# Forensic Investigation Report

## Summary

This report documents the findings of a forensic investigation into alleged illegal activities conducted by the suspect, [Suspect Name]. The investigation focused on examining forensic images provided, which contained data from the suspect's computer systems. The forensic images included the suspect's hard drives, emails, browsing history, chat logs, and other digital footprints. The objective of the investigation was to:

1. Uncover Evidence Related to the Offence:

- Identify and recover illegal content, including images, videos, and documents, stored on the suspect's devices.

- Examine system logs, internet browsing history, and file access records to establish the nature and extent of the illegal activities.

2. Identify the Suspect:

- Correlate user profiles, login records, and document metadata to the suspect's identity.

- Analyze email accounts, social media profiles, and other digital identifiers that link the activities to the suspect.

3. Demonstrate Intent:

- Investigate search queries, encrypted files, and hidden directories to establish the suspect's intent to conceal illegal activities.

- Review communications, such as emails and chat logs, that indicate deliberate planning and coordination of illegal activities.

4. Establish the Extent of the Suspect's Activities:

- Quantify the number and types of illegal files and their distribution across the suspect's devices.

- Analyze network activity logs to identify any sharing or distribution of illegal content.

- Examine financial records, payment receipts, and other evidence of monetary transactions related to the illegal activities.

The investigation was conducted using industry-standard forensic tools such as Autopsy, FTK (Forensic Toolkit), and OSForensics. These tools allowed for comprehensive analysis and cross-verification of findings, ensuring the integrity and reliability of the evidence. The detailed analysis provided a clear timeline of events, showing the suspect's activities and their attempts to evade detection. The findings from this investigation will be used to support legal proceedings against the suspect, providing a robust evidence base to demonstrate the suspect's involvement in the illegal activities. The report includes a detailed analysis of the evidence, timelines, and supporting documentation, which will be submitted to the prosecution team and law enforcement for further action.

## Issue Chapters

### Content Relating to the Offence

During the investigation, multiple files were identified that are relevant to the alleged offence. These files included:

### Illegal Content

Several images and videos were found in directories labeled "Hidden" and "Encrypted." These files were identified as illegal based on their content and metadata. The specifics of these files are as follows:

- \*\*Images:\*\*

- \*\*Filename:\*\* `illegal\_image1.jpg`

- \*\*Location:\*\* \Users\Suspect\Hidden

- \*\*Size:\*\* 5,215 KB

- \*\*Created:\*\* 15/06/2023 08:32:14 AM

- \*\*MD5 Checksum:\*\* a3b4c3d4e5f6a7b8c9d0e1f2g3h4i5j6

- \*\*Analysis:\*\* Image depicts prohibited content.

- \*\*Filename:\*\* `illegal\_image2.png`

- \*\*Location:\*\* \Users\Suspect\Encrypted

- \*\*Size:\*\* 3,104 KB

- \*\*Created:\*\* 20/06/2023 11:42:19 AM

- \*\*MD5 Checksum:\*\* f3g4h5i6j7k8l9m0n1o2p3q4r5s6t7u8

- \*\*Analysis:\*\* Image depicts prohibited content.

- \*\*Videos:\*\*

- \*\*Filename:\*\* `illegal\_video1.mp4`

- \*\*Location:\*\* \Users\Suspect\Hidden

- \*\*Size:\*\* 125,742 KB

- \*\*Created:\*\* 25/06/2023 02:15:45 PM

- \*\*MD5 Checksum:\*\* v4w5x6y7z8a9b0c1d2e3f4g5h6i7j8k9

- \*\*Analysis:\*\* Video contains illegal material.

- \*\*Filename:\*\* `illegal\_video2.mkv`

- \*\*Location:\*\* \Users\Suspect\Encrypted

- \*\*Size:\*\* 89,204 KB

- \*\*Created:\*\* 30/06/2023 04:21:33 PM

- \*\*MD5 Checksum:\*\* l6m7n8o9p0q1r2s3t4u5v6w7x8y9z0a1

- \*\*Analysis:\*\* Video contains illegal material.

### Communications

Email exchanges and chat logs retrieved from the forensic images show correspondence with other individuals discussing the sharing and distribution of illegal content. Notable findings include:

- \*\*Emails:\*\*

- \*\*Sender:\*\* suspect\_email@example.com

- \*\*Recipient:\*\* associate@example.com

- \*\*Subject:\*\* New Files

- \*\*Date:\*\* 28/06/2023 10:14:23 AM

- \*\*Content:\*\* "I have new files that you might be interested in. Check the hidden folder for the latest additions."

- \*\*Sender:\*\* suspect\_email@example.com

- \*\*Recipient:\*\* another\_contact@example.com

- \*\*Subject:\*\* Re: Encrypted Content

- \*\*Date:\*\* 02/07/2023 03:32:45 PM

- \*\*Content:\*\* "The encrypted folder contains the files we discussed. Use the password 'secureaccess123' to decrypt."

- \*\*Chat Logs:\*\*

- \*\*Chat Application:\*\* WhatsApp

- \*\*Conversation with:\*\* [Contact Name]

- \*\*Date:\*\* 01/07/2023 07:45:18 PM

- \*\*Content:\*\*

- Suspect: "Did you get the new batch?"

- Contact: "Yes, it's perfect. Any more coming soon?"

- Suspect: "I'll let you know once I have more."

- \*\*Chat Application:\*\* Telegram

- \*\*Conversation with:\*\* [Another Contact]

- \*\*Date:\*\* 03/07/2023 08:22:56 PM

- \*\*Content:\*\*

- Suspect: "Ensure the files are well-hidden. We can't afford any slip-ups."

- Contact: "Already taken care of. They're encrypted and stored safely."

### Browsing History

Analysis of the browser history revealed visits to websites known for hosting illegal content. The suspect's browsing activities indicate a pattern of accessing and downloading prohibited material. Specific findings include:

- \*\*Browser:\*\* Google Chrome

- \*\*Date:\*\* 24/06/2023 11:18:22 AM

- \*\*URL:\*\* `http://www.illegalcontentwebsite.com`

- \*\*Activity:\*\* Accessed and downloaded multiple files.

- \*\*Date:\*\* 27/06/2023 02:37:44 PM

- \*\*URL:\*\* `http://www.darkwebillegalcontent.com`

- \*\*Activity:\*\* Used a Tor browser to navigate to a hidden service site and download content.

- \*\*Browser:\*\* Mozilla Firefox

- \*\*Date:\*\* 29/06/2023 09:54:11 AM

- \*\*URL:\*\* `http://www.prohibitedcontentforum.com`

- \*\*Activity:\*\* Engaged in discussions about secure methods to share and store illegal content.

### Conclusion

The investigation uncovered substantial evidence that the suspect was actively involved in accessing, storing, and distributing illegal content. The recovered files, communications, and browsing history collectively demonstrate the suspect's engagement in illegal activities. The findings will be crucial in supporting legal proceedings against the suspect.

### Identification

Evidence linking the suspect to the investigated computer systems includes:

- \*\*User Profiles:\*\* The forensic images contained user profiles with the suspect's name, email address, and other personal information.

- \*\*Login Records:\*\* System logs show multiple logins by the suspect's user account during the period when the illegal activities occurred.

- \*\*Document Metadata:\*\* Several documents and files created on the suspect's computer contained metadata indicating they were authored by the suspect.

### Intent

Evidence demonstrating the suspect's intent to commit the alleged offence includes:

- \*\*Search Queries:\*\* Analysis of the search history revealed queries related to hiding illegal content and methods of avoiding detection.

- \*\*File Organization:\*\* The suspect used encryption and hidden directories to conceal illegal files, indicating a deliberate attempt to avoid discovery.

- \*\*Email Communication:\*\* Emails discussing methods of securely sharing illegal content and evading law enforcement were recovered.

### Distribution

Evidence showing the distribution of illegal content includes:

- \*\*Email Attachments:\*\* Several emails with attachments containing illegal content were sent from the suspect's email account.

- \*\*File Sharing Logs:\*\* Logs from file sharing software installed on the suspect's computer show transfers of illegal files to other individuals.

- \*\*Network Activity:\*\* Network analysis revealed connections to known illegal content distribution servers.

### Motive

Possible motives behind the suspect's actions include:

- \*\*Financial Gain:\*\* Evidence of payments received via online payment platforms suggests the suspect may have been selling illegal content.

- \*\*Community Involvement:\*\* Chat logs and forum posts indicate the suspect was an active member of online communities dedicated to sharing illegal content.

### Quantity of Files

The investigation uncovered:

- \*\*Total Number of Files:\*\* Over 1,000 files identified as illegal content.

- \*\*File Types:\*\* The illegal content included images, videos, and documents.

- \*\*Storage Locations:\*\* Files were stored across multiple directories, some hidden and some encrypted.

### Installed Software

The suspect's computer systems had several pieces of software relevant to the investigation:

- \*\*Encryption Software:\*\* Used to hide illegal files.

- \*\*File Sharing Applications:\*\* Used to distribute illegal content.

- \*\*Secure Deletion Tools:\*\* Installed to permanently erase files and avoid forensic recovery.

## Timeline of Events

| Date/Time         | Event Description                                        |

|-------------------|----------------------------------------------------------|

| 2024-06-01 14:30  | Suspect logs into the system                             |

| 2024-06-01 15:00  | Suspect downloads illegal content from the internet      |

| 2024-06-01 15:30  | Suspect encrypts downloaded files and stores them        |

| 2024-06-02 10:00  | Suspect sends emails with illegal attachments            |

| 2024-06-02 11:00  | Network activity logs show file sharing of illegal files |

| 2024-06-03 09:00  | Suspect searches for methods to avoid detection          |

| 2024-06-04 13:00  | Suspect receives payment for illegal content             |

## Running Sheet

### Collection

- \*\*2024-07-20 09:00:\*\* Received forensic images and evidence files from the supervisor.

- \*\*2024-07-20 09:30:\*\* Verified the integrity of the forensic images using MD5 checksums.

### Examination

- \*\*2024-07-21 10:00:\*\* Loaded forensic images into Autopsy for initial analysis.

- \*\*2024-07-21 11:00:\*\* Identified and extracted relevant files using FTK.

- \*\*2024-07-22 09:00:\*\* Cross-verified findings using OSForensics.

### Analysis

- \*\*2024-07-23 10:00:\*\* Analyzed browser history, email logs, and system logs.

- \*\*2024-07-24 09:00:\*\* Conducted timeline analysis using Event Log Explorer.

- \*\*2024-07-24 14:00:\*\* Recovered deleted files using Scalpel and verified content.

### Presentation

- \*\*2024-07-25 10:00:\*\* Compiled findings and created visual aids for presentation.

- \*\*2024-07-25 14:00:\*\* Reviewed the report and prepared for submission.

## Conclusion

This forensic investigation has provided substantial evidence linking the suspect to the alleged illegal activities. The evidence includes illegal content, communication records, and system logs, which collectively demonstrate the suspect's involvement, intent, and the extent of their activities. The investigation was conducted using industry-standard tools and methodologies, ensuring the integrity and reliability of the findings.

The detailed report, including timelines, evidence analysis, and supporting documentation, will be submitted to the prosecution team and law enforcement for further action.