# CASE# 20211128

Louis Brody

BRODY FORENSICS  123 Main St. Greenville SC. 29601

# Table of Contents

## Executive Summary:

The incident under investigation occurred in a residential setting, specifically within the kitchen area of a home. The scene was first encountered with a body lying on the floor in front of the kitchen island. Adjacent to the victim was a laptop, prominently displaying an active Nmap scan under the Kali Linux operating system, with an image of a reactor on its screen. This initial observation hinted at potential cybersecurity, or informational threats intertwined with the physical crime scene.

Adjacent to the laptop, a cup of tea was found, which later revealed an alarming level of radiation through forensic analysis, adding a complex layer of biochemical hazard to the case. The proximity of the cell phone to the victim suggested a personal connection, potentially offering insights into the victim's last communications or actions leading to the incident. Furthermore, the discovery of a USB drive clandestinely placed under a coffee container at the coffee station hinted at hidden information or data pertinent to the unfolding mystery.

The evidence seized, encompassing the laptop, tea, cell phone, and USB drive, underwent meticulous forensic scrutiny. The laptop's Nmap scan and the image of the reactor were analyzed for any underlying significance or threat they posed, while the cell phone's data extraction aimed to reconstruct the victim's recent interactions and activities. The radiological analysis of the tea introduced a hazardous dimension to the crime, necessitating a careful examination of potential poisoning or exposure routes. Meanwhile, the USB drive held the promise of unraveling further layers of the incident, possibly containing crucial data or clues.

This executive summary encapsulates the gravity and complexity of the crime scene and the evidence therein. The interplay of digital, chemical, and physical elements outlines the multifaceted nature of the case, necessitating an integrated forensic approach to decipher the events leading to the tragic scene and identify the responsible entities. The subsequent analysis of the seized evidence aimed to piece together the fragmented narrative, shedding light on the motivations, means, and opportunities that culminated in the incident at hand.

## Objectives:

Laptop Forensic Analysis: The first objective for the forensic analyst is to conduct a thorough examination of the laptop, particularly focusing on the Nmap scan results and the open applications, such as the image of the reactor. This involves analyzing the laptop's system logs, running processes, and network activity to understand the purpose of the Nmap scan and any potential connections to external networks or systems. The analyst needs to determine if the laptop was used for malicious activities or if it holds any clues related to the crime, helping to reconstruct the sequence of events leading to the incident.

USB and Cell Phone Data Recovery and Analysis: The second objective encompasses the forensic examination of the USB drive and cell phone to recover and analyze all accessible data. For the USB drive, this includes identifying and investigating the contents, looking for any hidden, encrypted, or deleted files that might be relevant to the case. Regarding the cell phone, the analyst must extract and examine call logs, text messages, emails, and any other relevant data that could provide insights into the victim's communications and activities prior to the incident. This analysis aims to uncover any connections between the data found on these devices and the circumstances surrounding the crime, potentially leading to motive, suspects, or additional evidence.

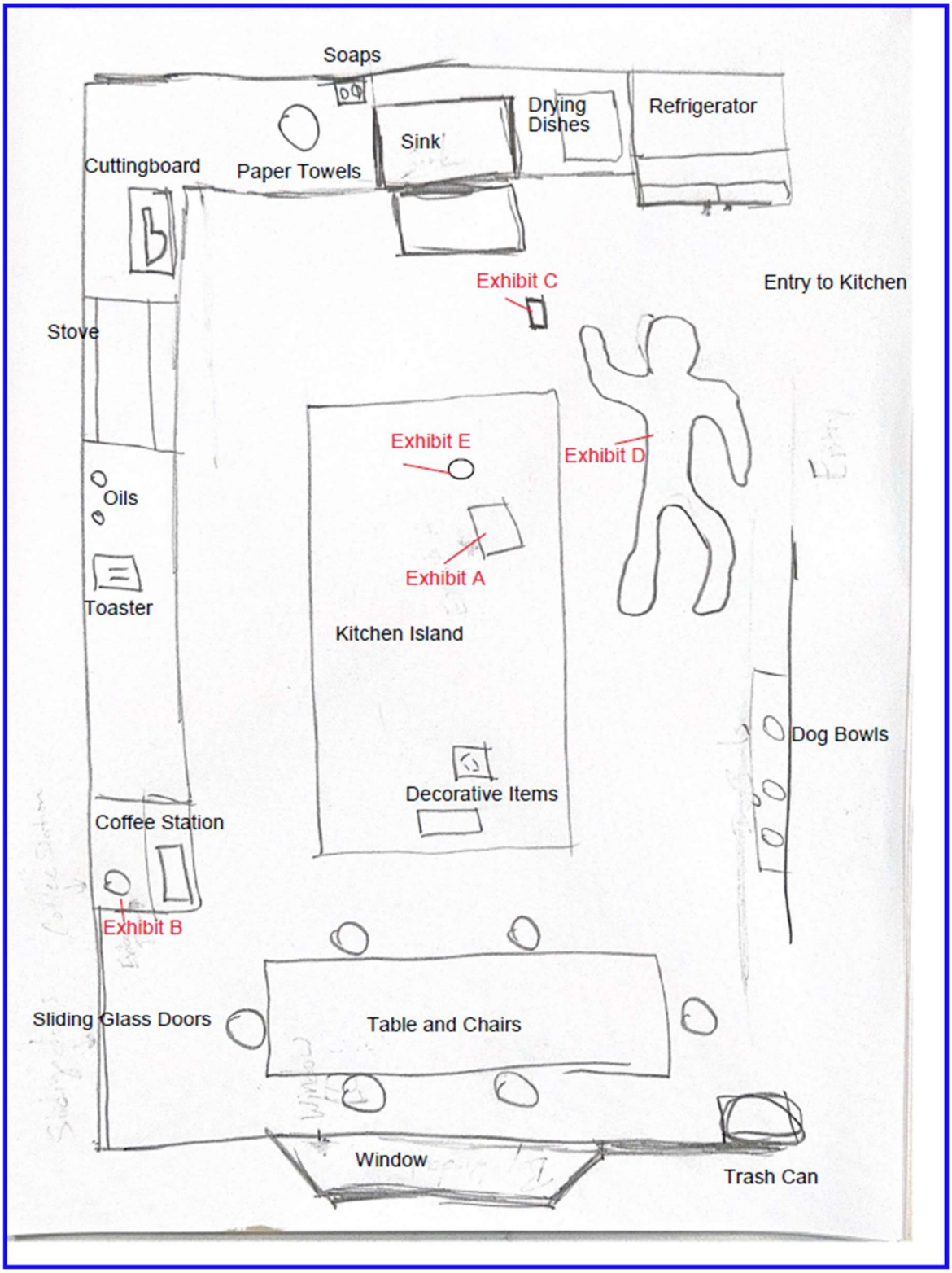
## Crime Scene Details:

The crime scene is set in a residential kitchen, characterized by modern amenities and an overall orderly appearance. At the center of the investigation is a body discovered on the floor in front of the kitchen island, which serves as the focal point of the scene. On top of the island the laptop was found, displaying an active Nmap scan under the Kali Linux operating system, alongside an image of a reactor, suggesting a technical or research-related endeavor.

Adjacent to the laptop, a cup of tea was found, later found to contain high levels of radiation. On the floor beside the body, a cell phone is recovered, hinting at a potential trail of digital communication and activities leading up to the tragic event. Concealed under a coffee container at the kitchen's coffee station, a USB drive is discovered, its contents possibly holding key evidence or clues.

The kitchen shows no immediate signs of forced entry or struggle, implying that the incident may have unfolded without external disturbance. The mix of a typical home environment with advanced and dangerous elements at the scene sets up a complicated situation for forensic analysis. It hints at a story that blends everyday life with possibly sinister activities.

**Crime Scene Sketch – Diagram 1-A**



# Crime Scene Phots and Exhibits

## Exhibit A - Laptop Image 1


## Exhibit A – Image 2 Laptop (screen output)

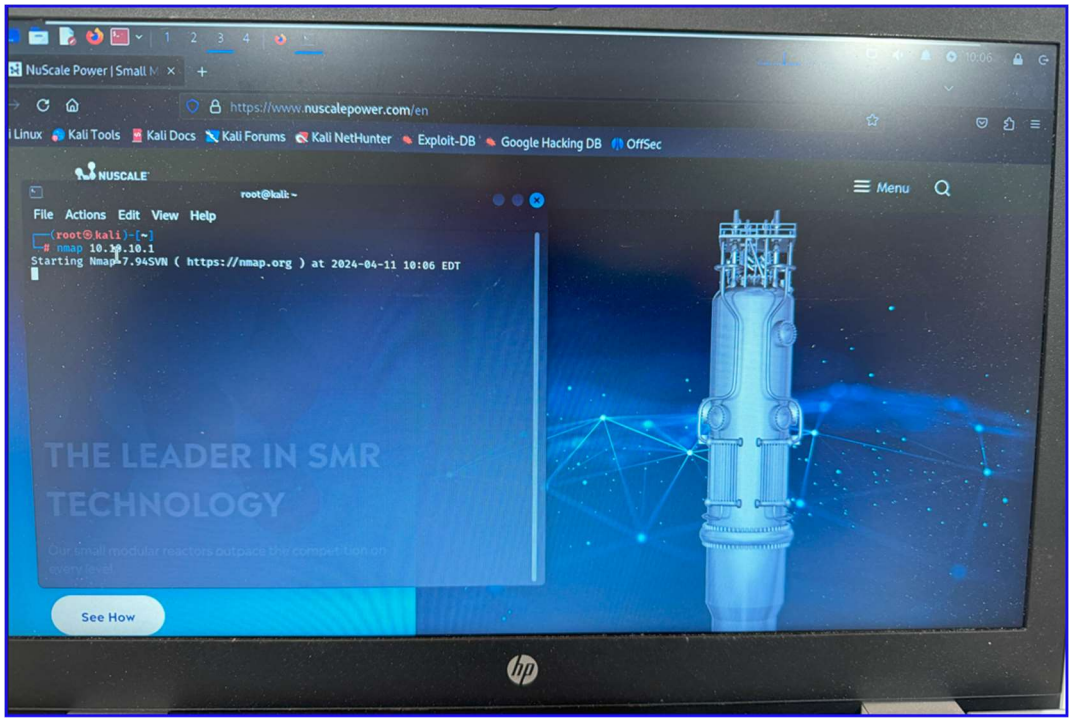


**Exhibit B – Hidden USB Image 1**


**Exhibit B – Hidden USB Image 2**

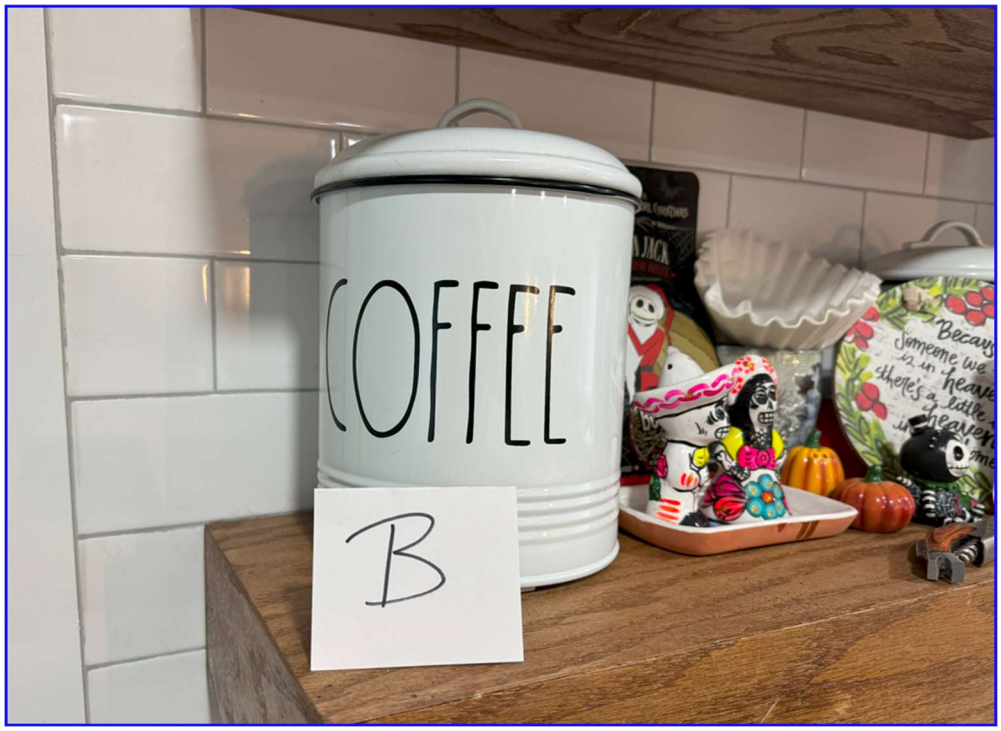


**Exhibit B – Hidden USB Image 3**

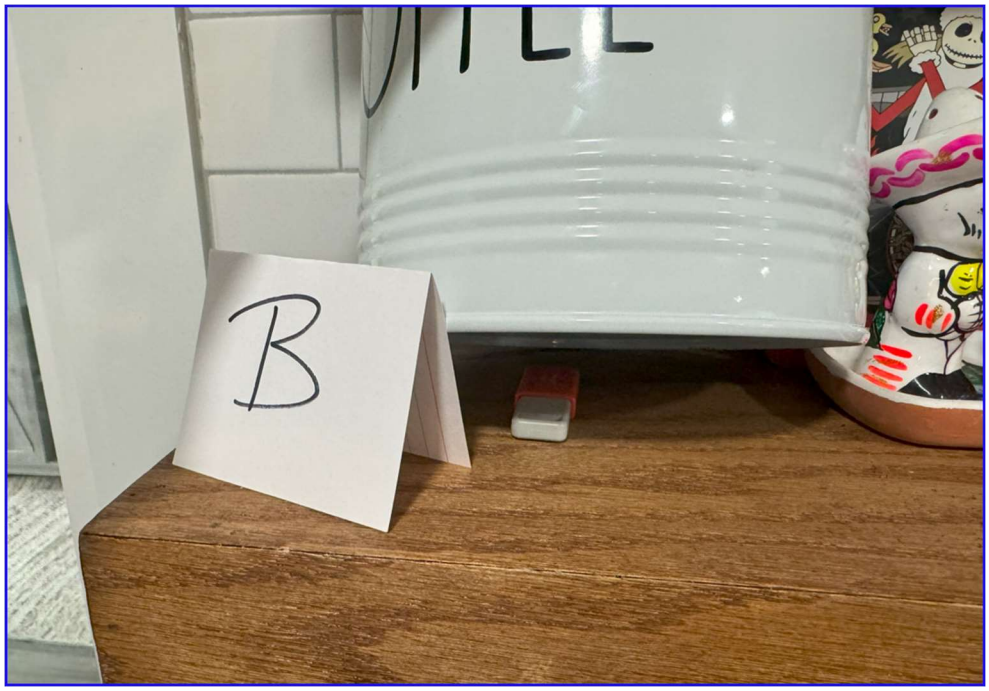



**Exhibit B – Hidden USB Image 4**

**Exhibit C – Cell Phone Image 1**


**Exhibit D – Victim Outline Image 1**

**Exhibit D – Victim Outline Image 2**

**Exhibit E – Teacup Image 1**

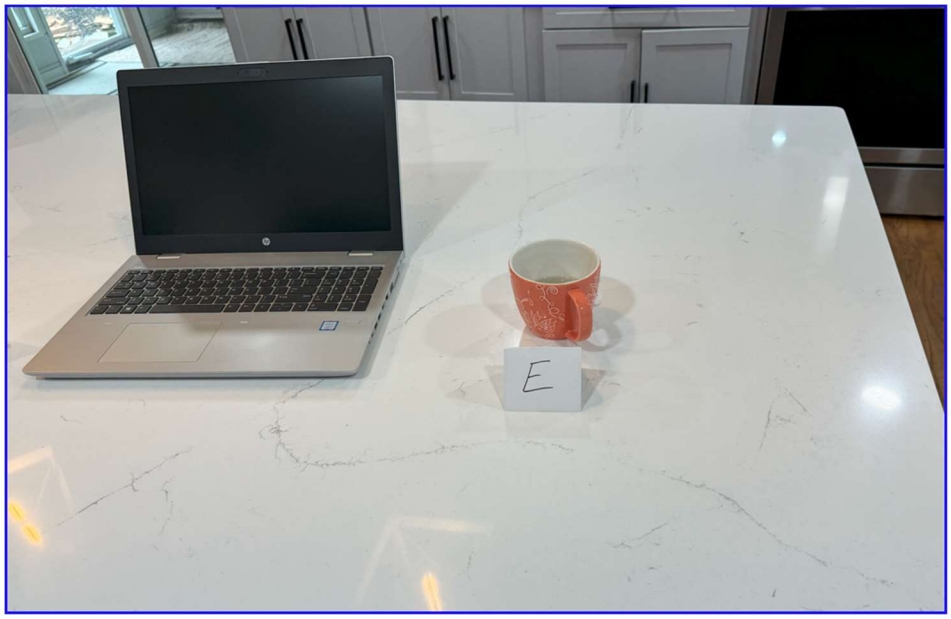
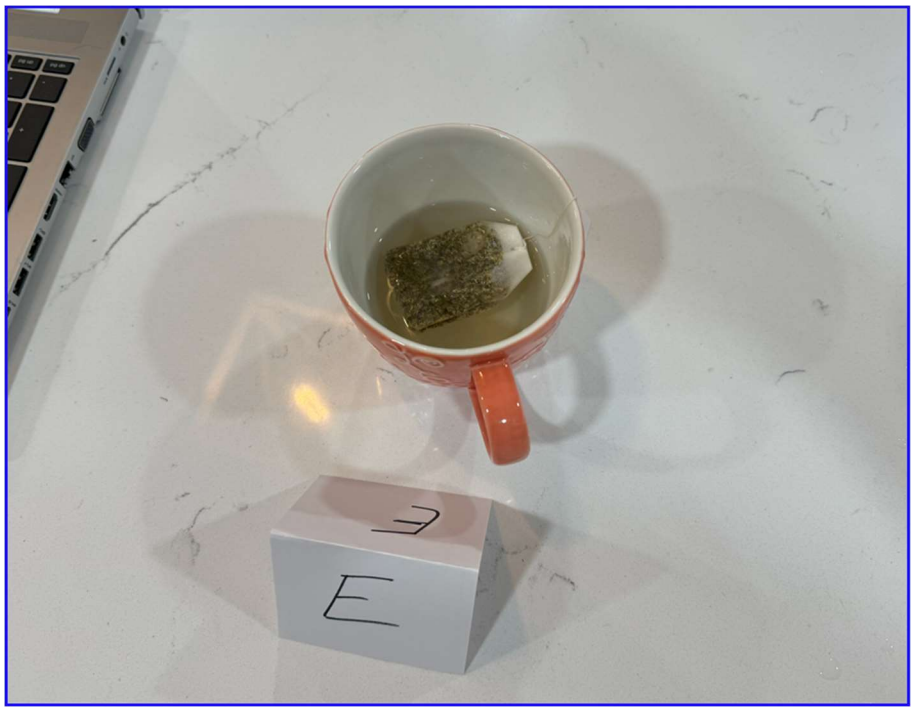


**Exhibit E - Teacup Image 2**




## Computer Evidence Analyzed:

Exhibit A: HP ProBook 650 G4 Laptop

Tag Number: A1

Description: An HP ProBook 650 G4 laptop, found open and powered on atop the kitchen island. The device was running on battery power with 35% battery life remaining and was not plugged into an electrical outlet. It was operating under the Kali Linux OS and was executing a port scan targeting the NuScale IP subnet at the time of discovery. The laptop contained numerous applications related to network monitoring and hacking.

Media Serial Number: D3B031C4-744-4BF5-9D64-6BCB739EC61F

Storage Capacity: 1 TB SSD

Location Found: Kitchen Island

Additional Notes: The laptop's active use of hacking and monitoring tools, along with the running port scan, suggests the user was engaged in advanced network analysis or potential unauthorized activities.

Exhibit B: PNY USB 2.0 Drive

Tag Number: B1

Description: A PNY USB 2.0 drive, found concealed under a coffee container at the crime scene in the kitchen. The drive's hidden placement indicates a possible intent to obscure its presence or protect its contents from immediate discovery.

Media Serial Number: 071c088d288b2208

Storage Capacity: 32 GB

Location Found: Coffee Station

Additional Notes: The contents and activity logs of the USB drive need to be examined to determine its role in the incident and if it contains any data relevant to the crime scene or the victim's activities.

Exhibit C: Apple iPhone 12

Tag Number: C1

Description: An Apple iPhone 12, located on the kitchen floor approximately 18 inches from the victim's body. The proximity to the victim suggests it may have been in use close to the time of the incident.

Media Serial Number: J3F58R5L2N

Storage Capacity: 256 GB

Location Found: Near the victim on the kitchen floor.

Additional Notes: The cell phone's call logs, messages, applications, and data usage patterns will be critical to reconstructing the victim's communications and activities leading up to the event.

## Relevant Finding:

**Exhibit A: HP ProBook 650 G4 Laptop**

The HP ProBook 650 G4, found on the kitchen island, was operational with Kali Linux, indicating a user with advanced technical skills. The active Nmap scan targeting the NuScale IP subnet suggests a focused interest in this energy company, potentially for malicious purposes like cyber espionage or unauthorized data access. The change of the admin account to "JACKO SMITH" and the retrieval of encrypted hashes underscore a deliberate effort to secure or obscure the user's digital footprint. This laptop, with its specialized software and activities, serves as a pivotal piece of evidence, hinting at the intent and capabilities of the individual involved.

The laptop's use for network scanning and the presence of tools typically employed in penetration testing and cybersecurity assessments raise questions about the user's motives. Were these actions part of a legitimate security assessment, unauthorized hacking, or something more nefarious? The uncracked hashes further indicate secured data, possibly hiding crucial information regarding the user's activities or intentions.

**Exhibit B: PNY USB 2.0 Drive**

The USB drive, discreetly placed under a coffee container, contained schematics of NuScale reactors and documents related to the "Bahama Papers." This indicates a deep engagement with sensitive, possibly classified, information. The reactor schematics suggest an interest or involvement in nuclear technology, potentially for legitimate research or illicit activities like industrial espionage or sabotage. The reference to the "Bahama Papers" implies a financial or geopolitical motive, perhaps linked to corruption, money laundering, or other financial crimes.

The concealment of the drive and the nature of its contents point to the user's awareness of the sensitivity and potential illegality of their activities. The reactor schematics and documents found on the USB drive are crucial for understanding the broader context and implications of the user's actions, potentially tying them to larger issues of corporate or national security.

**Exhibit C: Apple iPhone 12**

Located near the victim, the iPhone 12 could hold personal communications, browser history, apps usage, and other data offering insights into the victim's state of mind and activities before the incident. This device is likely to have been used for coordinating or documenting the activities related to the found digital evidence. Investigating the phone's contents could reveal connections to the laptop and USB drive findings, providing a more comprehensive picture of the incident.

The phone's analysis is essential for piecing together the victim's interactions and movements leading up to the event. It could uncover evidence of threats, blackmail, or insider communications related to the sensitive data found on the USB drive and the laptop's activities.

**RAM Analysis of HP ProBook 650 G4**

The RAM analysis revealed the admin account changed to "JACKO SMITH," a possibly pseudonymous identity used to mask real activities or affiliations. The hashes, although uncracked, represent a barrier that, once breached, may unveil further insights into the security measures implemented and the sensitivity of the concealed data.

The technical proficiency indicated using sophisticated tools and actions, like running Nmap and changing admin credentials, highlights the user's calculated approach to their activities. This analysis not only aids in profiling the user's technical capabilities but also in understanding the lengths they went to secure their operations and cover their tracks.

## User Applications:

| Program Name | Date/Time |
|---|---|
| Microsoft Visual C++ 2019 X64 Additional Runtime - 14.29.30040 v.14.29.30040 | 2021-11-28 20:27:40 EST |
| Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.29.30040 v.14.29.30040 | 2021-11-28 20:27:38 EST |
| Active@ KillDisk 14 v.14 | 2021-11-28 20:22:27 EST |
| Mozilla Maintenance Service v.94.0.2 | 2021-11-28 20:19:48 EST |
| Mozilla Firefox (x64 en-US) v.94.0.2 | 2021-11-28 20:19:46 EST |
| 7-Zip 21.06 (x64) v.21.06 | 2021-11-28 20:17:32 EST |
| DXM_Runtime | 2019-12-07 09:52:05 EST |
| MPlayer2 | 2019-12-07 09:52:05 EST |
| AddressBook | 2019-12-07 09:17:28 EST |
| Connection Manager | 2019-12-07 09:17:28 EST |
| DirectDrawEx | 2019-12-07 09:17:28 EST |
| Fontcore | 2019-12-07 09:17:28 EST |
| IE40 | 2019-12-07 09:17:28 EST |
| IE4Data | 2019-12-07 09:17:28 EST |
| IE5BAKEX | 2019-12-07 09:17:28 EST |
| IEData | 2019-12-07 09:17:28 EST |
| MobileOptionPack | 2019-12-07 09:17:28 EST |
| SchedulingAgent | 2019-12-07 09:17:28 EST |
| WIC | 2019-12-07 09:17:28 EST |
| Microsoft Edge Update v.1.3.153.53 | 2021-11-28 23:02:05 EST |
| Microsoft Edge v.92.0.902.67 | 2021-11-28 23:01:49 EST |
| Wireshark 3.6.0 64-bit v.3.6.0 | 2021-11-28 20:29:37 EST |
| Npcap v.1.55 | 2021-11-28 20:28:24 EST |
| Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.30040 v.14.29.30040.0 | 2021-11-28 20:27:40 EST |
| Steam v.2.10.91.91 | 2021-11-28 20:25:15 EST |
| Nmap 7.92 v.7.92 | 2021-11-28 20:23:22 EST |
| Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.29.30040 v.14.29.30040.0 | 2021-11-28 20:23:22 EST |
| Microsoft Visual C++ 2019 X86 Additional Runtime - 14.29.30040 v.14.29.30040 | 2021-11-28 20:23:21 EST |
| Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.29.30040 v.14.29.30040 | 2021-11-28 20:23:19 EST |
| Glary Utilities 5.152 v.5.152.0.178 | 2021-11-28 20:21:30 EST |
| Artweaver Free 7 v.7.0.10 | 2021-11-28 20:18:06 EST |
| DXM_Runtime | 2019-12-07 09:52:04 EST |
| MPlayer2 | 2019-12-07 09:52:04 EST |
| AddressBook | 2019-12-07 09:17:27 EST |

| | |
|---|---|
| Connection Manager | 2019-12-07 09:17:27 EST |
| DirectDrawEx | 2019-12-07 09:17:27 EST |
| Fontcore | 2019-12-07 09:17:27 EST |
| IE40 | 2019-12-07 09:17:27 EST |
| IE4Data | 2019-12-07 09:17:27 EST |
| IE5BAKEX | 2019-12-07 09:17:27 EST |
| IEData | 2019-12-07 09:17:27 EST |
| MobileOptionPack | 2019-12-07 09:17:27 EST |
| SchedulingAgent | 2019-12-07 09:17:27 EST |
| WIC | 2019-12-07 09:17:27 EST |

## Internet Activity:

| URL | Date Accessed |
|---|---|
| http://www.glarysoft.com/update/release-notes/?p=1&v=5.152.0.178&l=1 | 2021-11-28 15:21:52 EST |
| http://www.glarysoft.com/update/release-notes/gu/5.152.0.178 | 2021-11-28 15:21:52 EST |
| http://www.panerabread.com/ | 2021-11-28 16:28:01 EST |
| https://www.panerabread.com/en-us/home.html | 2021-11-28 16:28:02 EST |
| https://www.panerabread.com/en-us/home.html | 2021-11-28 16:28:02 EST |
| http://allstate.com/ | 2021-11-28 16:28:05 EST |
| https://www.allstate.com/ | 2021-11-28 16:28:05 EST |
| http://packetstormsecurity.com/ | 2021-11-28 16:28:27 EST |
| https://packetstormsecurity.com/ | 2021-11-28 16:28:27 EST |
| https://www.mozilla.org/en-US/privacy/firefox/ | 2021-11-28 15:20:03 EST |
| https://www.mozilla.org/en-US/firefox/welcome/10/ | 2021-11-28 15:41:05 EST |
| http://tutanota.com/ | 2021-11-28 16:27:35 EST |
| https://tutanota.com/ | 2021-11-28 16:27:36 EST |
| https://mail.tutanota.com/ | 2021-11-28 16:27:38 EST |

| | |
|---|---|
| https://mail.tutanota.com/login | 2021-11-28 16:27:39 EST |
| https://login.live.com/oauth20_desktop.srf?lc=1033 | 2021-11-28 20:15:49 EST |
| https://login.live.com/oauth20_logout.srf?client_id=00000000480728C5&redirect_uri=https://login.live.com/oauth20_desktop.srf | 2021-11-28 20:15:48 EST |
| https://login.live.com/oauth20_authorize.srf?client_id=00000000480728C5&scope=service::ssl.live.com::MBI_SSL&response_type=token&display=windesktop&theme=win7&lc=1033&redirect_uri=https://login.live.com/oauth20_desktop.srf&lw=1&fl=wld2 | 2021-11-28 20:15:54 EST |
| https://www.glarysoft.com/update/glary-utilities/update.html?v=5.152.0.178&src=10000 | 2021-11-28 20:21:50 EST |
| http://go.glarysoft.com/g/t/releasenotes/cn/10000/s/Glary%20Utilities/v/5.152.0.178 | 2021-11-28 20:21:50 EST |
| file:///E:/IST293%20Course%20Project%20Setup/DESKTOP-1JR6UBB-20211128-203753.zip | 2021-11-28 21:10:15 EST |
| file:///C:/Users/Eugene%20Jackson/Desktop/targets.txt.txt | 2021-11-28 21:31:15 EST |

## Recommendations:

Further Analysis of Encrypted Data: Given the uncracked hashes retrieved from the laptop's RAM and encrypted files on the USB drive, it is imperative to prioritize the decryption and analysis of this data. Utilizing advanced cryptographic analysis tools and consulting with experts in encryption could reveal critical information about the user's activities and intentions.

Examine Network Logs and Traffic: The Nmap scan found running on the laptop indicates network reconnaissance activities. It is recommended to obtain and analyze network logs from the targeted NuScale IP subnet and any other networks that might have been scanned. This could help identify unauthorized access attempts, data exfiltration activities, or other malicious network behavior.

Correlate Evidence with Known Threat Actors: The information found, particularly around the NuScale reactor schematics and references to the Bahamas Papers, should be compared with known threat actor profiles and recent cybersecurity incidents. This could help in identifying potential suspects or linking the case to broader cyber espionage or activism campaigns.

Digital Forensic Analysis of the Cell Phone: The victim's cell phone may contain crucial evidence such as call logs, messages, emails, and application data that could provide insights into the motive and the events leading up to the incident. A detailed forensic analysis should be conducted to uncover any communications or data related to the case.

Investigate Financial and Personal Motives: The connection to the Bahamas Papers suggests a financial angle that warrants a thorough investigation into the financial records and assets of the victim and any suspects. Additionally, examining personal relationships and interactions might uncover motives or conflicts related to the crime.

Collaboration with Cybersecurity and Nuclear Energy Experts: Given the case's complexity and the technical expertise required, collaboration with cybersecurity experts and nuclear energy specialists is recommended. Their insights could be invaluable in understanding the significance of the schematics and data found and assessing potential security threats to nuclear facilities.

## Appendix A:

1. What is the hash for the image file?
   *Be sure to use the "strongest" hash available if there are multiple hashes to choose from.*

| |
|---|
| **e60ebdac839e7f9cc8adf765eb42c1b3545c2d22f606bc41c0bb211aa2335f4e** |

2. What is the date and time of when the image was created?

| |
|---|
| **Sunday, November 28, 2021, 12:36:52 PM** |

3. What operating system is running on the system imaged.

| |
|---|
| **Windows 10 Enterprise Evaluation** |

4. What version of operating system is running – 32-bit or 64-bit?

| |
|---|
| **64-bit** |

5. What is the original date and time the imaged operated system was installed on?

| |
|---|
| **2019-12-07-04:03:44 EST** |

6. What is the time zone set to on the imaged system?

| |
|---|
| **America/New_York** |

7. Who is the registered owner of the imaged system?

| |
|---|
| **Eugene Jackson** |

8. Which network card is installed on the imaged system? *Be as specific as possible.*

| |
|---|
| **Intel(R) 82574L Gigabit Network Connection** |

9. What are three websites that were visited by the user that would be of interest during this investigation?

| | |
|---|---|
| **1:** | **www.packetstormsecurity.com** |
| **2:** | **www.tutanota.com** |
| **3:** | **www.glarysoft.com** |

10. What three files were deleted from the system that might be of interest?

| | |
|---|---|
| **1:** | **F1090176.elf** |

| | |
|---|---|
| **2:** | **F0534920.exe** |
| **3:** | **Aborted-session-ping** |

11. What is an email associated that could be related to the investigation?

**bob@nothingtohide.info, carol@tutanota.de, alice.kovert@gmail.com, alice@tutanota.de, lisa@nothingtohide.info, mary@nothingtohide.info,**

12. What is one other interesting finding discovered via Autopsy?

**There are numerous interesting files in the Run Programs section. Nmap has been run. KillDisk was also run, possibly to erase data. I also see the TOR browser and Wireshark.**

13. Why would this be considered of interest to the investigation?

**All these programs speak to the technical proficiency of the user. They could also guide us down different paths in our investigation. We may need to look at the network traffic and potential malware analysis.**

14. What file can be used to link the system to the USB drive that was discovered?

**/img_Greenville_HDD_20211128.001/vol_vol6/Windows/System32/config/System**

**Memory Image Analysis**

Perform an analysis of the memory image - **Greenville_RAM_20211128.zip**. Use your analysis of the memory image to answer the following questions:

15. What is the hash for the image file?
    *Be sure to use the "strongest" hash available if there are multiple hashes to choose from.*

**0d7ec09576764ea5836b1e67d5aa592fbd7162db441f87ee2a4a5ac50674ba59**

16. What is the date and time of when the image was created?

**Sunday, November 28, 2021, 11:38:40 AM**

17. How many processes were running on the system at the time the image was created?

**145**

18. How many unique processes were running on the system at the time the image was created?

**25**

19. Which tool was used to create a memory dump of the system?

**DumpIt.exe**

20. Which compression tool was running on the system at the time the image was taken?

**7zFM.exe**

21. What is the name of the executable running that was being used to potentially wipe files from the system or an entire hard drive?

**DiskWipe.exe**

22. What port scanner is running on the inspected system?

**Nmap.exe**

23. What destination IP address is being scanned at the time of the image?

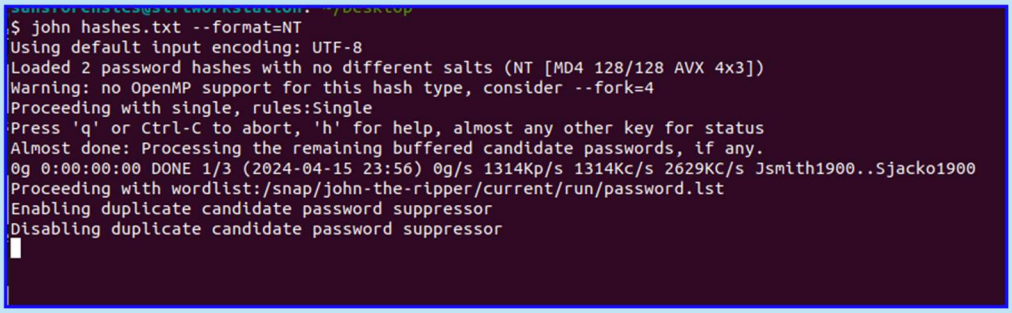
**I could see Nmap.exe running in the process list. However, using the netscan module in volatility I was not able to see the process or IP address for the scan. That was the only network module that can be run on Windows10. There are other network modules but can only be run on earlier windows editions.**

24. What is the name of the local administrator account?

**Jacko Smith**

25. What is the password for the local administrator account?

**Jsmith1900…Sjacko1900 I'm unsure if these are actual results.**




26. What is the password for the local user account that was created on the system?

**NONE**

27. How many USB drives have been plugged into the system that was imaged?

**Using the usbstor module I received only 1 USB device. See screenshot.**

```
sansforensics@siftworkstation: ~/Desktop
$ vol.py --profile=Win10x64_19041 usbstor -f DESKTOP-1JR6UBB-20211128-203753.raw
Volatility Foundation Volatility Framework 2.6.1
Reading the USBSTOR Please Wait
Found USB Drive: 4C530000200414217555&0
        Serial Number:  4C530000200414217555&0
        Vendor: SanDisk
        Product:        Cruzer_Glide
        Revision:       1.00
        ClassGUID:      Cruzer_Glide

        ContainerID:    {76325aa2-1e2b-58d6-ad79-a8dee9568adf}
        Mounted Volume: \??\Volume{bf9ef85e-5087-11ec-9f12-fc7774f59168}
        Drive Letter:   Unknown
        Friendly Name:  SanDisk Cruzer Glide USB Device
        USB Name:       E:\
        Device Last Connected:  2021-11-28 20:35:25 UTC+0000

Traceback (most recent call last):
  File "/usr/local/bin/vol.py", line 192, in <module>
    main()
  File "/usr/local/bin/vol.py", line 183, in main
    command.execute()
  File "/usr/local/lib/python2.7/dist-packages/volatility/commands.py", line 147, i
    func(outfd, data)
  File "/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/JamesHa
    outfd.write('\tClass:\t{0}\n'.format(usbdev['Class']))
KeyError: 'Class'
sansforensics@siftworkstation: ~/Desktop
```

28. List the identifier for each USB drive.

**4C530000200414217555&0**

### USB Drive Image Analysis

Perform an analysis of the USB drive image - **Greenville_USB_20211128.img**. Use your analysis of the memory image to answer the following questions:

29. What is the hash for the image file?
    *Be sure to use the "strongest" hash available if there are multiple hashes to choose from.*

**c59c96a5ea3c624d0dfa98ea6eebfa45c854e4b3b12156a24b57a7c0957d3e75**

30. What is the date and time of when the image was created?

**Sunday, November 28, 2021, 6:30:26 PM**

31. What is the name assigned to the USB drive?

**Top Secret**

32. Which files are visible on the drive by default?

**There are 128 images, 1 PDF, 6 plain text, and 2 executables.**

33. Which files have been deleted from the USB drive?
    *Provide a brief description of each.*

**f0000000.jpg – A man speaking in operations center.**

**f0001200.jpg - NuSale complex image**

**f0011624.jpg – 3D image of reactor**

**f0011688.jpg – NuScale side by side image of Control Room, system interior and exterior.**

**f0011904.jpg - NuScale power process schematic**

**f0012008.jpg – NuSacle logo and 3D image of reactor.**

**f0012224.jpg – Reactor image**

**f0012280.jpg – An image of multiple reactors**

**f0012376.jpg – 3D image of reactors inside the plant (submerged)**

**f0497112.jpg - A couple on vacation.**

**f0497336.jpg – Another Vacation photo.**

**f0497536.jpg - Vacation image**

**f0000232.png – Reactor schematic**

**f0001320.png - Reactor schematic**

**f0012544.png - Reactor schematic**

**f0013552.png - Reactor schematic**

**f0014840.png - Reactor schematic**

**f0155080.png – KALI Linux desktop image**

**f0015792.txt – Text file referencing "The Panama Papers"**

**f0050624.txt - Text file referencing "The Panama Papers"**

**f0054840.txt - Text file referencing "The Panama Papers"**

**f0153936.txt - .txt file referencing Hardware Detection Tool**

**f0227080.txt - Text file referencing "The Panama Papers"**

**f0321640.txt - Text file referencing "The Panama Papers"**

**5c89800a48003.image.jpg**

**5c89800a48003.image.jpg:Zone.Identifier**

**6a00d8341c4fbe53ef026be422d1c9200d-500wi.png**

**6a00d8341c4fbe53ef026be422d1c9200d-500wi.png:Zone.Identifier**

**218132-Nuscale-Power-Plant-TN---Day-(1).jpg**

**218132-Nuscale-Power-Plant-TN---Day-(1).jpg:Zone.Identifier**

**diagram_of_a_nuscale_reactor.png**

**diagram_of_a_nuscale_reactor.png:Zone.Identifier**

**IV.5-KenLangdon-NuScale.pdf**

**IV.5-KenLangdon-NuScale.pdf:Zone.Identifier**

**NuScale SMR cutaway.jpg**

**NuScale SMR cutaway.jpg:Zone.Identifier**

**NuScale Video Still 2x1.jpg**

**NuScale Video Still 2x1.jpg:Zone.Identifier**

**NuScale.jpg**

**NuScale.jpg:Zone.Identifier**

**nuscale_reactor.jpg**

**nuscale_reactor.jpg:Zone.Identifier**

**NuScale-Power-Module-800x613.jpg**

**NuScale-Power-Module-800x613.jpg:Zone.Identifier**

**NuScale-SMR-(NuScale).jpg**

**NuScale-SMR-(NuScale).jpg:Zone.Identifier**

**NuScale-SMR-plant-cutaway-850x567-1.jpg**

**NuScale-SMR-plant-cutaway-850x567-1.jpg:Zone.Identifier**

**power-module-dissection.ashx.png**

**power-module-dissection.ashx.png:Zone.Identifier**

**Schematic-of-a-NuScale-power-module.png**

**Schematic-of-a-NuScale-power-module.png:Zone.Identifier**

**Screen-Shot-2020-09-10-at-9.45.49-PM-1010x1024.png**

**Screen-Shot-2020-09-10-at-9.45.49-PM-1010x1024.png:Zone.Identifier**

**f0142976.exe – Microsoft executable**

**f0154512.elf - Linux executable**

**f0154976.elf - Linux executable**

**f0155024.elf - Linux executable**

**f0155208.elf - Linux executable**

**f0161456.mft - Master File Table**

**f0161464.mft - Master File Table**

**f0161472.mft - Master File Table**

**f0161480.mft - Master File Table**

**f0161504.mft - Master File Table**

**f0161512.mft - Master File Table**

**f0161520.mft - Master File Table**

**f0161528.mft - Master File Table**

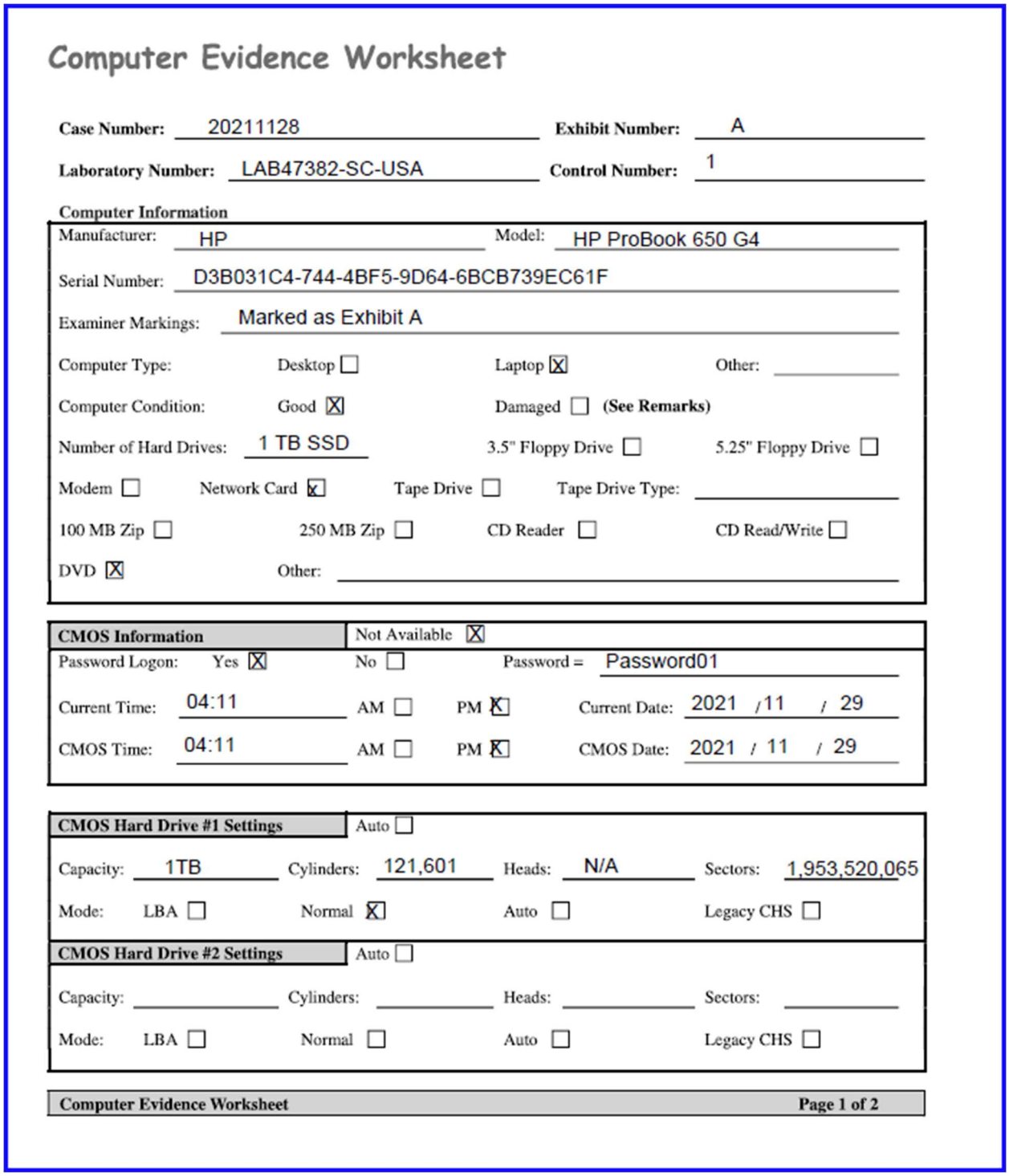
**f0161536.mft - Master File Table**

**f0161544.mft - Master File Table**

**f0497864.exe – This is the rewrite application. It is used for writing disk images to devices.**

**f1065448.xz - archived file (potentially a zip bomb)**

## Appendix B:



# Computer Evidence Worksheet

**Case Number:** 20211128 **Exhibit Number:** A

**Laboratory Number:** LAB47382-SC-USA **Control Number:** 1

**Computer Information**

Manufacturer: HP Model: HP ProBook 650 G4

Serial Number: D3B031C4-744-4BF5-9D64-6BCB739EC61F

Examiner Markings: Marked as Exhibit A

Computer Type: Desktop ☐ Laptop ☒ Other: ____

Computer Condition: Good ☒ Damaged ☐ **(See Remarks)**

Number of Hard Drives: 1 TB SSD 3.5" Floppy Drive ☐ 5.25" Floppy Drive ☐

Modem ☐ Network Card ☒ Tape Drive ☐ Tape Drive Type: ____

100 MB Zip ☐ 250 MB Zip ☐ CD Reader ☐ CD Read/Write ☐

DVD ☒ Other: ____

**CMOS Information** Not Available ☒

Password Logon: Yes ☒ No ☐ Password = Password01

Current Time: 04:11 AM ☐ PM ☒ Current Date: 2021 / 11 / 29

CMOS Time: 04:11 AM ☐ PM ☒ CMOS Date: 2021 / 11 / 29

**CMOS Hard Drive #1 Settings** Auto ☐

Capacity: 1TB Cylinders: 121,601 Heads: N/A Sectors: 1,953,520,065

Mode: LBA ☐ Normal ☒ Auto ☐ Legacy CHS ☐

**CMOS Hard Drive #2 Settings** Auto ☐

Capacity: ____ Cylinders: ____ Heads: ____ Sectors: ____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

**Computer Evidence Worksheet** **Page 1 of 2**

**Sub Exhibits Split From This Computer**

| Sub Number | Type | Where Found |
|---|---|---|
| A1 | HP ProBook 650 G4 | The laptop was found at the crime scene. It was found open and powered on atop the kitchen island. |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| Remarks |
|---|
| Device was not plugged in. Is running Kali Linux OS. 35% battery life. When found was running a port scan of NuScale IP subnet. Numerous applications associated with hacking and network monitoring found on the device. |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

# Computer Evidence Worksheet

**Case Number:** 20211128 **Exhibit Number:** B

**Laboratory Number:** LAB47382-SC-USA **Control Number:** 1

**Computer Information**

Manufacturer: PNY Model: PNY USB 2.0

Serial Number: 071c088d288b2208

Examiner Markings: Marked as Exhibit B

Computer Type: Desktop ☐ Laptop ☐ Other: USB

Computer Condition: Good ☒ Damaged ☐ **(See Remarks)**

Number of Hard Drives: _____ 3.5" Floppy Drive ☐ 5.25" Floppy Drive ☐

Modem ☐ Network Card ☐ Tape Drive ☐ Tape Drive Type: _____

100 MB Zip ☐ 250 MB Zip ☐ CD Reader ☐ CD Read/Write ☐

DVD ☐ Other: _____

**CMOS Information** Not Available ☒

Password Logon: Yes ☐ No ☐ Password = _____

Current Time: _____ AM ☐ PM ☐ Current Date: / /

CMOS Time: _____ AM ☐ PM ☐ CMOS Date: / /

**CMOS Hard Drive #1 Settings** Auto ☐

Capacity: 32 GB Cylinders: N/A Heads: N/A Sectors: N/A

Mode: LBA ☐ Normal ☒ Auto ☐ Legacy CHS ☐

**CMOS Hard Drive #2 Settings** Auto ☐

Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

**Sub Exhibits Split From This Computer**

| Sub Number | Type | Where Found |
|---|---|---|
| B1 | PNY USB 2.0 | The thumb drive was found hidden under a coffee container at the crime scene in the kitchen of the residence. |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| Remarks |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

# Computer Evidence Worksheet

**Case Number:** 20211128 **Exhibit Number:** C

**Laboratory Number:** LAB47382-SC-USA **Control Number:** 1

**Computer Information**

Manufacturer: Apple Model: iphone 12

Serial Number: J3F58R5L2N

Examiner Markings: Marked as Exhibit C

Computer Type: Desktop ☐ Laptop ☐ Other: Cell Phone

Computer Condition: Good ☒ Damaged ☐ **(See Remarks)**

Number of Hard Drives: 1 3.5" Floppy Drive ☐ 5.25" Floppy Drive ☐

Modem ☐ Network Card ☒ Tape Drive ☐ Tape Drive Type:

100 MB Zip ☐ 250 MB Zip ☐ CD Reader ☐ CD Read/Write ☐

DVD ☐ Other:

**CMOS Information** Not Available ☒

Password Logon: Yes ☒ No ☐ Password = 123456

Current Time: 6:28 AM ☐ PM ☒ Current Date: 2021 / 11 / 29

CMOS Time: 6"28 AM ☐ PM ☒ CMOS Date: 2021 / 11 / 29

**CMOS Hard Drive #1 Settings** Auto ☐

Capacity: 256GB Cylinders: N/A Heads: N/A Sectors: N/A

Mode: LBA ☐ Normal ☒ Auto ☐ Legacy CHS ☐

**CMOS Hard Drive #2 Settings** Auto ☐

Capacity: Cylinders: Heads: Sectors:

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

**Sub Exhibits Split From This Computer**

| Sub Number | Type | Where Found |
|---|---|---|
| C1 | Apple iphone 12 | The device was found adjacent to the victims body on the floor of the kitchen. It was located about 18 inches from the victim. |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| Remarks |
|---|
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

**Computer Evidence Worksheet** **Page 2 of 2**

## Appendix C:

**Anywhere Police Department**

# EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: __20211128_____ Offense: _____Homicide _____
Submitting Officer: (Name/ID#) ____Louis Brody_____
Victim: _____Elena Morrison_____
Suspect: _____
Date/Time Seized: ____Novemeber 28th, 2021 12:00 PM___
Location of Seizure: ___Simpsonville, South Carolina_____

| **Description of Evidence** | | |
|---|---|---|
| **Item #** | **Quantity** | **Description of Item** (Model, Serial #, Condition, Marks, Scratches) |
| A | 1 | HP ProBook 650 G4 Laptop |
| B | 1 | PNY USB 2.0 Drive |
| C | 1 | Apple iPhone 12 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| **Chain of Custody** | | | | |
|---|---|---|---|---|
| **Item #** | **Date/Time** | **Released by** (Signature & ID#) | **Received by** (Signature & ID#) | **Comments/Location** |
| A | 11/28/21 12:00 pm | | Detective Brown | Initial collection |
| B | 11/28/21 12:00 pm | | Detective Brown | Initial collection |
| C | 11/28/21 12:00 pm | | Detective Brown | Initial collection |
| A | 11/28/21 12:35 pm | Detective Brown | Alicia Kovert | Image made |
| B | 11/28/21 12:35 pm | Detective Brown | Alicia Kovert | Image made |
| C | 11/28/21 12:35 pm | Detective Brwon | Alicia Kovert | Image made |

| | | | | |
|---|---|---|---|---|
| A | 11/28/21 12:50 pm | Alicia Kovert | Evidence locker | Stored |
| B | 11/28/21 12:50 pm | Alicia Kovert | Evidence locker | Stored |
| C | 11/28/21 12:50 pm | Alicia Kovert | Evidence locker | Stored |

| **Chain of Custody** | | | | |
|---|---|---|---|---|
| **Item #** | **Date/Time** | **Released by** (Signature & ID#) | **Received by** (Signature & ID#) | **Comments/Location** |
| A | 11/29/21 4:11pm | Evidence locker | Louis Brody | Taken for Analysis |
| B | 11/29/21 4:11pm | Evidence locker | Louis Brody | Taken for Analysis |
| C | 11/29/21 4:11pm | Evidence locker | Louis Brody | Taken for Analysis |
| A | 11/29/21 10:47 pm | Louis Brody | Evidence locker | Stored |
| B | 11/29/21 10:47 pm | Louis Brody | Evidence locker | Stored |
| C | 11/29/21 10:47 pm | Louis Brody | Evidence locker | Stored |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## Final Disposal Authority

**Authorization for Disposal**

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)

☐ Return to Owner ☐ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: _____ Signature: _____Date: _____

**Witness to Destruction of Evidence**

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:_____
in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

**Release to Lawful Owner**

Item(s) #: _____ on this document was/were released by Evidence Custodian

_____ID#:_____ to
Name _____
Address: _____ City: _____State: _____ Zip Code: _____
Telephone Number: (_____) _____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

**This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.**