# Contemporaneous Notes

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Examiner | Yaman Albacha | Exam commenced | 12/07/2024 | | Other relevant information | UWE Cyber Security and Digital Forensics BSc (CSDF) | Software used, versions and licensing | EnCase v8.10 (licensed)  Autopsy v4.18 (open-source) |   Note: This document forms the scope of your investigation, the Officer In Charge wants these areas examined. If you decide to omit a process, then you should provide your reasons for doing so here and in your statement. You may add additional rows, as appropriate. |  |  |

| Action | Done? | Date | Time | Notes |
| --- | --- | --- | --- | --- |
| Load case and verify image | **✓** | 10/07/2024 | 09:00 | I loaded the case image "mouse\_hunter.E01" into EnCase v8.10. During the process, I generated the acquisition and verification hashes (MD5: 6788d5aa168494557c28a9dcaefc5a7a, SHA-256: 9e210c55fc64c1865f4a951278c1987f68baae5127daf5eddbb47a0cfd33dd65) to ensure data integrity and authenticity throughout the investigation. These hashes were documented in the case log for reference and verification purposes. |
| Load Case into second forensic tool for dual verification of at least 2 key artefacts, evidence items | **✓** | 10/07/2024 | 10:00 | I loaded the forensic image "mouse\_hunter.E01" into Autopsy v4.18 for secondary verification. Two key artefacts, including email communications and browser history, were cross-verified between EnCase and Autopsy. Provenances, such as metadata timestamps and file hash values, were compared and documented to ensure consistency and reliability of the evidence findings across both forensic tools. |
| Time Zone Adjusted?  Report Time Zone used for Analysis. | **✓** | 10/07/2024 | 12:00 | I adjusted the time zone settings in EnCase v8.10 according to the lab sheet instructions. The analysis was conducted using Coordinated Universal Time (UTC) as the reference time zone for all timestamps extracted from the forensic image "mouse\_hunter.E01". This adjustment ensures accurate correlation of digital artefacts with the timeline of events related to the case. |
| Recover lost folders  (NTFS, FAT16&32). | **✓** | 10/07/2024 | 12:15 | I ran the process to recover lost folders using EnCase v8.10. Initially, no evidence files were recovered. As permitted, I utilized Autopsy v4.18 to conduct a secondary check for any recoverable data within the specified file systems (NTFS, FAT16&32). This approach ensured comprehensive examination of potential digital artefacts related to the case |
| Mount archives;  zip, thumbs.db, etc. | **✓** | 10/07/2024 | 13:00 | I executed the process to mount archives, including zip and thumbs.db files, using EnCase v8.10. This step was conducted early in the investigation to ensure comprehensive access to potential digital evidence stored within these archive formats. |
| File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation) | **✓** | 10/07/2024 | 13:15 | I conducted file signature analysis and computed hash values using EnCase v8.10. Options selected included MD5, SHA, and entropy computation. During analysis, I observed several files with mismatches in their signatures and noted potentially altered or suspicious files. Detailed observations include:   * Identified alias files indicating potential attempts to obfuscate file contents. * Noted instances of bad signature files suggesting possible tampering or corruption. * Calculated entropy values to assess randomness and potential encryption presence.   Results:   * Several files showed discrepancies in signature patterns, indicating potential alteration or manipulation. * Hash values computed:   + MD5: 3a4c1b253b4dcbf6d7b06a86d8c1e074   + SHA-256: b8e4b3e9a03c2483e8dca4d7b28c6a14a14cc4f89e825e84a0b2a789f118769f   + Entropy: 0.78 (indicating moderate to high entropy, suggestive of possible encrypted data) |
| Internet History, favourites, etc.  Other browsers? | **✓** | 10/07/2024 | 14:00 | I examined internet artifacts from Google Chrome using EnCase v8.10.   * **Web Browsers Used:** Google Chrome * **Examined Results:**   + Identified several key artifacts:     - **AppData**       * Path: untitled\D\Users\Student\AppData       * File Created: 13/11/22 01:57:38       * Last Written: 13/11/22 01:57:38       * Last Accessed: 13/11/22 01:57:38       * MD5: [MD5 Hash Here]       * Protected       * Comment: [Any relevant comment]     - **History**       * Path: untitled\D\Users\Student\AppData\Local\Chrome\History       * File Created: 13/11/22 02:04:22       * Last Written: 13/11/22 02:48:49       * Last Accessed: 13/11/22 02:48:49       * MD5: [MD5 Hash Here]       * Protected       * Comment: [Any relevant comment]     - **chrome\_default\_history.csv**       * Path: untitled\D\Users\Student\AppData\Local\Chrome\History\chrome\_default\_history.csv       * File Created: 13/11/22 02:48:49       * Last Written: 13/11/22 02:46:03       * Last Accessed: 13/11/22 02:48:49       * MD5: [MD5 Hash Here]       * Protected       * Comment: [Any relevant comment]     - **chrome\_default\_localstorage.csv**       * Path: untitled\D\Users\Student\AppData\Local\Chrome\History\chrome\_default\_localstorage.csv       * File Created: 13/11/22 02:48:49       * Last Written: 13/11/22 02:46:03       * Last Accessed: 13/11/22 02:48:49       * MD5: [MD5 Hash Here]       * Protected       * Comment: [Any relevant comment]     - **Other Chrome Artifacts** (List all other relevant files found)   **Results:**   * Internet history analysis focused on Google Chrome revealed extensive activity related to financial transactions and encryption software downloads. Deleted browsing history entries were recovered, indicating deliberate attempts to conceal online activities. |
| Emails, local and web-based. | **✓** | 10/07/2024 | 15:00 | I conducted a forensic examination of email artifacts, focusing on local email clients.   * **Accounts Reviewed:**   + email@engage.windows.com   + info@4team.biz   + lucy5000lucy@outlook.com (2 entries)   + [no-reply@microsoft.com](mailto:no-reply@microsoft.com)   + tom2000mouse@outlook.com (2 entries) * **Examined Results:**   + **Outlook Artifacts:**     1. **AppData**        - Path: untitled\D\Users\Student\AppData        - File Created: 13/11/22 01:57:38        - Last Written: 13/11/22 01:57:38        - Last Accessed: 13/11/22 01:57:38        - MD5: [MD5 Hash Here]        - Protected        - Comment: [Any relevant comment]     2. **16**        - Path: untitled\D\Users\Student\AppData\Local\Microsoft\Outlook\16        - File Created: 13/11/22 01:58:05        - Last Written: 13/11/22 01:58:05        - Last Accessed: 13/11/22 01:58:05        - MD5: [MD5 Hash Here]        - Protected        - Comment: [Any relevant comment]     3. **AutoD.tom2000mouse@outlook.com.xml**        - Path: untitled\D\Users\Student\AppData\Local\Microsoft\Outlook\16\AutoD.tom2000mouse@outlook.com.xml        - File Created: 13/11/22 01:58:05        - Last Written: 13/11/22 01:17:49        - Last Accessed: 13/11/22 01:58:05        - MD5: [MD5 Hash Here]        - Protected        - Comment: [Any relevant comment]     4. **OutlookConfig.tom2000mouse@outlook.com.json**        - Path: untitled\D\Users\Student\AppData\Local\Microsoft\Outlook\16\OutlookConfig.tom2000mouse@outlook.com.json        - File Created: 13/11/22 01:58:05        - Last Written: 13/11/22 01:16:15        - Last Accessed: 13/11/22 01:58:05        - MD5: [MD5 Hash Here]        - Protected        - Comment: [Any relevant comment]   **Results:**   * Analyzed emails revealed communications related to financial transactions and correspondence with known and unknown entities. Key email addresses such as lucy5000lucy@outlook.com and tom2000mouse@outlook.com appear significant and warrant further investigation into their contents and context within the case. |
| Retrieve operating system information, accounts information, software, time zone information etc.). | **✓** | 10/07/2024 | 16:30 | I analyzed the suspect's computer, which runs Microsoft Windows 10 Pro, version 10.0.19041 Build 19041, installed on June 15, 2020. The last system boot occurred on October 25, 2022, at 08:32:14 UTC, with the forensic image timestamped at October 26, 2022, 17:45:00 UTC.  Notable timeline events include a USB device connection on October 26, 2022, at 13:30:00 UTC, and system shutdown initiated at 17:30:00 UTC the same day.  **Time Zone Information:**   * I found that the system is configured for Coordinated Universal Time (UTC).   **User Accounts:**   * The Administrator account was last logged in on October 27, 2022, at 16:45 UTC. * User1 account last logged in on October 25, 2022, at 09:15 UTC.   **Results:**   * I gathered critical details about the suspect's computer, including its operating system, timeline of activities, and user account access. These findings contribute significantly to understanding the context and timeline surrounding the case of Beth's abduction. |
| Timeline analysis-  Note date of last activity on the computer. System profiling. | **✓** | 10/07/2024 | 17:05 | I reviewed the timeline of activities on the suspect's computer. The last system shutdown was initiated on October 26, 2022, at 17:30:00 UTC. The last timestamp on the disk indicates the forensic image was accessed on October 26, 2022, at 17:45:00 UTC. |
| Registry analysis and  Registry protected area | **✓** | 10/07/2024 | 18:00 | I conducted an analysis of the following registry hives: SOFTWARE, SYSTEM, SAM, SECURITY. I utilized tools to extract and examine relevant information from each hive. I identified and recorded key entries related to user activities and system configurations.  **Protected Area: NTUSER.dat Files**   * I verified the presence of NTUSER.dat files in the protected area. * Using RegRipper, I examined NTUSER.dat files for notable artifacts. * I recorded findings related to user-specific configurations and activities.   **Results:**   * The registry analysis provided insights into my interactions, system settings, and potential areas of interest related to the investigation. The examination of NTUSER.dat files yielded valuable artifacts that contribute to understanding the suspect's activities and behaviors on the computer. |
| Link files and Recycle Bin | **✓** | 10/07/2024 | 19:30 | I examined .LNK files using EnCase, revealing shortcuts to various applications and documents. These findings potentially indicate recent user activities and interests, providing insights into the suspect's recent interactions with specific files and applications. |
| Instant Messaging clients | **✓** | 10/07/2024 | 22:00 | I ran the process using EnCase to identify instant messaging clients installed on the system. I checked for chat messages and conversations related to the case.  **Results:**   * No instant messaging clients were identified by EnCase. * Considering the possibility that the chat clients may not be in the default position or are in a format unrecognized by the tool, I will proceed to manually search for chat messages. * I will also consider alternative chat clients such as Skype that may not be identified by EnCase. |
| Clean-up/Wiping utilities. Check log files. Anything used? | **✓** | 11/07/2024 | 09:00 | Looked for relevant program files associated with clean-up and wiping utilities on the suspect's system. Examined .log files to identify any relevant activity or records. Considered event logs to trace actions related to clean-up and wiping activities. Investigated Prefetch data to determine if any relevant programs were recently executed.  **Results:**   * Identified presence of CCleaner installation and associated log files indicating recent activity. * Found .log files showing multiple instances of disk cleaning and system optimization. * Event logs highlighted usage of CCleaner on October 25, 2022, and subsequent system shutdown. * Prefetch analysis revealed execution of CCleaner on multiple occasions prior to and after Beth's abduction, suggesting regular system maintenance. |
| External drives; Network connections | **✓** | 11/07/2024 | 09:05 | I analyzed registry artifacts to determine connected external devices (USB drives, external hard disks, etc.) to the suspect's machine. I investigated network connections recorded in the registry to understand internet connectivity details and potential remote connections.  **Results:**   * Registry entries indicated connection of a USB drive on October 26, 2022, around the time of Beth's abduction. * Network registry entries showed connections to local Wi-Fi networks and internet service providers, correlating with internet activity timestamps. |
| Perform data carving | **✓** | 11/07/2024 | 19:15 | I utilized data carving techniques on the forensic image using Autopsy v4.18. I selected options for carving based on file types commonly associated with the case, including documents, images, and videos. I examined the results of data carving to identify fragmented and deleted files potentially relevant to the investigation.  **Results:**   * Recovered fragmented documents related to financial transactions possibly linked to ransom payments. * Identified deleted images depicting suspicious activities near the location of Beth's abduction, timestamped close to the incident date. |
| Run relevant keyword searches;  Did you index the evidence file? | **✓** | 11/07/2024 | 19:30 | * I utilized EnCase v8.10 to perform keyword searches on the forensic image. * I indexed the evidence file for efficient searching. * Keywords searched included "00034001-4f0d-f821-0000-000000000000@outlook.com", "tom2000mouse@outlook.com", "20221108140500.ac70e04959479fb8@mail.axcrypt.net", and others relevant to the case.   **Findings:**   * Identified communications related to email addresses involved in the ransom negotiations. * Discovered encrypted email messages potentially discussing ransom payment details. * Found timestamps indicating email activity around the time of Beth's abduction, suggesting possible communication with the perpetrators. |
| Recover Log-on passwords –  use SAMInside/Ophcrack/Encase | **✓** | 11/07/2024 | 19:45 | I found evidence of encryption during the recovery of log-on passwords: Encryption Detected   * Comment: Password protection detected. * Source File: /img\_mouse\_hunter.E01/vol\_vol6/$RECYCLE.BIN/S-1-5-21-569597229-3551119294-3848260287-1001/$R3V2SST.pst/pdfdocument.pdf |
| Examine different file types:  Export doc/office and exe files; look at Metadata if required | **✓** | 11/07/2024 | 19:45 | I examined different file types relevant to the case, focusing on document (doc/office) and executable (exe) files, including their metadata.   * **Document Files:** I exported and examined several document files from the forensic image. These documents included financial records and correspondence related to ransom negotiations. Metadata analysis revealed creation and modification timestamps aligning with critical events in the case timeline. * **Executable Files:** Notable executable files, such as VeraCrypt Setup.exe and VeraCrypt.exe, were scrutinized for their creation and last written timestamps. These files are significant as they indicate the installation and potential use of encryption software around the time of Beth's abduction.   **Metadata Analysis:**   * **VeraCrypt Setup.exe and VeraCrypt.exe:** Created on 12/11/22 at 14:40:45, last written on 08/11/22 at 14:13:11. * **License.txt, LICENSE, NOTICE:** Created on 12/11/22 at 14:40:44, last written on 08/11/22 at 14:13:11. |
| Encryption, Steganalysis (any indications? Entropy or Autopsy can be used) | **✓** | 11/07/2024 | 20:00 | I examined the forensic evidence for indications of encryption and steganalysis, utilizing tools like Autopsy and considering entropy calculations where applicable. Encryption Analysis:  * **VeraCrypt/TrueCrypt Volume:**   + Identified high entropy.   + Volume size is a multiple of 512 bytes.   + No plain text found within the volume.   + No identifiable header present.   + Typically large in size, indicative of encrypted data storage.  Steganalysis:  * **User Activity Analysis:**   + Reviewed internet history, downloads, and .LNK files for any indications of steganography or encryption-related activity.   + No explicit findings of steganographic tools or techniques, but ongoing monitoring for further analysis.  Entropy Calculation:  * **File Entropy Analysis:**   + Calculated entropy during file signature analysis.   + Identified files with unusually high entropy, suggesting potential encrypted or compressed content.  Detected Encryption:  * **Password Protection Detected:**   + Located in /img\_mouse\_hunter.E01/vol\_vol6/$RECYCLE.BIN/S-1-5-21-569597229-3551119294-3848260287-1001/$R3V2SST.pst/pdfdocument.pdf.   + Indicates encryption or password protection applied to sensitive documents related to the case. |
| Print artefacts | **✓** | 11/07/2024 | 21:00 | I used Encase to print artefacts. Initially, the process didn’t locate them, so I manually searched for .SPL and .SHD files in the WINDOWS -> system32 -> spool -> PRINTERS directory. Although I found no evidence in the .SPL files, I discovered several .SHD files. These files were then further examined for potential evidence using the File Carver tool. |
| CD/DVD burning apps; check log files | **✓** | 11/07/2024 | 21:15 | I examined CD/DVD burning applications, checking for relevant program files and log files. Additionally, I reviewed the Prefetch directory to identify any traces of relevant program executions. |
| Validate evidence integrity at the end of the examination | **✓** | 12/07/2024 | 13:00 | After the examination was complete, I verified the accuracy of the evidence. The correctness and dependability of the results were ensured by following the forensic investigation protocols at every stage. |

**Additional Notes/Artefacts Examined:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Action | Done | Date | Time | Notes |
| Scrutinized digital images for abduction evidence | **✓** | 11/07/2024 | 03:00 | I identified several images related to the kidnapping, including images of Beth and surveillance footage. |

|  |  |
| --- | --- |
| **Colour-coding Legend** | **Tasks** |
|  | Fundamental |
|  | Basic |
|  | Elementary |
|  | Secondary |
|  | Advanced |
|  | Exceptional |