CFR101 Final: Summary Report

Ramon Lopez Jr

Department of Cybersecurity: University of Advancing Technology

CFR101: Computer Forensic Essentials

Professor Aaron Rodriguez

December 16th, 2022

CRIMINAL REPORT

CASE

REPORT DATE	CASE NAME	PREPARED BY
12/8/2022	ATM2022BoA	Ramon Lopez Jr

STATUS SUMMARY

On **December 13, 2022**, the forensic examination of the provided case files commenced. The first step in the investigation was to create a forensic copy of the original files to ensure the integrity of the evidence before analysis (see Image 1.1).

To verify that the files remained untampered, hash values were generated and examined. Using **FTK Imager**, the files were loaded into the program. The process involved selecting **File > Export Logical Image (AD1)** (see Image 2.1). A separate window appeared, where I selected **"Add"** under the image destination options (see Image 2.2). Next, I filled out the required metadata fields in a second window (see Image 2.3), followed by specifying the storage location and naming convention for the forensic image in a third window (see Image 2.4). Once configured, the scanning process began, generating hash values for the extracted files (see Image 2.5). After confirming the integrity of the evidence, FTK Imager was closed, and the forensic analysis phase began.

The evidence contained data from three devices: **an iPhone, a tablet, and a Windows laptop**.

- **iPhone Analysis:** Four images stood out among the stored data. Two images contained the names "James" and "John." The image labeled "James" depicted a man holding a firearm, while the image labeled "John" showed a man in handcuffs. This evidence directly linked **John Campbell** as the suspect currently in custody and identified **James** as an accomplice still at large. Additional data from the iPhone included **text messages** between James and multiple contacts:
  - **James → Mary:** In one conversation, Mary rejected James, stating, *"Please leave me alone, you're broke!"* James responded, *"I'm working on something big,"* which referred to the bank heist.
  - **UberEATS Notification:** A delivery notification contained a precise **location for James's residence:** 2625 W. Baseline Rd., Tempe, AZ 85283, Room 909.
  - **James → John:** A message instructed John to meet at a **Starbucks on Baseline**, indicating a potential rendezvous point. Another message suggested John should use James's password—likely to access an ATM.
- **Laptop Analysis:** Seven files were examined, two of which contained critical evidence about ATM hijacking techniques.
  - **HI_THERE.jfif:** This image contained hidden instructions for withdrawing $8,000 from an ATM. When opened in Notepad, the file revealed a **step-by-step guide** on executing the attack.
  - **jackpotting.py:** This Python script was the actual tool used to exploit ATMs, aligning with the methodology described in HI_THERE.jfif. The script was found in James's user directory under "Documents."

This digital evidence directly links James and John to the ATM fraud operation and helps reconstruct the events leading to the crime.

Provide a detailed synopsis of the events based on what you found on the devices with reference to who was involved, the motive, and how the crime was committed. Use every possible piece of information provided to lay out the case to make sure that the criminal does not get away.

The forensic investigation identified **James and John** as the two primary individuals involved in the **Bank of America ATM fraud incident**.

- **James** was the mastermind behind the operation. He orchestrated the planning, including selecting the **meeting location, execution method, and money drop-off site**. His **motive** was revealed in text messages exchanged with **Mary**, where he implied that the heist was his attempt to win her back.
- **John** executed the operation by physically interacting with the ATM. Messages found on the iPhone indicate that James provided John with **login credentials** for unauthorized access.

How the Crime Was Committed:

The **jackpotting attack** was executed using a **Python script (jackpotting.py)**, found in James's laptop files. The **HI_THERE.jfif** file contained explicit instructions on how to manipulate the ATM to dispense $8,000. By inserting a **USB drive** containing the Python script into the ATM, they were able to extract the money without triggering security measures.

Key Findings:

- James planned the attack and provided John with instructions.
- John physically accessed the ATM and executed the script.
- Evidence from text messages, images, and scripts confirm their involvement.
- Ted and Larry Fix were **wrongfully detained** and should be released.

This forensic analysis provides conclusive proof that James and John orchestrated the ATM fraud. James remains at large, while John is in custody.

Images:

Image 1.1

The result of copying the files meant to be examined.

Image 2.1

Exporting an AD1 image

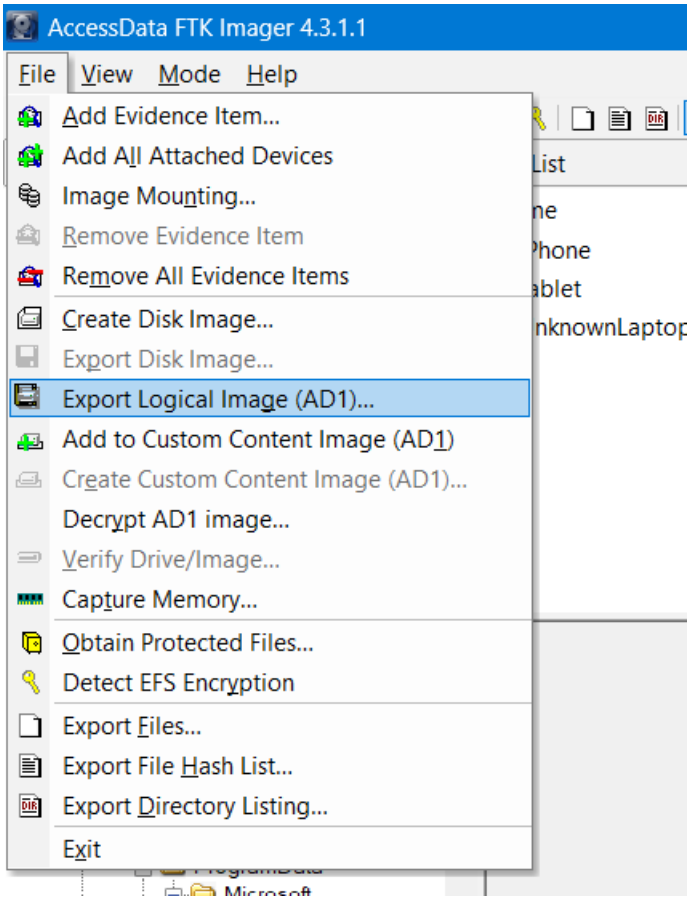

Image 2.2

In the create image window, clicked on add.

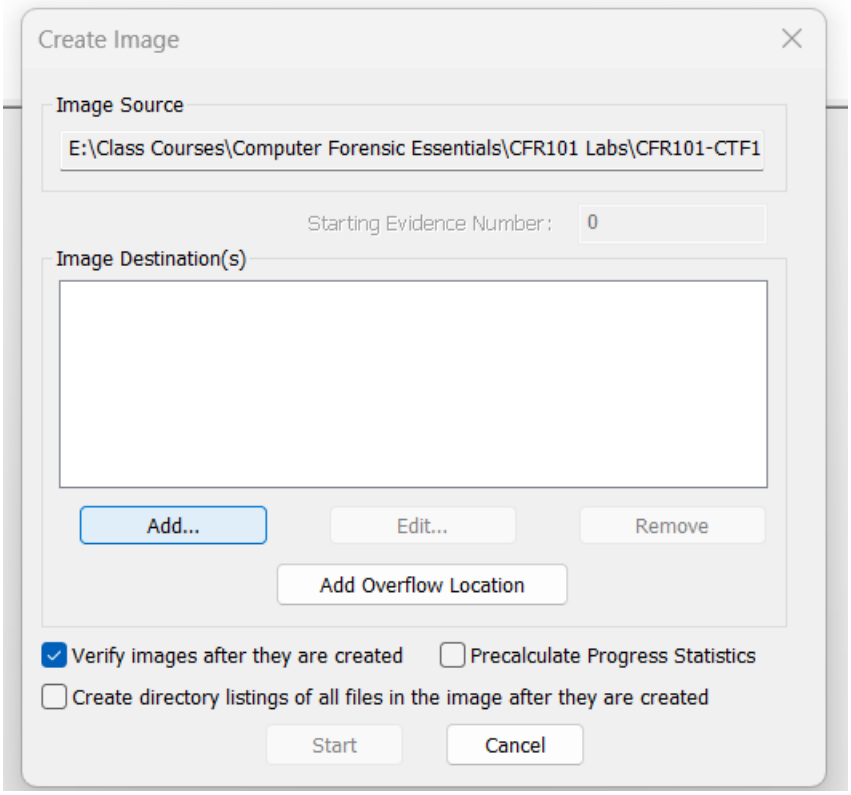

Image 2.3

Filling out the information for the evidence.

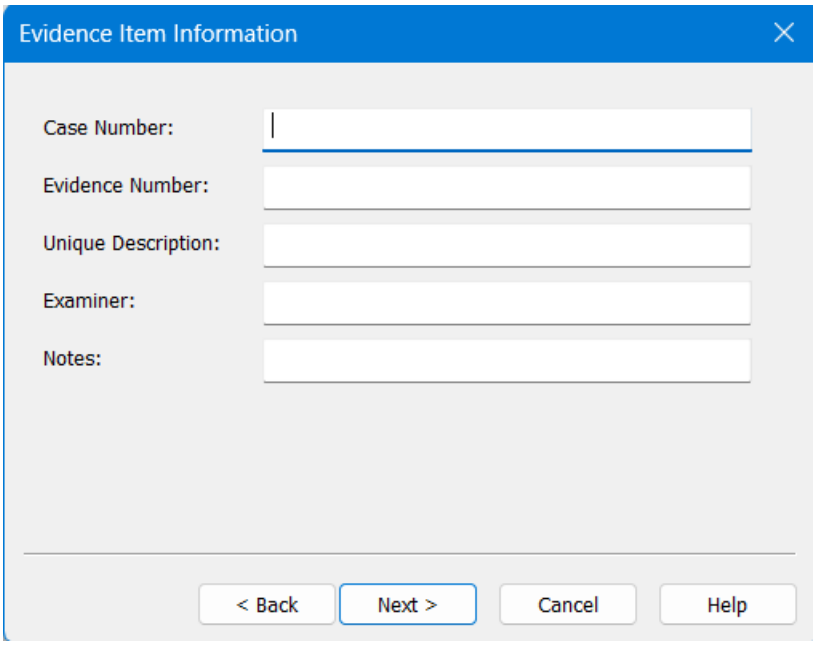

Image 2.4

Finding the file path and giving it a name

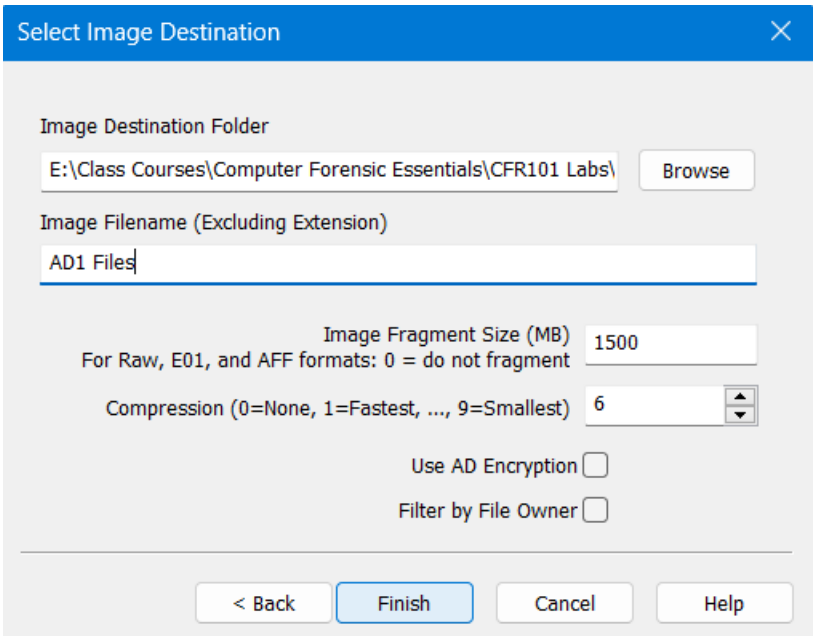

Image 2.5

The results of the scanning process