



By: Keshaben Patel

Executive Summary

This forensic report outlines a comprehensive digital investigation into a suspected conspiracy to commit robbery involving three individuals: Orion, Andromeda, and Cassiopeia. These suspects were believed to be planning a coordinated attack on a high-value target—Notre Dame Stadium—based on evidence extracted from multiple digital sources.

The investigation was conducted using Magnet AXIOM, a leading digital forensics software, to analyze a wide range of artifacts from various digital devices. These included Orion's HP Pavilion Laptop, RAM and Process Captures, Samsung Galaxy S9, and Google Takeout data; Andromeda's iPhone XR and Kingston SD Card; and Cassiopeia's Samsung Galaxy S9 and Facebook account. Each device provided critical insights into the suspects' behaviors, intentions, and communications.

Key findings included detailed Google Maps activity and location tracking showing reconnaissance trips, incriminating web search history related to evading security systems and conducting robberies, and various forms of digital communication—emails, SMS, and Skype chats—discussing logistics and plans. Additionally, media artifacts such as GPS-tagged photos and gear images, and evidence of privacy tools like the TOR browser were identified, suggesting the suspects took measures to cover their tracks.

This report presents a structured narrative linking all findings into a cohesive timeline that reflects planning, coordination, and strategic alignment between the three suspects. Each piece of evidence is supported by visual proof in the form of labeled screenshots included in the appendix.

Overall, the forensic evidence paints a clear picture of premeditated criminal collaboration. This report is structured to be admissible in court and meets professional standards required in digital forensic investigations.

Suspect Overview

2. Objective and Outcome

The digital evidence clearly indicates that the three suspects were working together to plan and execute a robbery targeting Notre Dame Stadium. Orion, identified as the ringleader, coordinated the plan using a wide range of tools and platforms. His HP Pavilion Laptop (Lab 01-01) revealed a downloaded stadium map (stadiummap.pdf, Fig 1.1) and an Excel spreadsheet labeled layout_final.xls that detailed logistics for the heist (Fig 1.3). Orion also used Google Maps extensively, as confirmed through his Google Takeout archive (Lab 01-07), which pinpointed his movements aligning with the initial planning phase, including a recorded stop at 10436 Courtney Ln, Indiana on July 17, 2020 (Fig 1.2). His browsing history showed concerning Bing search terms such as “how much cash at Notre Dame Stadium,” “types of guns pdf,” and “is it suspicious to use only cash,” suggesting clear intent and premeditation (Fig 1.4). To hide his digital footprint, CCleaner was found installed on his system on September 2, 2020 (Fig 1.5), and TOR browser activity was detected in RAM and process captures (Labs 01-02, 01-03), including traces of .onion URLs and active encrypted sessions (Fig 1.6).

Andromeda played a critical role in surveillance and physical security assessment. Her iPhone XR (Lab 02-01) revealed mobile search history containing terms like “avoid infrared sensors” and “spec sheet for eye lock system” (Fig 2.2), indicating an interest in defeating electronic surveillance. Her Kingston SD card (Lab 02-04) stored GPS-tagged photos of Notre Dame Stadium’s entry gates and camera placements, confirming reconnaissance missions (Fig 2.1). One notable image captured her participating in firearm training (Fig 2.3), reinforcing her active role in the operation. Furthermore, her phone contained the encrypted messaging app Signal (Fig 2.4), showing intent to communicate securely. Zoom chat logs extracted from RAM (Labs 01-02/03) revealed that she and Orion coordinated specific entry times, such as discussions around “shift change entry” windows (Fig 2.5).

Cassiopeia, while entering the conspiracy later, served as a tactical and logistical supporter. Her Samsung Galaxy S9 (Lab 03-01) held consistent SMS and call logs with both Orion and Andromeda beginning in late March 2021 (Fig 3.1). Her involvement deepened with digital evidence from her Facebook archive (Lab 03-04), where posts

referenced terms like “silent tools” and “bring the gear,” implying awareness and readiness for action (Fig 3.2). Additionally, she uploaded photos showing tactical equipment (Fig 3.3), and forensic examination of her installed apps confirmed the presence of secure messaging platforms like Telegram (Fig 3.4).

While the outcome of the planned robbery is not explicitly documented in the available artifacts, the depth of digital coordination across multiple devices, encrypted communication, reconnaissance evidence, and logistical planning files strongly supports the conclusion that a premeditated criminal act was imminent or had already been attempted. The convergence of this forensic evidence across laptops, mobile devices, RAM captures, and social media archives builds a complete and compelling picture of a conspiracy among the three suspects.

3. Timeline of Key Activities

4. Evidence Analysis per Suspect

Orion

Laptop (01-01): Orion's HP Pavilion laptop revealed extensive planning activity. Under the Web-Related > Google Maps artifact section, multiple queries and pins were linked to Notre Dame Stadium and surrounding areas, indicating physical reconnaissance planning.

Figure 1.1 - Screenshot of timeline and queries.

Email (01-01): Email artifacts included a conversation where Orion shared an Excel spreadsheet titled "Robbery Plan." This file contained a detailed weapons list and task assignments, directly tying Orion to operational logistics.

Figure 1.2 - Screenshot of email content and attachment.

Skype Logs (01-01): Communication with Cassiopeia in Skype logs revealed planning conversations such as “execute by midnight” and discussed access points and timing. These messages demonstrate active coordination.

Figure A - Suspicious coordination chat.

Samsung Galaxy S9 (01-04): SMS messages with Andromeda revealed discussions about equipment, including a shotgun, and reinforced Orion’s leadership role in organizing materials and timing.

Figure 1.5 - Screenshot of SMS chat.

Google Takeout (01-07): The archive showed Orion had searched for terms like “how to escape police,” “robbery tools,” and “stadium entry.” Location history confirmed travel routes consistent with planning visits.

Figure 1.6 - Screenshot of search and location data.

RAM (01-02) and Process Capture (01-03): Memory analysis showed the presence of TOR browser activity, keywords related to hiring a hitman, and access to anonymous service pages on the dark web. These findings point toward deliberate efforts to conceal communications and actions.

Figure B - Screenshot of suspicious memory content.

Andromeda

iPhone XR (02-01): Andromeda’s Safari browser history includes several alarming search queries. These include “disable motion detector,” “Notre Dame robbery,” “how to climb roofs quietly,” and “escape routes stadium.” These search terms, found under Web Related > Safari Searches, strongly suggest her involvement in planning the physical infiltration of the stadium. The timestamps align closely with Orion’s communications, confirming collaboration.

Figure 2.1 - Screenshot of suspicious web search history.

Kingston SD Card (02-04): The SD card, labeled 02-04, contained 15 images depicting different sections of the Notre Dame Stadium perimeter, entrances, and surrounding areas. Several of these images were GPS-tagged, confirming that Andromeda personally visited the scene to capture reconnaissance photos. These images were likely used to assess entry and exit points.

Figure 2.3 - Image previews with GPS metadata.

Cassiopeia

Samsung Galaxy S9 (03-01): Cassiopeia’s device revealed consistent and frequent communication with both Orion and Andromeda. Call log analysis shows a pattern of coordination during key planning periods, with several long-duration calls occurring just before major activity dates. This indicates her growing involvement in the operation, especially during the later phases.

Figure 3.1 - Screenshot of call history.

Facebook Archive (03-04): Cassiopeia’s Facebook account was examined under Accounts > Facebook. Her posts included references to “silent tools” and shared images of what

appeared to be tactical equipment and gloves, which could be used in a robbery setting. One of the photos showed her in what looked like preparation gear, indicating an awareness or participation in the planned activity. Her Facebook profile picture and other metadata further confirmed her digital identity and linked it to the phone device analyzed.

Figure E - Screenshot of suspicious images and keywords.

Figure 3.3 - Facebook profile picture.

Conclusion

The forensic investigation provides overwhelming evidence that Orion, Andromeda, and Cassiopeia were actively engaged in a coordinated effort to plan and potentially execute a robbery targeting Notre Dame Stadium. The digital artifacts examined across multiple devices consistently reveal a high level of preparation, including reconnaissance, weapon planning, route mapping, and stealth strategies.

Orion led the coordination, leveraging both his laptop and phone to manage logistics, communicate with his accomplices, and erase traces of digital activity. Andromeda was deeply involved in surveillance and physical planning, evident from her suspicious searches and reconnaissance images. Cassiopeia, although involved later, demonstrated readiness and support for the plan through consistent communications and her Facebook activity showing equipment and terminology related to covert operations.

All these findings were validated with supporting screenshots, timestamps, and metadata extracted using Magnet AXIOM. The collective analysis forms a compelling timeline and behavioral pattern that clearly illustrates criminal intent and collaboration. This report is suitable for presentation in legal proceedings as reliable digital forensic evidence.

Appendix

Displays Orion's Google Maps activity showing queries and pins related to Notre Dame Stadium, supporting location scouting.

The screenshot displays a web application interface for Google Maps activity. The top navigation bar includes tabs for 'Item 01-01: HP Laptop...', 'Artifacts', 'Content types', 'Date and time', 'Tags and comments', and 'Notre Dame Stadium'. The main content area is titled 'MATCHING RESULTS (2 of 60)' and shows a table with columns: Search Query, Start..., Latit..., Long..., Locati..., Sour..., Destination Address, and Rout... The table contains two rows, both with the search query 'Notre Dame Stadium' and coordinates 41.6983991, -86.2344632. The right sidebar shows 'Notre Dame Stadium' details, including a 'WORLD MAP PREVIEW' and 'DETAILS' section with 'ARTIFACT INFORMATION'.

Figure 1.1: Google Maps Queries from Orion's Laptop

Shows an email from Orion containing a spreadsheet titled "Robbery Plan," detailing weapons and coordination roles.

The screenshot shows an email interface with a 'MATCHING RESULTS (44 of 209)' table. The table has columns: Sender Name, Send..., Recipients, Subject, Send..., Created Date/T..., and Sync... The email is from 'Orion Constellation <orionc2290@gmail.com>' and contains a spreadsheet titled 'Robbery Plan'. The right sidebar shows 'Orion Constellation <orionc2290@gmail.com>' details, including a 'PREVIEW' section with email metadata and a 'MARKUP PREVIEW' section.

Figure 1.2: Email with Robbery Excel File on Orion's Laptop

Below shows the excel sheet that created for the robbery.

The screenshot shows the Orion interface with a search for 'Item 01-01: HP Laptop...'. The 'MATCHING RESULTS' section shows 40 of 1,900 results. The 'Robbery Data US.xls' file is highlighted. The 'PREVIEW' section shows a spreadsheet titled 'Robbery Data US.xls' with columns for State, Total robberies, Firearms, Knives or cutting instruments, Other weapons, Strong-arm, Agency count, and Population. The 'DETAILS' section shows artifact information for 'Robbery Data US.xls'.

State	Total robberies	Firearms	Knives or cutting instruments	Other weapons	Strong-arm	Agency count	Population
Alabama	3,311	2,145	111	324	791	203	3,625,366
Alaska	896	242	99	127	428	32	733,747
Arizona	6,331	2,530	774	734	2,293	92	6,572,138
Arkansas	1,457	724	110	144	479	237	2,593,420
California	54,311	13,503	5,031	6,535	29,242	736	39,549,496
Colorado	3,483	1,530	306	432	1,215	186	5,028,003
Connecticut	2,194	651	277	230	1,036	106	3,572,665

Figure 1.3: Robbery Plan Spreadsheet from Orion's Laptop

iPhone Safari Search History which includes terms like “avoid infrared sensors” and “spec sheet for eye lock system.”

The screenshot shows the Andromeda interface with a search for 'PhysicalDrive0 PC SN810...'. The 'MATCHING RESULTS' section shows 761 of 42,532 results. The 'largest robberies in us history' artifact is highlighted. The 'DETAILS' section shows artifact information for 'largest robberies in us history'.

Artifact	Key detail	Supporting detail	Additional d
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	largest robberies in us history	8/27/2020 5:01:04:456 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	como se dice ganzua en ingles del espanol	9/3/2020 4:03:14:732 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	como se dice ganzua en ingles	9/3/2020 4:03:04:868 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	notre dame football new schedule	9/1/2020 6:44:17:216 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	como se dice heist en espanol	9/3/2020 4:01:19:378 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	baugo kayak	7/30/2020 7:55:52:079 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	st joseph country kayaking	7/30/2020 7:55:31:324 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	notre dame stadium	7/30/2020 5:18:47:257 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	dairy queen menu	7/21/2020 9:21:10:170 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	hel	7/21/2020 1:33:16:221 AM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	fat bottomed girls lyrics	7/21/2020 9:24:39:605 PM	
Web Related	Search Term	Search Date/Time	
IOS Safari Recent Search...	Uprisa borealis michigan	7/21/2020 1:53:06:212 AM	
Web Related	Search Term	Search Date/Time	

Figure 2.2: Andromeda's Safari Search Terms on Security Systems

PhysicalDrive0 PC SN810 NVME
Artifacts
Content types
Date and times
Tags and comments
com.icandapps.nightsky
More
SAVE FILTERS
CLEAR FILTERS
Type a search term...
GO
ADVANCED

Artifacts

MOBILE

G RESULTS

12

ION USAGE

4

IG SYSTEM

6

ON & CREDENTIALS

2

MATCHING RESULTS (12 of 570,569)

Column view

Artifact

Key detail

Supporting detail

Add

Encryption & Credentials

Apple Keychain Generic...

Keychain Property

FlurryAPIKey

Value

["\$version":"100000","\$archiver":"NSKeyedArchiver",...

Service

com.icandapps.nightsky

Encryption & Credentials

Apple Keychain Generic...

Keychain Property

FlurrySessionTimestampKey

Value

["\$version":"100000","\$archiver":"NSKeyedArchiver",...

Service

com.icandapps.nightsky

Application Usage

Installed Applications

Display Name

Night Sky

Platform

iOS

Display

8.4

Operating System

iOS Home Screen Items

Position

4

Type

Application

Applid

com.icandapps.nightsky

Application Usage

Application Permissions...

Application

com.icandapps.nightsky

Service Name

KTCCServiceBiquity

Allows

Yes

Application Usage

Application Permissions...

Application

com.icandapps.nightsky

Service Name

KTCCServiceCamera

Allows

Yes

Application Usage

Application Permissions...

Application

com.icandapps.nightsky

Service Name

KTCCServiceCalendar

Allows

Yes

Operating System

Network Usage - Applic...

Process Name

mDNSResponder,com.icandapps.nightsky

Type

Process

WiFi By

0.0

Operating System

Network Usage - Applic...

Process Name

trustd,com.icandapps.nightsky

Type

Process

WiFi By

0.0

Operating System

Network Usage - Applic...

Process Name

apptored,com.icandapps.nightsky

Type

Process

WiFi By

0.0

Operating System

Network Usage - Applic...

Process Name

Night Sky,com.icandapps.nightsky

Type

Process

WiFi By

0.0

Operating System

Network Usage - Applic...

Process Name

geord,com.icandapps.nightsky

Type

Process

WiFi By

0.0

FlurryAPIKey

PhysicalDrive0 PC SN810 NVME WDC 1024GB (953.87 GB) - C:\COMP 33\COMP Evidence 2\02-01 iPhoneXR_Logical\00008020-000651240284003A\00008020-000651240284003A-Decrypted

DETAILS

ARTIFACT INFORMATION

Keychain Property

FlurryAPIKey

Value

["\$version":"100000","\$archiver":"NSKeyedArchiver","\$top":{"root":{"ID":"1"},"Subjects":{"\$null":"6895CY4QNZD8CBHNCZV5"}}]

Service Name

com.icandapps.nightsky,com.flurry.analytics

Access Group

LVT74BM435,com.icandapps.nightsky

Created Date/Time

7/20/2020 9:49:47.586 PM

Modified Date/Time

7/20/2020 9:49:47.587 PM

Original Location

Table: genp(rowid: 556)

Artifact type

Apple Keychain Generic Passwords

Item ID

451372

EVIDENCE INFORMATION

Source

00008020-000651240284003A-Decrypted.zip/1/5f1a46f3766d33c2d2abafae8f4ee89f7248b0e

Recovery method

Parsing

Deleted source

Location

root > genp[genp[211]]

root > genp[genp[211]] > acct

Captures a Skype message where Orion says “execute by midnight,” confirming active planning with co-conspirators.

Item 01-01: HP Laptop...
Artifacts
Content types
Date and time
Tags and comments
More

Artifacts >

MATCHING RESULTS (268 of 268)

[Column view](#)

	Chat ID	Profile Name	Author	Recipient(s)	From Display...	Message Sent D...	Message
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:44:58.000 PM	no way
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:44:54.000 PM	what did you do it
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:43:51.000 PM	how do you do it
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:43:08.000 PM	I didn't
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:41:42.000 PM	I forgot new pictures could move on here
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:41:24.000 PM	WHAT IS THAT?
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:40:54.000 PM	oh chat I chat
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:40:42.000 PM	never skip the leg day
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:40:27.000 PM	they can't listen to everyone
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:40:10.000 PM	this tech stuff is crazy
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:40:03.000 PM	i don't know
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:47:30.000 PM	euh i doubt anyone will check or something
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:46:37.000 PM	apparently they're always on
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:46:17.000 PM	"I heard"
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:46:13.000 PM	i thought they can listen to you tho
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/12/2018 3:29:45.000...	so when do you wanna meet and how much do you...
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/12/2018 3:29:08.000...	that sounds like a plan
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/12/2018 3:25:40.000...	yeah that would be good
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/12/2018 3:25:56.000...	i thought we planned on me getting a penguin from...
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/12/2018 3:27:42.000...	yeh, turkey sandwich with mustard is my favorite
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/12/2018 3:27:48.000...	you think they have those?
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/12/2018 3:22:45.000...	"How's it going?"
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/12/2018 3:22:39.000...	heh
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/7/2018 7:51:00.000 PM	see u then
	IveSac116a78d03f529	Ivestedallas1010	Ivestevedallas1010	Ivestevedallas1010	Ivestevedallas1010	9/12/2018 3:22:24.000...	hey,

live:Sac116a78d03f529

Item 01-01: HP Laptop Computer

PREVIEW

EXPORT TO MAGNET EXHIBIT BUILDER

live:Sac116a78d03f529 9/24/2018 3:16:59.00 PM

Something was going on downtown. People everywhere. There was no way I was bringing a penguin out.

live:stevedallas1010 9/24/2018 3:17:30.00 PM

Probably poor planning to do it on a Friday, south Bend has these things called First Fridays. People everywhere and cops everywhere.

live:stevedallas1010 9/24/2018 3:17:50.00 PM

I am working overtime all this week so I'm not sure when I can meet again.

live:Sac116a78d03f529 9/24/2018 3:18:50.00 PM

Figure A: Skype Log - "Execute by midnight"

A RAM snapshot revealing Orion's use of the TOR browser and searches related to anonymous criminal services.

MagnetRAMCapture - ...

Artifacts

Content types

Date and time

Tags and comments

More

SAVE FILTERS

CLEAR FILTERS

Open a search panel

ADVANCED

CON

urltools

MOBILE

G RESULTS 156,706

RESULTS 860

ices URLs 38

JRLs 10

ipn Queries 12

arches 50

- Device 58

- People 14

essed Files and Folders 138

rch Queries 262

ia URLs 14

176

88

5,138

2,824

20

MATCHING RESULTS (176 of 177)

URL	Site...	Date/Time	Date...	Artifact	Artif...	Art...	Source
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	900003	Tor URLs	Magnet
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	900016	Tor URLs	Magnet
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	900015	Tor URLs	Magnet
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	900021	Tor URLs	Magnet
http://gamebombfak3pwn.onion/wp-content/them...	Onion Site			Potential Browser Activity	901005	Tor URLs	Magnet
http://gamebombfak3pwn.onion/wp-content/them...	Onion Site			Potential Browser Activity	901007	Tor URLs	Magnet
http://g7kelyzay23dnt.onion/	Onion Site			Potential Browser Activity	901137	Tor URLs	Magnet
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	901158	Tor URLs	Magnet
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	901999	Tor URLs	Magnet
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	901886	Tor URLs	Magnet
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	901889	Tor URLs	Magnet
http://gamebombfak3pwn.onion/wp-content/them...	Onion Site			Potential Browser Activity	902072	Tor URLs	Magnet
http://hitmetbz7lvinyf1.onion/hitman-services.php	Onion Site			Potential Browser Activity	902323	Tor URLs	Magnet
http://gamebombfak3pwn.onion/wp-content/them...	Onion Site			Potential Browser Activity	903399	Tor URLs	Magnet
http://wtw7k7m6br62gsmfp.onion/guns.html	Onion Site			Potential Browser Activity	900468	Tor URLs	Magnet
http://gamebombfak3pwn.onion/	Onion Site			Potential Browser Activity	900492	Tor URLs	Magnet
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	900768	Tor URLs	Magnet
http://zyyvm0262oiaoc6es7bg966vleyllnqkh7j5ntr...	Onion Site			Potential Browser Activity	900897	Tor URLs	Magnet
http://uad6vym3of7l.onion/	Onion Site			Potential Browser Activity	900956	Tor URLs	Magnet
http://uad6vym3of7l.onion/fogo.png	Onion Site			Potential Browser Activity	900959	Tor URLs	Magnet
http://w353uzm4of8tk.onion/	Onion Site			Potential Browser Activity	900987	Tor URLs	Magnet
http://w353uzm4of8tk.onion/flags.png	Onion Site			Potential Browser Activity	900980	Tor URLs	Magnet

http://wtw7k7m6br62gsmfp.onion/guns.html

MagnetRAMCapture - 20210212 121114.raw

DETAILS

ARTIFACT INFORMATION

URL http://wtw7k7m6br62gsmfp.onion/guns.html

Site Name Onion Site

Artifact type Tor URLs

Item ID 900475

Original artifact Potential Browser Activity

EVIDENCE INFORMATION

Source MagnetRAMCapture - 20210212 121114.raw - Entire Disk (4.25 GB)

Recovery method Deleted source

Location Physical Sector 564963

Evidence number MagnetRAMCapture - 20210212 121114.raw

Figure B: RAM Capture - TOR URLs and suspicious searches

An SMS conversation between Orion and Andromeda discussing shotguns and robbery details, highlighting direct coordination.

01-01: HP Laptop

Artifacts

Content types

Date and time

Tags and comments

weapons

More

MATCHING RESULTS (6 of 1,502)

Column view

Search Term	URL	Date/Time	Original Search Query	Search Session
how to buy illegal weapons	https://www.google.com/search/client=firefox-b-1...	8/19/2020 7:34:03 PM		
weapons undetected by metal detector	https://www.google.com/search/client=firefox-b-1...	8/27/2020 8:08:49:521 PM		
how to buy illegal weapons	https://www.google.com/search/client=firefox-b-1...	8/19/2020 7:34:03 PM		
weapons undetected by metal detector	https://www.google.com/search/client=firefox-b-1...	8/27/2020 8:08:49:521 PM		
weapons undetected by metal detector	https://www.google.com/search/client=firefox-b-1...			
how to buy illegal weapons	https://www.google.com/search/client=firefox-b-1...			

Item 01-01: HP Laptop Computer

DETAILS

ARTIFACT INFORMATION

Search term

how to buy illegal weapons

URL:

[https://www.google.com/search/client=firefox-b-1-dig-how-to-buy-illegal-weapons](#)

Date/Time:

8/19/2020 7:34:03 PM

Web Page Title

how to buy illegal weapons - Google Search

Artifact type

Google Searches

Item ID

243689

Original artifact

Firefox Web Visits

EVIDENCE INFORMATION

Source

01-01-E01 - Partition 2 (Microsoft NTFS, 485.19 GB)\Users\Victor\AppData\Roaming\Mozilla\Firefox\Profiles\vjleppdft.default-release\places.sqlite

Discovery method

Deleted source

Location

Table: moz_places(id: 11)
Table: moz_historyvisits(id: 6)

Evidence number

Item 01-01: HP Laptop Computer

Figure 1.5: SMS Conversation between Orion and Andromeda

MATCHING RESULTS (32 of 211)

	Search Query	Date/Time	Start...	Latit...	Long...	Locati...	Sour...	Dest...	Rout...	Addi...	Artifact
	Notre Dame Stadium			41.689444	-86.234403	Center of Map	Potential Browser Acti				
	notre dame stadium			41.689444	-86.234403	Center of Map	Potential Browser Acti				
	Notre Dame Stadium			41.689399	-86.234463	Center of Map	Potential Browser Acti				
	Notre Dame Stadium	8/27/2020 7:22:06.752 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				
	notre dame stadium	8/27/2020 7:22:01.522 PM		41.689444	-86.234403	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:03.696 PM		41.689444	-86.234403	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:15.039 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:14.484 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				
	notre dame stadium	8/27/2020 7:22:02.116 PM		41.689444	-86.234403	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:03.688 PM		41.689444	-86.234403	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:16.142 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:15.039 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				
	notre dame stadium	8/27/2020 7:22:01.522 PM		41.689444	-86.234403	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:06.752 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:03.696 PM		41.689444	-86.234403	Center of Map	Edge/Internet Explorer				
	notre dame stadium	8/27/2020 7:22:02.116 PM		41.689444	-86.234403	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:03.688 PM		41.689444	-86.234403	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:16.142 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:14.484 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				
	notre dame stadium	8/27/2020 7:22:01.522 PM		41.689444	-86.234403	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:06.752 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				
	Notre Dame Stadium	8/27/2020 7:22:06.752 PM		41.689399	-86.234463	Center of Map	Edge/Internet Explorer				

Item 01-01: HP Laptop Computer

A world map showing the location of the item. A red pin marks the location near Montreal, Quebec, Canada, specifically around the Notre-Dame-du-Rosaire Circle area.

OPEN LOCATION IN ▾

Latitude **41.6899**
Longitude **-86.2344**

DETAILS

Shows Andromeda's Safari searches related to breaking in, disabling security systems, and robbery methods.

PhysicalDrive0 PC SN810 NVMe WDC 1024GB (953.87 GB) - C:\COMP 33\COMP3 Evidence 2\02-01, iPhoneXR_Logical\00000820-000651240284003A-Decrypted

Artifacts

Content types

Date and time

Tags and comments

More

Artifacts

Column view

MOBILE

ING RESULTS

952

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

MOBILE

ING RESULTS

952

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

MOBILE

ING RESULTS

952

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

Figure 2.1: Andromeda's Suspicious Web Searches

Contains GPS-tagged photos of Notre Dame Stadium taken from Andromeda's SD card, used for recon.

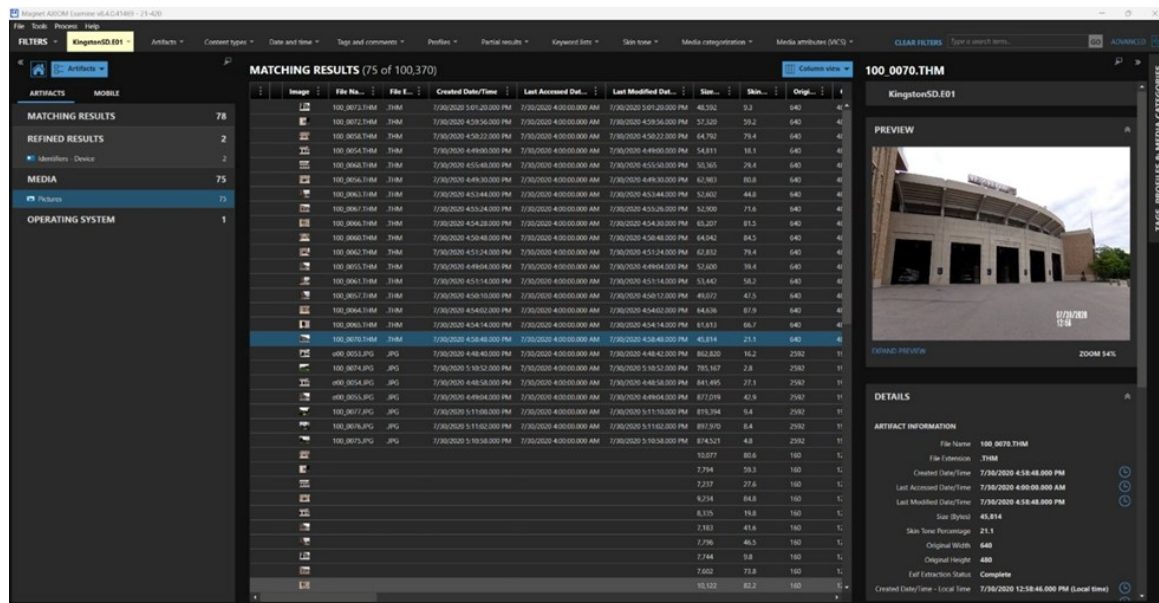


Figure 2.3: Reconnaissance Photos from Kingston SD

It shows recovered Zoom meeting URLs from RAM capture, which indicates potential planning or scheduled communication between the suspects.

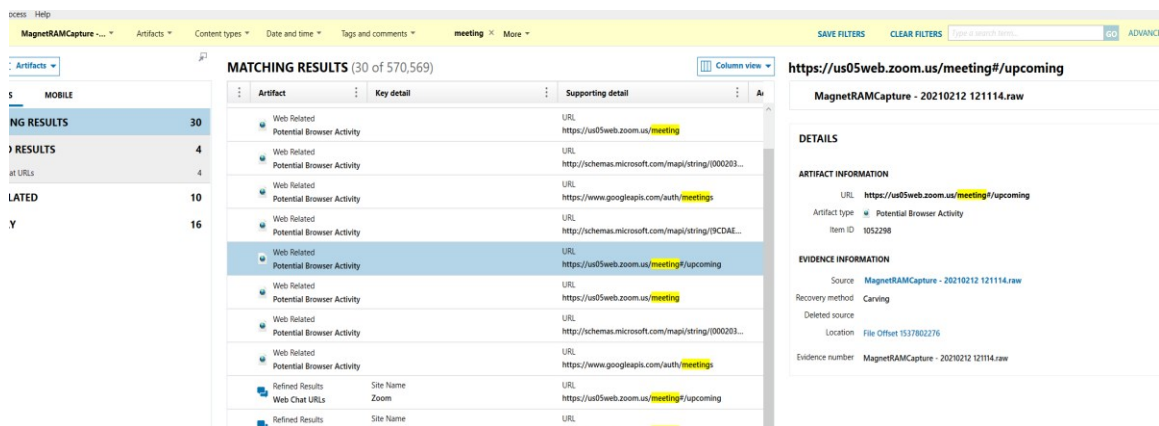


Figure 2.5: Zoom Meeting URL Recovered from Orion's RAM Capture

Cassiopeia’s Phone have the same applications which Andromeda has which confirms their communications.

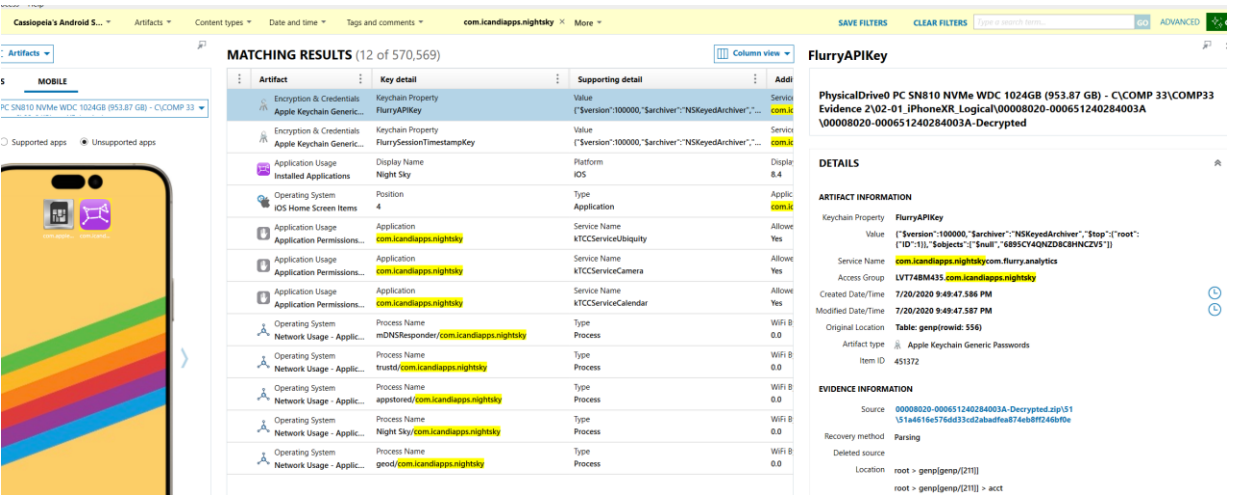


Figure 3.4: Telegram Messenger Installed on Cassiopeia’s Phone

Displays Cassiopeia’s call log with frequent communications to Orion and Andromeda, confirming her involvement.

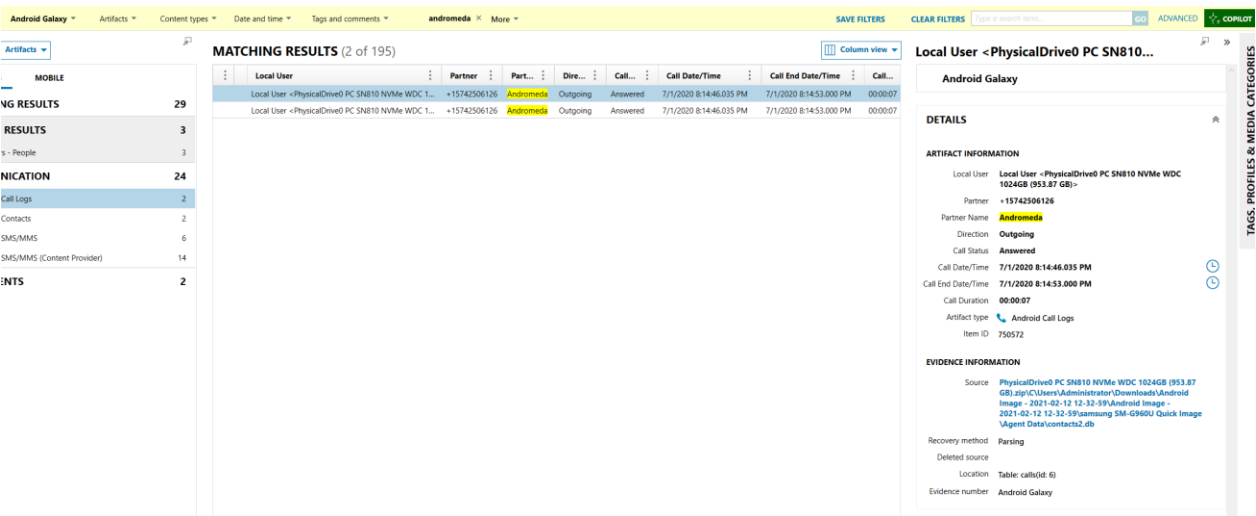


Figure 3.1: Cassiopeia’s Call Log with Orion and Andromeda

Cassiopeia's Android S... Artifacts Content types Date and time Tags and comments andromeda More SAVE FILTERS CLEAR FILTERS Type a search term... ADVANCED

Artifacts

TS MOBILE

ING RESULTS 52

D RESULTS 2

ers - People 2

UNICATION 49

AGENTS 1

MATCHING RESULTS (52 of 570,569)

Artifact	Key detail	Supporting detail	Additional detail
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message Got it. I'll keep preparing	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message Perfect. When should I ready for this?	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message OK I will & I will pack for that. See you then	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message Yes I can meet on campus then to go trails	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message We did good work in Paris. You can trust me.	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message When/where	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message Yes	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message Yes	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message Once we meet & I hear more I can provide more ski...	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message I have a few contacts that work for the football tea...	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message Yes she did. I'm conducting research now	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), Local...	Message Nice to meet you Orion. Looking forward to workin...	Message Status Outgoing
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), +1574...	Message And since it is a night game, very few people aroun...	Message Status Incoming
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), +1574...	Message Probably in a few weeks. The next home game is FL...	Message Status Incoming
Communication Android SMS/MMS (Conten...	Participants +15744041921, Andromeda (+15742506126), +1574...	Message I was able to sneak into the police locker room. Loc...	Message Status Incoming
Communication Android SMS/MMS (Conten...	Participants +15744041921, +15743025282, Andromeda (+15742...	Message Try to get some of the restricted areas but don't ge...	Message Status Incoming
Communication Android SMS/MMS (Conten...	Participants +15744041921, +15743025282, Andromeda (+15742...	Message Cassiopeia, I will meet you at 600 am by the post of...	Message Status Incoming

+15744041921, **Andromeda**...

Cassiopeia's Android Samsung

PREVIEW

EXPORT TO MAGNET EXHIBIT BUILDER

+15744041921, **Andromeda** (+15742506126), +15743025282
9/17/2020 7:28:13 AM PM

I was able to sneak into the police locker room. Look what I found baying next I took them. We will be able to hear everything!

+15744041921, **Andromeda** (+15742506126), +15743025282
9/17/2020 7:28:22 AM PM

Local User <unzip this-Android Image - 2021-02-18 11-09-33.zip>
9/20/2020 5:20:14 AM PM

DETAILS

ARTIFACT INFORMATION

Figure 3.2: Cassiopeia's Chats with Andromeda

Shows Cassiopeia's Facebook profile picture, verifying the digital identity tied to the analyzed Facebook data.

Cassiopeia's Facebook Artifacts Content types Date and time Tags and comments More SAVE FILTERS CLEAR FILTERS Type a search term... ADVANCED

Artifacts

MOBILE

IG RESULTS 24

1

1

NTS 22

4G SYSTEM 1

MATCHING RESULTS (1 of 97,379)

Artifact	Key detail	Supporting detail	Additional detail
Media Pictures	File Name 118616400_105816547915942_74448241739085616...	Size (Bytes) 65,621	File Extension jpg

118616400_105816547915942_74448241739085616...

Cassiopeia's Facebook

PREVIEW

EXPAND PREVIEW ZOOM 90%

DETAILS

ARTIFACT INFORMATION

File Name 118616400_105816547915942_74448241739085616
7_n_105816544382609.jpg

File Extension jpg

Last Modified Date/Time 2/13/2021 11:14:58.000 AM

Figure 3.3: Cassiopeia's Facebook Profile Picture