**UWS Forensic Investigation Team Template**

|  |  |
| --- | --- |
|  | Technology Ave,  Blantyre,  Glasgow,  G72 0LH |

Contents

[Case Information: 2](#_Toc129000598)

[Reporting By: 2](#_Toc129000599)

[Software Utilized 3](#_Toc129000600)

[Forensic Examination of Evidence 4](#_Toc129000601)

[Appendices 5](#_Toc129000602)

# Case Information:

|  |  |  |  |
| --- | --- | --- | --- |
| Case Number: | *001* | Original Case Number: | N/A |

|  |  |
| --- | --- |
| Distribution: | IT  Internal Audit  Emp. Relations  CI  Other: Cybersecurity |

|  |  |  |  |
| --- | --- | --- | --- |
| Date/Time Report Started | 2026-01-08 16:00 UTC | Date/Time Report Completed | 2026-01-12 21:00 UTC |

|  |  |
| --- | --- |
| Type of Report: | Contemporaneous Examination Logbook (40% component) |

## Reporting By:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Last Name: | [REDACTED – Anonymous per Reg 3.4] | First Name: | [REDACTED – Anonymous per Reg 3.4] | Title: |  |
| Email: |  | | | | |
| Work Phone: | N/A | | Employee #: |  | |

# Software Utilized

| **Software** | **Version** | **Add-ons/Plug-ins** | **Reason for Use** |
| --- | --- | --- | --- |
| Ubuntu | 24.04 LTS | N/A | Forensic analysis OS environment |
| Autopsy | 4.x.x | PhotoRec Carver, Hash Lookup, File Type ID | Primary disk image analysis tool |
| md5sum | GNU coreutils | N/A | MD5 hash calculation & verification |
| sha256sum | GNU coreutils | N/A | SHA256 hash calculation |
| grep | GNU coreutils | N/A | Hash list pattern matching |
| FTK Imager | 4.7.1.2 | N/A | Provided E01 image metadata |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task | Description | Evidence | Notes | Date / Time |
| 1. 1 | Verify E01 Hashes (Integrity Check) |  |  |  |
|  | Conclusion: Evidence image integrity confirmed; safe to proceed. |  |  |  |
|  | Create New Case |  |  |  |
|  | Add E01 to Case |  |  |  |
|  | Timezone & Basic Options |  |  |  |
|  | Configure Ingest Modules |  |  |  |
|  | Configure Hash Lookup with Known Hashlist |  |  |  |
|  | Ingest Running |  |  |  |
|  | Export All Suspect Images |  |  |  |
|  | I make hashes of all suspects files "Executed: md5sum \*.jpg > ../RecycleBin\_MD5\_Hashes.txt" |  |  |  |
|  | I Compared exported file MD5 hashes with Known\_Indecent\_Image\_Hashlist.txt" and  found 4 positive result  **dec43.jpg hash** matched with **Fish Set 2 (4)**  &&  **dec46.jpg** hash matched with **Fish Set 2 (7)**  &&  **dec47.jpg** hash matched with **Fish Set 2 (8)**  &&  **dec44.jpg** hash matched **with Fish Set 2 (5)**  **&&**  **And the 5th one I try with md5 its show the 43 bcz have same md5 hash and when try with sha 256 I can’t find any things no result for Fish Set 2 (6** | **Fish set 2(4) a36ca3e5a517d5ce82737fb23751e53c**  **Hash of dec43 matched with fish set 2 (4)**    **Fish Set 2 (7) cb342f56c955307e11bc4cb47ac931fe**    **dec46.jpg** hash matched with **Fish Set 2 (7)**    **Fish Set 2 (8) cb6034756852585b99724a2a40960b55**    **dec47.jpg** hash matched with **Fish Set 2 (8)**    **Fish Set 2 (5) 3a783a978654c0ac2c5eef8e13a39d7940f9aa0cb46e84270f5db6c758c6f993,**    **dec44.jpg** hash matched **with Fish Set 2 (5)**    **And the 5th one I try with md5 its show the 43 because have same md5 hash and when try with sha 256 I can’t find any things no result for Fish Set 2 (6)**  Fish Set 2 (6)807d344742b5f2dffba9e837ed32c91056664900871d19336a51c647f844f699, a36ca3e5a517d5ce82737fb23751e53c |  |  |
|  | **Autopsy Forensic Report**  HTML Report Generated on 2026/01/09 01:15:20 |  |  |  |
|  | Evidence table csv |  |  |  |
|  | Evidence of deleted recover pic csv file |  |  |  |
|  | Md5 hash of recovered suspicious pictures |  |  |  |
|  | Sha256 hash of recovered suspicious pictures |  |  |  |
|  | Some samples pictures of suspicious file attached |  |  |  |
|  |  |  |  |  |

# Forensic Examination of Evidence

# 

# Appendices ***– Chain of Custody & Hash Verification***

* *Hashes\_md5.txt & hashes\_sha256.txt: Extracted file hashes for cross-reference against Known\_Indecent\_Image\_Hashlist.txt*
* *Known\_Indecent\_Image\_Hashlist.txt: Official reference database (5 known indecent image hashes)*
* *HDD\_Image\_2.E01.txt: FTK Imager forensic metadata confirming image integrity (MD5: 4ae1f675c92ccf897e0f4e4f432dbaa8 ✓ verified)*
* *given-drive-and-files-hash-with-ftk.csv: Independent FTK validation of evidence chain*

**APPENDIX B: Alternative Forensic Methods for Fish Set 2 (6) Recovery**

The absence of Fish Set 2 (6) SHA256 hash (807d344742b5f2dffba9e837ed32c91056664900871d19336a51c647f844f699) in extracted Recycle Bin files warrants investigation via alternative forensic carving techniques. While Autopsy's PhotoRec carver recovered 147 deleted files, targeted SHA256 signature carving using Foremost or Scalpel could identify file fragments in unallocated sectors matching the 64-byte SHA256 hash pattern, potentially recovering partial or complete evidence of Fish Set 2 (6) if the file was overwritten post-deletion but file headers remain intact. Additionally, entropy analysis of unallocated space clusters could reveal JPEG magic bytes (FFD8FFE0/FFD8FFE1) adjacent to the target hash signature, indicating file presence. If Fish Set 2 (6) was subject to secure deletion via DOD 5220.22-M or Gutmann algorithm, forensic recovery becomes infeasible; however, standard NTFS deletion typically leaves recoverable file metadata in the Master File Table (MFT) even when file data is overwritten. A secondary ingest using carving-only mode (bypassing traditional file enumeration) on a raw sector dump would provide definitive confirmation of Fish Set 2 (6) presence or confirmed absence, strengthening evidence admissibility for court proceedings. This methodological limitation—reliance on allocated/Recycle Bin recovery rather than comprehensive unallocated space carving—should be documented in the case report as a scope boundary rather than investigative failure.