**Jurnal E-Komtek**
**Vol. 9, No. 2 (2025) pp. 421-433**
**https://jurnal.politeknik-kebumen.ac.id/index.php/E-KOMTEK**
**p-ISSN : 2580-3719 e-ISSN : 2622-3066**

# Digital Forensics Implementation on CCTV Using ISO/IEC 27037 and ISO/IEC 27042

Zakaria Dwi Arman Maulana[1], Mukhlis Prasetyo Aji[2], Agung Purwo Wicaksono[3], Harjono[4]

[1-4] Department of Informatics Engineering, Universitas Muhammadiyah Purwokerto, Indonesia, 53182

zakariadwi.arman@gmail.com

https://doi.org/10.37339/e-komtek.v9i2.2920

**Published by Politeknik Piksi Ganesha Indonesia**

***Artikel Info***
*Submitted:*
14-12-2025
*Revised:*
15-12-2025
*Accepted:*
17-12-2025
*Online first :*
*31-12-2025*

**Abstract**

Digital evidence, such as CCTV footage, plays a vital role in legal investigations; however, its credibility is often challenged due to the absence of standardized forensic handling procedures. This study designs and evaluates a digital forensic framework based on international standards, namely ISO/IEC 27037:2012 for evidence acquisition and preservation, and ISO/IEC 27042 for analysis and interpretation. The proposed methodology applies the four stages of ISO/IEC 27037—Identification, Collection, Acquisition, and Preservation—on a CCTV V380 MicroSD card. Subsequently, forensic analysis is conducted in accordance with ISO/IEC 27042 principles using the Autopsy software. The findings indicate that the framework effectively preserves evidence integrity, as evidenced by identical MD5 and SHA-1 hash values across the acquisition and analysis preparation stages. Additionally, deleted video files were successfully recovered from Unallocated Space along with relevant forensic metadata. These results confirm that the ISO/IEC-based framework ensures evidence authenticity and reliability, making it suitable as a scientifically and legally valid standard operating procedure for digital forensic practitioners.

**Keywords**: *Digital Forensics, CCTV V380, ISO/IEC 27037, ISO/IEC 27042, Evidence Integrity.*

***Abstrak***

Bukti digital dalam bentuk rekaman CCTV memainkan peran penting dalam penyelidikan hukum; namun, kredibilitasnya sering dipertanyakan karena kurangnya prosedur penanganan forensik yang terstandarisasi. Studi ini merancang dan mengevaluasi kerangka kerja forensik digital berdasarkan standar internasional, yaitu ISO/IEC 27037:2012 untuk pengumpulan dan pelestarian bukti, serta ISO/IEC 27042 untuk analisis dan interpretasi. Metodologi penelitian ini yaitu Identifikasi, Pengumpulan, Pengadaan, dan Pelestarian—pada kartu MicroSD CCTV V380. Selanjutnya, analisis forensik dilakukan sesuai prinsip ISO/IEC 27042 menggunakan perangkat lunak Autopsy. Hasil penelitian menunjukkan bahwa kerangka kerja ini secara efektif menjaga integritas bukti, sebagaimana dibuktikan oleh nilai hash MD5 dan SHA1 yang identik sepanjang tahap pengumpulan dan persiapan analisis. Selain itu, file video yang dihapus berhasil dipulihkan dari Ruang Tidak Teralokasi bersama dengan metadata forensik yang relevan. Hasil ini membuktikan bahwa kerangka kerja berbasis ISO/IEC memastikan keaslian dan keandalan bukti, menjadikannya standar operasional yang valid secara ilmiah dan hukum bagi praktisi forensik digital.

***Kata-kata kunci*: :** *Forensik Digital, CCTV V380, ISO/IEC 27037, ISO/IEC 27042, Integritas Bukti*

## 1. Introduction

In the context of law enforcement, Closed Circuit Television (CCTV) footage is crucial digital evidence containing vital information **[1], [2], [3]**. However, vulnerability to data modification and contamination demands high integrity and authenticity of evidence for legal admissibility **[4], [5]**. Forensic investigations on modern devices such as the V380 are still hampered by the lack of standard procedures for handling digital video evidence that risk compromising the authenticity of the data **[6], [7]**. Furthermore, the use of proprietary storage formats requires adaptive handling methods that are scientifically and legally consistent [8], [9], **[10], [11]**. Therefore, this study focuses on the implementation of a digital forensic framework based on the ISO/IEC 27037:2012 and ISO/IEC 27042 standards applied to V380 CCTV digital evidence to test the effectiveness of the procedures in maintaining data integrity **[12], [13].**

As a solution to the non-standardization issue, the ISO/IEC 27037:2012 standard provides comprehensive guidance on the identification, collection, acquisition, and preservation of digital evidence **[14], [15], [16]**. The implementation of this standard minimizes the risk of contamination and increases the validity of forensic findings **[17], [18], [19]**. However, the acquisition stage must be complemented by a methodical analysis based on ISO/IEC 27042 to ensure a solid foundation for data interpretation. Based on this urgency, the main objective of this study is to implement an integrated ISO framework, which includes the application of key steps of ISO/IEC 27037 to CCTV evidence **[1], [20]**, testing acquisition scenarios on V380 units **[21],** and evaluating the procedures' compliance with the principles of ISO/IEC 27037 and ISO/IEC 27042 to ensure the authenticity of evidence **[19]**.

The novelty of this research lies in the integrated implementation of the ISO/IEC 27042 standard in the data analysis and interpretation phases to complement the ISO/IEC 27037:2012 acquisition procedures. This approach fundamentally distinguishes this research from previous studies, most of which only partially applied the NIST or ISO/IEC 27037 framework without including the formal interpretation phase. Furthermore, unlike previous investigations that tended to focus on conventional storage media, this research specifically examines the forensic challenges posed by MicroSD cards used in V380 CCTV devices, a low-cost consumer security device characterized by a proprietary storage format. Through the implementation of this integrated framework, this research makes a significant methodological contribution to ensuring

the procedural integrity and analytical validity of digital evidence in the modern, non-standardized CCTV ecosystem.

The results of this research are expected to provide a practical contribution in the form of a procedural implementation model that can serve as a reference Standard Operating Procedure (SOP) for forensic practitioners and law enforcement in Indonesia in handling V380 CCTV evidence. Theoretically, this research supports the development of information security protocols and enriches the literature on the application of international standards to low-cost consumer security devices.

## 2. Method

This research is designed based on previous digital forensic studies focusing on standardization and legal aspects. The three main studies that serve as a foundation are: Ramadhan, R. A., Rachmat Setiawan, P., & Hariyadi, D. (2022), which applied a hybrid evaluation (ISO/IEC 27037 and NIST SP 800-86) for non-volatile memory forensics, confirming the relevance of using ISO/IEC 27037 as a framework guide. Putra, A. S., et al. (2022), which analyzed digital forensic stages specifically for CCTV video recordings, relevant to the research object. And Davis, T. (2023), who emphasized the importance of legal standards, chain of custody, and the reliability of digital evidence for court admissibility, which aligns with the research goal of ensuring the legal strength of CCTV video evidence.

### 2.1. Research Flow

This research follows a systematic process divided into four main stages and is visually presented in **Figure 1.**

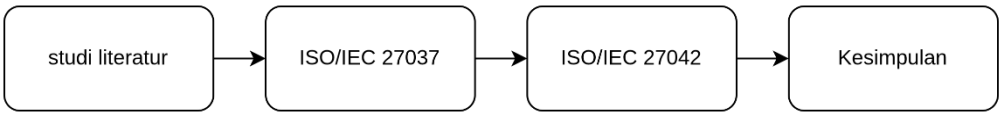


**Figure 1.** Research Flow

(1) Literature review to build a conceptual foundation based on ISO/IEC 27037 and 27042; (2) Implementation of the ISO/IEC 27037 Standard, which covers the process from identification to evidence preservation; (3) Implementation of the ISO/IEC 27042 Guidelines, which focuses on metadata analysis and interpretation of findings; and (4) Conclusions to validate the effectiveness of the framework and the integrity of the resulting data.

### 2.2. Framework ISO/IEC 27037

Implementation is carried out through four technical phases to ensure the validity of the acquisition as shown in **Figure 2**.

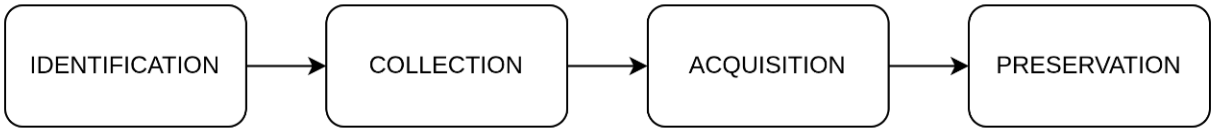


**Figure 2**. Framework ISO/IEC 27037

Identification: Determining the digital storage medium (DSM) on the V380 CCTV unit and documenting the physical condition of the evidence in detail. Collection: Physically removing the MicroSD card from the CCTV device and conducting a comprehensive inventory of all hardware to prevent contamination. Acquisition: Performing disk imaging on the MicroSD card using a forensic write-blocker and FTK Imager software to ensure the data is unmodified. The authenticity of the acquisition results is verified by matching identical hash values (MD5 and SHA1) between the original evidence and the forensic copy. Preservation: Securing the verified digital copy on a protected storage medium and storing the original MicroSD card as physical evidence in a secure container for legal purposes.

### 2.3. Framework ISO/IEC 27042

The analysis and interpretation phase is conducted methodically based on three main phases according to **Figure 3.**


**Figure 1**. Framework ISO/IEC 27042

Preparation: Establishing an isolated forensic work environment, re-verifying the integrity of the acquired hash values, and configuring Autopsy software for data scanning. Analysis: In-depth examination of the MicroSD image using Autopsy to identify deleted video recording files by examining unallocated space sectors. Interpretation and Reporting: Documenting metadata findings and compiling a comprehensive forensic report as final evidence of the integrity of the forensic process.

## 3. Results and Discussion

This research employs the ISO/IEC 27037:2012 digital forensic framework across four main stages: identification, collection, acquisition, and preservation. The implementation of this methodology aims to ensure that digital evidence sourced from the CCTV MicroSD card can be recognized, retrieved, forensically copied, and documented. By adhering to this standard, the integrity and authenticity of the evidence are maintained, thereby conferring scientific credibility and legal standing on the investigative results and the submitted evidence in the judicial domain.

### 3.1. Identification

The Identification phase is executed in accordance with Figure 4, which is the ISO/IEC 27037 guideline for recognizing digital evidence and the Digital Storage Medium (DSM). Identification of the V380 CCTV device can be seen in **Figure 5**, with specifications detailed in Table 1, concluded that the MicroSD card is the relevant storage medium, providing the legitimate basis for the data recovery effort.

**Table 1.** V380 CCTV Camera Specifications

| Category | Specification |
|---|---|
| Brand | V380 |
| Video Resolution | 1080p |
| Memory Card Type | Micro SD |
| Frame Rate | 30fps |
| Camera Type/Shape | Round |
| Item Type | CCTV Camera |

**Figure 5.** Physical appearance of the V380 CCTV

### 3.2. Collection

The Collection phase focuses on the physical securing of the MicroSD card without contamination, in accordance with Figure 6. The collection stage begins by disconnecting the power source and retrieving the V-Gen brand 4GB MicroSD card (Figure 7) from the CCTV, which is then secured as digital evidence. This action affirms compliance with guidelines for handling powered-off devices and ensures the physical integrity and content of the data

contained within. The physical evidence successfully collected has specific details documented in Table 2.

**Figure 6.** 4GB Micro SD card

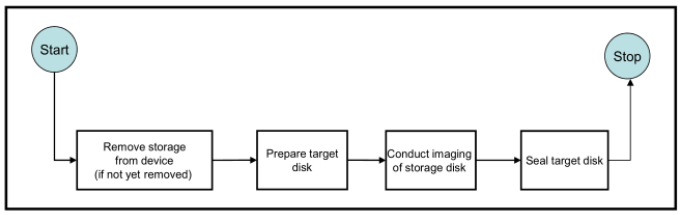


**Figure 7**. Guidelines for the acquisition of powered-off devices.

**Table 2**. Digital Evidence Description (Micro SD Card)

| Category | Description |
|---|---|
| Storage Medium | MicroSD Card |
| Brand | V-Gen |
| Capacity | 4 GB |
| Physical Condition | Intact, no visible physical damage |

### 3.3. Aqcuisition

The Acquisition phase is the technical process of creating a copy of the digital evidence. The MicroSD card is acquired using the software FTK Imager, as shown in **Figure 8.**

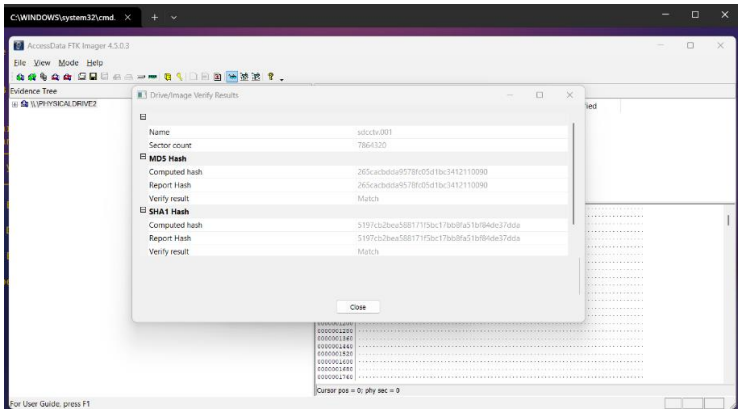

**Figure 8.** Acquisition process using FTK Imager

During this process, a USB write blocker tool is mandatory, as shown in Figure 9, to prevent modification of the source MicroSD card, ensuring compliance with the forensic principle that the source evidence must not be altered.

After acquisition, Data Integrity Verification is carried out by calculating the hash values of the source and copy evidence. The hash calculation process and its results are documented as in Table 3.

**Table 3.** Hash Values of the Acquired Image File

| Category | Detail |
|---|---|
| MD5 | 265cacbdda9578fc05d1bc3412110090 |
| SHA1 | 5197cb2bea588171f5bc17bb8fa51bf84de37dda |

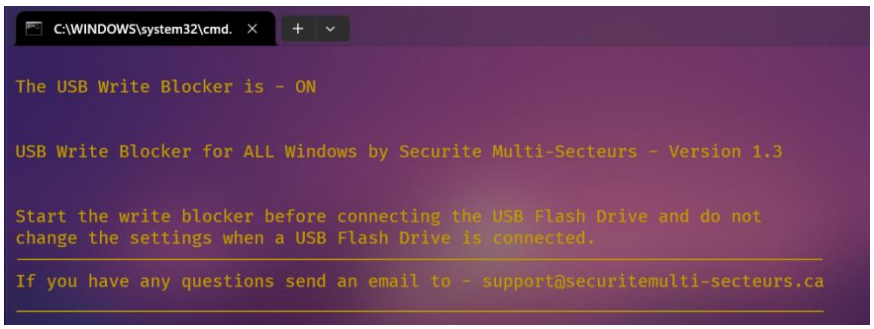


**Figure 9.** Running the USB Write Blocker

### 3.4. Preservation

Figure 10 shows the hash value of the acquired file after being checked using HashCalc. Subsequently, the hash value is verified using WinMD5Free to ensure that no changes have occurred.

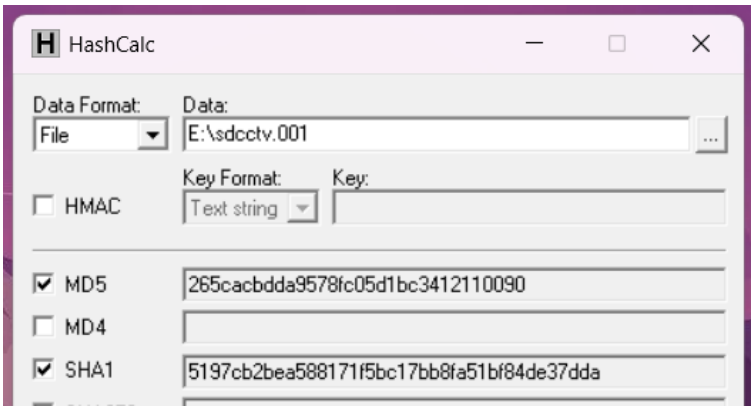


**Figure 10.** Checking Hash Value using HashCalc

The verification result using WinMD5Free, as shown in Figure 11, indicates "Matched," proving that the acquisition file is identical to its source, thereby fully guaranteeing the integrity of the digital evidence.

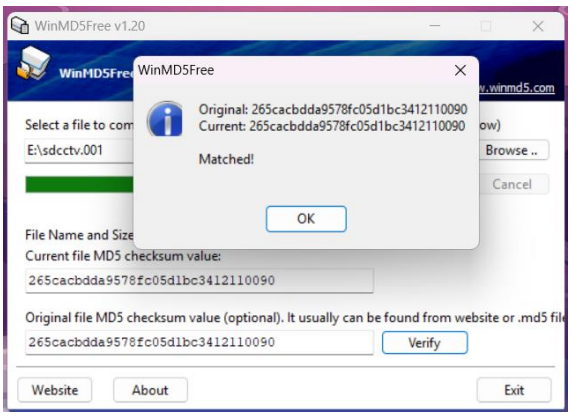


**Figure 11.** Verification of the Acquisition File's Hash Value

### 3.5. Preparation

Figure 12 shows the initial Preparation procedure, which is activating the USB write blocker hardware before the acquired file (forensic image) is connected to the analyst's laptop. This action is taken to prevent accidental data modification by the operating system, ensuring the preservation of the evidence according to forensic standards.

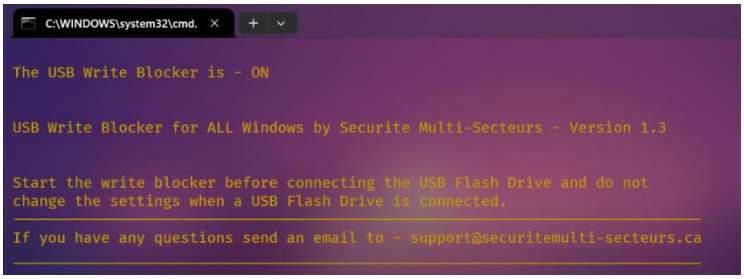


**Figure 12.** Running the USB Write Blocker

Figure 13 displays the checking of the hash values (MD5 and SHA1) against the acquired file, obtaining the values shown in Table 4. This check is performed using the HashCalc tool to get the hash value of the acquisition file.

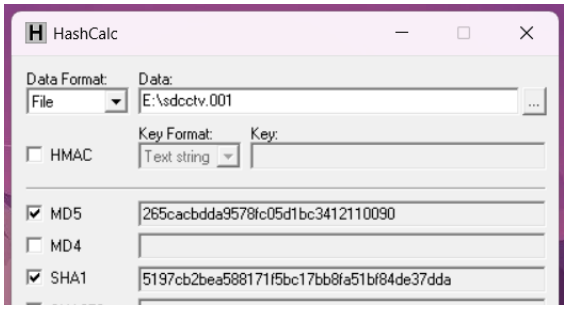


**Figure 13**. Checking the Hash Value Of The File From the Acquisition Results

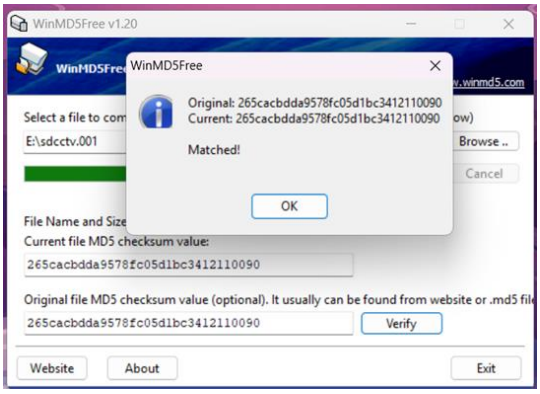


**Figure 14.** Verification of the Hash Value of the File From the Acquisition Results

**Table 4**. Hash Check Results of the Acquired Image File during the Preparation Phase

| Category | Detail |
|---|---|
| MD5 | 265cacbdda9578fc05d1bc3412110090 |
| SHA1 | 5197cb2bea588171f5bc17bb8fa51bf84de37dda |

**Figure 14** shows the core data integrity verification in the Preparation Phase, which is the comparison of the hash value obtained from the Preservation stage of ISO 27037 and the Preparation stage of ISO 27042. WinMD5 yields a "Matched" status, indicating the similarity of the hash values and simultaneously confirming that the integrity of the acquired file is verified and ready for further analysis.

### 3.6. Analysis

**Figure 15** shows the metadata details of the deleted video file found in the Unallocated area of the storage medium, which indicates the file was deleted. Data obtained from the deleted video file is presented in Table 5.

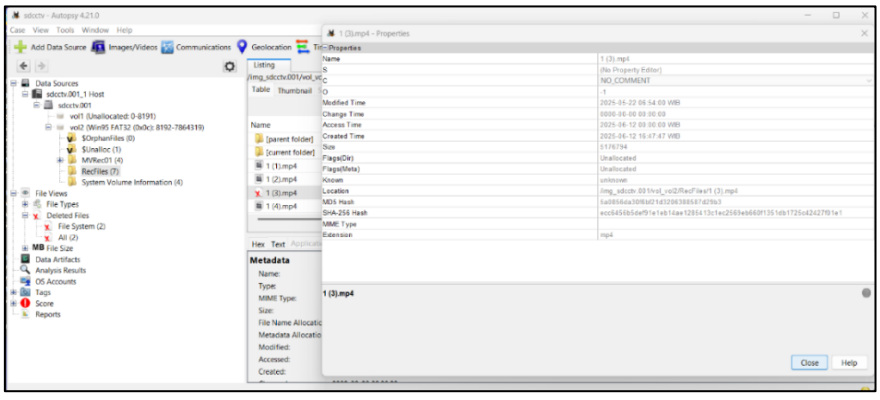

**Figure 2.** Analysis of the acquisition file using autopsy

**Table 5**. Metadata of the Deleted Video File

| Atribut | Nilai |
|---|---|
| File Name | 1 (3).mp4 |
| File Size | 5.176.794 bytes |
| Time Created | 2025-06-12 16:47:47 WIB |
| Time Modified | 2025-05-22 06:54:00 WIB |

**Figure 16** displays the verification result for the CCTV recording file "1 (3).mp4" using the WinMD5Free application, which yielded a "Matched" value. This verifies that the file is still intact and has not undergone any changes.

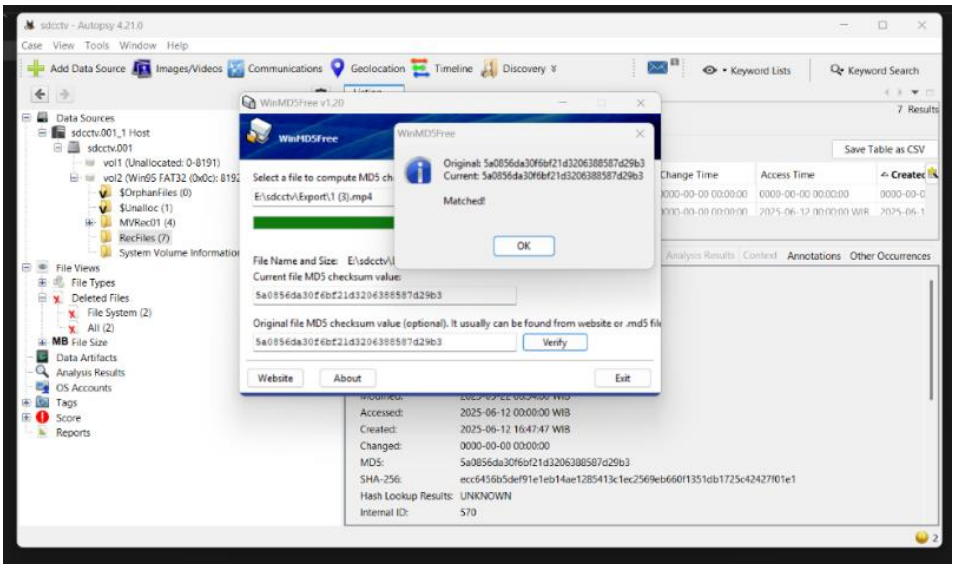


**Figure 16.** Verification of the Hash Value of the Recovered Video File

### 3.7. Interpretation and Reporting

The Interpretation and Reporting phase confirms the success of the forensic process in accordance with ISO/IEC 27037 and 27042 standards. The integrity of the digital evidence from the V380 CCTV is guaranteed through the consistency of the acquisition file's hash values, which were "Matched" across three sequential stages. The Autopsy analysis successfully retrieved data from a deleted video file in the Unallocated area. The evidence obtained, as detailed in Table 6, holds crucial information that ensures the validity and accountability of the digital evidence found.

**Table 6.** Summary of Forensic Findings Data

| Data Category | Description | Key Technical Details |
|---|---|---|
| Source Evidence Specifications | The hardware source evidence identified in the Identification Phase. | Brand: V380, Resolution: 1080p, Storage Medium: Micro SD. |
| Acquisition Integrity (Image File Hash) | Consistent hash values across three stages (Acquisition, Preservation, Preparation), proving the forensic copy is identical to the original source. | MD5: 265cacbdda9578fc05d1bc3412110090<br>SHA1: 5197cb2bea588171f5bc17bb8fa51bf84de37dda |
| Identification of Deleted File | The name and location status of the video file successfully recovered from the **Unallocated Space** (it was deleted). | File Name: 1 (3).mp4 |
| Critical Time Metadata | The last modification timestamp of the file, which is relevant to the time context of the investigation. | Time Modified: 2025-05-22 06:54:00 WIB |
| Recovered Video Evidence Hash | The unique fingerprint of the recovered file, used for verifying the integrity of the video file itself. | MD5 Hash: 5a0865da30f612d320638587d29b3<br>SHA-256 Hash: ecc645b5d9fe11eb14ae1285413c1ec2659eb660f135d1b1725c42427f01e1 |

### 3.8. Research Contribution

The implementation of the integrated ISO/IEC 27037 and 27042 framework in this study provides methodological advantages by enabling deeper metadata validation of proprietary CCTV V380 storage media, distinguishing it from previous studies that used the NIST scope or partial ISO frameworks. Legally, compliance with repeated hash value verification guarantees the authenticity of digital evidence and the integrity of the chain of custody in accordance with applicable legal regulations (UU ITE), thereby strengthening the validity of evidence in court. However, this study has technical limitations in the success rate of data recovery which is highly dependent on the integrity of the unallocated space sector, where data that has been permanently overwritten by the cycle recording feature cannot be fully recovered, as well as testing conditions that are still limited to a controlled laboratory environment.

## 4. Conclusion

This research demonstrates that implementing an integrated digital forensic framework based on ISO/IEC 27037:2012 and ISO/IEC 27042 is effective in standardizing evidence handling for V380 CCTV devices. The systematic application of acquisition and preservation procedures successfully mitigates the risk of data contamination, while the analysis and interpretation stages ensure the validity of information retrieved from the storage media. The consistency of evidence integrity across all stages confirms that this workflow demonstrates robust scientific accountability and legal standing in accordance with the Electronic Information and Transactions (ITE) Law in Indonesia.

The primary scientific contribution of this study is the consolidation of procedural and analytical aspects into a single, unified implementation model, which addresses the methodological gaps found in previous studies that were generally partial in nature. Furthermore, this research provides practical evidence that international standards can be reliably applied to low-cost consumer security devices with proprietary storage systems. This model can be adopted as a reference for Standard Operating Procedures (SOP) by forensic practitioners and law enforcement agencies to ensure the integrity and purity of digital evidence.

## References

[1] R. A. Ramadhan, P. R. Setiawan, and D. Hariyadi, "Implementation of Hybrid Evaluation (ISO 27037 and NIST SP 800-86) for Non-Volatile Memory Forensics," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 8, no. 4, pp. 550–560, 2022.

[2] S. Mehta, "The Critical Role of CCTV Footage in Modern Criminal Investigation," *Journal of Digital Forensics & Law*, vol. 14, no. 2, pp. 45–58, 2023.

[3] F. Mualfah and R. A. Ramadhan, "Analisis Forensik Video CCTV untuk Identifikasi Pelaku Kejahatan," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 5, pp. 890–896, 2020.

[4] R. Ahmed, "Challenges in Maintaining Integrity of Digital Video Evidence," *International Journal of Cyber Security*, vol. 9, no. 1, pp. 112–125, 2021.

[5] P. Johnson, "Preservation of Digital Evidence: Protocols for Long-term Integrity," *Journal of Digital Forensics, Security and Law*, vol. 16, no. 3, 2021.

[6] M. I. Asy'ari and others, "Analisis Forensik Digital pada Rekaman CCTV Menggunakan Metode NIST," *Jurnal Teknologi dan Sistem Komputer*, vol. 12, no. 1, pp. 23–30, 2024.

[7] K. Miller and J. Harris, "Best Practices for Bit-Stream Acquisition of Solid State Storage," *Forensic Science International: Digital Investigation*, vol. 40, p. 301340, 2022.

[8] A. S. Putra and others, "Analisis Tahapan Forensik Digital pada Rekaman CCTV untuk Deteksi Kejahatan," *Jurnal Sistem Informasi dan Komputer*, vol. 11, no. 2, pp. 200–210, 2022.

[9] B. Nugraha and others, "Forensic Analysis of V380 Smart Camera Storage System," *Procedia Comput Sci*, vol. 230, pp. 445–454, 2024.
[10] L. Taylor, "Procedural Inconsistency in Digital Forensics: A Legal Perspective," *Computer Law & Security Review*, vol. 44, p. 105642, 2022.
[11] B. Williams, "Standardizing Digital Evidence Handling in Law Enforcement," *Policing: A Journal of Policy and Practice*, vol. 15, no. 3, pp. 1820–1835, 2021.
[12] A. Kumar, "Framework for Scientifically Validated Digital Forensic Investigation," *IEEE Access*, vol. 10, pp. 12345–12356, 2022.
[13] A. Mubarok and others, "Designing Digital Forensic Framework for IoT Devices based on ISO 27037," in *Journal of Physics: Conference Series*, 2024.
[14] E. Faizal and A. Luthfi, "Implementasi Standar ISO 27037 dalam Penanganan Bukti Elektronik," *Jurnal Keamanan Siber dan Forensik Digital*, vol. 7, no. 1, p. 27037, 2024.
[15] E. Faizal and A. Luthfi, "Analisis Kepatuhan Prosedur Forensik Digital Berbasis ISO 27037," *Indonesian Journal of Computing*, vol. 10, no. 1, pp. 45–55, 2025.
[16] R. Anderson and T. Moore, "Integrity Challenges in SD Card Forensics for IoT Devices," *Comput Secur*, vol. 108, p. 102345, 2021.
[17] H. Setya and D. Suganda, "Peran First Responder dalam Menjaga Chain of Custody Bukti Digital," *Jurnal Kriminologi Indonesia*, vol. 18, no. 2, pp. 101–115, 2022.
[18] T. Davis, "Admissibility of Digital Evidence: Legal Standards and Technical Reliability," *Journal of Law and Technology*, vol. 29, no. 1, pp. 112–130, 2023.
[19] D. Hariyadi and others, "Digital Evidence Integrity Assurance using Blockchain," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, 2023.
[20] B. Santoso, "Aspek Legalitas Bukti Digital dalam Hukum Acara Pidana di Indonesia," *Jurnal Hukum dan Peradilan*, vol. 12, no. 3, pp. 301–318, 2022.
[21] E. Mirfandaresky, "Hash-Based Integrity Verification in Multimedia Forensics," *Journal of Information Security*, vol. 13, no. 4, pp. 201–215, 2022.