



---

# ANDROID MOBILE FORENSICS INVESTIGATION: ARTIFACT EXTRACTION AND ANALYSIS

---

CYBER SECURITY CAPSTONE PROJECT



REPORT ADDRESSED TO: INSTRUCTOR

PREPARED BY EUNICE ALAO

CASE NUMBER: 007

EVIDENCE FILENAME: ANDROID\_IMAGE.DD

JULY 18, 2025  
THE INCUBATOR HUB

# Introduction

This report presents a digital forensic analysis of a provided Android device image. The objective was to simulate a real-world mobile investigation by extracting and examining key artifacts such as SMS messages, call logs, contacts, browser history, application data, and deleted content. The investigation aimed to uncover user activity patterns and potential digital evidence that may be relevant to a legal or security-related inquiry.

## Tools Used

1. Autopsy
2. 7-zip File Manager

## Methodology

To begin the forensic investigation, the provided Android image file was first extracted using 7-Zip, a reliable open-source utility for handling compressed archives. Once the image was successfully extracted, Autopsy, a digital forensics platform was used to analyze the contents of the image.

A new case was created in Autopsy, and the extracted image file was added as the primary data source. The platform automatically indexed the file system and parsed key artifact categories including communications (SMS, call logs, contacts), web activity, images, application data, and deleted content. Each artifact was then reviewed manually within the Autopsy interface, and relevant findings were documented through screenshots and notes for inclusion in this report.

## Findings

### SMS and Call Log Analysis

A total of 8 SMS messages were recovered during the forensic analysis of the Android image. These messages revealed an ongoing fraudulent planning and collaboration. These involved discussions around creating a fake investment platform, soliciting victims using false promises, and transacting through cryptocurrency to avoid traceability. Notable artifacts include:

- A proposal for a scam involving fake cryptocurrency investments
- Reference to a previously used Bitcoin wallet address:  
16AtGJbaxL2kmzx4mW5ocpT2ysTWxmacWn

- Operational terms such as “promotional activities,” “payment gateway,” and “when we dey go live?” clearly point to premeditated cybercrime.
- Use of code-switching (mix of English and informal language), indicating familiarity and possible attempt at concealment.

Screenshots of some of the message threads were taken to document the artifacts.

com.google.android.music (2)  
com.google.android.onetimeinitializer (2)  
com.google.android.packageinstaller (3)  
com.google.android.partnersetup (2)  
com.google.android.printservice.recommend  
com.google.android.sdksetup (2)  
com.google.android.setupwizard (3)  
com.google.android.syncadapters.contacts (2)  
com.google.android.tts (8)  
com.google.android.videos (2)  
com.google.android.webview (2)  
com.google.android.youtube (3)  
com.squareup.cash (4)  
com.twitter.android (4)  
com.us.two.lwp (2)  
com.whatsapp (2)  
org.chromium.webview\_shell (2)  
walletrust.apkpy.crypto (2)  
vendor (5)  
vendor\_ce (1)  
vendor\_de (1)

jes  
d Files  
e  
acts  
gs (14)  
unication Accounts (12)  
rice (1)  
jne (7)  
d Programs (5)  
jes (9)  
ookies (207)  
istory (12)  
arch (4)  
results  
its

Source NameS C O Message Type Date/Time Read Phone Number Text Thread ID

mmssms.db0 SMS messages 2024-03-17 03:09:45 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Calvary greetings brother Sam, I trust you are doing fine 4

mmssms.db0 SMS messages 2024-03-17 03:19:10 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Hey, I've got a new scam idea. we need to discuss. 5

mmssms.db0 SMS messages 2024-03-17 03:20:44 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Let's create a fake investment website and lure people in 5

mmssms.db0 SMS messages 2024-03-17 03:23:45 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Yes, use the same Bitcoin wallet address as before: 16At 5

mmssms.db0 SMS messages 2024-03-17 03:29:45 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Sure, enough of this text messages. Meet me over Goog 5

mmssms.db0 SMS messages 2024-03-17 04:29:40 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Nice work, Sammy. I'll take a look at the site. Are we usir 6

mmssms.db0 SMS messages 2024-03-17 04:35:36 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Sounds convincing. Payment gateway nkor? Are we still . 6

mmssms.db0 SMS messages 2024-03-17 04:46:40 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Got it. I'll update the payment instructions on the websit 6

mmssms.db0 SMS messages 2024-03-17 04:48:57 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Understood omo iya mi. I'll handle the promotional acti 6

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 5 of 13 Result

Messages

From: 2024-03-17 03:19:10 EDT

To:

CC:

Subject:

Headers Text HTML RTF Attachments (0) Accounts

Original Text

Hey, I've got a new scam idea. we need to discuss.

com.google.android.music (2)  
com.google.android.onetimeinitializer (2)  
com.google.android.packageinstaller (3)  
com.google.android.partnersetup (2)  
com.google.android.printservice.recommend  
com.google.android.sdksetup (2)  
com.google.android.setupwizard (3)  
com.google.android.syncadapters.contacts (2)  
com.google.android.tts (8)  
com.google.android.videos (2)  
com.google.android.webview (2)  
com.google.android.youtube (3)  
com.squareup.cash (4)  
com.twitter.android (4)  
com.us.two.lwp (2)  
com.whatsapp (2)  
org.chromium.webview\_shell (2)  
rust.apkpy.crypto (2)

s (12)

Source NameS C O Message Type Date/Time Read Phone Number Text Thread ID

mmssms.db0 SMS messages 2024-03-17 03:09:45 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Calvary greetings brother Sam, I trust you are doing fine 4

mmssms.db0 SMS messages 2024-03-17 03:19:10 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Hey, I've got a new scam idea. we need to discuss. 5

mmssms.db0 SMS messages 2024-03-17 03:20:44 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Let's create a fake investment website and lure people in 5

mmssms.db0 SMS messages 2024-03-17 03:23:45 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Yes, use the same Bitcoin wallet address as before: 16At 5

mmssms.db0 SMS messages 2024-03-17 03:29:45 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Sure, enough of this text messages. Meet me over Goog 5

mmssms.db0 SMS messages 2024-03-17 04:29:40 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Nice work, Sammy. I'll take a look at the site. Are we usir 6

mmssms.db0 SMS messages 2024-03-17 04:35:36 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Sounds convincing. Payment gateway nkor? Are we still . 6

mmssms.db0 SMS messages 2024-03-17 04:46:40 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Got it. I'll update the payment instructions on the websit 6

mmssms.db0 SMS messages 2024-03-17 04:48:57 EDT 1 890852c0-64c3-45dc-89f3-c96432674654 Understood omo iya mi. I'll handle the promotional acti 6

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 6 of 13 Result

Messages

From: 2024-03-17 03:20:44 EDT

To:

CC:

Subject:

Headers Text HTML RTF Attachments (0) Accounts

Original Text

Let's create a fake investment website and lure people into investing in a non-existent cryptocurrency. We'll promise huge returns.

com.google.android.inputmethod.pinyin (2)	
com.google.android.music (2)	
com.google.android.onetimeinitializer (2)	
com.google.android.packageinstaller (3)	
com.google.android.partnersetup (2)	
com.google.android.printservice.recommen	
com.google.android.sdksetup (2)	
com.google.android.syncwiz	
com.google.android.syncwiz (3)	
com.google.android.syncadapters.contacts (	
com.google.android.tts (8)	
com.google.android.videos (2)	
com.google.android.webview (2)	
com.google.android.youtube (3)	
com.squareup.cash (4)	
com.twitter.android (4)	
com.musto.hwp (2)	
com.whatsapp (2)	
org.chromium.webview_shell (2)	
wallettrustapp/jpy/crypto (2)	
ndor (5)	
ndor_ce (1)	
ndor_de (1)	

  

Source Name	S	C	O	Message Type	Date/Time	Read	Phone Number	Text	Thread ID
mmssms.db	0		0	SMS messages	2024-03-17 03:09:45 EDT	1	890852c0-64c3-45dc-89f3-c96432674654	Calvary greetings brother Sam, I trust you are doing fine	4
mmssms.db	0		0	SMS messages	2024-03-17 03:19:10 EDT	1	890852c0-64c3-45dc-89f3-c96432674654	Hey, I've got a new scam idea, we need to discuss.	5
mmssms.db	0		0	SMS messages	2024-03-17 03:20:44 EDT	1	890852c0-64c3-45dc-89f3-c96432674654	Let's create a fake investment website and lure people in	5
mmssms.db	0		0	SMS messages	2024-03-17 03:23:45 EDT	1	890852c0-64c3-45dc-89f3-c96432674654	Yes, use the same Bitcoin wallet address as before: 16At.5	5
mmssms.db	0		0	SMS messages	2024-03-17 03:29:45 EDT	1	890852c0-64c3-45dc-89f3-c96432674654	Sure, enough of this text messages. Meet me over Goog	5
mmssms.db	0		0	SMS messages	2024-03-17 04:29:40 EDT	1	890852c0-64c3-45dc-89f3-c96432674654	Nice work, Sammy. I'll take a look at the site. Are we usin	6
mmssms.db	0		0	SMS messages	2024-03-17 04:35:36 EDT	1	890852c0-64c3-45dc-89f3-c96432674654	Sounds convincing, Payment gateway nkor? Are we still i	6
mmssms.db	0		0	SMS messages	2024-03-17 04:46:40 EDT	1	890852c0-64c3-45dc-89f3-c96432674654	Got it, I'll update the payment instructions on the websit	6
mmssms.db	0		0	SMS messages	2024-03-17 04:48:57 EDT	1	890852c0-64c3-45dc-89f3-c96432674654	Understood omo Iya mi, I'll handle the promotional acti	6

  

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 7	of 13	Result							
From:									2024-03-17 03:23:45 EDT
To:									
CC:									
Subject:									
Headers	Text	HTML	RTF	Attachments (0)	Accounts				
Yes, use the same Bitcoin wallet address as before: 16AtGlbaxL2kmz4mW5ocpT2yTWxmacWn.									Original Text

The call log artifact contained records of 14 outgoing calls made to 7 unique phone numbers. Due to the nature of the associated SMS messages, it is plausible that some or all these contacts were linked to the planning or execution of the suspected fraudulent scheme. Each call log entry included a call ID.

## Application Usage History

Analysis of the installed applications on the Android image revealed the presence and usage of several high-interest apps, suggesting the device owner's behavioural and digital footprint. Notably, the following applications were identified: YouTube, twitter, WhatsApp, Square up cash app, and Trust wallet.

The presence of these applications, particularly Cash App and Trust Wallet, in conjunction with SMS messages discussing a fake investment scam, indicates deliberate use of crypto-fintech tools to conceal financial trails. Combined with communication apps like WhatsApp and Twitter, the device likely served as a hub for both planning and executing digital fraud.

## Browser History Analysis

The suspect's browser history reveals a pattern of visits and searches that suggest an intent to engage in fraudulent online activities and a concern about law enforcement tracking. Key websites accessed include:

- Google – Used for multiple search queries.

**com.google.a**

**com.google.a**

**com.google.a**

**com.google.a**

**com.google.a**

**com.google.a**

**com.google.a**

**com.google.a**

**com.google.a**

**com.google.a**

**com.squareu**

**com.twitter.a**

**com.ustwo.lw**

**com.whatsap**

**org.chromium**

**wallettrust.ap**

Source Name	S	C	O	Date Created	Date Accessed	URL	Title
LogicalFileSet1				2024-03-17 03:49:04 EDT	2024-03-17 03:49:04 EDT	https://www.google.com/search?client=ms-unknown&... how to know if efcc is tracking you - Google Search	how to know if efcc is tracking you - Google Search
LogicalFileSet1				2024-03-17 03:47:51 EDT	2024-03-17 03:47:51 EDT	https://www.nairaland.com/6982372/scared-being-arres Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria
LogicalFileSet1					2024-03-17 03:39:59 EDT	https://www.google.com/search?q=new+and+latest+in_ new and latest investment scam format - Google Sea	new and latest investment scam format - Google Sea
LogicalFileSet1					2024-03-17 03:40:47 EDT	https://www.google.com/search?client=ms-unknown&... Fake investment website - Google Search	Fake investment website - Google Search
LogicalFileSet1					2024-03-17 03:40:55 EDT	https://www.google.com/url?q=https://businessday.ng/. Here are 7 fake cryptocurrency investment platforms	Here are 7 fake cryptocurrency investment platforms
LogicalFileSet1					2024-03-17 03:40:55 EDT	https://businessday.ng/technology/article/here-are-7-fa Here are 7 fake cryptocurrency investment platforms	Here are 7 fake cryptocurrency investment platforms
LogicalFileSet1					2024-03-17 03:42:06 EDT	https://www.google.com/search?q=How+to+avoid+b... How to avoid being caught by the EFCC - Google Ser	How to avoid being caught by the EFCC - Google Ser
LogicalFileSet1					2024-03-17 03:42:59 EDT	https://www.google.com/url?q=https://www.nairaland... Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria
LogicalFileSet1					2024-03-17 03:42:59 EDT	https://www.nairaland.com/6982372/scared-being-arres Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria
LogicalFileSet1					2024-03-17 03:48:57 EDT	https://www.google.com/search?client=ms-unknown&... how to know if efcc is tracking you - Google Search	how to know if efcc is tracking you - Google Search
LogicalFileSet1					2024-03-17 03:48:31 EDT	https://www.google.com/url?q=https://www.nairaland... EFCC Devises Discreet Means Of Tracking Yahoo Boy	EFCC Devises Discreet Means Of Tracking Yahoo Boy
LogicalFileSet1					2024-03-17 03:48:51 EDT	https://www.nairaland.com/5033957/efcc-devises-discr... EFCC Devises Discreet Means Of Tracking Yahoo Boy	EFCC Devises Discreet Means Of Tracking Yahoo Boy

**Vendor**

- vendor (5)
- vendor\_ce (1)
- vendor\_de (1)

**aws**

**Types**

**Files**

**Size**

**rtifacts**

**I Logs (14)**

**munication Accounts (12)**

**Device (1)**

**Phone (7)**

**talled Programs (5)**

**sages (9)**

**b Cookies (207)**

**History (12)**

**Search (4)**

**is Results**

**counts**

**Hex** | **Text** | **Application** | **Source File Metadata** | **OS Account** | **Data Artifacts** | **Analysis Results** | **Context** | **Annotations** | **Other Occurrences**

Result: 230 of 250    Result    🔍 ➡️

---

### Visit Details

**Title:** how to know if efcc is tracking you - Google Search

**Date Accessed:** 2024-03-17 03:49:04 EDT

**Date Created:** 2024-03-17 03:49:04 EDT

**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&aqs=heirloom-srp.0l03

---

### Other

**Comment:** Chrome Offline Pages

---

### Source

**Host:** LogicalFileSet 1 Host

Listing

Web History

Source Name	S	C	O	Date Created	Date Accessed	URL	Title	Comment
LogicalFileSet1				2024-03-17 03:49:04 EDT	2024-03-17 03:49:04 EDT	https://www.google.com/search?client=ms-unknown&... how to know if efcc is tracking you - Google Search	how to know if efcc is tracking you - Google Search	Chrome Offline Pag
LogicalFileSet1				2024-03-17 03:47:51 EDT	2024-03-17 03:47:51 EDT	https://www.nairaland.com/6982372/scared-being-arres Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome Offline Pag
LogicalFileSet1					2024-03-17 03:39:59 EDT	https://www.google.com/search?q=new+and+latest+in. new and latest investment scam format - Google Search	new and latest investment scam format - Google Search	Chrome History
LogicalFileSet1					2024-03-17 03:40:47 EDT	https://www.google.com/search?client=ms-unknown&... Fake investment website - Google Search	Fake investment website - Google Search	Chrome History
LogicalFileSet1					2024-03-17 03:40:55 EDT	https://www.google.com/url?q=https://businessday.ng/. Here are 7 fake cryptocurrency investment platforms on. Chrome History	Here are 7 fake cryptocurrency investment platforms on. Chrome History	Chrome History
LogicalFileSet1					2024-03-17 03:40:55 EDT	https://businessday.ng/technology/article/here-are-7-fa Here are 7 fake cryptocurrency investment platforms on. Chrome History	Here are 7 fake cryptocurrency investment platforms on. Chrome History	Chrome History
LogicalFileSet1					2024-03-17 03:42:06 EDT	https://www.google.com/search?q=How+to+avoid+b... How to avoid being caught by the EFCC - Google Searc	How to avoid being caught by the EFCC - Google Searc	Chrome History
LogicalFileSet1					2024-03-17 03:42:59 EDT	https://www.google.com/url?q=https://www.nairaland... Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History
LogicalFileSet1					2024-03-17 03:42:59 EDT	https://www.nairaland.com/6982372/scared-being-arres Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History
LogicalFileSet1					2024-03-17 03:48:57 EDT	https://www.google.com/search?client=ms-unknown&... how to know if efcc is tracking you - Google Search	how to know if efcc is tracking you - Google Search	Chrome History
LogicalFileSet1					2024-03-17 03:48:31 EDT	https://www.google.com/url?q=https://www.nairaland... EFCC Devises Discreet Means Of Tracking Yahoo Boys.... Chrome History	EFCC Devises Discreet Means Of Tracking Yahoo Boys.... Chrome History	Chrome History
LogicalFileSet1					2024-03-17 03:48:51 EDT	https://www.nairaland.com/5033957/efcc-devises-discr... EFCC Devises Discreet Means Of Tracking Yahoo Boys.... Chrome History	EFCC Devises Discreet Means Of Tracking Yahoo Boys.... Chrome History	Chrome History

Result: 231 of 250

Visit Details

Title: Scared Of Being Arrested By EFCC - Crime - Nigeria

Date Accessed: 2024-03-17 03:47:51 EDT

Date Created: 2024-03-17 03:47:51 EDT

URL: https://www.nairaland.com/6982372/scared-being-arrested-efcc

Other

Comment: Chrome Offline Pages

Source

Listing

Web History

Source Name	S	C	O	Date Created	Date Accessed	URL	Title	Comment
LogicalFileSet1				2024-03-17 03:49:04 EDT	2024-03-17 03:49:04 EDT	https://www.google.com/search?client=ms-unknown&... how to know if efcc is tracking you - Google Search	how to know if efcc is tracking you - Google Search	Chrome Offline Pages
LogicalFileSet1				2024-03-17 03:47:51 EDT	2024-03-17 03:47:51 EDT	https://www.nairaland.com/6982372/scared-being-arres Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome Offline Pages
LogicalFileSet1					2024-03-17 03:39:59 EDT	https://www.google.com/search?q=new+and+latest+in. new and latest investment scam format - Google Search	new and latest investment scam format - Google Search	Chrome History
LogicalFileSet1					2024-03-17 03:40:47 EDT	https://www.google.com/search?client=ms-unknown&... Fake investment website - Google Search	Fake investment website - Google Search	Chrome History
LogicalFileSet1					2024-03-17 03:40:55 EDT	https://www.google.com/url?q=https://businessday.ng/. Here are 7 fake cryptocurrency investment platforms on. Chrome History	Here are 7 fake cryptocurrency investment platforms on. Chrome History	Chrome History
LogicalFileSet1					2024-03-17 03:40:55 EDT	https://businessday.ng/technology/article/here-are-7-fa Here are 7 fake cryptocurrency investment platforms on. Chrome History	Here are 7 fake cryptocurrency investment platforms on. Chrome History	Chrome History
LogicalFileSet1					2024-03-17 03:42:06 EDT	https://www.google.com/search?q=How+to+avoid+b... How to avoid being caught by the EFCC - Google Searc	How to avoid being caught by the EFCC - Google Searc	Chrome History
LogicalFileSet1					2024-03-17 03:42:59 EDT	https://www.google.com/url?q=https://www.nairaland... Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History
LogicalFileSet1					2024-03-17 03:42:59 EDT	https://www.nairaland.com/6982372/scared-being-arres Scared Of Being Arrested By EFCC - Crime - Nigeria	Scared Of Being Arrested By EFCC - Crime - Nigeria	Chrome History
LogicalFileSet1					2024-03-17 03:48:57 EDT	https://www.google.com/search?client=ms-unknown&... how to know if efcc is tracking you - Google Search	how to know if efcc is tracking you - Google Search	Chrome History
LogicalFileSet1					2024-03-17 03:48:31 EDT	https://www.google.com/url?q=https://www.nairaland... EFCC Devises Discreet Means Of Tracking Yahoo Boys.... Chrome History	EFCC Devises Discreet Means Of Tracking Yahoo Boys.... Chrome History	Chrome History
LogicalFileSet1					2024-03-17 03:48:51 EDT	https://www.nairaland.com/5033957/efcc-devises-discr... EFCC Devises Discreet Means Of Tracking Yahoo Boys.... Chrome History	EFCC Devises Discreet Means Of Tracking Yahoo Boys.... Chrome History	Chrome History

Result: 234 of 250

Visit Details

Title: new and latest investment scam format - Google Search

Date Accessed: 2024-03-17 03:39:59 EDT

URL: https://www.google.com/search?q=new+and+latest+invest+scam+format&oq=new+and+latest+investment+scam+format&aqs=chrome..6957j17928j0j7&client=ms-unknown&sourceid=chrome-mobile&ie=

Other

Comment: Chrome History

Source

## Conclusion and Recommendations

### Conclusion

The forensic examination of the Android device image revealed compelling evidence suggestive of coordinated fraudulent activity which involved planning and potentially executing cyber-enabled financial fraud.

## Recommendation

1. Deeper Dive into Cryptocurrency Transactions
2. Cross-reference findings with law enforcement databases
3. Secure all extracted data and logs for legal proceedings, ensuring the integrity of evidence for prosecution