# Contemporaneous Notes

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Examiner | Alish Mahat (23000965) | Exam commenced | 8/04/2025 | | Other relevant information |  | Software used, versions and licensing | Autopsy (4.21.0)  Regripper(4.0)  AcessData FTK imager (3.1.2.0)  Windows Event Viewer |   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 | Yes | 8/04/2025 | 8:15 AM | Autopsy > New Case > Load james\_laptop\_forensic\_image.E01. Set timezone. Verified MD5/SHA hash using 'Data Source Integrity' module. |
| Load Case into second forensic tool for dual verification of at least 2 key artefacts, evidence items | Yes | 9/04/2025 | 8:15 AM | using AcessData FTK imager to matched hash value and MD5.     1. Utilized FTK Imager to examine the NTUSER.DAT file. 2. Extracted relevant information from the NTUSER.DAT file using FTK Imager. |
| Time Zone Adjusted?  Report Time Zone used for Analysis. | Yes | 9/04/2025 | 8:16 AM | 1. In Autopsy, go to Tools > Options > Timezone 2. **A screenshot of a computer     AI-generated content may be incorrect.**Confirmed GMT+00:00 UTC is selected |
| Recover lost folders  (NTFS, FAT16&32). | Yes | 9/04/2025 | 8:30 AM | 1. A screenshot of a computer     AI-generated content may be incorrect. check Views > File Types > Deleted |
| Mount archives;  zip, thumbs.db, etc. | Yes | 9/04/2025 | 8:35 AM | 1. Go to Data Artifacts > File Types > Archives 2. Filter .zip, .rar, .thumbs.db |
| File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation) | Yes | 9/04/2025 | 8:39 AM | 1. Go to Analysis Results> Extension Mismatch Detector A screenshot of a computer     AI-generated content may be incorrect. |
| Internet History, favourites, etc.  Other browsers? | Yes | 9/04/2025 | 8:42 AM | 1. Go to Data Artifacts > Web History   A screenshot of a computer  AI-generated content may be incorrect. |
| Emails, local and web-based. | Yes | 9/04/2025 | 8:45 AM | 1. Go to Data Artifacts > E-Mail Messages   A screenshot of a computer  AI-generated content may be incorrect.   1. Go to Data Artifacts > Communication Accounts > Email |
| Retrieve operating system information, accounts information, software, time zone information etc.). | Yes | 9/04/2025 | 8:50 AM | 1. Open SYSTEM, SAM, SOFTWARE hives from Data Artifacts  * path: "img\_james\_laptop.E01/WINDOWS/system32/config"       A screenshot of a computer  AI-generated content may be incorrect.  A screen shot of a computer  AI-generated content may be incorrect.     1. SAM hive was analyzed, the username is “user.” 2. No password is required to access the user. 3. SYSTEM hive was analyzed, the timezone of the device is GMT. 4. The SOFTWARE hive was analyzed, the OS of the device is Windows 10 Enterprise. |
| Timeline analysis-  Note date of last activity on the computer. System profiling. | Yes | 9/04/2025 | 8:55 AM | 1. Extracted Security.evtx and System.evtx from:  path: /Windows/System32/winevt/Logs/  Opened and analyzed the files using **Windows Event Viewer** via Open Saved Log feature.   NOTE: as these time are in NPT not in UTC  A screenshot of a computer  AI-generated content may be incorrect.  **Security Log Events:**  • Logon – 22 Feb 2024, 8:11:42 PM (NPT) • Special/Privileged Logon– same time  • Logoff – 8:11:42 PM(NPT)    **System Log Events:**  • User-initiated shutdown – 8:11:42 PM (NPT) • System shutdown completed– 8:11:57 PM (NPT) • DHCP client shutdown – 8:11:57 PM (NPT)  A screenshot of a computer  AI-generated content may be incorrect. |
| Registry analysis and  Registry protected area | Yes | 9/04/2025 | 9:00 AM | 1. SAM, SYSTEM and SOFTWARE hives have already been analyzed. 2. Utilized RegRipper to analyze the extracted registry hives.   C:\Users\Alish\Desktop\a\registry.jpg |
| Link files and Recycle Bin | Yes | 9/04/2025 | 9:10 AM | 1. Data Artifacts > Recycle Bin, Recent Documents 2. Data Artifacts > Recent Documents   A close up of a screen  AI-generated content may be incorrect. |
| Instant Messaging clients | Yes | 9/04/2025 | 9:20 AM | 1. Data Artifacts > Installed Programs 2. Data Artifacts > Web Downloads  * Email client mozilla thunderbird was found   A screenshot of a computer  AI-generated content may be incorrect.  A screenshot of a computer  AI-generated content may be incorrect. |
| Clean-up/Wiping utilities. Check log files. Anything used? | Yes | 9/04/2025 | 10:00 AM | Analysis Results >Interesting Items > Encryption Programs   * Checked previously extracted system.evtx file. No traces of cleaning utility use was found. |
| External drives; Network connections | Yes | 9/04/2025 | 10:30 AM | 1. Data Artifacts > USB Device Attached |
| Perform data carving | Yes | 9/04/2025 | 11:00 AM | A screenshot of a computer  AI-generated content may be incorrect.   1. Run PhotoRec Carver module > Carved Files |
| Run relevant keyword searches;  Did you index the evidence file? | Yes | 9/04/2025 | 12:00 PM | Reviewed the results under "Analysis Results > Keyword Hits > Single Literal Keyword Search."  A screenshot of a search engine  AI-generated content may be incorrect. |
| Recover Log-on passwords –  use SAMInside/Ophcrack/Encase | Yes | 9/04/2025 | 1:00  PM | 1. A screenshot of a computer     AI-generated content may be incorrect.SAM file was previously analyzed. No password is required for the login. 2. An image file was found potentially password to something.   Path: /img\_james\_laptop.E01/Users/User/Downloads/IMG\_4418.JPG |
| Examine different file types:  Export doc/office and exe files; look at Metadata if required | Yes | 9/04/2025 | 2:00 PM | 1. File Types > Metadata  * Metadata of Multiple images were analysed.   A screenshot of a computer  AI-generated content may be incorrect.   * A screenshot of a computer    AI-generated content may be incorrect.Click: Analysis Results> User Contents suspected |
| Encryption, Steganalysis (any indications? Entropy or Autopsy can be used) | Yes | 9/04/2025 | 3:00 PM | 1. Click: Analysis Reports> Encryption Suspected   A screenshot of a computer  AI-generated content may be incorrect.   1. Click: Data Artifacts> Run Programs |
| Print artefacts | Yes | 9/04/2025 | 3:30 PM | 1. Investigated /Windows/System32/spool/PRINTERS/ and searched entire image for .spl and .shd files.  No evidence of print spool files found. 2. Keyword searches for printer, .spl, and spool returned 0 relevant hits. 3. Also reviewed system.evtx log for PrintService events — none were recorded.   A screenshot of a computer  AI-generated content may be incorrect. |
| CD/DVD burning apps; check log files | Yes | 9/04/2025 | 4:00 PM | 1. Analysed the previously extracted system.evtx file and Path: img\_james\_laptop.E01/Documents and Settings/ 2. A screenshot of a computer     AI-generated content may be incorrect.No such events were present in the image. |
| Validate evidence integrity at the end of the examination | Yes | 9/04/2025 | 5:00 PM | 1. Hash values are consistent, indicating an examination conducted without data tampering. 2. Ran the Ingest module to verify Data Source Integrity. 3. Steps involved selecting "Tools" from the toolbar, running ingest modules for "Hunter XP for Dongled v6.E01," specifically targeting Data Source Integrity, and completing the process by selecting "Finish."   A screenshot of a computer  AI-generated content may be incorrect. |

**Additional Notes/Artefacts Examined:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Location Data | Yes | 9/04/2025 | 12:45 PM | 1. Click: Geolocation 2. Two picture showed a location of Botswana and Cape Town in recent 10 days . 3. image names: IMG\_6509.JPG and IMG\_6325.JPG |
|  |  |  |  |  |
|  |  |  |  |  |

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