Final VAPT Report

PREPARED BY: Esperanza Buitrago Díaz

Submitted To: Neuefische

Submission Date: February 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A digital forensic analysis was conducted on February 4th, 2026, focusing on evidence collection and recovery from a compromised system disk image. The investigation involved integrity verification of a forensic disk image (8-jpeg-search.dd) , creation of a proper chain of custody using *Autopsy forensic toolkit,* and recovery of hidden JPG files suspected of containing sensitive information.

The analysis successfully verified image integrity through MD5 hash matching, established a forensic case with proper metadata documentation, and recovered multiple hidden JPG files demonstrating systematic data concealment by threat actors. Evidence suggests use of obfuscated files extensions, compressed archives, and NTFS metadata manipulation.

2. ASSESSMENT SCOPE AND OBJECTIVES

2.1 Scope

- **Target Image:** 8-jpeg-search.dd, and 8-jpeg-search-copy.dd (161MB forensic disk image)
- **Tools used:** Autopsy Digital Forensics Platform, MD5 hash verification utilities
- **Analysis Type:** Dinks image analysis, file carving, hidden data recovery
- **Targeted Files:** 5 hidden JPG images (file1.jpg - file5.jpg)

2.2 Objectives

1. Verify integrity of forensic disk image through MD5 hash verification.
2. Create a proper Autopsy case with chain of custody documentation.
3. Recover 5 hidden JPG files using forensic analysis techniques.
4. Document findings and their forensic significance.

3. METHODOLOGY

3.1 Integrity Verification

- **MD5 hash generation:** Calculated hash of `8-jpeg-search.dd` using `md5sum`.
- **File-copy:** Copy of `8-jpeg-search.dd` to `8-jpeg-search-copy.dd` and verification of its integrity using `md5sum`, and `diff`.
- **Hash verification:** Compared against expected value: `9bdb9c76b80e90d155806a1fc7846db5`
- **Evidence preservation:** Stored hash in `evidence_md5_hash.txt` for chain of custody.

3.2 Autopsy case creation

- **Case setup:** Created new case with proper metadata:
    - Case name: Forensics pentester
    - Investigator: Esperanza Buitrago
    - Description: Verification of integrity.
- **Data source import:** Added disk image using “Copy” import method for evidence preservation.
- **Hash verification in tool:** Used Autopsy’s build-in hash calculation to verify integrity, and also `md5sum` in the terminal.

3.3 Forensic analysis and recovery

- **File system analysis:** Examined directory structure and file metadata.
- **Keyword search:** Searched for JPG files using ASCII, Unicode, case-insensitive parameters.
- **Deleted file recovery:** Extracted files from deleted space using Autopsy’s recovery tools.
- **Hex analysis:** Verified files signatures (`FF D8 FF` for JPEG headers)

3.4 Forensic artifacts and indicators

- **Obfuscation techniques detected:**
    - Extension manipulation: .jpg -> .dat, .hmm, .boo

    - Hidden in compressed archives: .zip, .tar.gz
    - Misleading directories: C:\invalid\, C:\misc\
- NTFS Metadata traces:
    - References found in $LogFile and $MFTS for
        - file1.jpg
        - file3.jpg
        - file4.jpg
        - File6.jpg
    - Indicates prior access/modification by threat actors.
- Malicious document indicators:
    - file12.doc contains references to file9.jpg - potential macro-based malware.
- Suspicious executable:
    - file13.dll.here in C:\misc\ - possible payload or loader.

Evidence Documentation

- **Screenshot documentation:** Captured critical analysis steps.
- **File export:** Recovered JPG files to secure location.
- **Chain of Custody:** Maintained throughout the process.

4. SUMMARY OF FINDINGS

4.1 Key Statistics

- **Image integrity:** Verified (MD5 hash matched expected value).
- **Hidden files recovered:** Multiple JPG files recovered (partial success on target 5).
- **Tools used:** Autopsy, standard Linux forensic utilities.

4.3 Overall Risk Rating: SUCCESSFULL

The forensic analysis successfully verified evidence integrity and recovered concealed files, demonstrating effective evidence collection procedures.

5. DETAILED FINDINGS WITH EVIDENCE

Finding 1: Image integrity verification

- **Risk Score:** 0/10
- **Status:** Critical verification step completed
- **Evidence:**
    - Terminal MD5Calculation

```
md5sum 8-jpeg-search.dd
# Output: 9bdb9c76b80e90d155806a1fc7846db5
```

    - Autopsy hash verification MD5: 9bdb9c76b80e90d155806a1fc7846db5
    - Matched expected value exactly.

- **Forensic significance:** Hash matching confirms the disk image has not been altered, tampered with, or corrupted since acquisition. This establishes integrity for legal purposes.

Finding 2: Proper Chain of Custody established

- **Risk Score:** 0/10 (Informational)
- **Status:** Best Practice followed

Evidence:

- Case metadata documentation:
    - Case name: Forensics pentester
    - Investigator: Esperanza Buitrago
    - Description: Verification of integrity of forensic disk image.
- Host information:
    - Host name: host 1

Forensic significance: Proper metadata documentation is essential for legal admissibility of evidence. It establishes who handled the evidence, when and for what purpose.

Finding 3: Hidden JPG files successfully recovered

- **Risk Score:** 7/10
- **Status:** Partial success - multiple files recovered.

Evidence:

- Recovered files:
    - Picture 3: Recovered from deleted files.
    - Picture 4: Recovered from deleted files.
    - Picture 9: Found in misc directory.
    - Additional images discovered in alloc directory.
- Search methodology:
    - Keyword for jpg (ASCII, Unicode, case-insensitive).
    - File carving from unallocated space.
    - Hex signature verification (FF D8 FF pattern).

File	Original location	State
file1.jpg	C:\alloc\	**Recovered from assigned space.**
file6.jpg	C:\del1\	**Recovered from deleted files.**
file8.jpg	C:\archive\file8.zip	**Extracted from compressed file.**
file9.jpg	C:\archive\file9.boo	**Extracted from obfuscated file.**
file10.jpg	C:\archive\file10.tar.gz	**Extracted from compressed file.**

Forensic significance: The recovery of hidden JPG files indicates potential data concealment by threat actors. Files were found in deleted space (attempted destruction) and misnamed directories (obfuscation), suggesting intentional hiding of sensitive information.

Finding 4: File signature analysis

- **Risk Score:** 5/10
- **Affected Module:** Technical verification completed.

Evidence:

- Hex analysis results:
    - Valid JPEG headers found: FF D8 FF
    - File extension mismatches detected (.dat files with JPEG signatures).
- Extension mismatch detection
    - Files with .dat extension contained valid JPEG data
    - This is a common obfuscation technique

```
Offset: 00000000  FF D8 FF E0 00 10 4A 46  49 46 00 01 01 00 00 01
```

Forensic Significance: File signature analysis bypasses extension-based obfuscation. Finding valid JPEG data in non-JPEG files indicates intentional hiding techniques were employed.

Finding 5: Systematic data concealment *via* obfuscation and compression

- **Risk Score:** 8/10

Evidence:

- Multiple JPG files hidden in compressed archives
    - file8.zip
    - file10.tar.gz
- Obfuscated extension usage
    - .boo
    - .hmm
    - .dat
- References in $MFT and $LogFile indicating intentional hiding.
- Suspicious document (file12.doc) with embedded image references.

Forensic Significance: Threat actors employed advanced hidden techniques including:

1. Compression to evade signature-based detection
2. Extension obfuscation to bypass files type filters
3. NTFS metadata manipulation to obscure file history
4. Malicious document integration for potential malware delivery.

ASSESSMENT FINDINGS

#	Finding	Risk Score	Risk	Exploitation Likelihood	Business impact	Remediation difficulty
1	Image Integrity verification verification	**0**	**Informational**	**N/A**	**N/A**	**Easy**
2	Proper chain of custody established	**0**	**Informational**	**N/A**	**N/A**	**Moderate**
3	Hidden JPG files successfully recovered	**7**	**High**	**Possible**	**Major**	**Hard**
4	File signature analysis	**5**	**Medium**	**Possible**	**Moderate**	**Easy**
5	Systematic data concealment *via* obfuscation and compression	**8**	**High**	**Likely**	**Major**	**Moderate**

6. FORENSIC SIGNIFICANCE ANALYSIS

Why these artefacts are significant:

- Data concealment evidence:
    - Files in deleted space suggest attempted destruction of evidence.
    - Misleading file extensions indicate obfuscation attempts.
    - Hidden directories suggest systematic hiding of sensitive data.
- Threat actor tradecraft indicators:
    - Use of deleted space for storage shows technical sophistication.
    - File renaming techniques suggest knowledge of forensic bypass methods.
    - Multiple hiding locations indicate persistence and planning
- Incident timeline reconstruction:
    - File creation/modification timestamps can establish a timeline.
    - Multiple locations suggest ongoing concealment activities.

    - Recovery from deleted space indicates recent deletion attempts.
- Data exfiltration indicators:
    - JPG files could contain:
        - Screenshots of sensitive information.
        - Photographs of documents.
        - Steganography (hidden data within images).
        - Credential information
- Legal and compliance implications:
    - Successful recovery demonstrates effective forensic procedures.
    - Hash verification ensures evidence admissibility.
    - Proper documentation supports legal proceedings.

6. RECOMMENDATIONS

6.1 Immediate Actions (0-7 days)

1. Analyse recovered files for steganography:
    a. Use steghide, zsteg, binwalk on recovery JPGs.
    b. Check file12.doc for macros embedded payloads.
2. Scan for additional hidden archives:
    a. Search for .rar, .7z, .iso, .cab in unallocated space.
    b. Look for encrypted volumes
3. Extract and analyse NTFS artifacts:
    a. Parse $MTF for timestamps and file movement.
    b. Reconstruct timeline using $LogFile entries.

6.2. Short term Improvements (7-30 days)

1. Implement file integrity monitoring (FIM):
    - Monitor changes to $MFT and critical system directories.
    - Alert on unauthorized compression tools execusion
2. Enhanced Forensic Procedures:
    - Implement automated hash verification for all evidence.
    - Standardise case metadata templates.

- Create evidence handling checklist.

3. Enhance forensic readiness:
    - Deploy automated evidence collection scripts
    - Standardize forensic workstation imaging procedures
4. Tool Configuration:
    - Configure Autopsy with custom keyword lists for command hiding techniques.
    - Set up automatic file signature analysis.
    - Implement regular tool updates and validation.
5. Threat hunting rule development:
    - Create Sigma rules for:
        - Unusual file extensions in system directories.
        - Compression tool usage outside normal patterns.
        - NTFS metadata manipulation attempts.
6. Training:
    - Train staff on proper chain of custody procedures.
    - Conduct regular forensic exercises.
    - Document lessons learned from this investigation.

6.3 Long term Strategy (1-6 months)

1. Forensic readiness program:
    - Develop organization-wide evidence handling policies.
    - Implement regular forensic capability testing.
    - Create incident response playbooks with forensic components.
2. Technology investments:
    - Consider enterprise forensic platforms.
    - Implement write-blocker hardware for physical evidence.
    - Deploy forensic workstations with validated toolkits.
3. Deploy endpoint detection and response (EDR):
    - Enable fileless attack detection.
    - Monitor process hollowing, LOLBins abuse
4. Implement data loss prevention (DLP):
    - Block unauthorized compression/archiving.
    - Restrict executable files in non-standard locations.
5. Compliance framework:

- Align with ISO 27037 (Digital Evidence Handling).
- Implement NIST SP 800-86 guidelines.
- Regular third-party forensic capability assessments.
- Conduct quarterly red team exercises with forensic analysis.

Conclusion

The forensic analysis not only verified evidence integrity and recovered concealed files but also uncovered systematic obfuscation techniques used by threat actors. The discovery of JPG files hidden within compressed archives, obfuscated, and NTFS metadata traces reveals a sophisticated data concealment campaign.

These findings elevate the incident from simple data hiding to planned adversarial tradecrafts, indicating potential exfiltration preparation or malware staging. The successful recovery demonstrates the effectiveness of methodical forensic analysis while highlighting the need for enhanced detection mechanisms against file obfuscation and compression-based evasion.

Key successes:

1. Evidence integrity verified and documented.
2. Chain of custody properly established.
3. Multiple hidden files successfully recovered.
4. Forensic methodology demonstrated effectively.

Areas of improvement:

1. Complete recovery of all targeted files.
2. Deeper analysis of recovered file contents.
3. Enhanced documentation of analysis steps.

Key forensic takeaways:

1. Threat actors used multi-layered hiding techniques.
2. NTFS artifacts provide valuable timeline data

3. Obfuscated extensions are a reliable indicator of malicious intent.
4. Compressed archives remain a common evasion vector.