**Digital Forensic Examination Report**

**Case ID:** Case001  
**Examiner:** Scott Terchiak  
**Date:** 08/24/2025

**1. Objective**

The purpose of this exercise was to simulate the acquisition and recovery of deleted digital evidence from a removable media device (USB drive). Specifically, the task involved creating, deleting, and recovering a test file (evidence.png) while preserving forensic integrity through hashing and controlled workflows.

**2. Evidence Acquisition**

**Source Media:**

* Device: USB Flash Drive (Disk 3)
* Capacity: 118 GB
* Partition Style: MBR

**Acquisition Method:**

* Tool: dd via FTK Imager / Autopsy imaging utility
* Output: Segmented RAW forensic image (case001.dd, case001.001 … case001.080)
* Segmentation Size: 2 GB per file

**Cryptographic Hashes (at time of acquisition):**

* **SHA256 (Original Evidence Image):**
* c6d8f4994d33975d41b6fd3475f9b0e068fd7248ceb3748223e115c448e77378

A computer screen with white text

AI-generated content may be incorrect.

**Integrity Verification:**

* Post-acquisition verification performed using certutil (Windows) and internal Autopsy hash verification.
* Result: Acquisition hash matched original SHA256 → *Integrity Confirmed*.

**3. Examination Process**

**Environment:**

* Platform: VirtualBox (Windows 11 VM & Kali Linux VM)
* Analysis Tool: Autopsy 4.22.1
* Supporting Tools: certutil, Excel (for CSV review)

**Steps:**

1. Mounted segmented image files (case001.dd series) into Autopsy.
2. Ingest modules used:
   * File Type Identification
   * PhotoRec Carver
   * Keyword & Metadata Search
3. Navigated Deleted Files view → confirmed presence of evidence.png.
4. Exported recovered file and recomputed SHA256 hash.

**4. Findings**

* **Deleted File Located:**
  + Name: evidence.png
  + Size: 169,862 bytes (~166 KB)
  + Location: Deleted Files → File System
  + Status: Successfully recovered
* **Recovered File Hash:**
* c6d8f4994d33975d41b6fd3475f9b0e068fd7248ceb3748223e115c448e77378

A screenshot of a computer

AI-generated content may be incorrect.

* **Hash Comparison:**
  + Original Hash (pre-deletion) = Recovered Hash
  + **Result:** Exact match → File integrity confirmed.

**5. Conclusion**

The test confirmed that deleted evidence (evidence.png) can be recovered and verified from a forensic image using Autopsy and standard hashing practices. The workflow preserved the forensic principle of integrity, demonstrating proper acquisition, analysis, and validation techniques.

**6. Appendix**

* **Screenshots:**
  + Evidence creation in Paint
  + File deletion
  + Imaging process (dd/Autopsy export)
  + Hash computation (certutil)
  + Autopsy recovery screenshot
* **Case Artifacts:**
  + case001.dd series
  + Recovered evidence.png
  + Hash verification log