

Final VAPT Report



PREPARED BY: Esperanza Buitrago Díaz

Submitted To: Neufische

Submission Date: February 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	2
HIGH LEVEL ASSESSMENT OVERVIEW.....	3
Observed Security Strengths.....	4
Areas for Improvement.....	4
Short Term Recommendations.....	4
Long Term Recommendations.....	4
SCOPE.....	4
Project Scope.....	5
Network Information.....	5
TESTING METHODOLOGY.....	5
CLASSIFICATION DEFINITIONS.....	6
Risk Classifications.....	7
Exploitation Likelihood Classifications.....	7
Business Impact Classifications.....	7
Remediation Difficulty Classifications.....	8
ASSESSMENT FINDINGS.....	8
FORENSIC EVIDENCE COLLECTION AND ANALYSIS.....	10
APPENDIX A - TOOLS USED.....	11
APPENDIX B - ENGAGEMENT INFORMATION.....	12
Client Information.....	12
Version Information.....	12
Contact Information.....	13

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 from various locations including deleted files and allocated space. The recovered artifacts demonstrate potential data concealment activities by threat actors.

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 of forensic disk image.
- **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 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 locations found:

```
/deleted_files/          # Pictures 3 & 4  
/misc/                  # Picture 9  
/alloc/                 # Additional images
```

Specific recovered files:

- file3.jpg - recovered with message “I AM PICTURE #3”.
- file4.jpg - recovered successfully.
- file9.jpg - recovered with message “I AM PICTURE #9”.
- Additional JPG files in allocated space.

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.

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

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. Complete file recovery: Continue searching for remaining target files (file1.jpg, file2.jpg, file5.jpg).
2. Metadata analysis: Extract EXIF data from recovered JPGs for additional clues.
3. Steganography Analysis: Check recovered images for hidden data using tools like steghide, zsteg.

6.2. Short term Improvements (7-30 days)

1. Enhanced Forensic Procedures:
 - Implement automated hash verification for all evidence.
 - Standardise case metadata templates.
 - Create evidence handling checklist.
2. Tool Configuration:
 - Configure Autopsy with custom keyword lists for command hiding techniques.
 - Set up automatic file signature analysis.
 - Implement regular tool updates and validation.
3. 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. Compliance framework:
 - Align with ISO 27037 (Digital Evidence Handling).
 - Implement NIST SP 800-86 guidelines.
 - Regular third-party forensic capability assessments.

Conclusion

The forensic analysis successfully demonstrated proper evidence handling procedures and effective recovery of concealed files. The verification of image integrity through MD5 hash matching establishes a solid foundation for legal admissibility. The recovery of JPG files from multiple hidden locations reveals systematic data concealment attempts by threat actors.

While not all five target files were recovered, the methodology proved effective and the recovered artifacts provide valuable intelligence about threat actor tradecraft. The findings underscore the importance of proper forensic procedures, tool proficiency, and methodical analysis incident response scenarios.

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.