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.

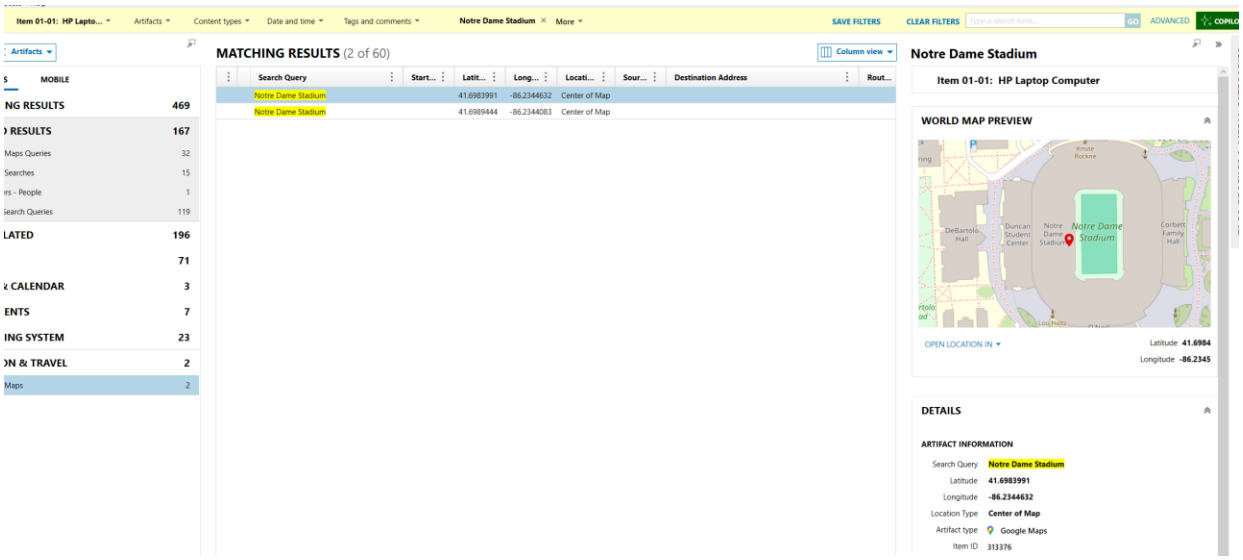

Figure 1.1: Google Maps Queries from Orion's Laptop

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

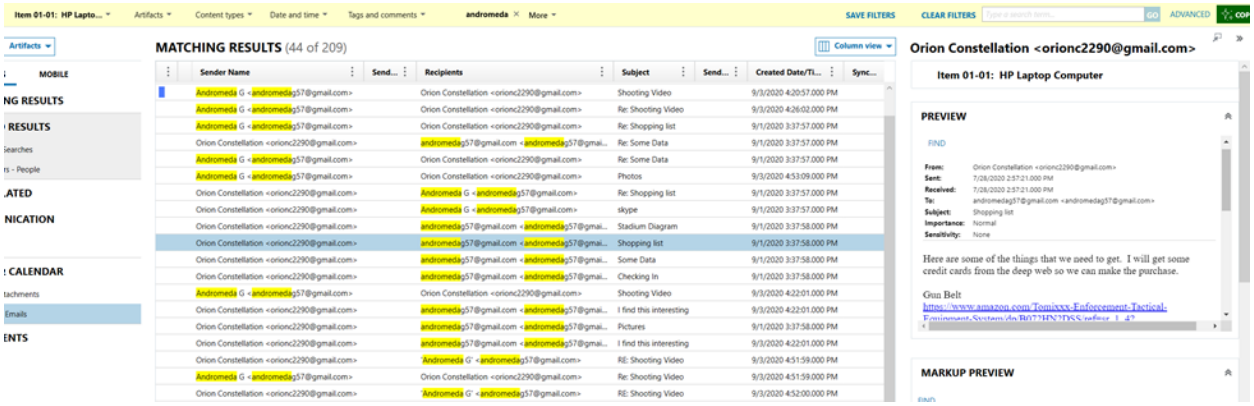

Figure 1.2: Email with Robbery Excel File on Orion's Laptop

Below shows the excel sheet that created for the robbery.

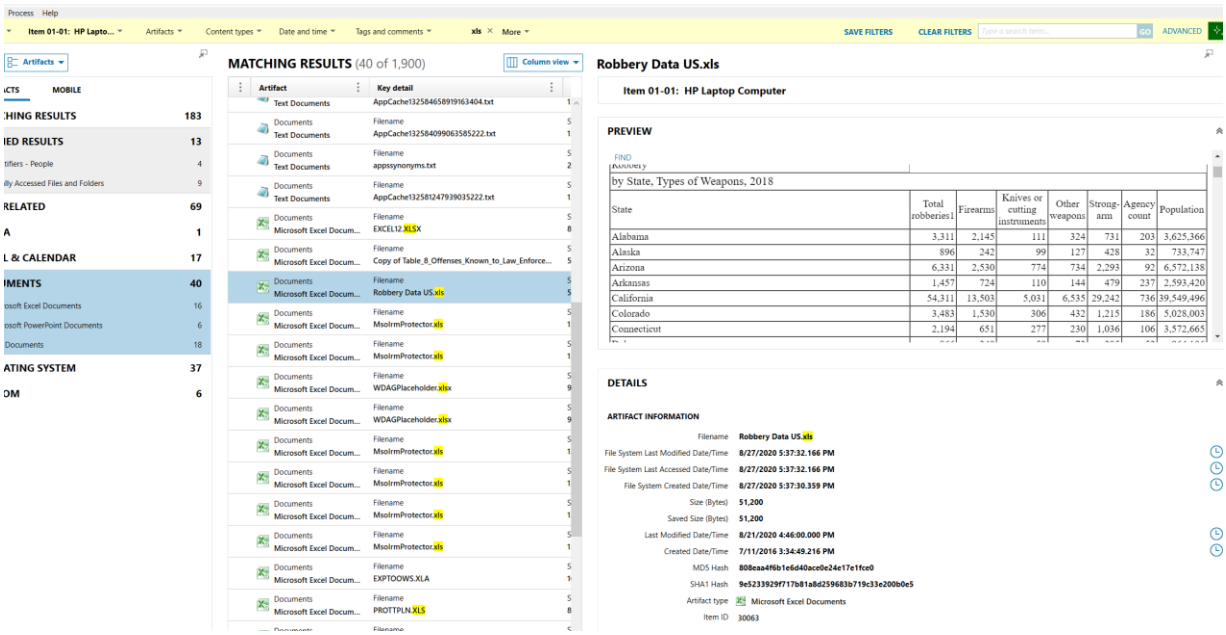

Figure 1.3: Robbery Plan Spreadsheet from Orion's Laptop

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

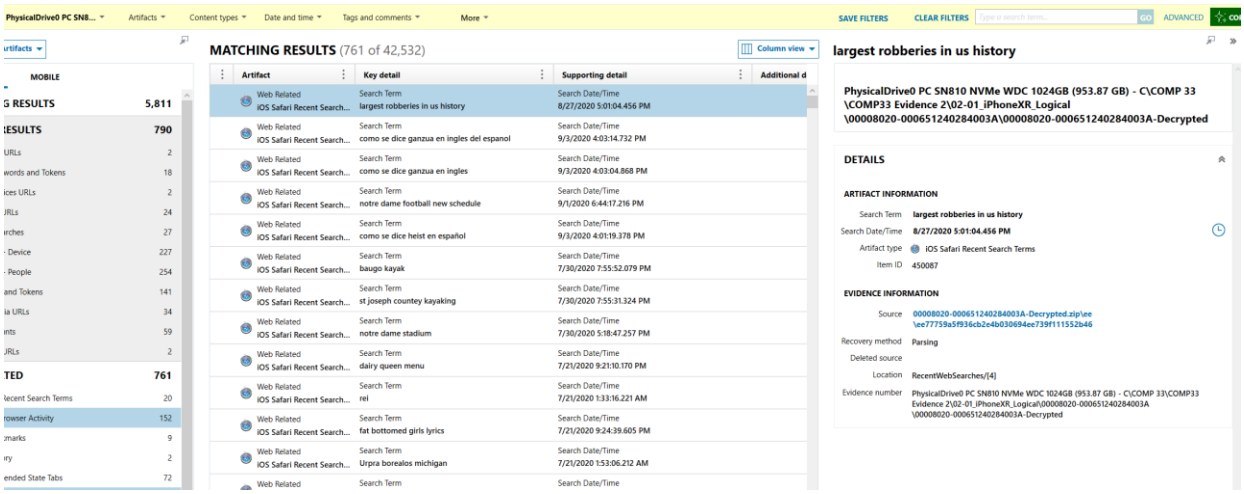

Figure 2.2: Andromeda's Safari Search Terms on Security Systems

Confirms Andromeda used Signal for encrypted communication by installing non supported application.

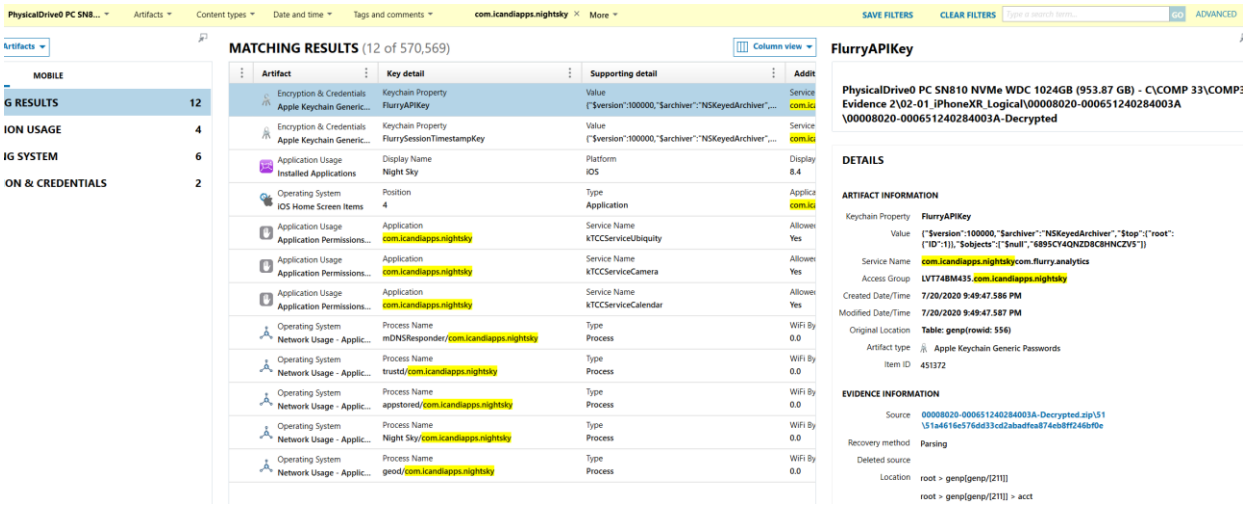

Figure 2.4: Signal Messenger App Installed on Andromeda's iPhone

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

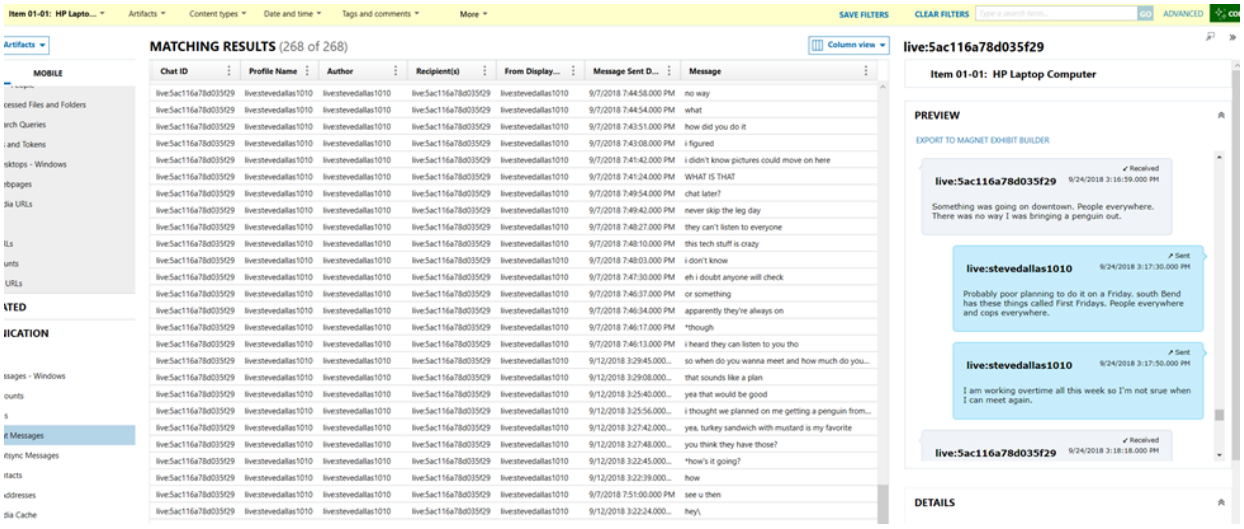

Figure A: Skype Log - "Execute by midnight"

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

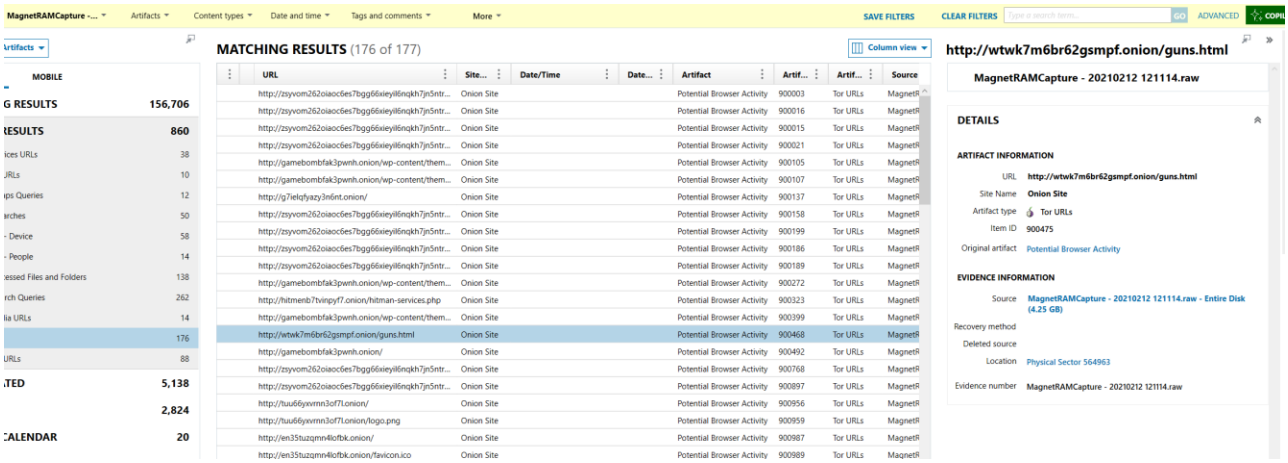

Figure B: RAM Capture - TOR URLs and suspicious searches

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

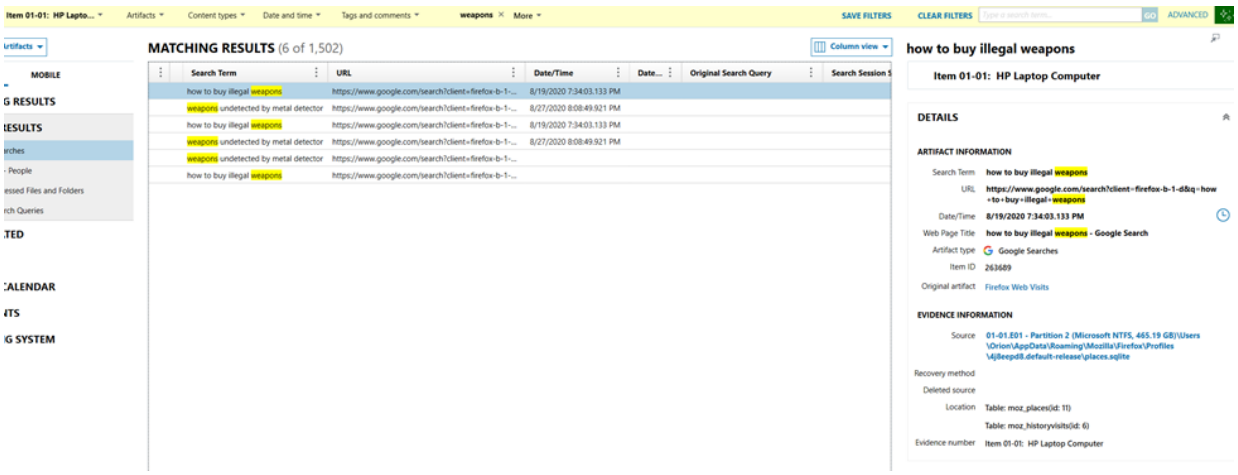

Figure 1.5: SMS Conversation between Orion and Andromeda

Reveals Orion's search and location history from his Google Takeout, including queries about escape routes and tools.

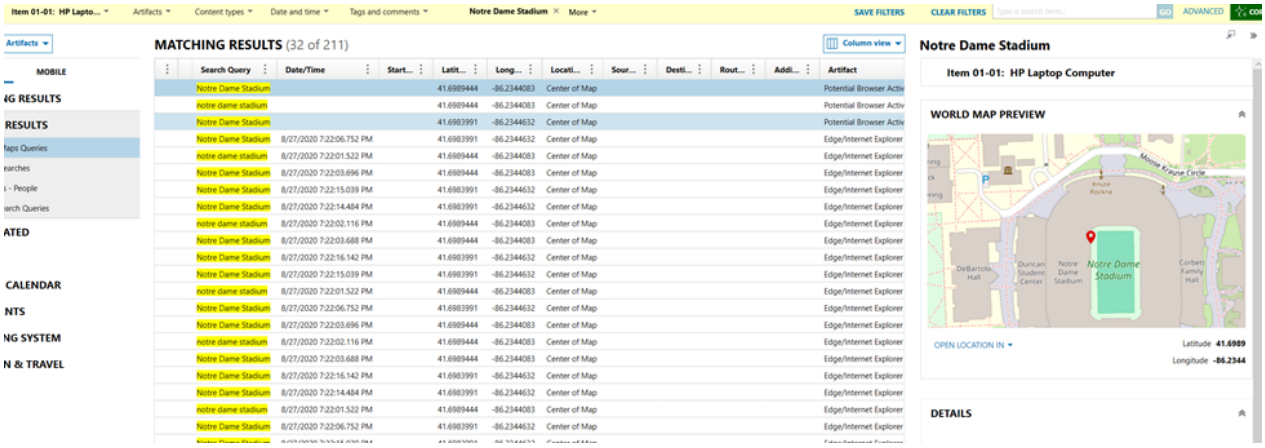

Figure 1.6: Google Takeout Search History from Orion

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

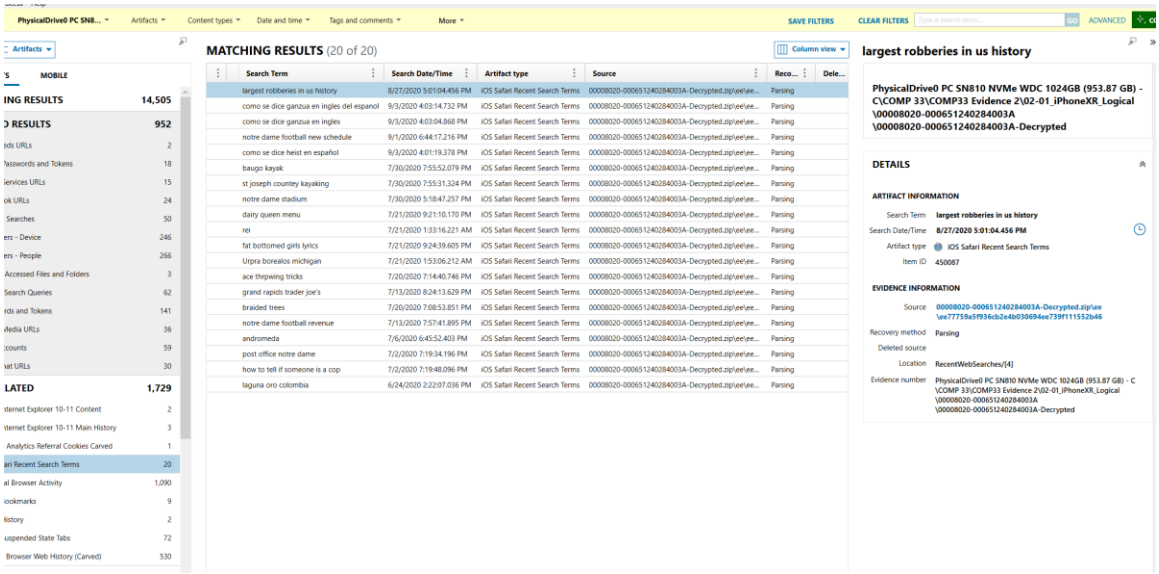

Figure 2.1: Andromeda's Suspicious Web Searches

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

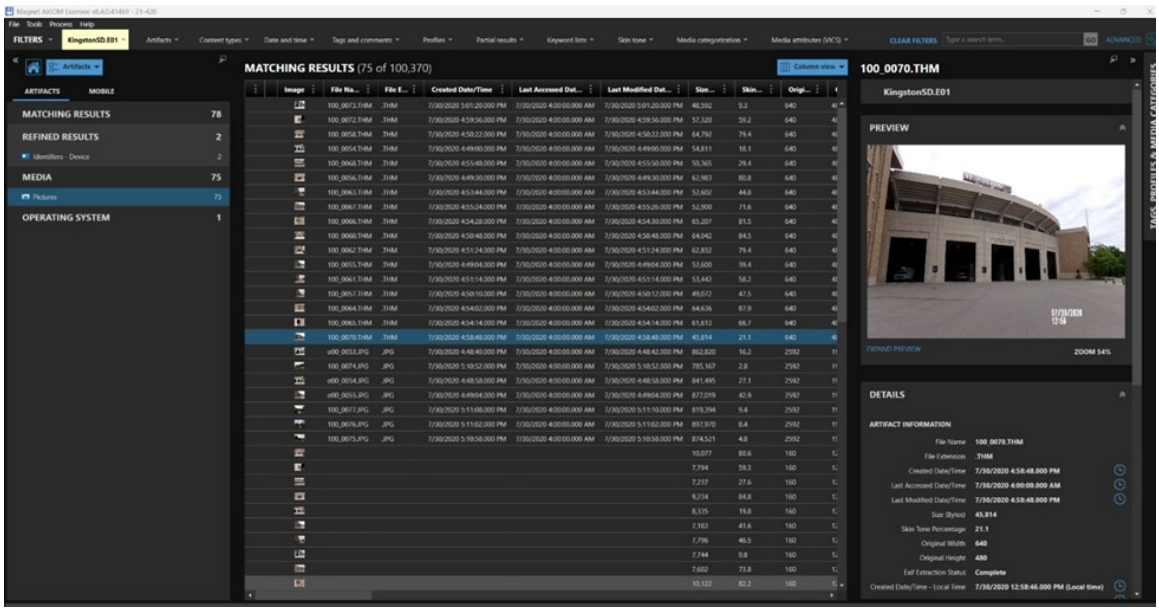

Figure 2.3: Reconnaissance Photos from Kingston SD

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

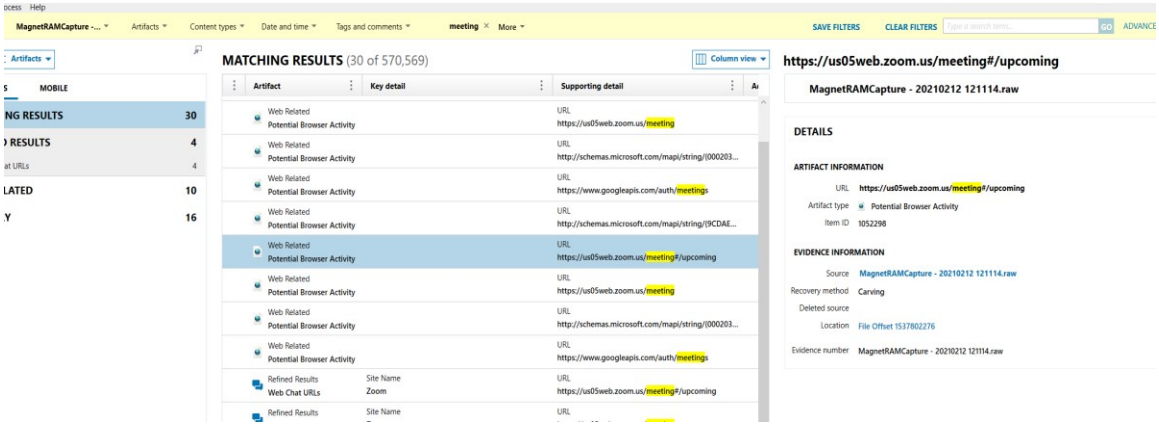

Figure 2.5: Zoom Meeting URL Recovered from Orion's RAM Capture

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

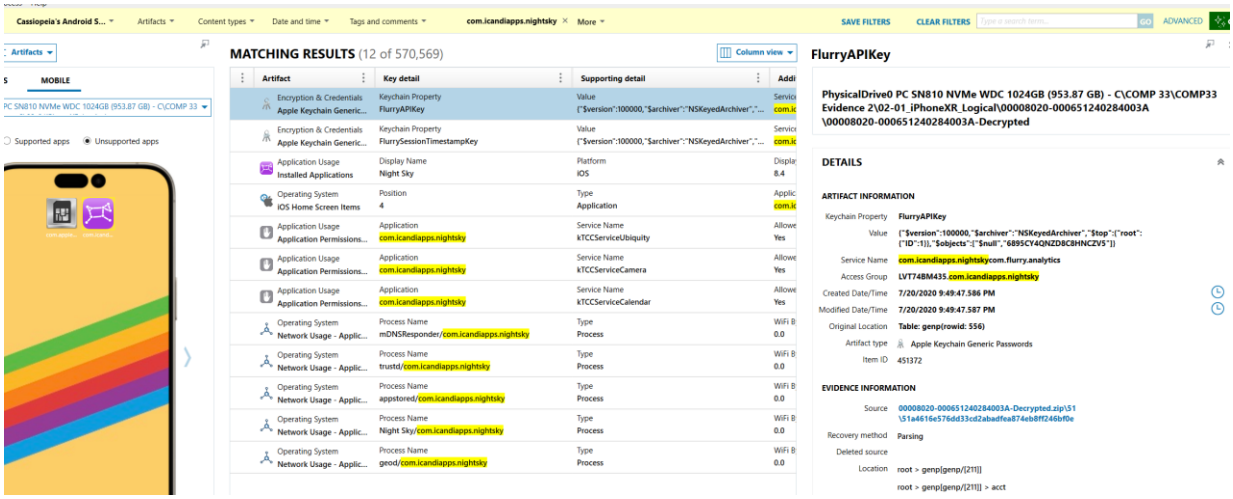

Figure 3.4: Telegram Messenger Installed on Cassiopeia's Phone

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

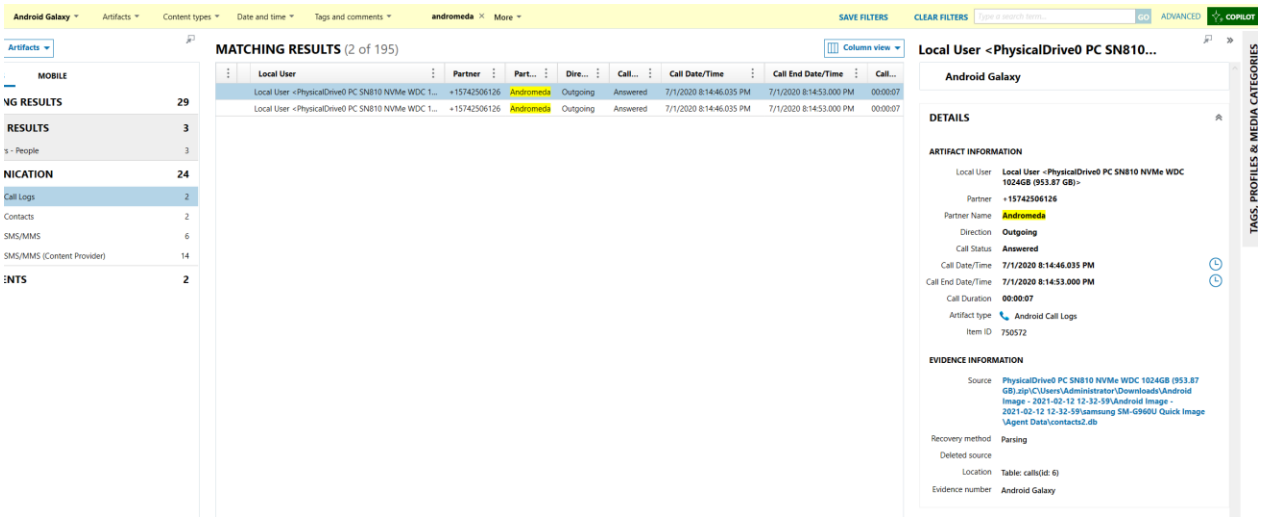

Figure 3.1: Cassiopeia's Call Log with Orion and Andromeda

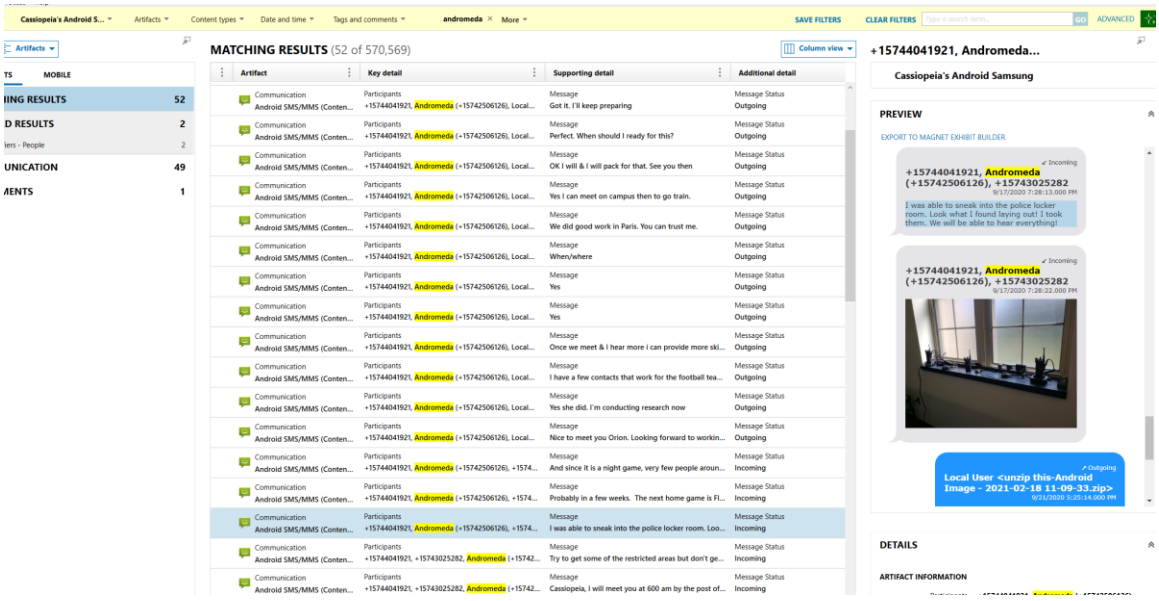

Figure 3.2: Cassiopeia's Chats with Andromeda

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

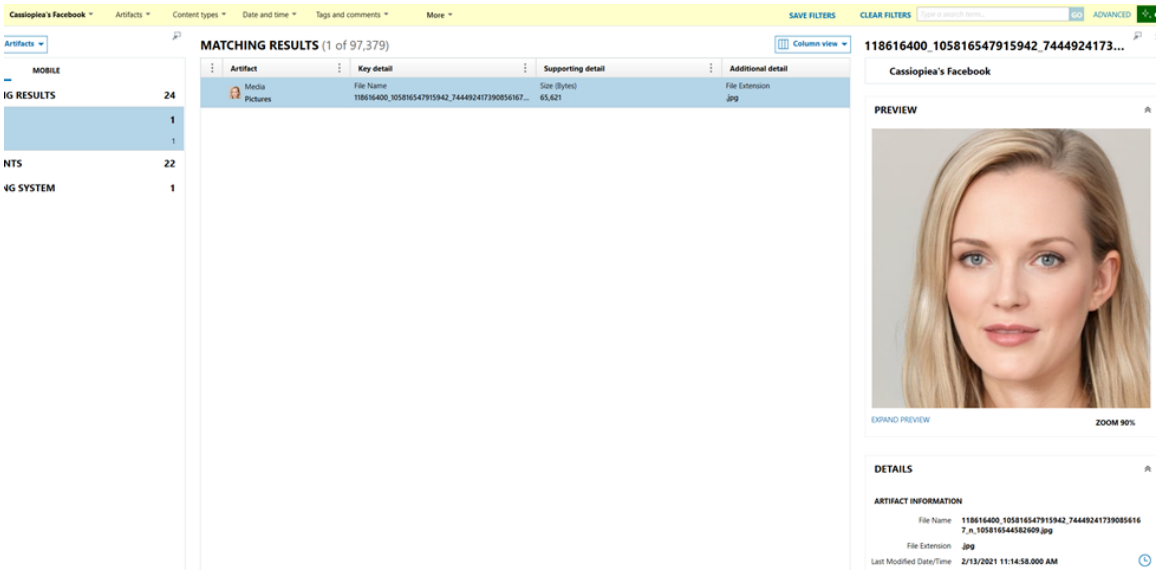

Figure 3.3: Cassiopeia's Facebook Profile Picture