UNCC Theft FORENSIC EXAMINATION REPORT

Case Number: C02_03012026
Evidence Item: A USB Thumb Drive (Forensic Image: ItemA_Evidence.E01)
Requesting Agency: UNCC Police Department
Original Imaging Officer: Ofc. Jimmy Johns
Forensic Examiner: Douglas Akwasi Kwarteng
Date of Report: 03/01/2026

1. Overview

On February 23, 2016, Officer Jimmy Johns obtained a USB thumb drive from an individual under investigation in connection with reported thefts of Apple computer equipment from Woodward Hall at the University of North Carolina at Charlotte (UNCC).

A forensic image of the thumb drive was created and preserved in E01 format. I was tasked with conducting a forensic examination of that image to determine:

- Whether photographs of Apple devices were present
- Whether deleted files could be recovered
- Whether GPS or other metadata was embedded in the images
- The make and model of the camera used
- Whether any additional images were relevant to the investigation

During examination, eighteen image files were identified, including deleted files recovered from the Recycle Bin and unallocated space. An image depicts Apple Mac Mini hardware installed in what appears to be a university laboratory environment. Embedded metadata indicates the images were captured on February 23, 2016, using an Apple iPhone 6s. GPS coordinates extracted from the images correspond to the UNC Charlotte campus near Woodward Hall.

This report presents factual findings derived from the digital evidence.

2. EVIDENCE DESCRIPTION & INTEGRITY

Evidence Received

- Item A: USB Thumb Drive (Forensic Image: ItemA_Evidence.E01)
- Image Type: E01
- File System: FAT32
- Bytes per Sector: 512
- Sector Count: 524,288
- Total Size: 256 MB

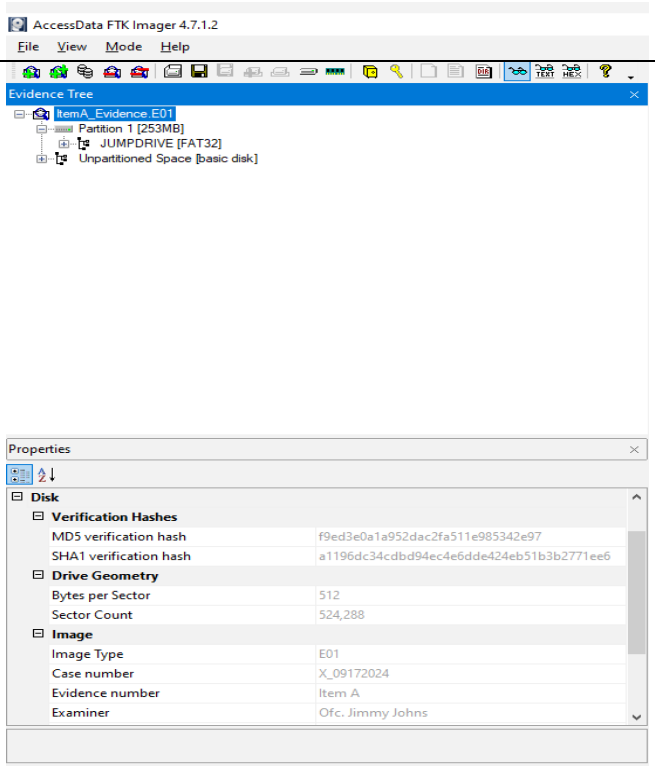


Figure 1: FTK drive geometry showing the sector count and sector size, and FAT32 as the file system.

Verification Hashes

The thumb drive's hashes were verified before analysis. This is to ensure the integrity of the image.

- **MD5:** f9ed3e0a1a952dac2fa511e985342e97
- **SHA1:** a1196dc34cdbd94ec4e6dde424eb51b3b2771ee6

Figure 2: Verification hashes for Item A demonstrating forensic integrity.

The MD5 and SHA1 hash values confirm that the forensic image examined is an exact bit-for-bit copy of the original media and has not been altered during analysis.

3. EXAMINATION ENVIRONMENT & PREPARATION

To ensure a controlled and isolated environment for forensic analysis, the examination was conducted on a dedicated forensic workstation with the following specifications:

- Host Hardware: Dell Laptop, 16GB RAM, 2TB HDD.
- Analysis Environment: Windows 10 Professional (64-bit) running within a Virtual Machine (VM).
- VM Allocation: 8GB RAM, 500GB Virtual Disk.
- Forensic Isolation: The analysis environment was isolated from the host network to prevent data leakage or unauthorized updates during the examination.
- Tool Validation: All forensic software was verified for proper installation and function before the ingestion of evidence.

4. TOOLS UTILIZED

- FTK Imager v4.7.1 for image verification and hash validation
- Autopsy v4.21.0 for primary forensic analysis and metadata extraction
- Autopsy Carver for recovery of deleted files from unallocated space
- OSFMount for read-only mounting of the image for secondary validation
- Recuva v1.53 for cross-tool validation and filename reconstruction

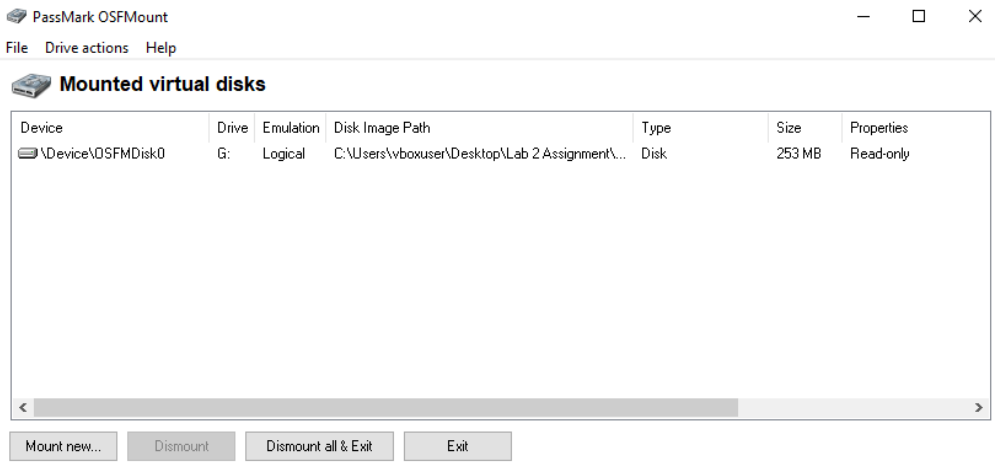


Figure 3: Forensic image mounted in read-only mode to preserve evidence integrity.

4. METHODOLOGY

4.1 Initial Examination

The E01 image was ingested into Autopsy. Standards ingest modules were executed, including:

- **EXIF Metadata Extraction**

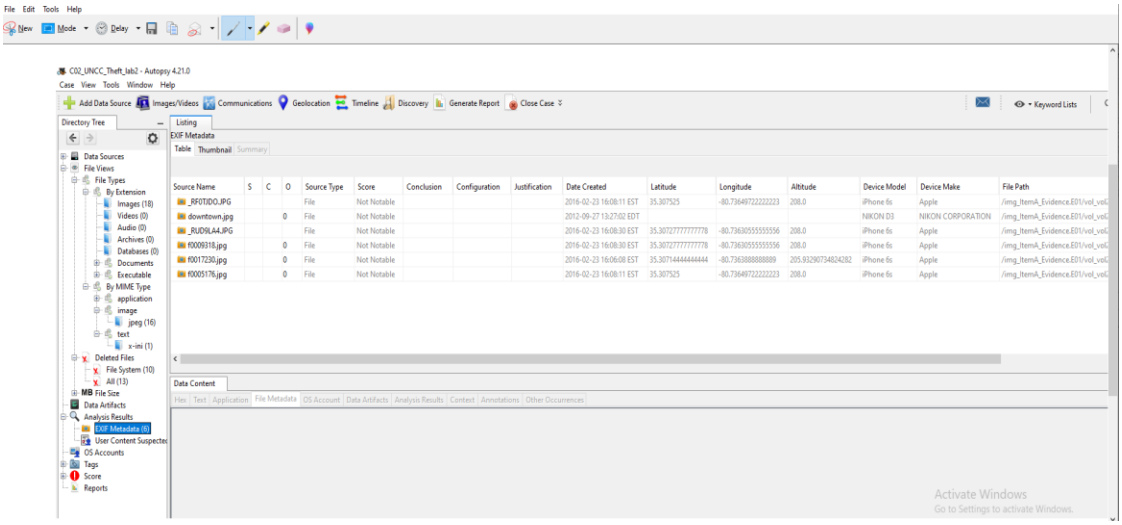


Figure 4: Exif image showing the metadata of images.

- **File Carving**

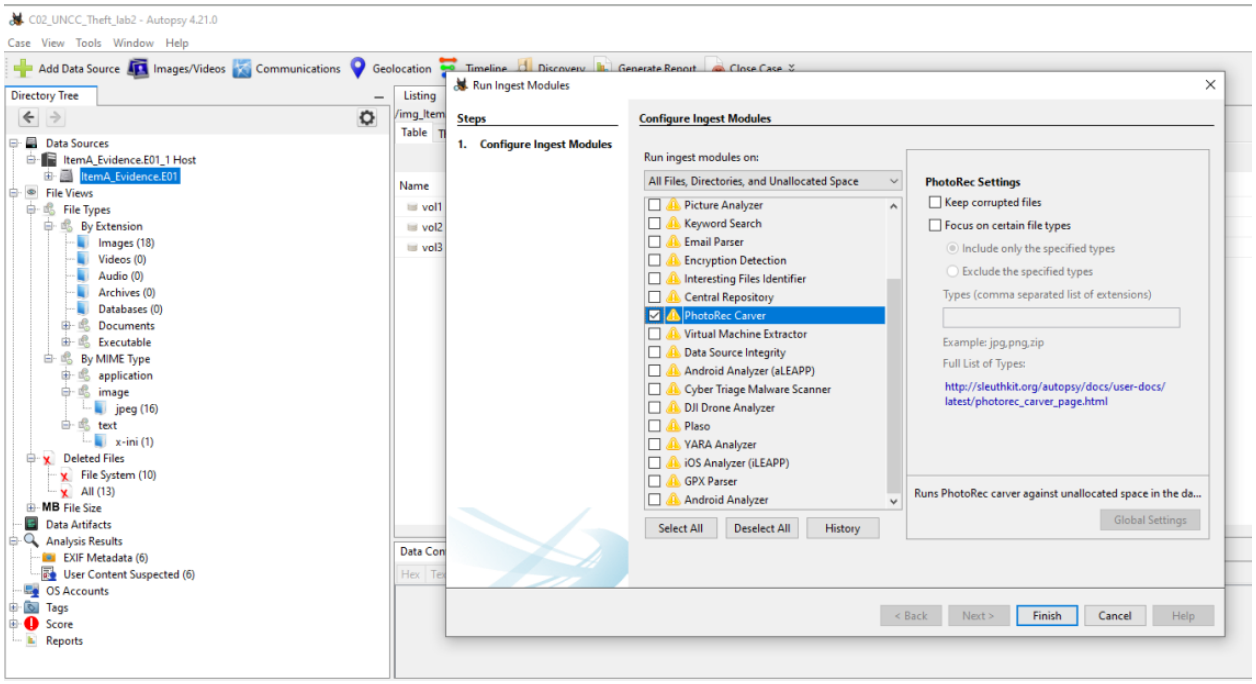


Figure 5: Image showing the carving process using PhotoRec Carver in Autopsty application.

4.2 Recovery of Deleted Files (Carving)

A deep carve using PhotoRec was conducted on unallocated space. Three additional files were recovered from unallocated space and placed in the $CarvedFiles directory.

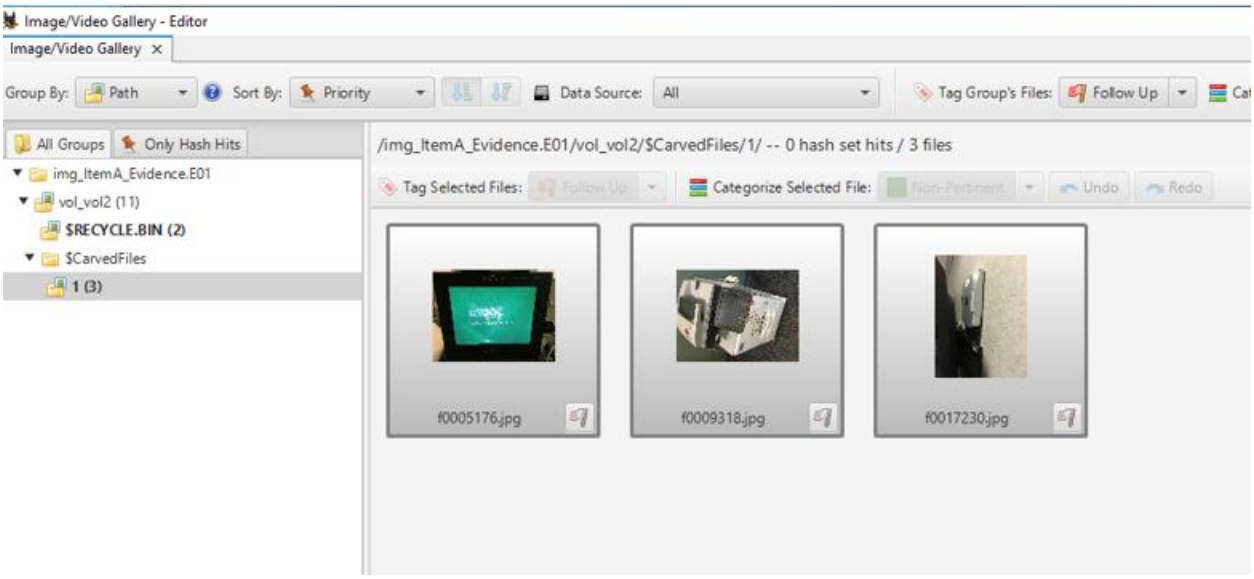


Figure 6: Images recovered from unallocated space via forensic carving.

Before Carving **After Carving**

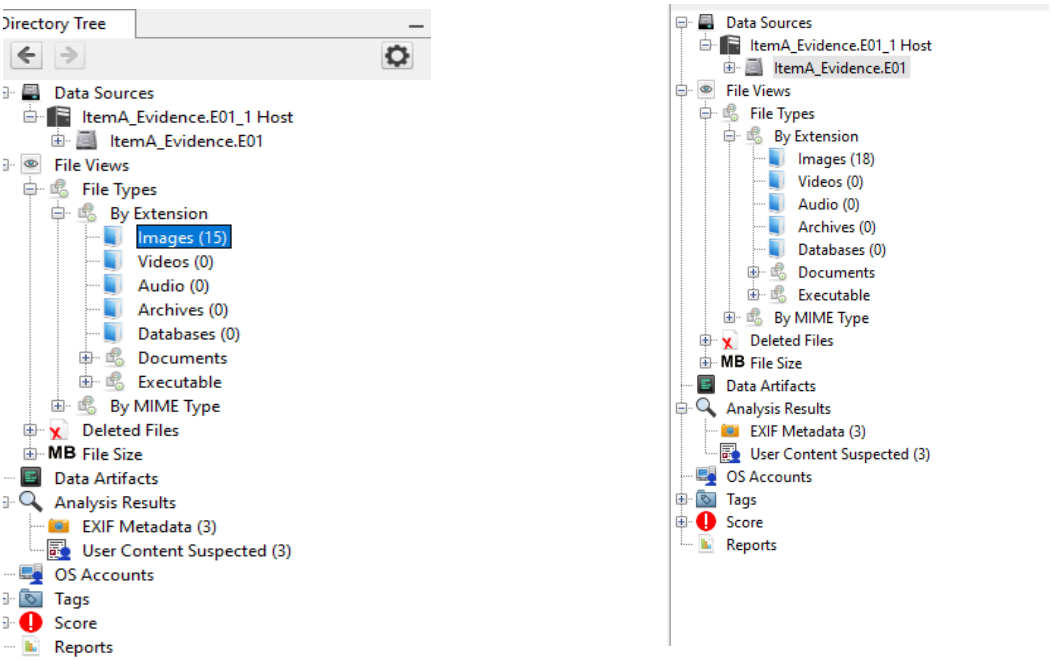


Figure 7: Evidence tree showing the total number of images increasing from 15 to 18 after carving.

4.3 Cross-Tool Validation

To validate findings, the forensic image was mounted as a read-only logical drive using OSFMount and scanned using Recuva with Deep Scan enabled.

Recuva recovered original camera-style filenames, including:

- _ifcd13k.JPG was recovered as IMG_1692.JPG
- _if0TJDOk .JPG was recovered as IMG_1693.JPG
- _IUD9L4A1.JPG was recovered as IMG_1694.JPG

These filenames corresponded to internal string references identified in Autopsy.

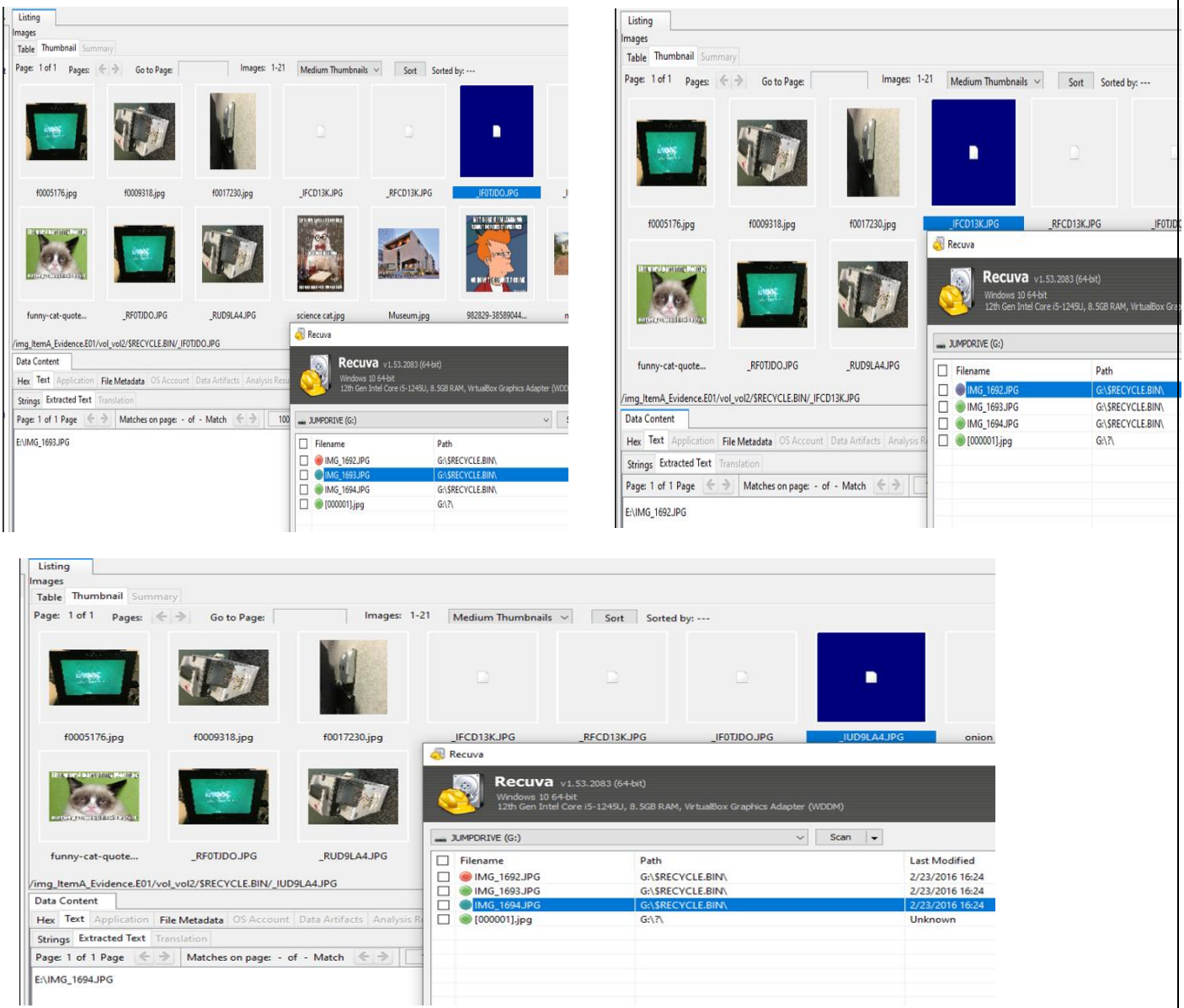


Figure 8: Cross-tool validation showing matching original filenames.

5. FINDINGS

Three images were recovered in our findings.

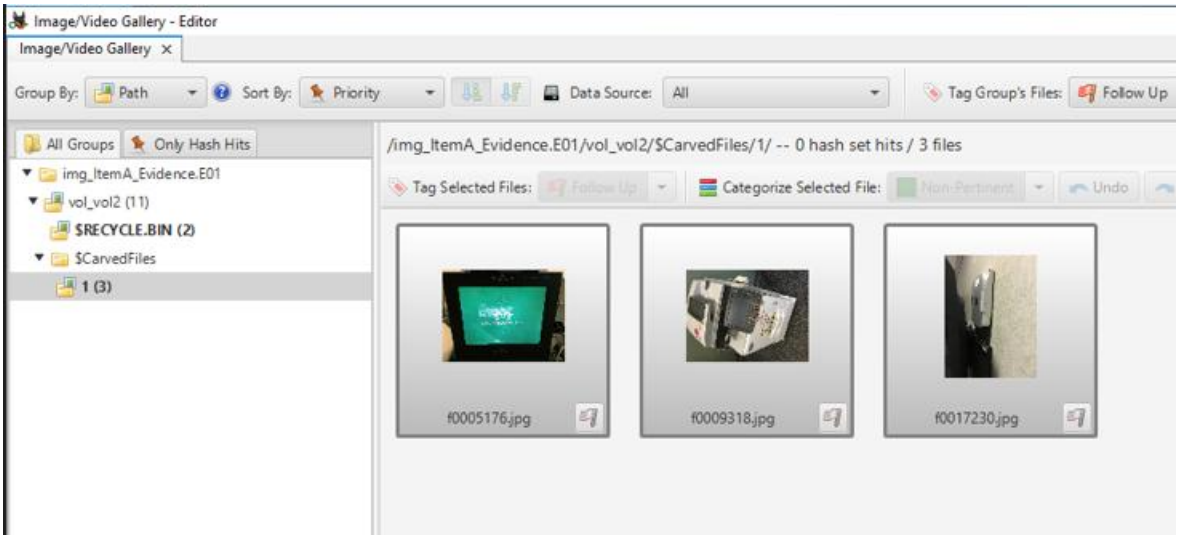
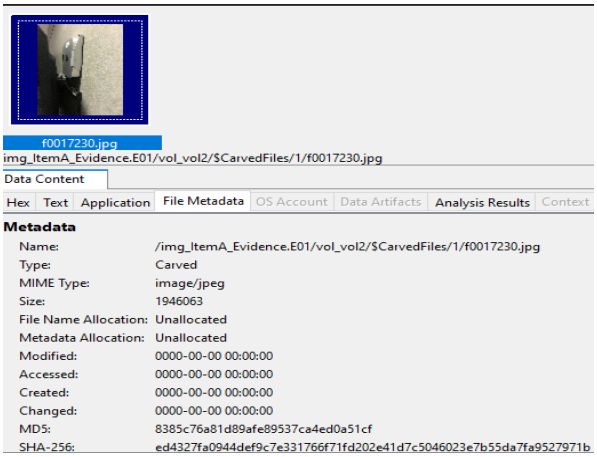


Figure 9: Image showing recovered files in Autopsy.

Photographs of the Apple Device recovered.



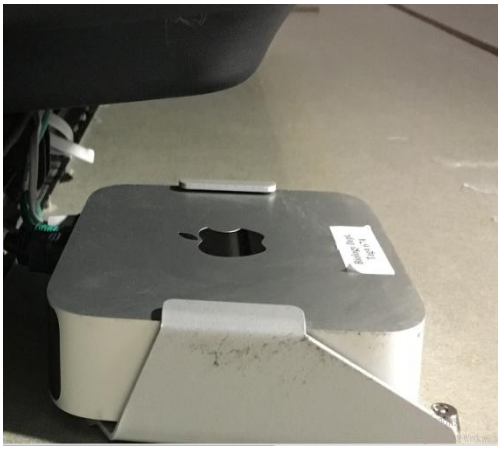


Figure 10: Recovered deleted image showing Apple Mac Mini hardware.

Photographs of other devices recovered.

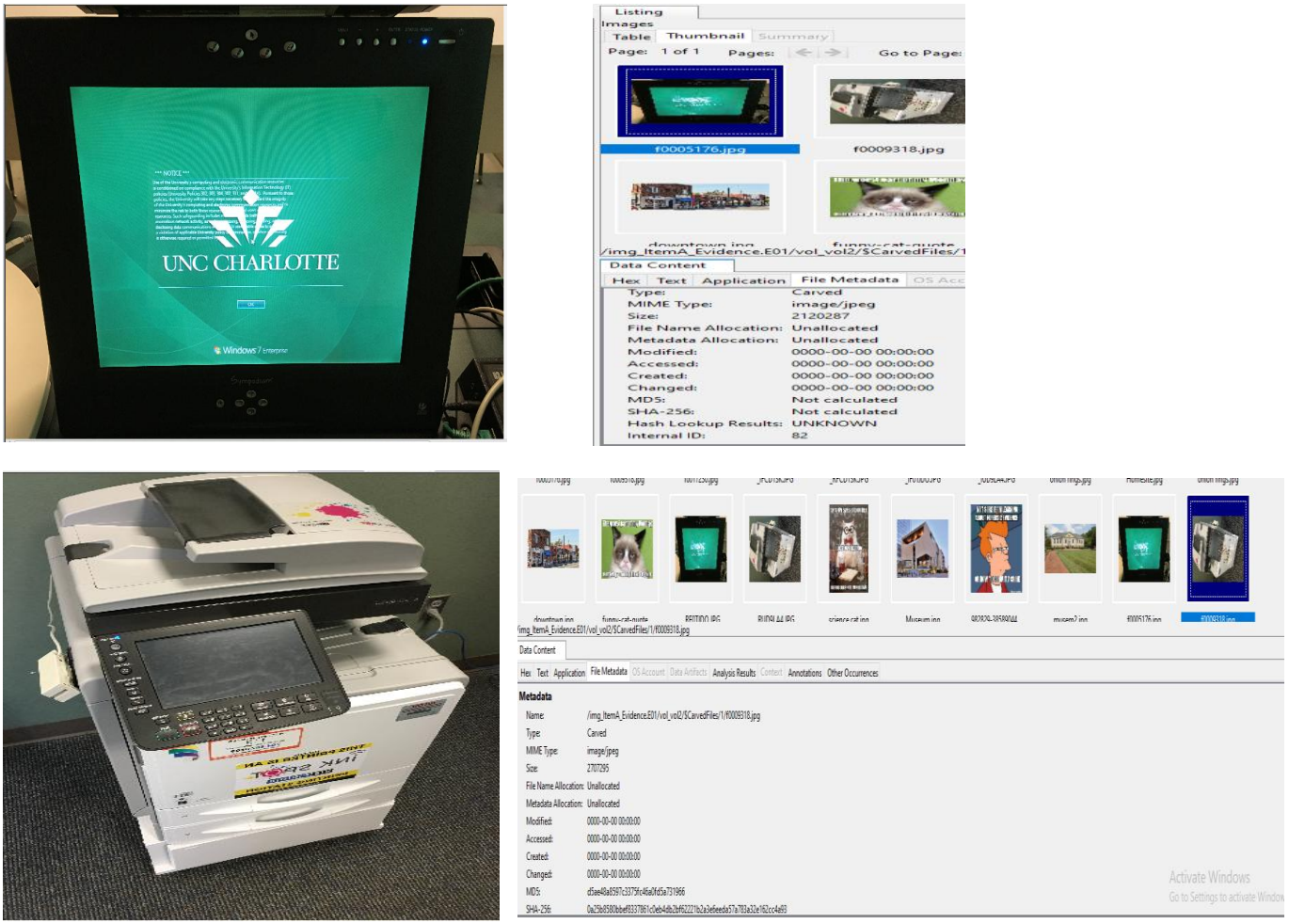


Figure 11: Image of a Printer and Sympodium Technology device recovered.

Recuva classified the file as:

- State: Excellent and one Unrecoverable
- Comment: No overwritten clusters detected

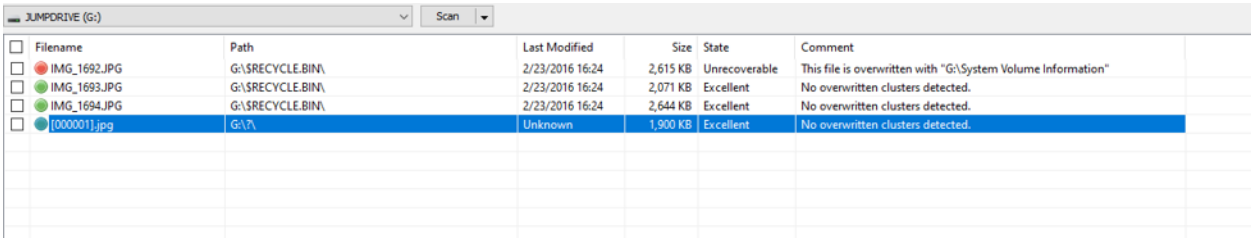


Figure 12: Recuva status indicating intact recovery from unallocated space.

5.2 Images Showing University Environment

Recovered images include:

- IMG_1693.JPG Monitor displaying “UNC Charlotte” login screen and university branding.
- IMG_1694.JPG Ricoh printer labeled “UNCC Printing Services Ink Spot.”

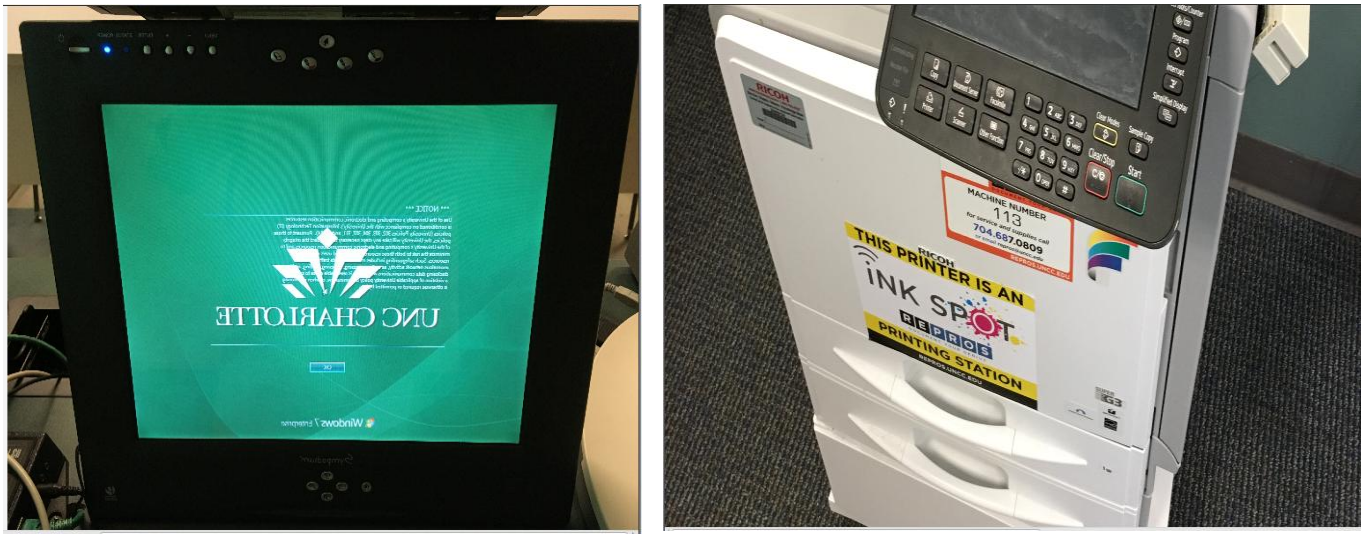


Figure 13: UNCC Printing Services Ink Spot and Monitor displaying UNC Charlotte login screen and university branding.

These images establish environmental context consistent with university facilities.

5.3 Camera Make, Model & Timeline

EXIF metadata extracted from multiple images indicates:

- Device Make: Apple
- Device Model: iPhone 6s
- Date: February 23, 2016
- Time: 16:08 EST

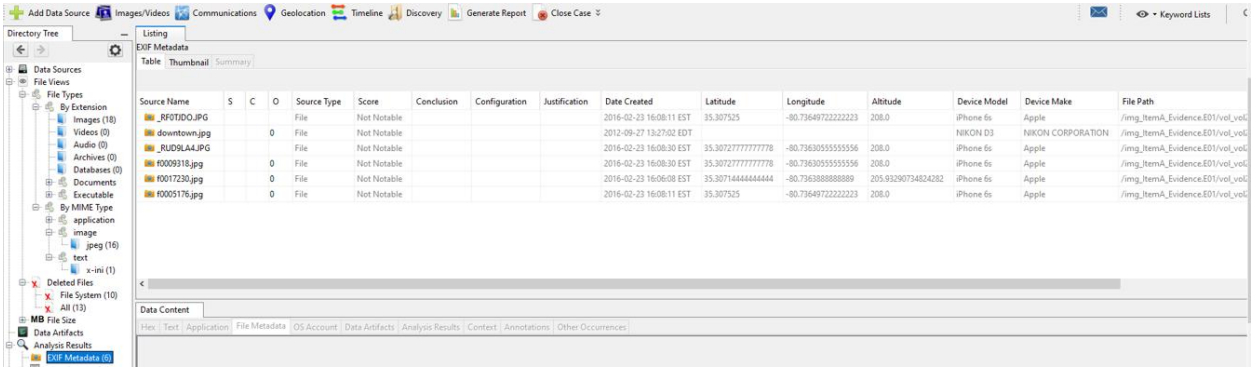


Figure 14: Exif metadata indicating that the images were captured using an Apple iPhone 6s during the reported timeframe.

5.4 GPS Location Data

Embedded GPS coordinates extracted from multiple images include:

- 35.30727777777778, -80.73630555555556
- 35.307525, -80.73649722222223

These coordinates correspond to Woodward Hall on UNCC Campus.

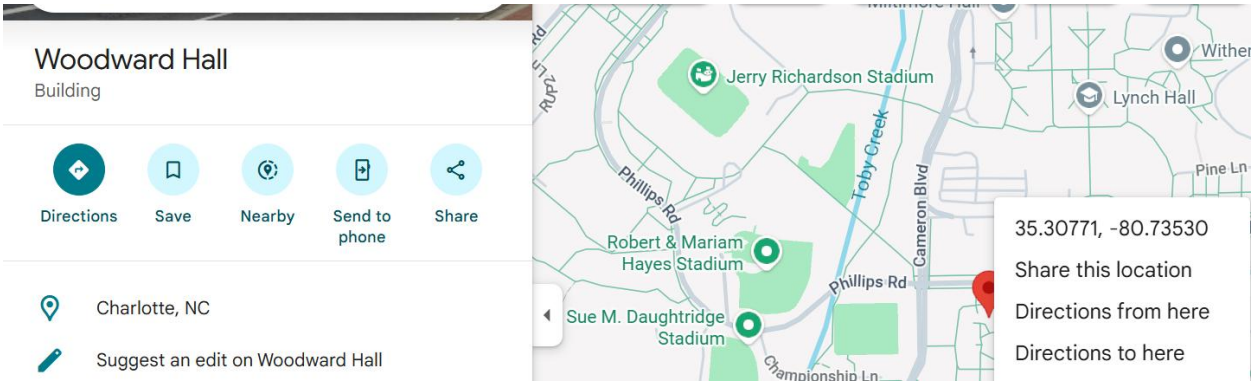


Figure 15: Image showing that the geolocation data is consistent with the reported location of the theft incidents.

5.5 Deleted Files & Overwriting Activity

Several files were located within the $RECYCLE.BIN directory, indicating manual deletion activity.

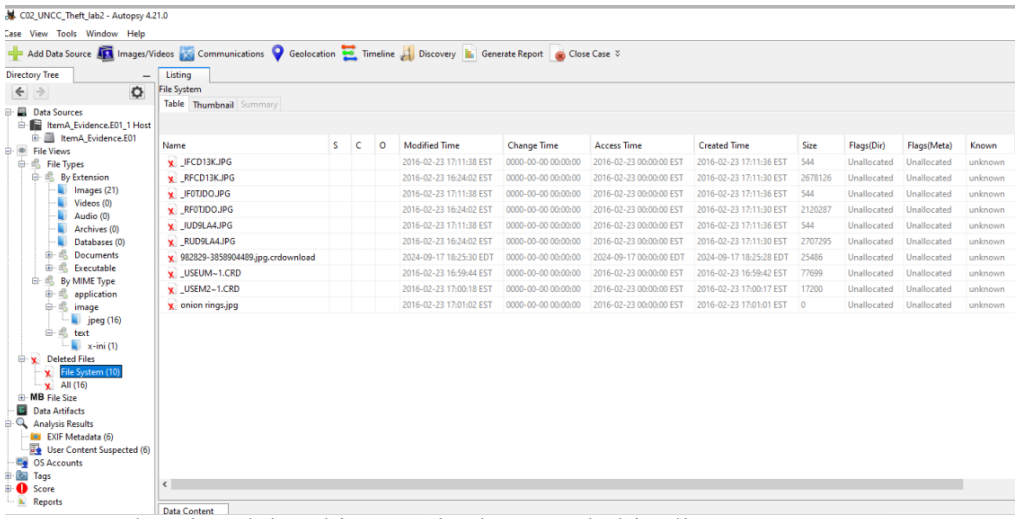


Figure 16: Image showing deleted images in the recycle bin directory.

Recuva reported IMG_1692.JPG as:

- State: Unrecoverable
- Comment: Overwritten by system data

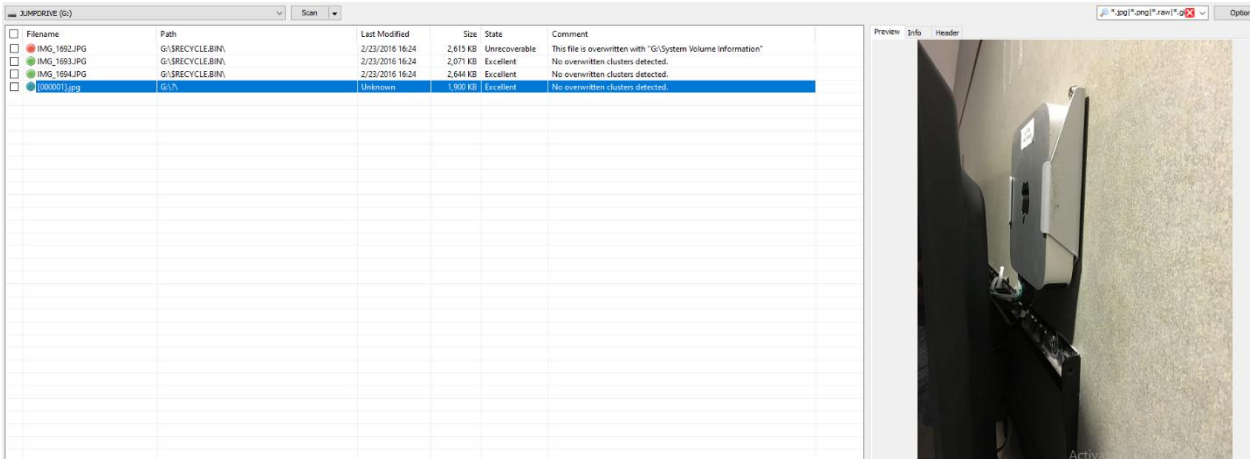


Figure 17: Image showing an unrecoverable image in Recuva.

7. CONCLUSION

The digital evidence recovered from the USB thumb drive includes photographs of Apple hardware and images captured within a UNCC environment on February 23, 2016. The images contain embedded metadata indicating they were captured using an Apple iPhone 6s and include GPS data consistent with the UNC Charlotte campus.

Deleted files were recovered through forensic carving, and additional file deletion activity was identified.

I am prepared to testify under oath regarding:

- The forensic tools and methodologies used
- The integrity and preservation of the evidence
- The recovery of deleted files
- The metadata and geolocation findings

I certify that this examination was conducted using accepted digital forensic principles and industry-standard practices.

Respectfully submitted,
Douglas Akwasi Kwarteng.
Digital Forensic Examiner UNCC.