Lab Assignment 5 Ana Sharma

# **Task – Windows Examination**

**Overview**

Dr. Quincy assigned me to investigate a forensic image collected from a desktop computer believed to be used by Eugene “Gene” Poole, a known felon under suspicion for drug production and distribution. The image, titled Gene2021.E01, was acquired under the authority of a North Carolina District Court search warrant requested by Detective Jessica Fletcher. My task was to examine the image for traces of digital activity that could help confirm ownership of the system, uncover potential locations of drug activity, and identify any technical tools Gene or his associates might have used to cover their tracks.

**Forensic Acquisition and Environment Setup**

The analysis was conducted using a Windows 11 Enterprise, 64-bit on version 23H2 and processor: Intel(R) Xeon(R) W-2255 CPU @ 3.70GHz 3.70 GHz and 1 TB storage. The forensic image, Gene2021.E01, was loaded into Access Data FTK Imager version 4.1.1.1 to begin the analysis and further used Autopsy version 4.18.0. I additionally made use of Arsenal Image Mounter version 3.6.188. For documentation purposes, I used Snipping Tool and Microsoft Word. The integrity of the image was verified using both **MD5** and **SHA1** hash algorithms. The hash values matched the expected outputs:

* **MD5**: 75b28a2dd3d0c58fd1b944d1707cba1a
* A screenshot of a computer

  AI-generated content may be incorrect.**SHA1**: 3459a1097f557d132ed8bc7a4331c828835390fd

This confirmed that the image had not been tampered with since its initial acquisition. To conduct deeper analysis, I mounted the image using ArsenalImageMounter and generated a .vhd file, which was then loaded into Autopsy for structured investigation. I also used WinPrefetchView for analyzing prefetch data and ExifTool to review image metadata.

Screenshot below: Verified Hash Values

A screenshot of a computer

AI-generated content may be incorrect.

1. Gene denies the computer is his. Who was the Owner and the Organization to whom it was registered?

A screenshot of a computer

AI-generated content may be incorrect.Gene denied the computer was his, so I checked the system registry. In the SOFTWARE hive, under the Windows NT CurrentVersion path, I found values that listed the RegisteredOwner and Organization. These entries clearly pointed to Gene as the primary user, contradicting his denial and providing strong evidence of ownership.

Screenshot shows owner information, and that Eugene Poole is the Registered Owner. The Registered Organization shows: “The Guild of Calamitous Intent”.

1. We believe the location of his mountain hideout might been in a text file. Can you tell us anything about that?

A screenshot of a computer

AI-generated content may be incorrect.Mountain Hideout Clue: In Autopsy, I went to File Types > By Extension > Documents > Plain Text, where I found a file titled $RC97QP5.txt, which was located in the Recycle Bin. This file contained a short note that read: *“Remember to take a new mosquito net. Also, remember to take more iodine tablets.”* These types of supplies suggest someone preparing for a remote location – possibly a survivalist or mountainous area. To support this theory, I checked the web search history, which showed the user had looked up directions from Charlotte to Boone and checked Boone-specific weather conditions. Boone is a known mountain town in the Blue Ridge Mountains of North Carolina, and these combined artifacts suggest Gene may have been planning a trip or stay in that area – possibly tied to the rumored hideout.

A screenshot of a computer

AI-generated content may be incorrect.

Screenshot above: $RC97QP5.txt in the file path ($Recycle.Bin\...)  
  
  
  
Screenshot: keyword search “boone”.   
A screenshot of a computer

AI-generated content may be incorrect.

1. We found a flash drive we believe may have been used with Gene's computer, but it was at the home of his associate. Can you determine what thumb drives may have been attached to Gene's computer to help us get new legal authority?

USB Activity: To investigate whether a flash frive found at an associate’s residence had ever been connected to Gene’s computer, I navigated to Data Artifacts > USB Devices Attached in Autopsy. There, I found a history of connected USB devices, including a Transcend JetFlash – a common type of flash drive. In addition to the JetFlash device, two other USB entries were listed:

* Root\_hub20
* root\_hub

These typically represent USB host controllers or hubs and suggest the system was actively handling external device connections during those sessions. The presence of the Transcend JetFlash strongly indicates that the system had contact with a flash drive, which could be the same one found with Gene’s associate – providing legal grounds to further link the devices and expand the investigation.

Screenshot below: external flash drive attached and device information under “Data Artifacts”, labeled as “Extracted Content” 🡪 “USB device attached” to reveal the SYSTEM information under Data Artifacts panel in the bottom right.

A screenshot of a computer

AI-generated content may be incorrect.

4. Was he using an office program to make documents? We think some files we got from our informant may have been created by Gene. Any idea how often he used the software?

Office Software Usage: To determine whether Gene had used office software to create or edit documents – possibly the same ones recovered from an informant – I first examined the list of installed programs in Autopsy. There, I found that LibreOffice 6.0.4.2 was present on the system, suggesting that office-style document editing was available. To investigate how frequently this software was used, I turned to prefetch file analysis. I navigated to the Windows\Prefetch directory within the image, exported the prefetch files, and examined them using WinPrefetchView. The prefetch file named SOFFICE.BIN-F133562F.pf (associated with LibreOffice) showed that the application had been launched 8 times. This provides strong evidence that LibreOffice was not just installed, but actively used, making it likely that Gene was responsible for creating or modifying the documents in question.

A screenshot of a computer

AI-generated content may be incorrect.

Screenshot: LibreOffice installed

A screenshot of a computer

AI-generated content may be incorrect.Screenshot: Path for prefetch folder showing SOFFICE.BIN

Screenshot: Files related to LibreOffice. File opened: Budget.xlsx

A screenshot of a computer

AI-generated content may be incorrect.Screenshot: Results of Prefetch files displayed using WinprefetchView

A screenshot of a computer

AI-generated content may be incorrect.

1. Gene may have had an interest in Cybersecurity and "hacking", even though his strengths are in chemistry, bio-engineering and machining. Is there any evidence he may have tried to use or learn anything about hacking tools?

Interest in Hacking Tools: To determine whether Gene had any involvement or interest in cybersecurity or hacking, I reviewed the system’s web search history through the Data Artifacts > Web History section in Autopsy. The analysis uncovered several notable searches related to disabling Windows Defender on a Windows machine. This action is commonly associated with users attempting to bypass basic system proterctions. Even more telling were search entries referencing “Mimikatz”, a well known post exploitation tool used to extract passwords and sensitive credentials from Windows systems. The presence of this search strongly suggests that Gene was exploring or testing tools associated with hacking and offensive security. These findings indicate that, despite his background in bioengineering and chemistry, Gene possessed a technical curiosity and potentially the intent, to explore hacking-related activities.

Screenshots show: relevant files and entries related to disabling windows defender, search results of MimiKatz, hacking tools and visited URLS, profiles as well as entire Web History.

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

6. Gene may have used a phone to photograph a secure location, according to our source. Any idea what? What happened to the device?

Secure Location Photos from Phone: To investigate whether Gene used a phone to capture sensitive content, I examined email communicationis by navigating to Data Artifacts > e-mail messages in autopsy. Among the email threads, I located a conversation with the subject line: “R: Android”. Upon reviewing the email contents, several messages referenced a mobile device. In one specific message, the sender stated, *“I have a phone,”* and went on to describe the Android device as *“kind of messed up.”* While the message does not explicitly mention photographing a secure location, it does confirm that Gene had access to an Android phone that may have been capable of taking pictures. This communication provides context and supports the possibility that Gene possessed a mobile device at the time, aligning with the theory that a phone was used to capture images of interest during the investigation.   
Screenshot shows: Gene’s email message clearly stating that she has a phone that she needs A screenshot of a computer

AI-generated content may be incorrect.help using.

Screenshot shows: Gene confirming that the phone in hand contains photos.

A screenshot of a computer

AI-generated content may be incorrect.

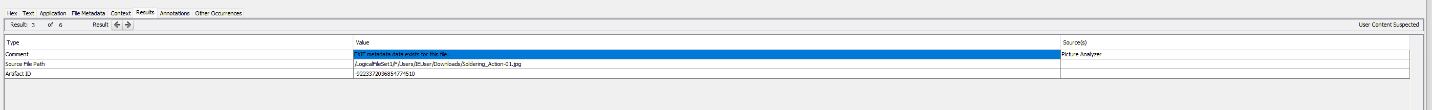
7. Any other devices he might have used to photograph sensitive technology?

Use of Other Photo Devices: To identify any additional devices that Gene may have used to capture sensitive material, I reviewed image metadata via Analysis Results > EXIF Metadata in Autopsy. Within this artifact set, I found an image that showed an individual soldering a computer chip, an activity commonly associated with tech modification or hardware tampering. Upon inspection of the EXIF data for the image, it was revealed that the photo had been taken with a Nikon D800 digital camera, manufactured by Nikon Corporation. This confirms that a professional grade camera was used at least once, suggesting Gene may have utilized higher-end equipment, not just mobile devices, to document or photograph technology-related subjects.

A screenshot of a computer

AI-generated content may be incorrect.A computer screen shot of a red and white computer

AI-generated content may be incorrect.Screenshot shows: Image of sensitive technology and it being taken on Nikon camera.



8. Gene has mentioned in recorded conversations he has a stash of drugs he keeps at a beach house just in case his lab gets raided. Is there anything that might tell us he is familiar with particular beaches, or towns near beaches?

Beach House Connection: To determine whether Gene had any connection to specific beaches or coastal towns, I examined the system’s web bookmarks within Autopsy. Several entries pointed to areas along the North Carolina coast, indicating a potential link to the beach house mentioned in recorded conversations. One bookmark referenced Robert Harrill, famously known as the Fort Fisher Hermit, with a saved image depicting what appears to be his bunker in Kure Beach, NC. This is a quiet coastal area that could plausibly host a hidden stash. Another bookmark pointed to Old Books on Front Street, an antique bookstore in Wilmington, NC, suggesting Gene’s interest in local landmarks or history. Additional searches showed interest in Melvin’s Hamburgers and Hot Dogs, a small diner in Elizabethtown, just inland from the coast. These saved items, when considered together, reveal Gene’s familiarity with specific beach towns and surrounding areas, supporting the possibility that he frequently or was planning to use a coastal location as a backup.

A screenshot of a computer

AI-generated content may be incorrect.Screenshot shows: Bookmarked webpages and search results of Robert Harrill and revealed details of beach and bookstores through: “tripadvisor.com”, “msn.com”, “charlotteobserver.com”

A screenshot of a computer

AI-generated content may be incorrect.

A concrete structure with a door open

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

Screenshot: Reverification of Hash Values

A screenshot of a computer

AI-generated content may be incorrect.

* **MD5**: 75b28a2dd3d0c58fd1b944d1707cba1a
* **SHA1**: 3459a1097f557d132ed8bc7a4331c828835390fd

Hash values are re-verified successfully.

**Conclusion**

Based on the evidence recovered, Gene Poole’s denial of ownership is contradicted by registry entries linking him directly to the system. The presence of external storage devices, frequent use of document software, interest in cybersecurity tools such as MimiKatz, and detailed search history paint a picture of a user who was both technically curious and cautious. Combined with geographic search patterns and deleted file contents, the investigation supports the theory that Gene was operating from remote and coastal hideouts. This report, supported by documented screenshots and extracted files, has been compiled for further legal consideration.

Digital Forensics Examiner,

Ananya Sharma

UNCC Forensics Lab

04/18/2025