

**DIGITAL FORENSICS**

**ASSESSMENT 2: INVESTIGATION REPORT**

**Table Of Contents**

1. **Abstract**
2. **Introduction**
3. **Purpose of report**
4. **Case Summary**
5. **Objectives**
6. **Early Hypothesis**
7. **Tools Used**
8. **Certificate**
9. **Start of Investigation**
10. **End of Investigation**
11. **U.A.E Laws**
12. **Critical Reflection**
13. **Conclusion**
14. **References**

**Abstract:**

This report presents a forensic investigation into a potential security breach at AlphaDocs, a document management firm, with a focus on the activities of Joffre Smith, a new web developer in the firm. The firm’s network, consisting of 35 PCs and 5 Macs, is crucial for storing vast amounts of sensitive data for various clients. Concerns arose when an anonymous staff member observed Joffre smith engaging in suspicious behavior, including unplugging a memory stick and making derogatory remarks about the management. With the previous incident of misconduct, the digital evidence of the incident was poorly constructed and therefore not accepted by the court and they ended up paying court costs and compensation. AlphaDocs is keen to ensure that any findings from this investigation are precisely documented and legally robust.

**Introduction:**

AlphaDocs operates in a highly sensitive environment dealing with highly sensitive data where trust and security is crucial. Any security breach could severely damage the firm’s reputation and jeopardize its client’s confidentiality. The firm has implemented strict policies to mitigate risks. Despite these measures concerns arisen regarding the activities of a new employee Joffre Smith known for working late and exhibiting suspicious behavior. This report aims to conduct a forensic investigation to determine if Joffre Smith’s actions pose a threat to AlphaDocs’ security and integrity.

**Purpose of Report:**

The purpose of this report is to provide a deadline account of the forensic investigation conducted at AlphaDocs following concerns raised about the activities of Joffre Smith. The report aims to identify any potential breaches, ascertain the extent of unauthorized activities, and provide evidence that can withstand legal scrutiny in the court. By documenting the process and findings, this report aims to assist AlphaDocs in safeguarding their data and reputation.

**Case summary:**

AlphaDocs, a document management firm, initiated a forensic investigation following suspicions raised about the activities of their new web developer Joffre Smith. Observations of Joffre’s behavior and making derogatory remarks about the management, prompted concerns about potential security breaches. With previous cases of misconduct mishandled, the company is committed to conducting a thorough investigation to ensure legal compliance and safeguard its reputation. In this case three employees of the company are under investigation

**Objectives:**

1. Gather digital evidence to support findings and ensure legal compliance.
2. Determine if Joffre Smith engaged in unauthorized activities that could compromise AlphaDocs security.
3. Analyze the digital footprint of Joffre Smith, including her access logs to establish a timeline of events and potential motives.
4. Identify any security breaches or violations within the firm’s network.

**Early Hypotheses:**

1. **Suspicious Files suggest role mismatch:** Since SMII101198 is a web developer, any files associated with other departments found in her possession is highly suspicious.
2. **Potential Framing by Colleagues:** There is evidence to suggest that MUL020402 and NOR011298 may have accessed the same device as SMII101198. This raises the hypothesis that they could be attempting to frame her.
3. **Detailed examinations:** Any discrepancies during the investigation must be carefully documented and explained. This includes any files or activities that do not align with SMII101198’s role as a web developer.

**Tools Used:**

* **Autopsy:** A digital forensic platform designed for analysis of digital devices and file systems. This tool aids in investigating activities on a computer by examining data like deleted files, web browsing history, and file access logs.
* **File Explorer:** It is file browser that allows tour access to, view, and manage all the files stored on the computer.
* **Kali Linux:** It is an open-source toll designed for various information security tasks including computer forensics. John the Ripper is a tool within Kali Linux used to crack passwords.
* **Snipping Tool:**  It is a screenshot utility included in Microsoft Windows. It can capture still screenshots of an open window.
* **WinRAR:**  It used to back up and compress data, reduce the size of email attachments, decompress RAR, ZIP, and other files.
* **Notepad:**  It is text editor tool used to for creating, viewing and documenting.

**Certification:**

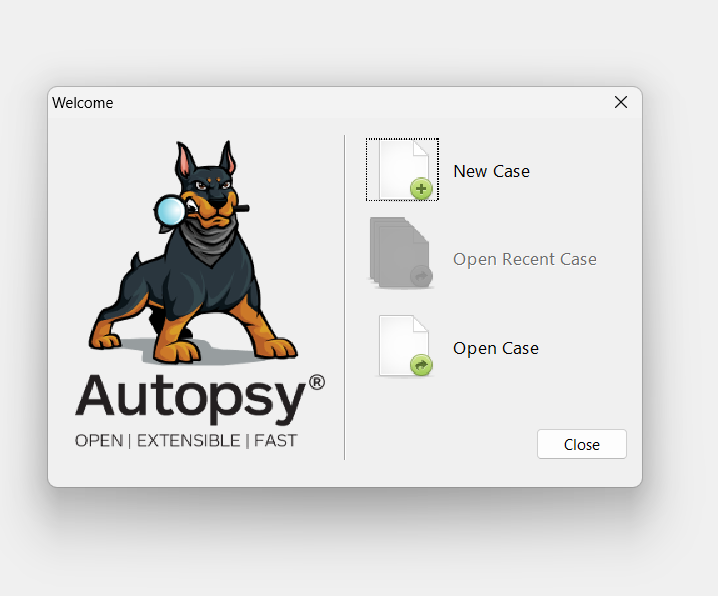
****

**Start of the investigation:**

**Case Name: AphaDocs**

**Case Number: 001-JJ**

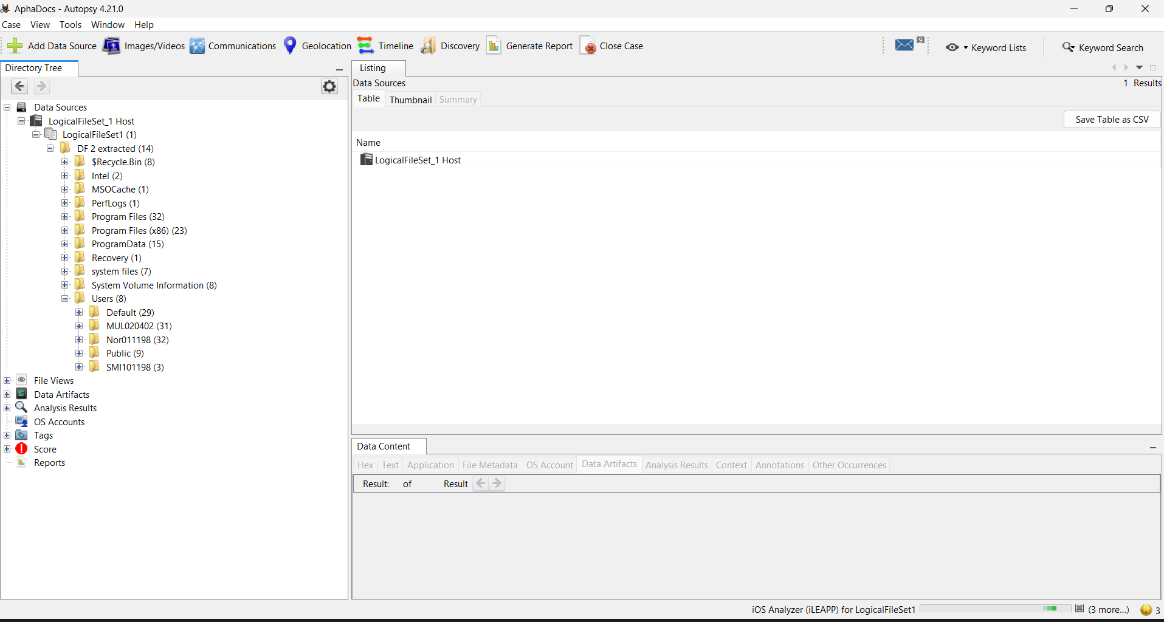
After I extracted the files from the “forensic files.zip”. I put all the contents of the file in different folder to avoid contamination of evidence. I opened the autopsy tools and created a new case



A screenshot of a computer

Description automatically generated

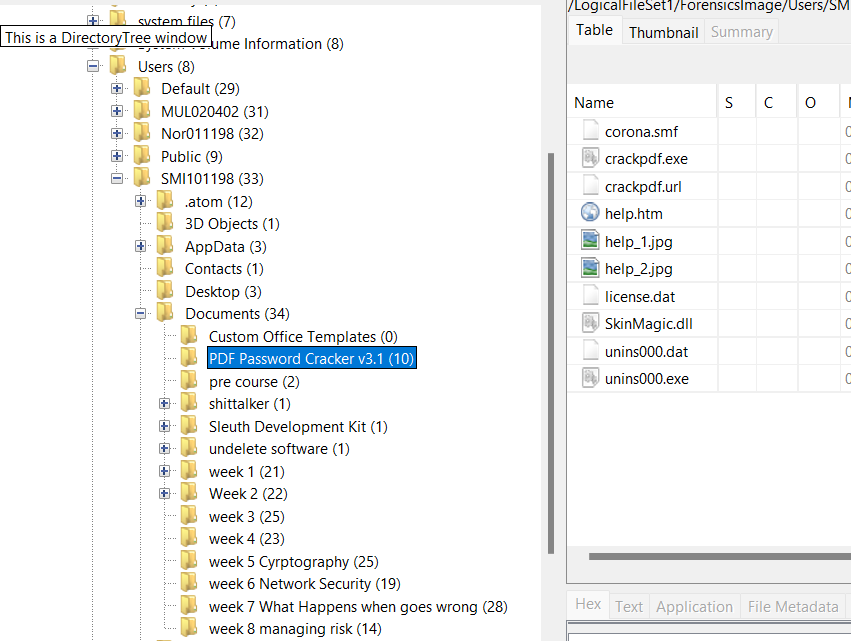
After creating the case I open the forensic folder in Autopsy to start my investigation.



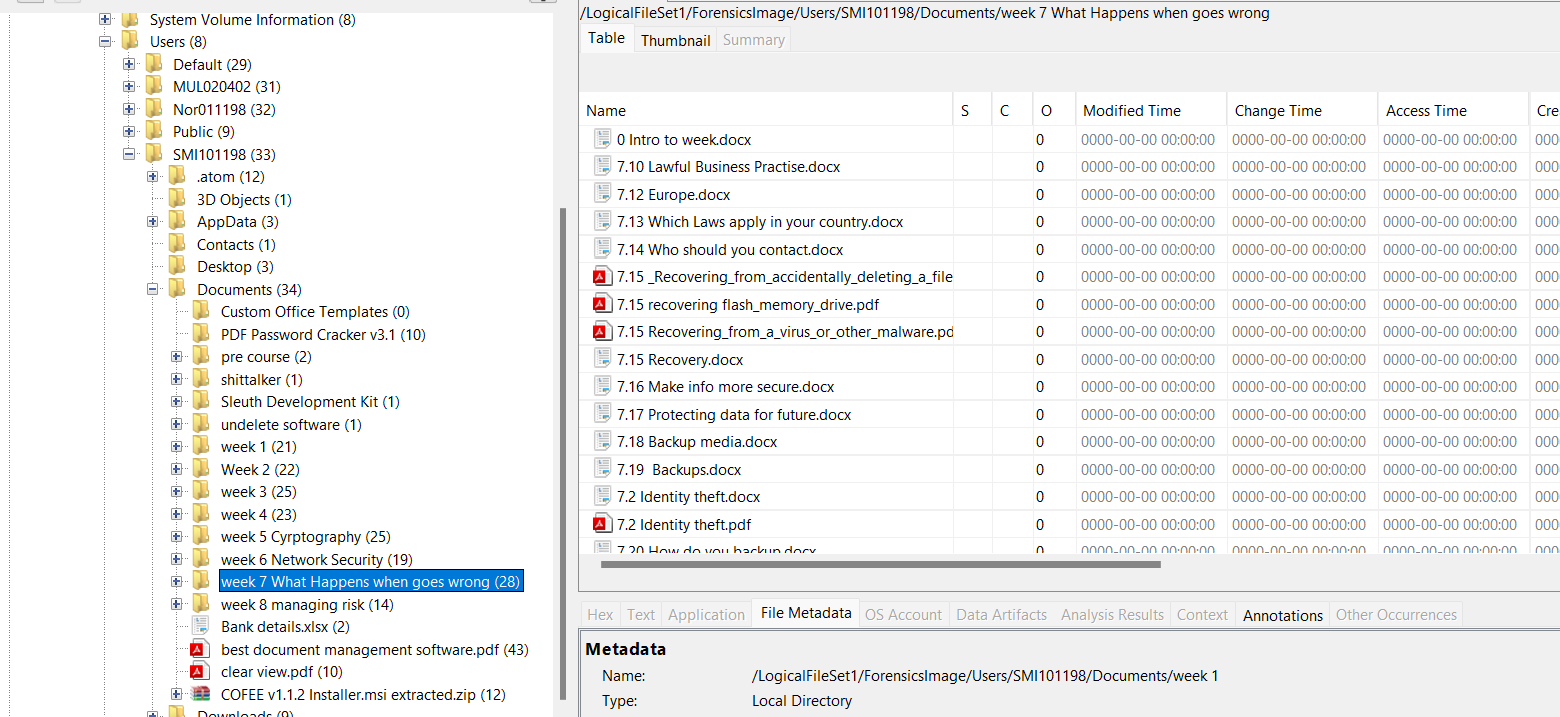
Evidence:

* **SMII101198**

1. The image displays several suspicious files associated with SMII101198, a web developer. Numerous files are unrelated to her job responsibilities, such as a “PDF password cracker”, a tool unnecessary for web development. This raises concerns about misuse of company resources and unauthorized activities.



1. Files revealing her interest in cybersecurity courses, including one titled “What Happens When Things Go Wrong” were found. This suggests she might be preparing for potential breaches or trying to cover her tracks, indicating a deeper involvement in activities beyond her duties.



1. Image (Fig 0.1) shows the file path leading to SMII101198’s desktop and documents, while Image (Fig 0.2) reveals that the accessed file belonged to MUL020402. This suggests a violation of company policy, indicating that MUL020402 was using SMII101198’s device, possibly for unauthorized activities or to frame her.

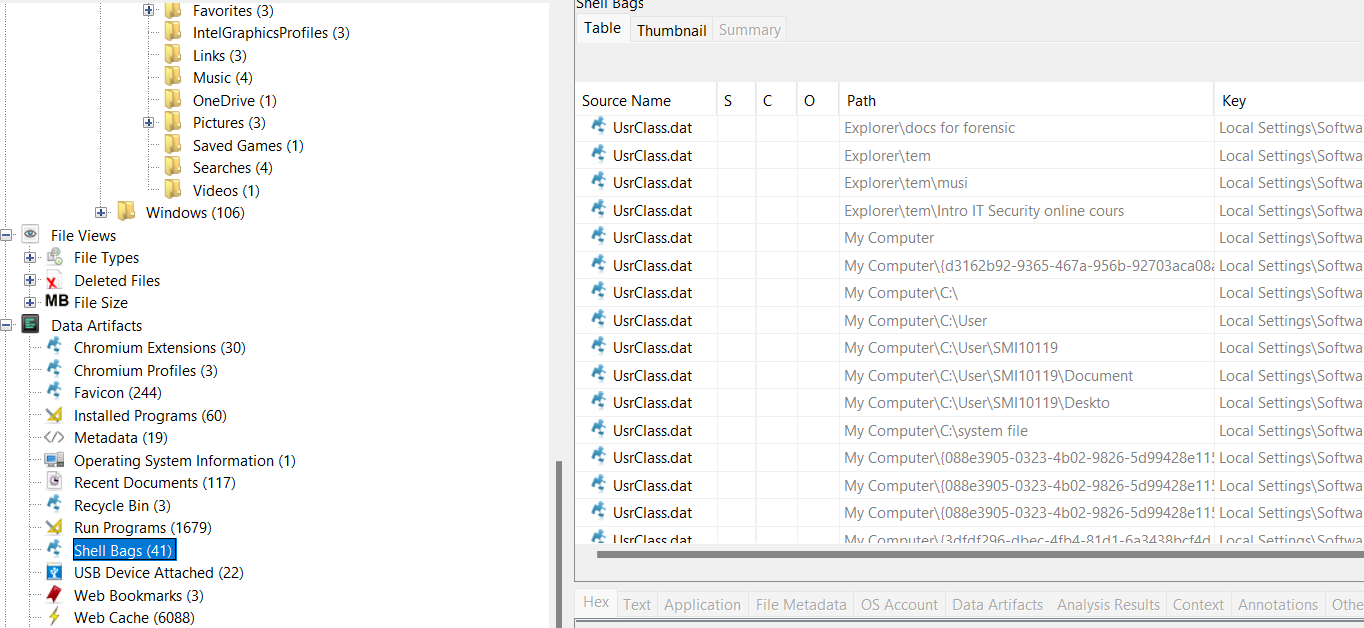


Fig 0.1

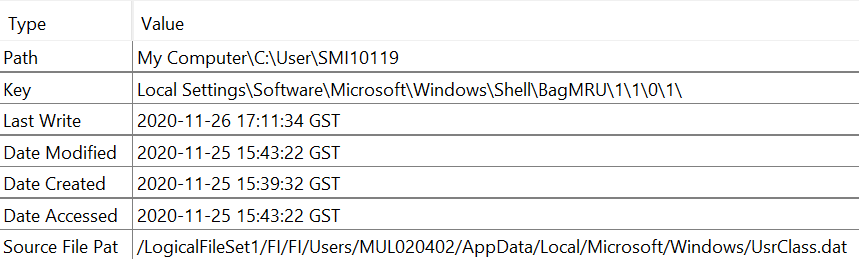
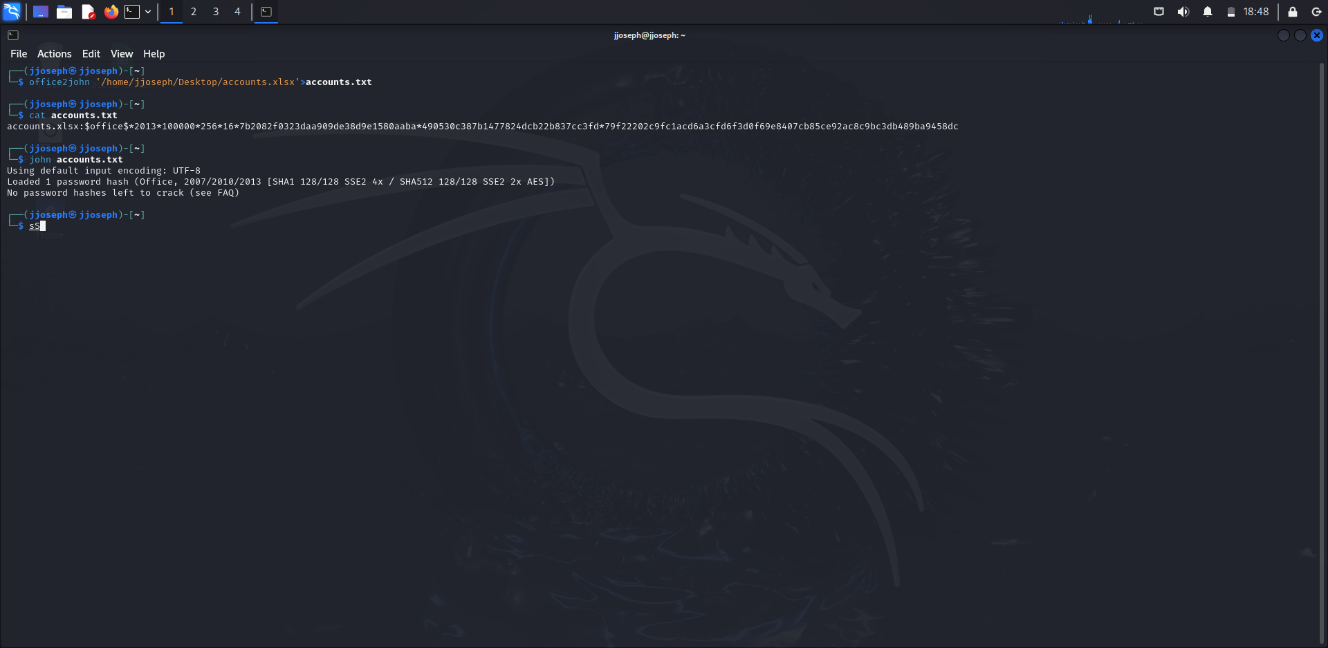
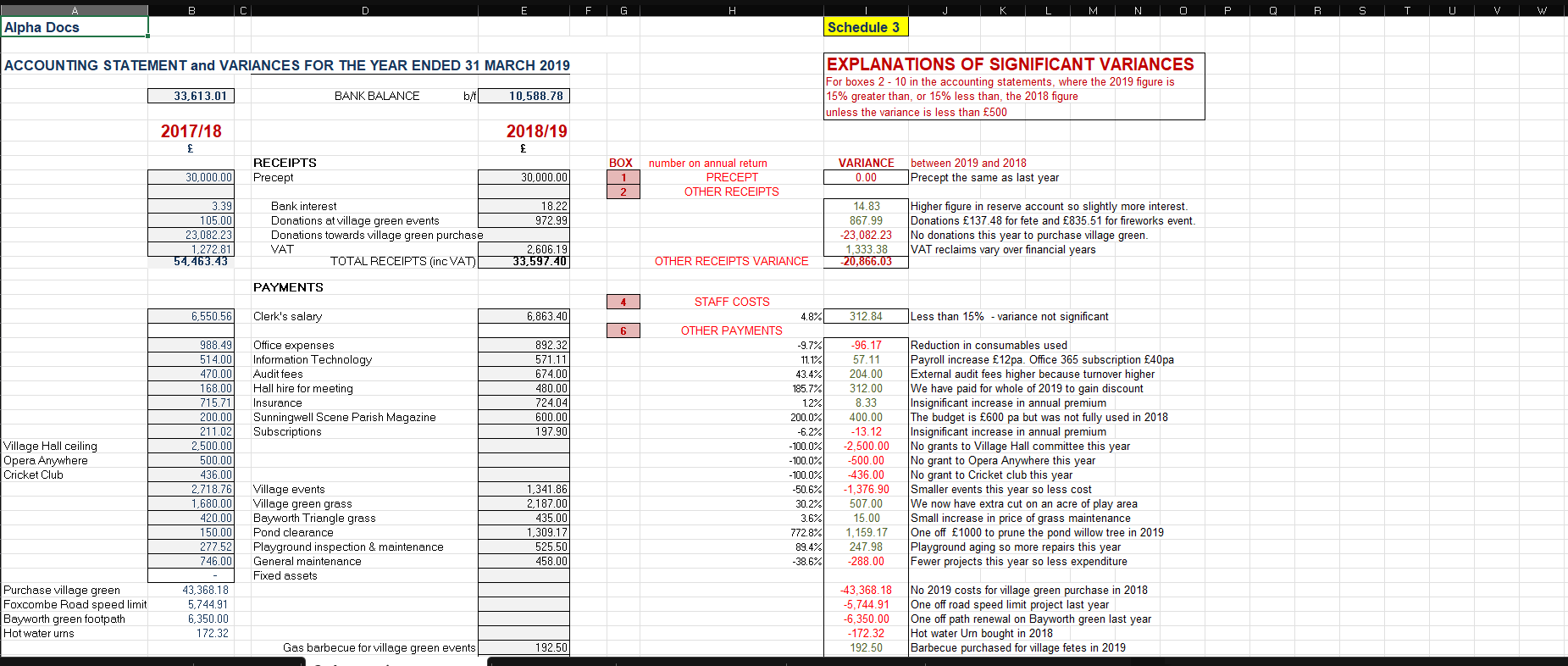


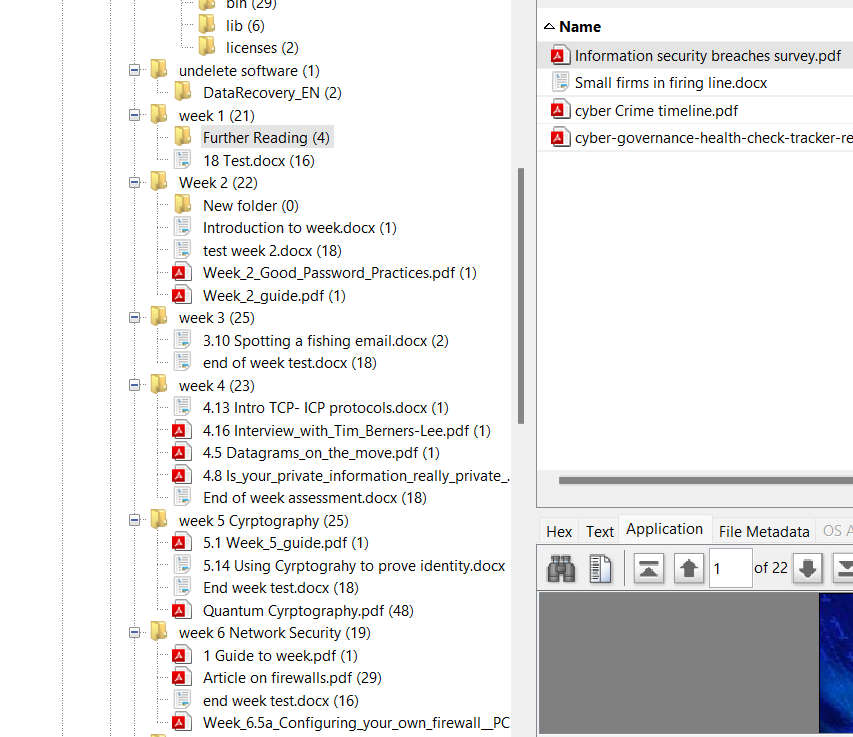
Fig 0.2

1. Despite being a Web developer, SMII101198 had access to the company’s banking information, which is unusual and suspicious. Files indicating her involvement in cybersecurity courses and activities related to password cracking were also discovered. Using John the Ripper tool in Kali Linux, I cracked the password and found that she had access to the company’ accounting details, this is a breach of the company’s policy.

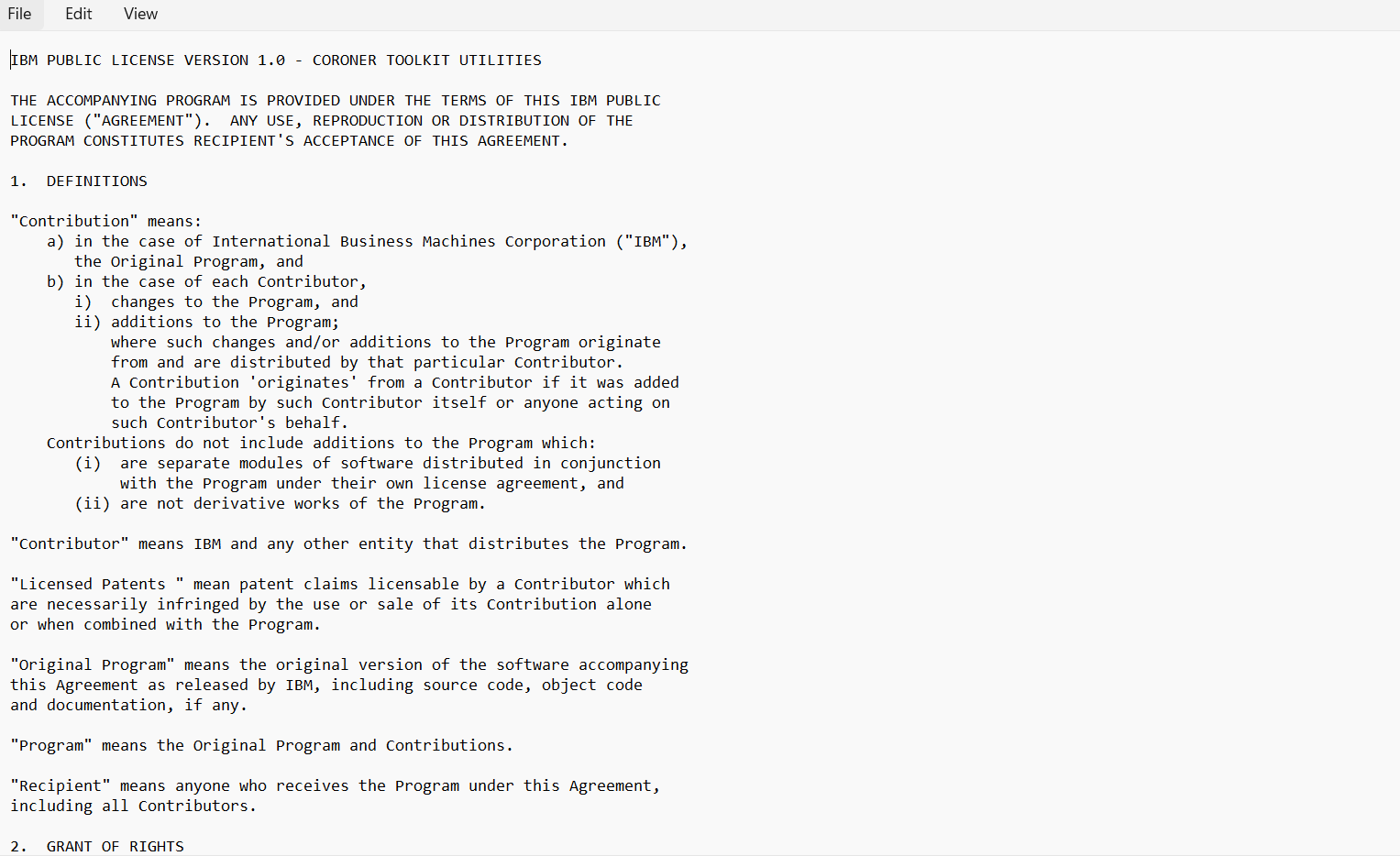




1. This image details all the files accessed by SMII101198, highlighting her focus on cybersecurity. This significant investment of time and effort into learning about cybersecurity, unrelated to her role, suggests a possible misuse of company time and resources.

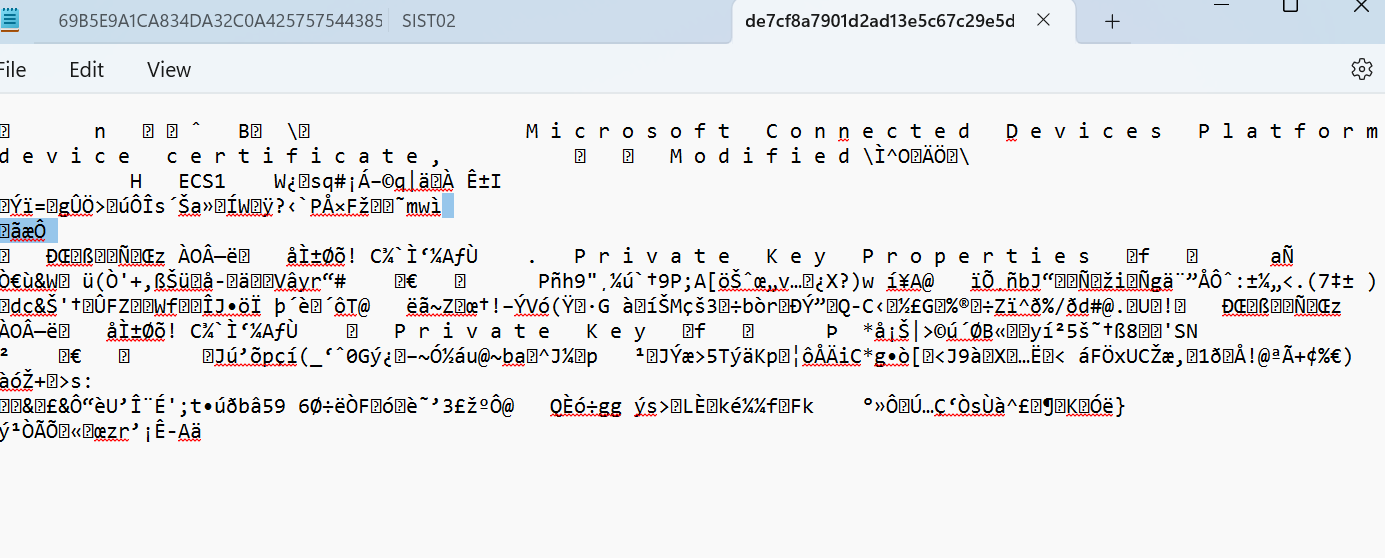


1. A suspicious file named “IBM-LICENSE” was found in SMII101198’s folder. This file is concerning as it is unrelated to her web development duties. The presence of such files suggests several possibilities, including the potential for misuse of software or licenses.

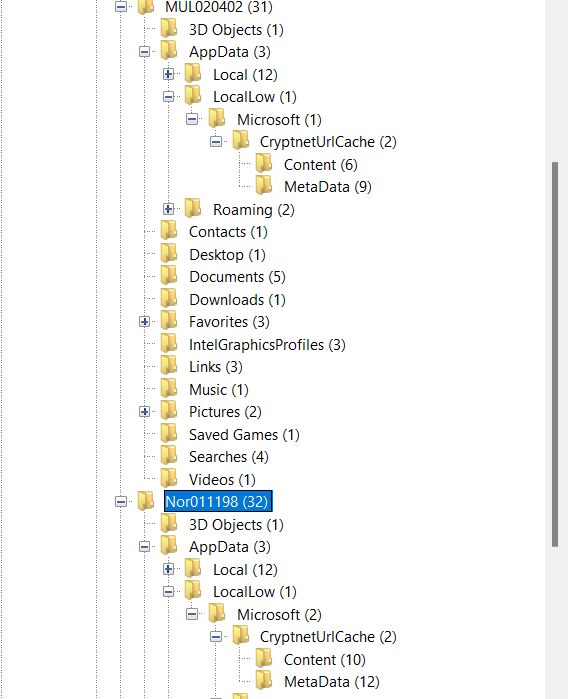


* **NOR011298**

1. A file in the crypto folder revealed where NOR011298 kept the private key for his main crypto folder, violating company policy by using the device for personal gain. The misuse of company devices for personal cryptocurrency transactions exposes the company to legal and financial risks.

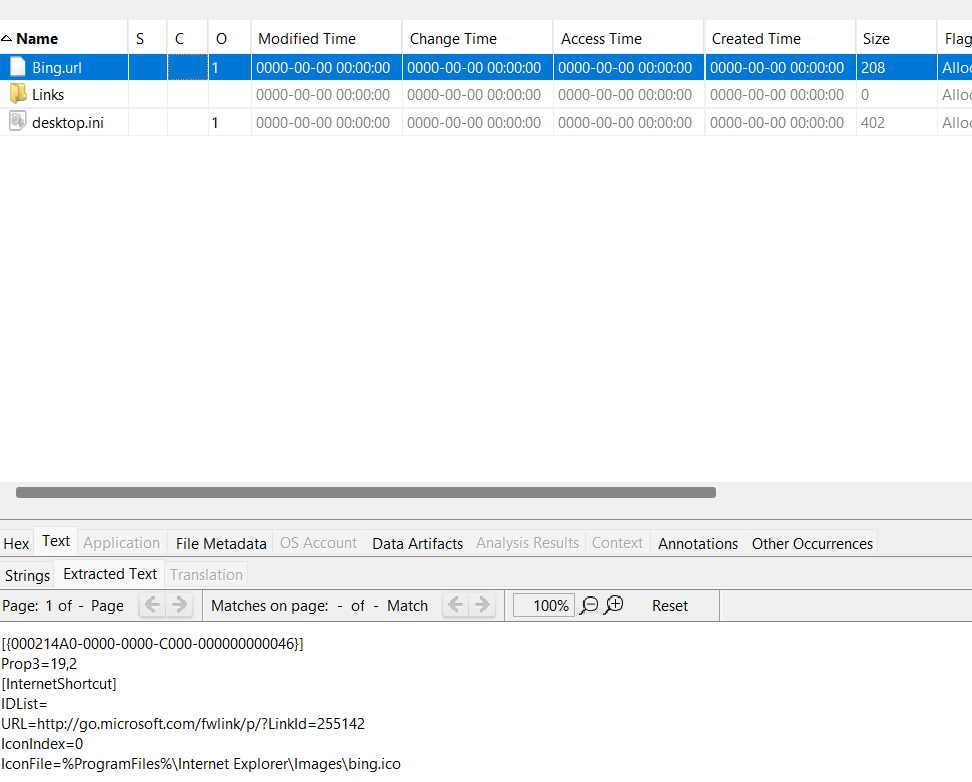


1. NOR011298 had identical files to MUL020402, indicating a possible collaboration to frame SMII101198. The similar files in both employees’ folders suggest a coordinated effort to cover their ow malpractice by shifting blame onto a new employee.

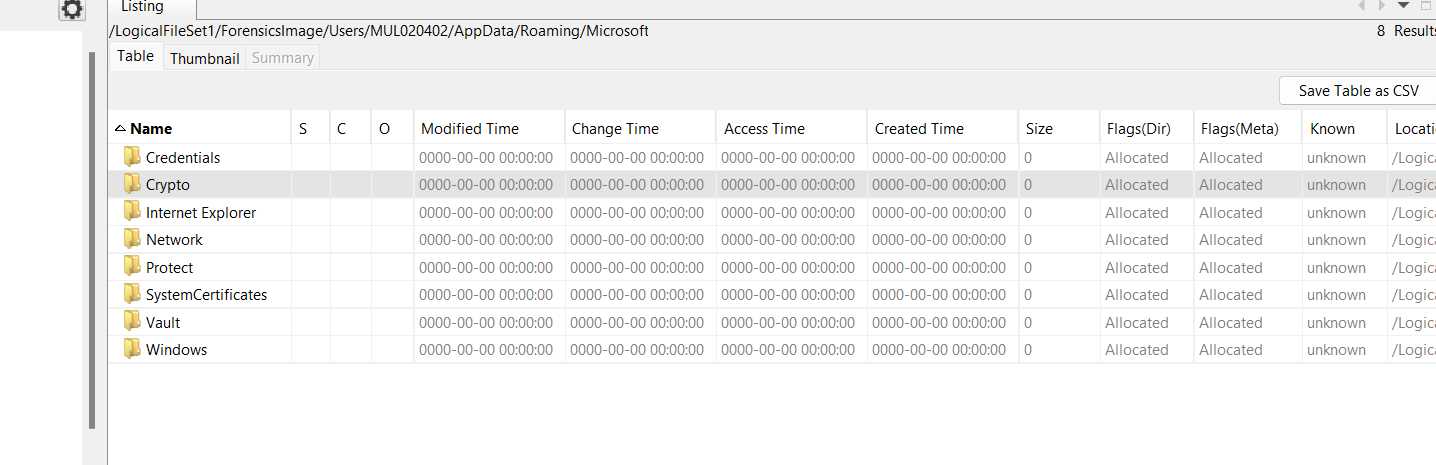


* **MUL020402**

1. Analyzing the cookies revealed that accessing non-work-related sites was more challenging for SMII101198 due to stringent monitoring. This monitoring also applies to MUL020402, implying that he could face similar disciplinary actions. The analysis highlights potential misuse of company internet resources and questions adherence to internet policies.



1. Suspicious files named “credentials” and “crypto” were found in MUL020402’s folder, suggesting plans to store employee credentials for unauthorized activities. The presence of cryptocurrency related files on a company device, intended strictly for professional use, indicates a serious breach of policies and possible fraudulent activities.



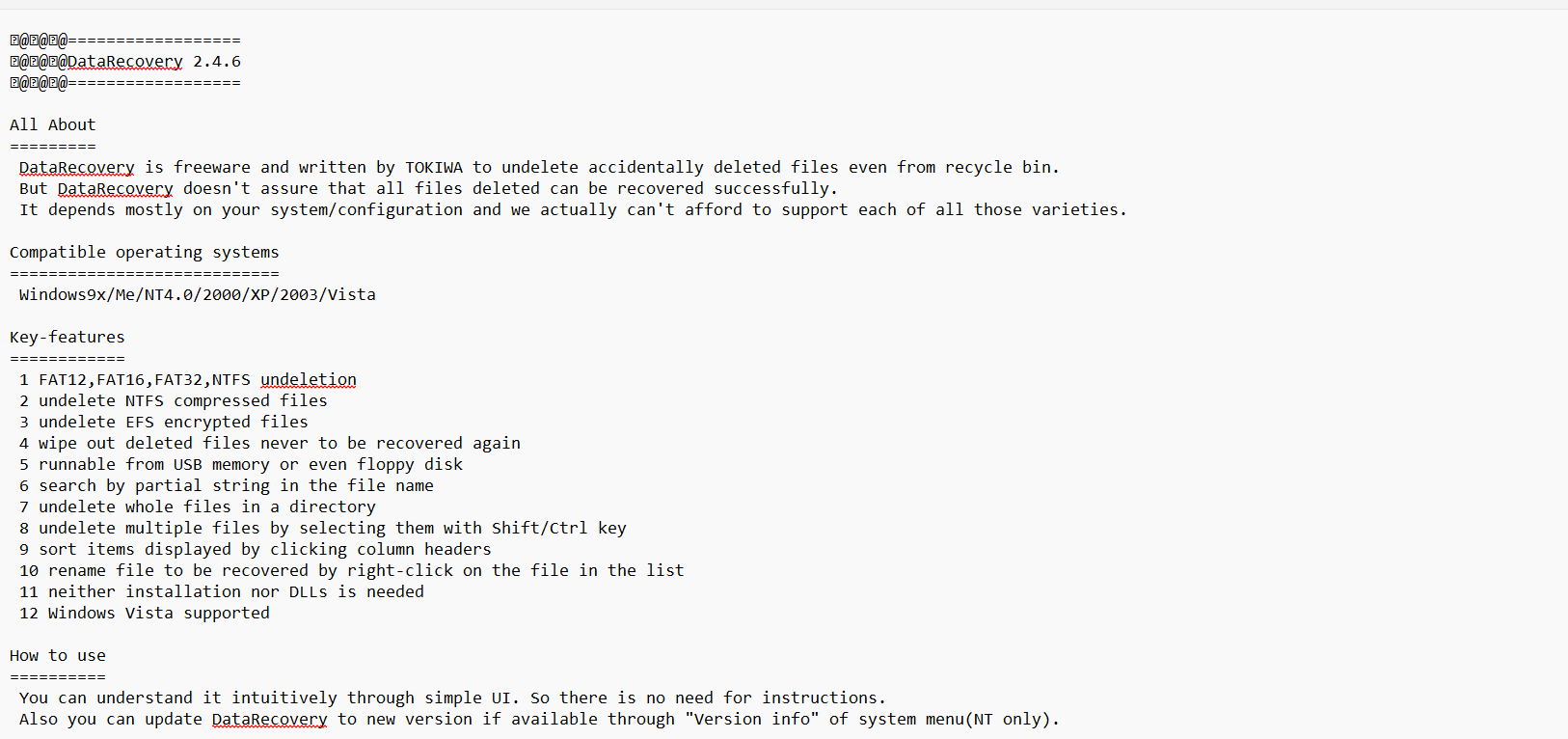
1. The “ConnectedDevicesPlatform” file implies MUL020402’s involvement in planting a USB device to tamper with files, potentially framing SMII101198. The deliberate planting of evidence is a serious offense.

A screenshot of a computer program

Description automatically generated

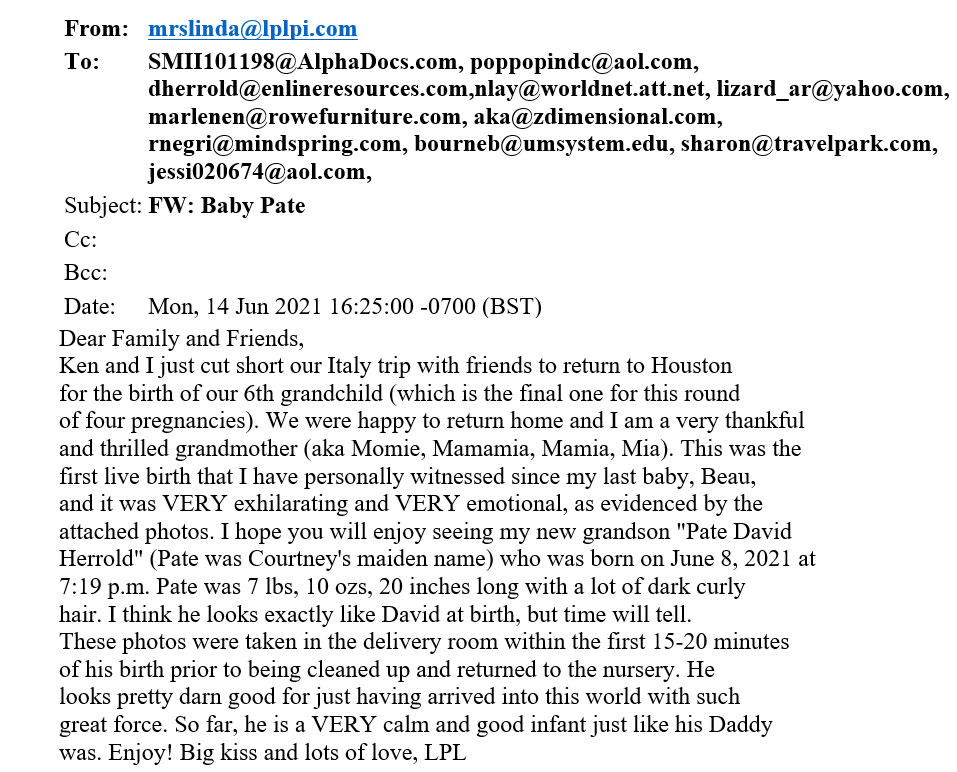
* **USB Device**

A file found in SMII101198’s folder indicated the use of data recovery software to retrieve deleted files, violating strict company policies against using USB devices to prevent data tampering and external threats. External devices like USBs can introduce malware, facilitate data v=breaches, and lead to significant security vulnerabilities. This indicates a deliberate attempt to bypass security measures.



* **Use of personal Email**

SMII101198 used her email for personal matters, contravening company policy. This poses significant cybersecurity risks, such as phishing, which could compromise the company’s data security. Using official email accounts for personal correspondence opens the door to potential cyber threats and undermines security protocols.



**End of Investigation:**

Upon completing the investigation, the evidence indicates several policy violations and potential security breaches involving multiple employees. SMII101198, web developer was found with numerous suspicious files, including tools irrelevant to her role, such a “PDF password cracker” and cybersecurity course materials. Despite her position, she had unauthorized access to sensitive company banking information. Additionally. Files and activities suggested possible collaboration between NOR011298 and MUL020402 to frame SMII101198 and cover up their own activities.

**UAE Laws:**  
The United Arab Emirates (UAE) has stringent cybercrime laws to protect against unauthorized access, data breaches, and misuse of digital information. Under Federal Law No. 5 of 2013 on combating cybercrimes, offenses such as unauthorized access to electronic information, breach of privacy, and data manipulation are punishable by imprisonment and substantial fines. For instance, accessing and sharing confidential information without authorization can result in imprisonment and fines ranging from AED 150,000 to AED 500,000. Additionally, using company resources for personal gain and introducing malware through external devices, like USBs, are serious offenses under UAE law. These laws emphasize the critical need for stringent cybersecurity measures and adherence to company policies to prevent legal repercussions and ensure data integrity.

**Critical Reflection:**

This investigation highlights significant gaps in the company’s internal security and employee training protocols. The misuse of company resources, unauthorized access to sensitive information, and potential internal conspiracies point to need for stronger security measures and more rigorous employee training. Implementing comprehensive training programs on cybersecurity, regular audits of employee activities, and strict enforcement of company policies are essential to safeguarding the company’s assets and reputation. Moreover, fostering a culture of integrity and accountability among employees is crucial to mitigating the risk of insider threats and ensuring a secure working environment.

**Conclusion:**

The investigation reveals that SMII101198 violated multiple company policies, including unauthorized use of company devices, misuse of sensitive information, and engaging in activities beyond her job responsibilities. Her involvement in cybersecurity activities and possession of unrelated tools and files indicate potential misuse of company resources. Furthermore, the evidence suggests that NOR011298 and MUL020402 may have colluded to frame SMII101198 to divert attention from their own misconduct. This situation underscores the importance of robust internal controls, regular audits, and stringent adherence to company policies to prevent such incidents.

**References**

* *Autopsy User Documentation: Autopsy User’s Guide* (no date) *Sleuthkit.org*. Available at: https://www.sleuthkit.org/autopsy/docs/user-docs/3.1/ (Accessed: June 8, 2024).
* *Cyber safety and digital security* (no date) *U.ae*. Available at: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security (Accessed: June 8, 2024).
* *EC-council learning* (no date) *Eccouncil.org*. Available at: https://codered.eccouncil.org/course/digital-forensics-essentials?logged=true (Accessed: June 8, 2024).
* *Federal decree-law no. 5 of 2012 on combating cybercrimes, United Arab Emirates* (no date) *Wipo.int*. Available at: https://www.wipo.int/wipolex/en/legislation/details/13909 (Accessed: June 8, 2024).
* *John* (no date) *Kali Linux*. Available at: https://www.kali.org/tools/john/ (Accessed: June 8, 2024).
* Shivanandhan, M. (2022) *How to crack passwords using John the Ripper – pentesting tutorial*, *freecodecamp.org*. Available at: https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/ (Accessed: June 8, 2024).
* The Cool One (2020) *Digital forensics with Autopsy*, *Medium*. Available at: https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d (Accessed: June 8, 2024).