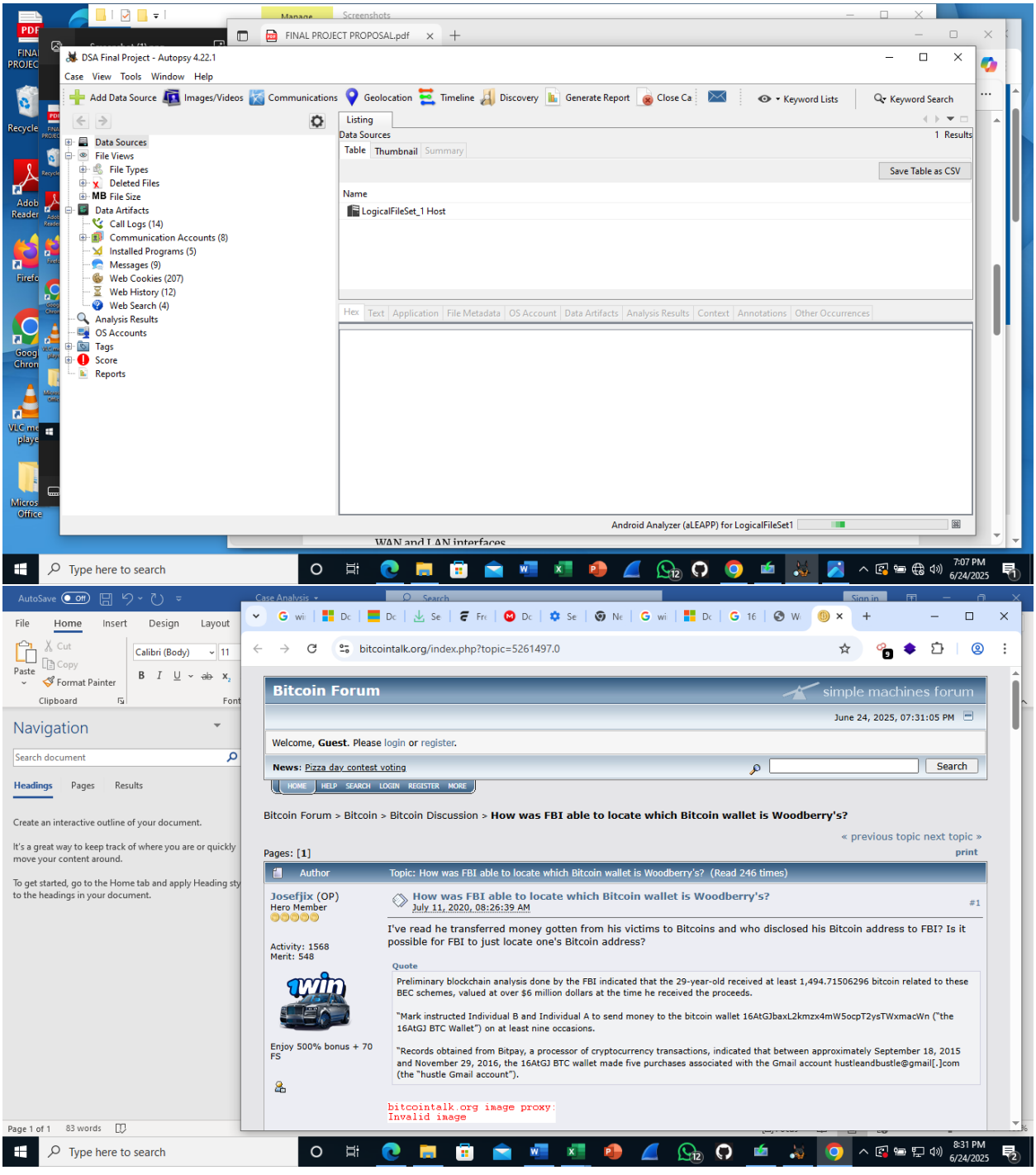

DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
3 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Account Type ID Data Source
android_image.tar DEVICE 72322f12-ce81-4ac3-ade5-87c54d60e113 LogicalFileSet1
LogicalFileSet1 DEVICE 72322f12-ce81-4ac3-ade5-87c54d60e113 LogicalFileSet1
mmssms.db DEVICE 72322f12-ce81-4ac3-ade5-87c54d60e113 LogicalFileSet1
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: of Result
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (28)
Communication Accounts (20)
Device (1)
Phone (7)
Installed Programs (10)
Messages (18)
Web Cookies (414)
Web History (24)
Web Search (8)
Analysis Results
OS Accounts
Tags
Score
Reports
Type here to search
7:19 PM
6/24/2025

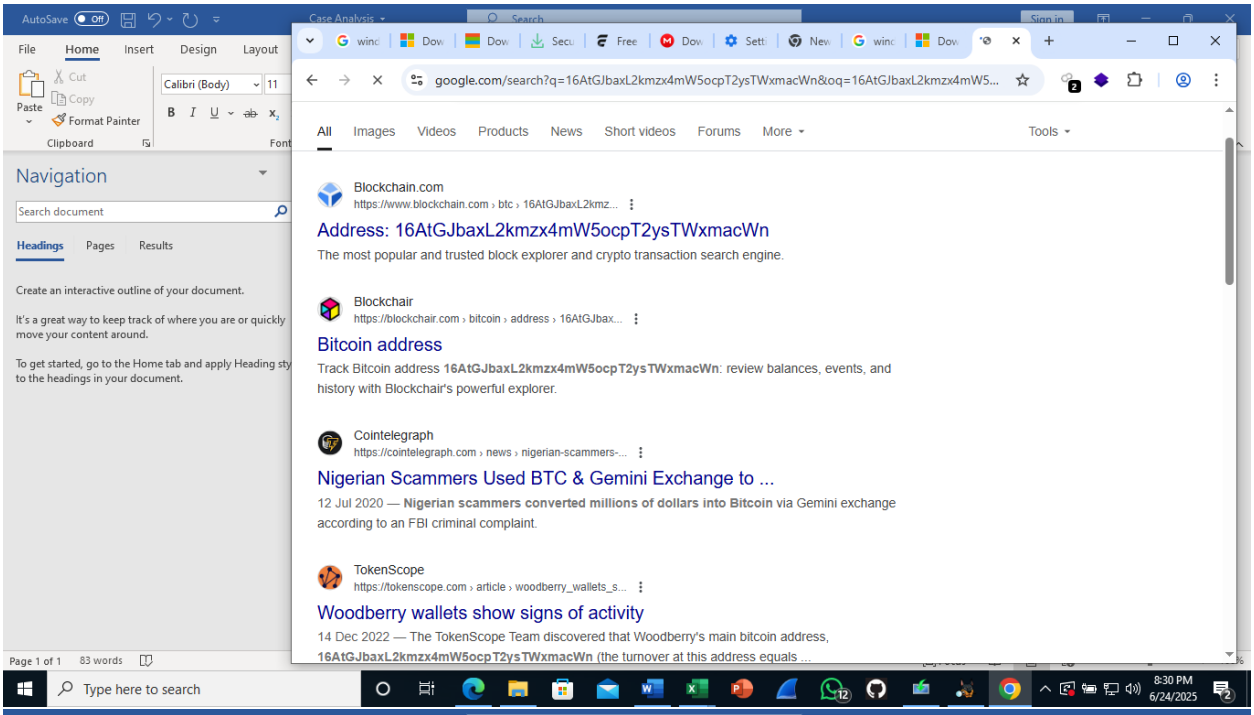

DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (28)
Communication Accounts (20)
Installed Programs (10)
Messages (18)
Web Cookies (414)
Web History (24)
Web Search (8)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Call Logs
28 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Start Date/Time Phone Number Data Source
android_image.tar 0 2024-03-16 20:45:54 WAT +971565505984 LogicalFileSet1
android_image.tar 0 2024-03-16 20:49:50 WAT 08032111669 LogicalFileSet1
android_image.tar 0 2024-03-16 20:51:59 WAT 08032111225 LogicalFileSet1
android_image.tar 0 2024-03-17 02:54:56 WAT 08032111669 LogicalFileSet1
android_image.tar 0 2024-03-17 16:17:36 WAT 08032111225 LogicalFileSet1
android_image.tar 0 2024-03-17 16:18:04 WAT 08032111225 LogicalFileSet1
android_image.tar 0 2024-03-17 16:18:22 WAT 08032111225 LogicalFileSet1
android_image.tar 0 2024-03-17 16:21:46 WAT 08012345678 LogicalFileSet1
android_image.tar 0 2024-03-17 16:24:09 WAT 08032111669 LogicalFileSet1
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 4 of 259 Result
Call Logs
Parties
From: +15555215554
Persona: Unknown Create
Metadata
Direction: Unknown
Date: 2024-03-16 20:45:54 WAT
Source
Host: LogicalFileSet_1 Host
Data Source: LogicalFileSet1
Type here to search
7:16 PM
6/24/2025

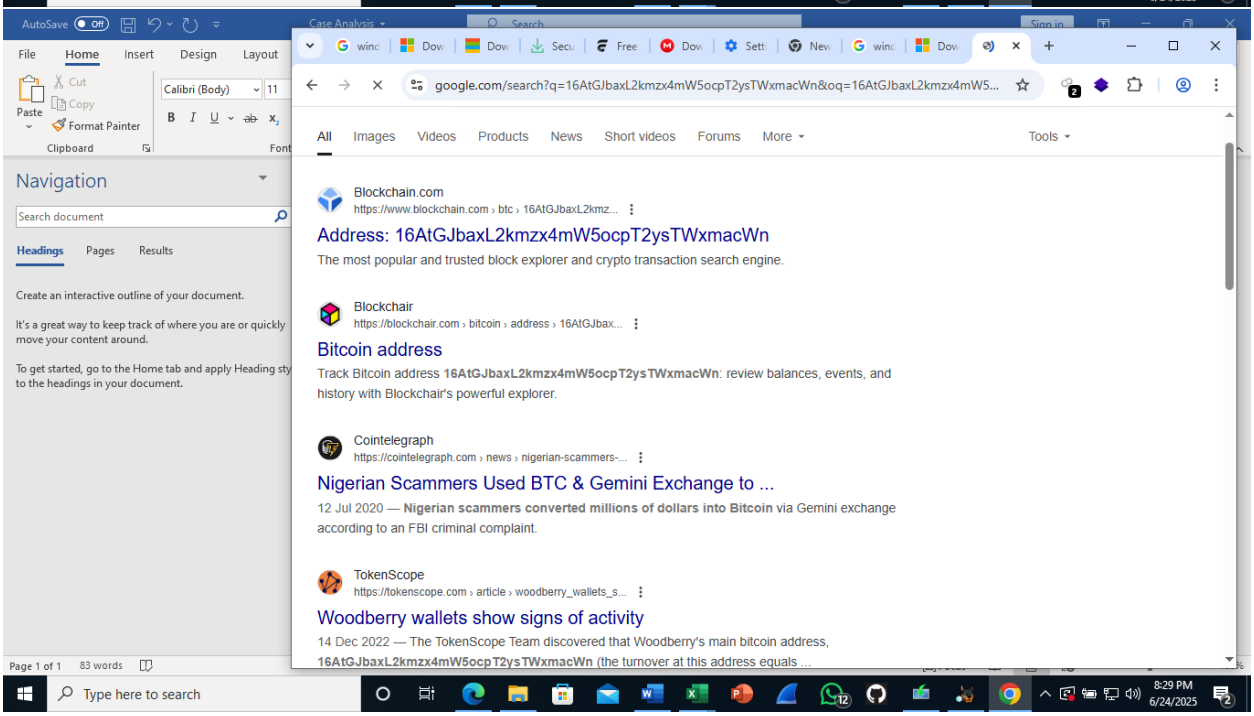

DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (28)
Communication Accounts (20)
Installed Programs (10)
Messages (18)
Web Cookies (414)
Web History (24)
Web Search (8)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Call Logs
28 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Start Date/Time Phone Number Data Source
android_image.tar 0 2024-03-16 20:45:54 WAT +971565505984 LogicalFileSet1
android_image.tar 0 2024-03-16 20:49:50 WAT 08032111669 LogicalFileSet1
android_image.tar 0 2024-03-16 20:51:59 WAT 08032111225 LogicalFileSet1
android_image.tar 0 2024-03-17 02:54:56 WAT 08032111669 LogicalFileSet1
android_image.tar 0 2024-03-17 16:17:36 WAT 08032111225 LogicalFileSet1
android_image.tar 0 2024-03-17 16:18:04 WAT 08032111225 LogicalFileSet1
android_image.tar 0 2024-03-17 16:18:22 WAT 08032111225 LogicalFileSet1
android_image.tar 0 2024-03-17 16:21:46 WAT 08012345678 LogicalFileSet1
android_image.tar 0 2024-03-17 16:24:09 WAT 08032111669 LogicalFileSet1
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Type here to search
7:15 PM
6/24/2025

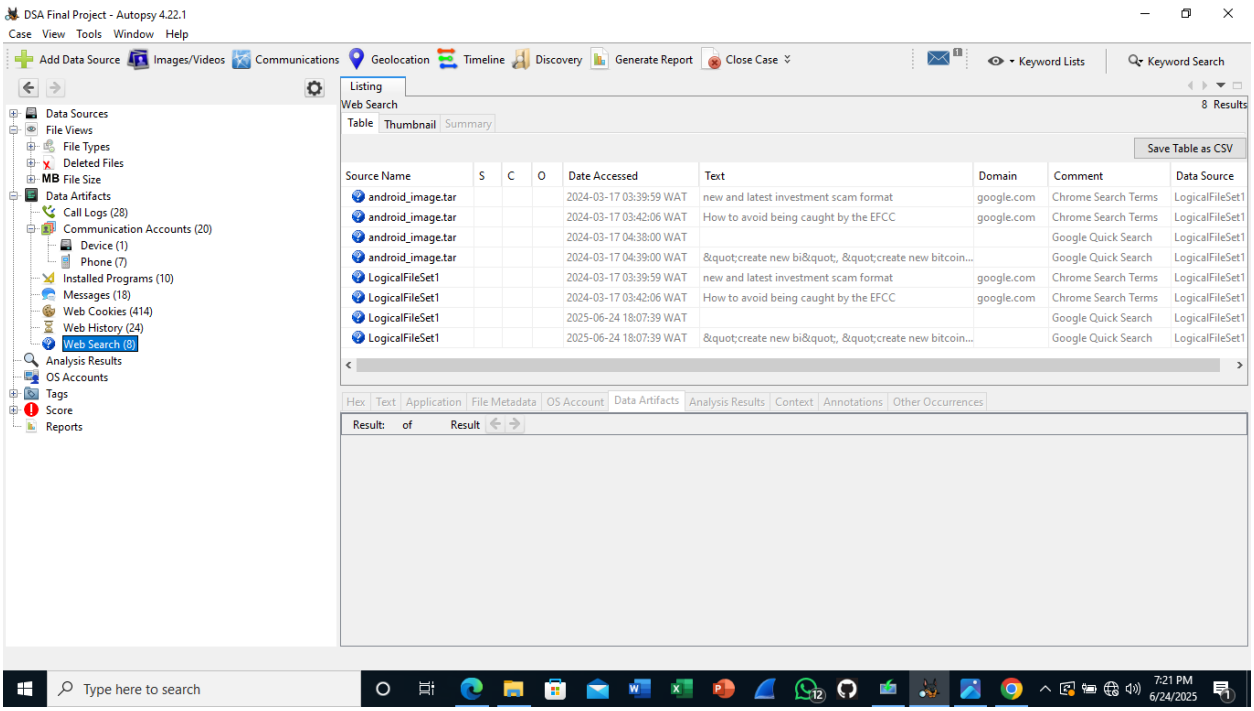

DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (14)
Communication Accounts (8)
Installed Programs (5)
Messages (9)
Web Cookies (207)
Web History (12)
Web Search (4)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Deleted Files
2 Results
Table Thumbnail Summary
Save Table as CSV
Type
File System (0)
All (0)
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Android Analyzer (aLEAPP) for LogicalFileSet1
Type here to search
7:13 PM
6/24/2025

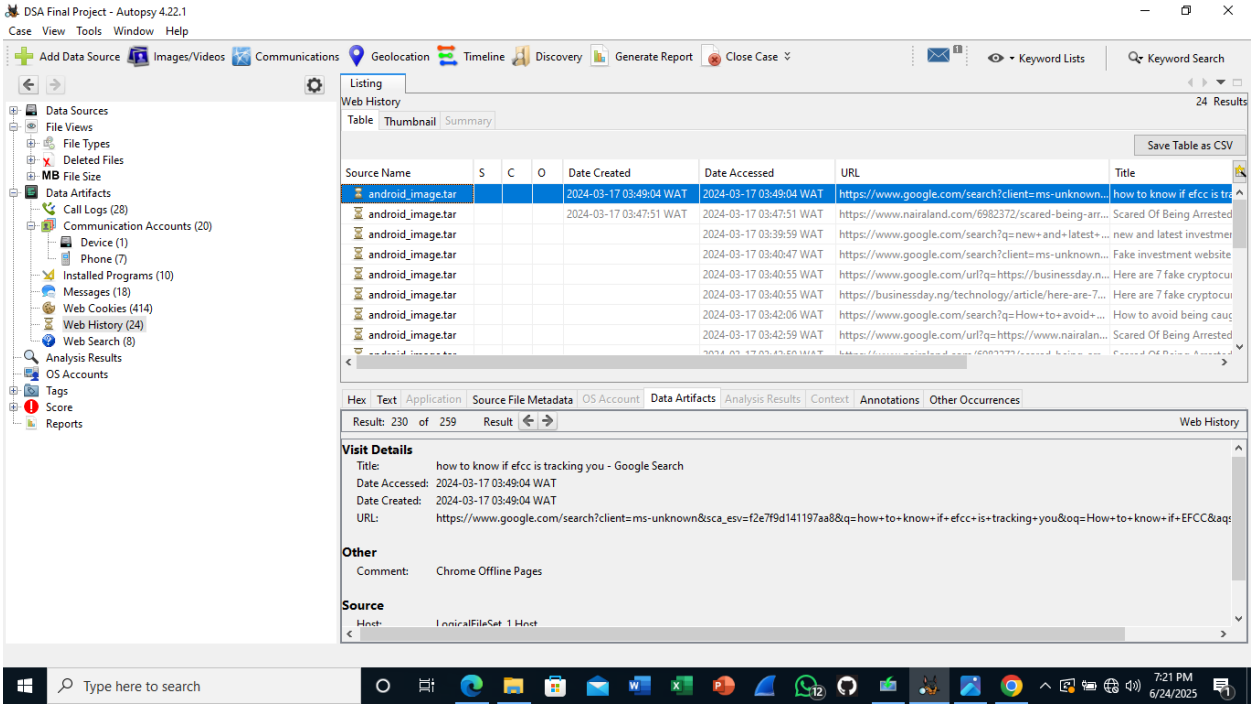

DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (28)
Communication Accounts (20)
Device (1)
Phone (7)
Installed Programs (10)
Messages (18)
Web Cookies (414)
Web History (24)
Web Search (8)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Web Search
8 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Date Accessed Text Domain Comment Data Source
android_image.tar 2024-03-17 03:39:59 WAT new and latest investment scam format google.com Chrome Search Terms LogicalFileSet1
android_image.tar 2024-03-17 03:42:06 WAT How to avoid being caught by the EFCC google.com Chrome Search Terms LogicalFileSet1
android_image.tar 2024-03-17 04:38:00 WAT Google Quick Search LogicalFileSet1
android_image.tar 2024-03-17 04:39:00 WAT "create new bi" "create new bitcoin... Google Quick Search LogicalFileSet1
LogicalFileSet1 2024-03-17 03:39:59 WAT new and latest investment scam format google.com Chrome Search Terms LogicalFileSet1
LogicalFileSet1 2024-03-17 03:42:06 WAT How to avoid being caught by the EFCC google.com Chrome Search Terms LogicalFileSet1
LogicalFileSet1 2025-06-24 18:07:39 WAT Google Quick Search LogicalFileSet1
LogicalFileSet1 2025-06-24 18:07:39 WAT "create new bi" "create new bitcoin... Google Quick Search LogicalFileSet1
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 232 of 259 Result
Web Search
Web Search
Term: new and latest investment scam format
Time: 2024-03-17 03:39:59 WAT
Domain: google.com
Other
Comment: Chrome Search Terms
Source
Host: LogicalFileSet_1 Host
Data Source: LogicalFileSet1
Type here to search
7:21 PM
6/24/2025

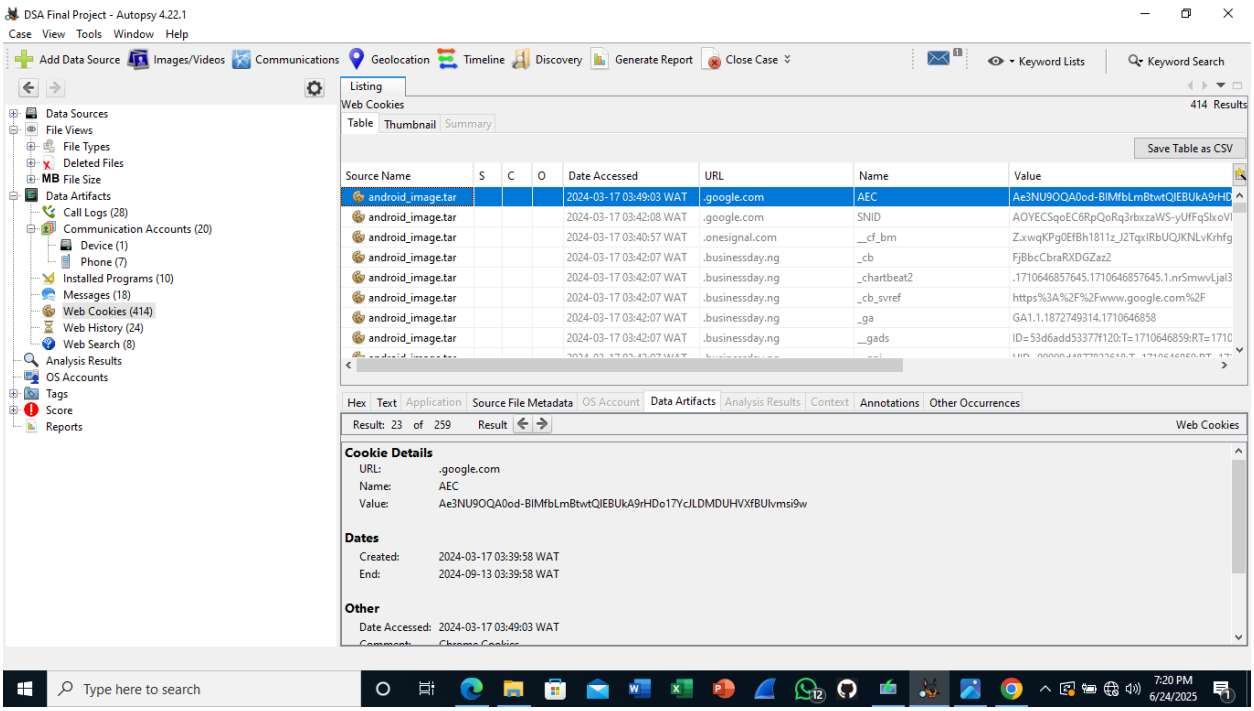

FINAL PROJECT PROPOSAL.pdf
DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Ca Keyword Lists Keyword Search
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (14)
Communication Accounts (8)
Installed Programs (5)
Messages (9)
Web Cookies (207)
Web History (12)
Web Search (4)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Data Sources
1 Results
Table Thumbnail Summary
Save Table as CSV
Name
LogicalFileSet_1 Host
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Android Analyzer (aLEAPP) for LogicalFileSet1
WAN and LAN interfaces
Type here to search
7:07 PM
6/24/2025
AutoSave
File Home Insert Design Layout
Paste Cut Copy Format Painter
Clipboard
Navigation
Search document
Headings Pages Results
Create an interactive outline of your document.
It's a great way to keep track of where you are or quickly move your content around.
To get started, go to the Home tab and apply Heading sty to the headings in your document.
Page 1 of 1 83 words
bitcointalk.org/index.php?topic=5261497.0
Bitcoin Forum
simple machines forum
June 24, 2025, 07:31:05 PM
Welcome, Guest. Please login or register.
News: Pizza day contest voting
Search
HOME HELP SEARCH LOGIN REGISTER MORE
Bitcoin Forum > Bitcoin > Bitcoin Discussion > How was FBI able to locate which Bitcoin wallet is Woodberry's?
« previous topic next topic »
Pages: [1]
print
Author
Topic: How was FBI able to locate which Bitcoin wallet is Woodberry's? (Read 246 times)
Josefjix (OP)
Hero Member
Activity: 1568
Merit: 548
How was FBI able to locate which Bitcoin wallet is Woodberry's?
July 11, 2020, 08:26:39 AM
#1
I've read he transferred money gotten from his victims to Bitcoins and who disclosed his Bitcoin address to FBI? Is it possible for FBI to just locate one's Bitcoin address?
Quote
Preliminary blockchain analysis done by the FBI indicated that the 29-year-old received at least 1,494.71506296 bitcoin related to these BEC schemes, valued at over $6 million dollars at the time he received the proceeds.
"Mark instructed Individual B and Individual A to send money to the bitcoin wallet 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn ("the 16AtGJ BTC Wallet") on at least nine occasions.
"Records obtained from Bitpay, a processor of cryptocurrency transactions, indicated that between approximately September 18, 2015 and November 29, 2016, the 16AtGJ BTC wallet made five purchases associated with the Gmail account hustleandbustle@gmail[.]com (the "hustle Gmail account").
1win
Enjoy 500% bonus + 70 FS
bitcointalk.org image proxy:
Invalid image
Type here to search
8:31 PM
6/24/2025

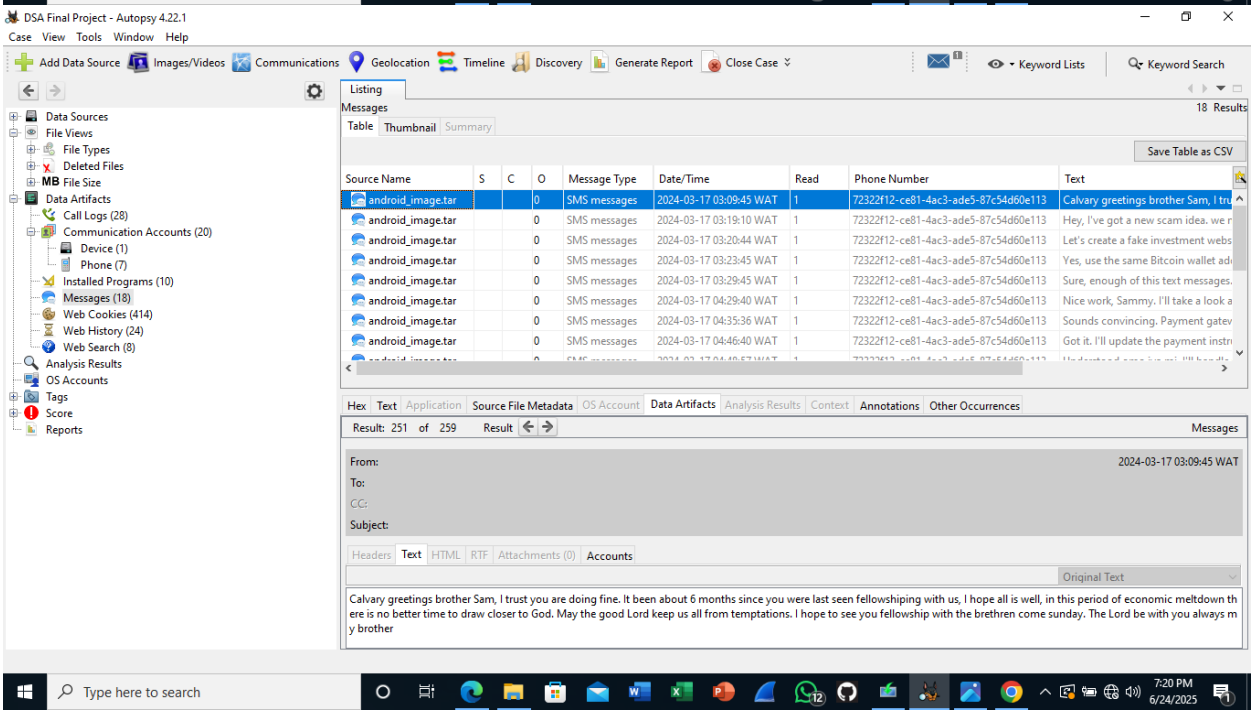

File Home Insert Design Layout
Navigation
Search document
Headings Pages Results
Create an interactive outline of your document.
It's a great way to keep track of where you are or quickly move your content around.
To get started, go to the Home tab and apply Heading sty to the headings in your document.
Page 1 of 1 83 words
google.com/search?q=16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn&oq=16AtGJbaxL2kmzx4mW5...
All Images Videos Products News Short videos Forums More Tools
Blockchain.com
https://www.blockchain.com › btc › 16AtGJbaxL2kmz...
Address: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn
The most popular and trusted block explorer and crypto transaction search engine.
Blockchair
https://blockchair.com › bitcoin › address › 16AtGJbax...
Bitcoin address
Track Bitcoin address 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn: review balances, events, and history with Blockchair's powerful explorer.
Cointelegraph
https://cointelegraph.com › news › nigerian-scammers-...
Nigerian Scammers Used BTC & Gemini Exchange to ...
12 Jul 2020 — Nigerian scammers converted millions of dollars into Bitcoin via Gemini exchange according to an FBI criminal complaint.
TokenScope
https://tokenscope.com › article › woodberry_wallets_s...
Woodberry wallets show signs of activity
14 Dec 2022 — The TokenScope Team discovered that Woodberry's main bitcoin address, 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn (the turnover at this address equals ...
Type here to search
8:30 PM
6/24/2025


File Home Insert Design Layout
Navigation
Search document
Headings Pages Results
Create an interactive outline of your document.
It's a great way to keep track of where you are or quickly move your content around.
To get started, go to the Home tab and apply Heading sty to the headings in your document.
Page 1 of 1 83 words
google.com/search?q=16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn&oq=16AtGJbaxL2kmzx4mW5...
All Images Videos Products News Short videos Forums More Tools
Blockchain.com
https://www.blockchain.com › btc › 16AtGJbaxL2kmz...
Address: 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn
The most popular and trusted block explorer and crypto transaction search engine.
Blockchair
https://blockchair.com › bitcoin › address › 16AtGJbax...
Bitcoin address
Track Bitcoin address 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn: review balances, events, and history with Blockchair's powerful explorer.
Cointelegraph
https://cointelegraph.com › news › nigerian-scammers-...
Nigerian Scammers Used BTC & Gemini Exchange to ...
12 Jul 2020 — Nigerian scammers converted millions of dollars into Bitcoin via Gemini exchange according to an FBI criminal complaint.
TokenScope
https://tokenscope.com › article › woodberry_wallets_s...
Woodberry wallets show signs of activity
14 Dec 2022 — The TokenScope Team discovered that Woodberry's main bitcoin address, 16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn (the turnover at this address equals ...
Type here to search
8:29 PM
6/24/2025


DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Web Search
8 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Date Accessed Text Domain Comment Data Source
android_image.tar 2024-03-17 03:39:59 WAT new and latest investment scam format google.com Chrome Search Terms LogicalFileSet1
android_image.tar 2024-03-17 03:42:06 WAT How to avoid being caught by the EFCC google.com Chrome Search Terms LogicalFileSet1
android_image.tar 2024-03-17 04:38:00 WAT Google Quick Search LogicalFileSet1
android_image.tar 2024-03-17 04:39:00 WAT "create new bi", "create new bitcoin... Google Quick Search LogicalFileSet1
LogicalFileSet1 2024-03-17 03:39:59 WAT new and latest investment scam format google.com Chrome Search Terms LogicalFileSet1
LogicalFileSet1 2024-03-17 03:42:06 WAT How to avoid being caught by the EFCC google.com Chrome Search Terms LogicalFileSet1
LogicalFileSet1 2025-06-24 18:07:39 WAT Google Quick Search LogicalFileSet1
LogicalFileSet1 2025-06-24 18:07:39 WAT "create new bi", "create new bitcoin... Google Quick Search LogicalFileSet1
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: of Result
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (28)
Communication Accounts (20)
Device (1)
Phone (7)
Installed Programs (10)
Messages (18)
Web Cookies (414)
Web History (24)
Web Search (8)
Analysis Results
OS Accounts
Tags
Score
Reports
Type here to search
7:21 PM
6/24/2025


DSA Final Project - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
Web History
24 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Date Created Date Accessed URL Title
android_image.tar 2024-03-17 03:49:04 WAT 2024-03-17 03:49:04 WAT https://www.google.com/search?client=ms-unknown... how to know if efcc is tra
android_image.tar 2024-03-17 03:47:51 WAT 2024-03-17 03:47:51 WAT https://www.nairaland.com/6982372/scared-being-arr... Scared Of Being Arrested
android_image.tar 2024-03-17 03:39:59 WAT https://www.google.com/search?q=new+and+latest+... new and latest investmer
android_image.tar 2024-03-17 03:40:47 WAT https://www.google.com/search?client=ms-unknown... Fake investment website
android_image.tar 2024-03-17 03:40:55 WAT https://www.google.com/url?q=https://businessday.n... Here are 7 fake cryptocu
android_image.tar 2024-03-17 03:40:55 WAT https://businessday.ng/technology/article/here-are-7... Here are 7 fake cryptocu
android_image.tar 2024-03-17 03:42:06 WAT https://www.google.com/search?q=How+to+avoid+... How to avoid being caug
android_image.tar 2024-03-17 03:42:59 WAT https://www.google.com/url?q=https://www.nairalan... Scared Of Being Arrested
Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Result: 230 of 259 Result
Web History
Visit Details
Title: how to know if efcc is tracking you - Google Search
Date Accessed: 2024-03-17 03:49:04 WAT
Date Created: 2024-03-17 03:49:04 WAT
URL: https://www.google.com/search?client=ms-unknown&sca_esv=f2e7f9d141197aa8&q=how+to+know+if+efcc+is+tracking+you&oq=How+to+know+if+EFCC&aq
Other
Comment: Chrome Offline Pages
Source
Host: LogicalFileSet 1 Host
Data Sources
File Views
File Types
Deleted Files
File Size
Data Artifacts
Call Logs (28)
Communication Accounts (20)
Device (1)
Phone (7)
Installed Programs (10)
Messages (18)
Web Cookies (414)
Web History (24)
Web Search (8)
Analysis Results
OS Accounts
Tags
Score
Reports
Type here to search
7:21 PM
6/24/2025





4. Findings of the Investigation

The forensic investigation yielded significant findings that shed light on the operation of the internet fraud scheme, the tactics employed by the perpetrators, and the extent of their illicit activities. The findings are categorized to provide a clear understanding of the various facets of the fraud.

Website Infrastructure and Deception: The fraudulent investment website was meticulously designed to appear legitimate, mimicking the aesthetics and functionalities of genuine cryptocurrency investment platforms. Analysis of the website's infrastructure revealed

Luring Tactics and Social Engineering: The perpetrators employed sophisticated social engineering tactics to attract and deceive victims

Cryptocurrency Transaction Analysis
The core of the fraud involved the illicit acquisition of legitimate cryptocurrency from victims. Analysis of blockchain data and associated transactions revealed

Conclusion

Sequel to the evidence above, it's safe to say the suspect is suspected to be involved in the internet related fraud activities having links with international internet fraudsters. Although there is no evidence of committing the actual act of defrauding anyone yet but I guess he is in the process of achieving that.

Recommendations

Based on the findings of this investigation, the following recommendations are put forth to aid in ongoing efforts to combat such frauds, enhance cybersecurity, and protect potential victims:

Enhanced Public Awareness Campaigns: Launch widespread public awareness campaigns to educate individuals about the red flags of investment scams, particularly those involving cryptocurrencies. Emphasize the importance of due diligence, skepticism towards unrealistic returns, and verification of platform legitimacy.

Strengthened Collaboration with Hosting Providers and Domain Registrars: Foster closer collaboration between law enforcement agencies and internet service providers, hosting companies, and domain registrars to facilitate the rapid identification, takedown, and preservation of evidence from fraudulent websites. Implement mechanisms for quicker response to abuse reports.

Improved Cryptocurrency Tracing Capabilities: Continue to invest in and develop advanced blockchain analytics tools and techniques to enhance the ability to trace illicit cryptocurrency flows, de-anonymize perpetrators, and identify associated entities. Encourage greater information sharing among blockchain intelligence firms and law enforcement.

International Cooperation: Given the transnational nature of internet fraud and cryptocurrency scams, strengthen international cooperation among law enforcement agencies, regulatory bodies, and financial intelligence units to

facilitate cross-border investigations, asset freezing, and extradition of perpetrators.

Regulatory Framework Development: Advocate for the development and enforcement of robust regulatory frameworks for cryptocurrency platforms and digital asset services, including mandatory KYC (Know Your Customer) and AML (Anti-Money Laundering) compliance, to prevent their exploitation by fraudsters.