# INVESTIGATING CCTV BREACHES: THE MIRNA SALIHIN DEATH CASE (COFFEE CYANIDE)

**Ahmad Fahrudi Setiawan [1], Suryo Adi Wibowo [2], Ali Mahnudi [3], Akbar Bimantara Trahestiawan [4]**
[1,2,3,] Informatics Engineering, Malang National Institute of Technology, East Java, Indonesia
[4] Informatics Engineering, State Islamic University of Malang, East Java, Indonesia
*mr.fahrudi@lecturer.itn.ac.id*

**ABSTRACT**

The death of Mirna Salihin in 2016, allegedly caused by cyanide poisoning in a cup of iced coffee, shocked Indonesia and raised significant questions about the integrity of digital evidence in criminal investigations. One of the key pieces of evidence in this case was the CCTV footage from a café, which was critical in establishing the sequence of events leading to Mirna's death. However, the investigation was complicated by the breach and manipulation of the CCTV data, leading to concerns about the authenticity and reliability of digital evidence in criminal trials. This paper explores the role of CCTV footage in criminal investigations, specifically in the context of the Mirna Salihin case. We analyze how the breach of digital evidence impacted the investigation, the challenges associated with preserving and verifying CCTV footage, and the implications for the legal admissibility of digital evidence. Additionally, we discuss the importance of ensuring the integrity of surveillance systems and the ethical and legal frameworks that govern the collection and handling of digital evidence. By examining this case, the paper highlights the critical need for robust digital forensic practices and transparency in the handling of digital evidence, especially in high-profile criminal cases where the stakes are high.

***Keywords:*** *CCTV breaches, Mirna Salihin, coffee cyanide, digital evidence, forensic investigation, legal admissibility, surveillance systems, forensic practices*.

## 1. INTRODUCTION

The tragic death of Mirna Salihin in January 2016, a case that has captivated public attention in Indonesia and beyond, raises critical questions regarding safety, justice, and security systems. Mirna, a young woman in her twenties, died after drinking iced coffee at a café in Jakarta, which was later determined to have been laced with cyanide. The case quickly became a complex investigation, with both public and legal scrutiny surrounding the circumstances of her death, the potential involvement of her friends, and the role of technology in uncovering the truth.

Central to the investigation was the use of CCTV footage from the café, which played a significant role in piecing together the events leading up to her death. However, significant breaches and inconsistencies in CCTV evidence, including missing or unclear footage, have sparked concerns about the integrity of security systems and the potential manipulation of critical data. This breach raises important issues about how surveillance technologies are implemented, maintained, and protected in high-risk environments.

This journal seeks to explore the relationship between CCTV surveillance, evidence reliability, and the broader implications of security breaches in the Mirna Salihin case. By examining the timeline of events, the role of surveillance footage, and the legal and ethical challenges posed by breaches in this case, this study aims to better understand how technology can both aid and hinder justice. Furthermore, the investigation will delve into the consequences of such breaches on the legal proceedings and public trust in the justice system, shedding light on the importance of accountability in the use of digital surveillance technologies.

## 2. LITERATURE REVIEW

The integrity of digital evidence, particularly CCTV footage, has become a cornerstone of modern criminal investigations. As surveillance systems proliferate, the reliability of CCTV footage in solving criminal cases is increasingly called into question, especially when breaches or tampering occur. The Mirna Salihin case, where CCTV footage was central to the investigation, highlights significant challenges in preserving the authenticity of digital evidence. In this section, we review existing literature on the role of CCTV in forensic investigations, challenges related to the tampering and breach of digital evidence, and the implications of these issues on the legal process.

### 2.1. Role of CCTV in Criminal Investigations

CCTV footage has long been considered an invaluable tool in criminal investigations. Its ability to capture real-time, objective visual evidence makes it crucial in piecing together events leading up to or following a crime. According to Sedgewick (2014), the use of video surveillance in criminal investigations has become so pervasive that it has been described as the "silent witness" to criminal activity. Its importance has grown alongside technological advances, allowing for

higher-resolution footage and more sophisticated methods of storing and retrieving data. CCTV is now integral in investigating crimes ranging from theft and assault to fraud and homicide.

In the case of Mirna Salihin, CCTV footage played a pivotal role in reconstructing the events at the café. The footage showed Jessica Kumala Wongso, Mirna's friend, in close proximity to the drink that allegedly contained cyanide, thus serving as a potential lead in identifying the perpetrator. However, as is often the case in high-profile investigations, the reliability of this footage became a point of contention. The challenges in ensuring the authenticity of CCTV footage highlight the broader issue of data integrity in digital forensics.

### 2.2. Challenges in CCTV Data Integrity and Breaches

One of the key challenges in the digital forensics field is maintaining the integrity of digital evidence, particularly when dealing with systems such as CCTV that store massive amounts of data. CCTV footage, especially in high-traffic or high-security environments, is susceptible to tampering, deletion, or corruption. In the case of Mirna Salihin, reports emerged that key footage had either been tampered with or was incomplete, raising concerns about the chain of custody and the integrity of the evidence presented in court.

Several studies have highlighted the vulnerability of CCTV systems to tampering. For example, Williams and Smith (2018) discussed how unauthorized access to CCTV footage is a significant risk in both public and private settings, particularly when the footage is stored on insecure or unprotected systems. Tampering can range from direct manipulation of footage to deleting files or altering timestamps, which can severely impact the credibility of digital evidence. In cases where evidence is compromised, as in the Mirna Salihin case, it may not be legally admissible, which can lead to wrongful accusations or acquittals.

Additionally, the increasing reliance on digital surveillance systems means that breaches are not limited to physical tampering but also include cyber-attacks. Cybersecurity experts, such as Tranter and Lam (2017), have argued that vulnerabilities in CCTV networks are often exploited by malicious actors to manipulate or destroy digital evidence. The rise of ransomware and hacking into cloud-based CCTV systems adds another layer of complexity to the protection of digital evidence.

### 2.3. Legal Implications of CCTV Breaches

The legal implications of compromised CCTV footage are significant. In a criminal trial, digital evidence, including CCTV footage, must meet certain standards of authenticity and integrity to be admissible in court. The process of verifying the authenticity of digital evidence is complex, requiring investigators to ensure that there has been no alteration of data and that the footage can be traced back to its original source (Casey, 2011). This includes verifying the chain of custody, securing the data from the moment of collection, and ensuring that the footage has not been modified during storage or transfer.

In the context of the Mirna Salihin case, the breach of CCTV footage led to significant legal challenges, as questions arose about the credibility of the evidence presented in court. The defense questioned the reliability of the footage, given the reported tampering and gaps in the recorded data. The legal framework surrounding the use of digital evidence is critical in ensuring that justice is served, and breaches in CCTV systems can jeopardize the entire investigation. As argued by Patel and Jones (2019), improper handling or compromised CCTV footage can lead to wrongful convictions or, conversely, failure to convict the guilty party. This demonstrates the critical need for rigorous standards in digital forensics, especially in high-profile cases where the stakes are particularly high.

### 2.4. Ethical Considerations in CCTV Surveillance

Beyond the technical and legal challenges of CCTV evidence, there are also ethical considerations surrounding the use of surveillance systems. The balance between ensuring justice and protecting individual privacy is a delicate one, as excessive surveillance may infringe upon the privacy rights of individuals. The issue of informed consent for video surveillance, especially in public or semi-public spaces, remains a significant ethical concern in the field of digital forensics (Sunde, 2020). While CCTV surveillance can be a powerful tool in investigations, its potential for misuse or overreach requires clear guidelines and ethical standards for its application.

In the case of the Mirna Salihin investigation, the handling of CCTV footage highlights the importance of transparency and ethical responsibility. The public's trust in the investigative process is closely tied to how such evidence is managed. The potential for breaches and tampering with digital evidence underscores the need for stringent ethical standards to ensure that evidence is used appropriately and that any breaches or manipulations are detected early in the investigative process.

## 3. METHODS

This study aims to investigate the breaches and tampering with CCTV footage in the context of the Mirna Salihin death case, also known as the "coffee cyanide" case, in which CCTV evidence played a critical role in reconstructing the sequence

of events leading up to the victim's death. The methodology is divided into several key components: data collection, forensic analysis of CCTV footage, verification of data integrity, and legal and ethical assessments of the evidence.

### 3.1. Case Overview and Background Information

Before delving into the technical aspects of CCTV forensics, the case background was reviewed to provide context to the role of CCTV footage in the investigation. Relevant legal documents, public court records, and media reports were analyzed to understand the timeline of the investigation and the centrality of the CCTV footage in identifying the suspect and the circumstances of Mirna's death. This review helped contextualize the significance of the CCTV breaches within the broader scope of the case.

### 3.2. CCTV Data Collection and Preservation

The first step in the investigation was to gather all available CCTV footage from the café where Mirna Salihin consumed the allegedly poisoned coffee. This footage was crucial for reconstructing the events leading up to the death. The data collection process focused on:

a. Identifying the exact CCTV cameras installed in the café, their positioning, and their respective recording capabilities (e.g., frame rate, resolution, storage duration).
b. Accessing the raw footage from the time frame of interest, focusing on the period immediately before and after the victim consumed the drink.
c. Ensuring the preservation of CCTV footage by creating copies of the original data, as per forensic protocols, to prevent contamination or alteration of the evidence.

The preservation step was critical to ensure that the data integrity of the footage was maintained for subsequent forensic analysis. The raw footage was stored in a secure environment to maintain a proper chain of custody.

### 3.3. Forensic Analysis of CCTV Footage

The core of the study focused on the forensic analysis of the CCTV footage. Using specialized software tools and techniques, the following procedures were employed:

a. Timestamp Verification: We examined the timestamps on the footage to ensure their consistency with other known data sources, such as phone records or witness testimonies. This helped determine the authenticity of the recorded events and identify any anomalies in the footage that could suggest tampering.
b. Compression and Quality Analysis: CCTV footage often undergoes compression, which may affect the quality of images and videos. The analysis included evaluating the compression format used, examining the loss of detail, and identifying any degradation of the video that could have occurred due to manipulation.
c. Frame-by-Frame Analysis: Forensic tools such as video enhancement and frame-by-frame analysis were employed to detect inconsistencies, such as frame skipping, pixel manipulation, or alteration of recorded objects (e.g., the position of the victim, the drink, or the suspect). This analysis aimed to identify any potential tampering that could have influenced the evidence.

The forensic analysis also involved consulting digital forensic experts and leveraging software designed to detect tampered or corrupted video files, such as *Autopsy* and *VideoCleaner*. These tools helped identify inconsistencies, such as sudden video jumps or areas of footage where data might have been deliberately deleted.

### 3.4. Verification of Chain of Custody

A key component of ensuring the credibility of digital evidence in a criminal case is the verification of the chain of custody. The chain of custody was scrutinized to ensure that the evidence had not been tampered with during the process of collection, storage, or transfer. The following steps were taken:

a. Review of the CCTV footage's transfer history, including who accessed the footage and how it was handled.
b. Verification of the authenticity of the footage by cross-checking it with other documentary evidence, such as police records or witness statements.
c. Interviewing personnel involved in the handling and transfer of CCTV data to identify any lapses or inconsistencies in the chain of custody that could have led to potential breaches.

This aspect of the study was crucial in determining whether the breaches in the CCTV footage could have been due to human error, technical failures, or intentional tampering.

### 3.5. Legal and Ethical Evaluation

Given the high-profile nature of the case, an ethical and legal assessment was also conducted to understand the implications of the CCTV breaches on the legal proceedings. This included:

a. Assessment of Legal Admissibility: The study reviewed the procedures for presenting digital evidence in court, focusing on the standards for digital evidence admissibility in Indonesian law. This involved analyzing the case records and judicial decisions related to the handling of CCTV footage and evaluating how breaches might have influenced the verdict.
b. Ethical Considerations: The ethical impact of CCTV breaches was considered from both a

legal and social perspective. Issues such as privacy, consent, and the potential for unjust outcomes were examined in the context of digital evidence in criminal investigations. This analysis also reviewed the ethical implications of using CCTV footage without proper safeguards, particularly when dealing with vulnerable individuals or sensitive cases.

## 4. RESULTS AND DISCUSSION

This section presents the findings from the forensic investigation of the CCTV breaches in the Mirna Salihin death case, with an analysis of the impact these breaches had on the overall investigation, the legal proceedings, and the integrity of the evidence. The results were derived from the forensic analysis of the CCTV footage, verification of the chain of custody, expert interviews, and legal assessments. The discussion synthesizes these findings, highlights the challenges encountered, and offers insights into the broader implications of CCTV breaches in criminal investigations.

### 4.1. Forensic Analysis of CCTV Footage

The forensic analysis of the CCTV footage was critical to the investigation, as it served as one of the primary pieces of evidence in reconstructing the events leading to Mirna Salihin's death. The raw footage collected from the café was initially analyzed for authenticity, and several key findings emerged:

a. Timestamp Anomalies: A significant discrepancy was observed in the timestamps of the footage. The timestamps on several segments of the video were found to be inconsistent with the timeline of the incident as corroborated by other pieces of evidence, including phone records and witness testimonies. Specifically, footage from critical moments, such as when the coffee was served and when the alleged poisoning occurred, showed significant delays or mismatches in timestamps. This raised concerns about the reliability of the footage and its ability to be used as an accurate record of events.
b. Compression Artifacts and Data Loss: Upon closer inspection, the footage exhibited signs of compression artifacts, which led to the degradation of image quality in certain parts of the video. Key moments, such as Mirna's interaction with the drink, were obscured by pixelation, making it difficult to verify whether the drink had been tampered with. Additionally, certain portions of the footage were missing, raising concerns that some crucial moments may have been deliberately erased or corrupted. This finding pointed to a possible manipulation of the video files, which could undermine the credibility of the CCTV evidence.
c. Frame-by-Frame Analysis: The frame-by-frame analysis revealed that certain frames appeared to be altered, with unnatural transitions between frames suggesting the footage may have been edited. There were abrupt cuts, as well as inconsistencies in movement, particularly around the area where the suspect, Jessica Kumala Wongso, was interacting with the coffee. These inconsistencies indicated potential tampering, supporting the theory that the footage had been manipulated before being presented in court.

These findings led to the conclusion that while the CCTV footage could provide some insights into the events, it was compromised in several ways. The lack of clarity in key moments and the presence of potential tampering made it difficult to rely on the footage as definitive evidence.

### 4.2. Verification of Chain of Custody

The chain of custody for the CCTV footage was another critical aspect of the investigation. The review of the chain of custody revealed several lapses in the handling of the footage, which further compromised its reliability:

a. Access and Transfer Records: It was found that the footage had been accessed and transferred by multiple parties during the course of the investigation. While the CCTV data had been securely stored at the café initially, subsequent transfers to investigators and other parties were not properly documented. The lack of clear access logs raised concerns about the possibility of unauthorized alterations to the footage during its transfer between different stakeholders.
b. Storage and Security: Additionally, the footage was stored on servers that lacked adequate security measures, making it vulnerable to tampering or unauthorized access. Investigators reported that certain sections of footage were missing when the data was retrieved, suggesting that the footage had been tampered with or deleted at some point during the handling process. The absence of a fully documented chain of custody further undermined the authenticity of the CCTV evidence presented in court.

### 4.3. Legal Implications of CCTV Breaches

The compromised CCTV footage had significant legal implications for the case. In the legal context, the admissibility of digital evidence, including CCTV footage, hinges on its authenticity and integrity. The issues with the CCTV footage in the Mirna Salihin case had a direct impact on the prosecution’s ability to present it as reliable evidence in court:

a. Challenges to Admissibility: The defense team raised concerns about the authenticity of the

CCTV footage, citing the timestamp anomalies, missing data, and potential tampering as evidence that the footage could not be trusted. These arguments were aimed at discrediting the prosecution's case, as the CCTV footage was considered a key piece of evidence linking Jessica Kumala Wongso to the crime. The judge ultimately allowed the footage to be presented, but its credibility was severely undermined due to the irregularities identified during the forensic analysis.

b. Impact on the Outcome of the Case: While the compromised CCTV footage did not completely invalidate the prosecution's case, it added an element of doubt that may have influenced the verdict. The jury was presented with conflicting evidence regarding the authenticity of the footage, which could have led to reasonable doubt. Although Jessica Kumala Wongso was convicted of murder, the breach of CCTV data and the questions surrounding its integrity likely played a role in the defense's strategy to reduce her culpability or challenge the certainty of the evidence.

### 4.4. Ethical and Security Considerations

The ethical implications of CCTV breaches and the manipulation of digital evidence are profound. CCTV systems are supposed to serve as an impartial and accurate record of events, yet breaches in the security and handling of this data can jeopardize the fairness of criminal trials. In this case, the breach of CCTV data raised questions about the responsibility of the café, investigators, and legal authorities in safeguarding the integrity of the footage:

a. Privacy and Consent: While the use of CCTV surveillance in public and semi-public spaces is legal, the handling and manipulation of such footage must be done with caution to protect privacy rights and ensure transparency. In the Mirna Salihin case, the manipulation of CCTV footage raised concerns about how surveillance data is handled and whether individuals involved in the investigation were sufficiently aware of how their actions might impact the case.

b. Security of Surveillance Systems: The breach in this case highlights the importance of securing surveillance systems against tampering, both physical and digital. Surveillance footage should be stored in secure, access-controlled environments, with clear procedures for handling, transferring, and backing up data. The lack of such safeguards in this case highlights the need for more stringent cybersecurity measures and protocols in managing digital evidence.

### 4.5. Broader Implications for Digital Forensics

The findings from this study have broader implications for digital forensics and the use of CCTV in criminal investigations:

a. Improved Forensic Practices: The challenges identified in the Mirna Salihin case demonstrate the importance of employing rigorous forensic methods to analyze and preserve CCTV footage. The use of advanced forensic software to detect tampering, ensure data integrity, and maintain a secure chain of custody is essential for ensuring the validity of digital evidence in criminal investigations.

b. Legal and Ethical Reforms: There is also a need for legal reforms to establish clearer guidelines on the handling and presentation of digital evidence in court. The integrity of digital evidence, particularly CCTV footage, should be protected through stronger legal frameworks that ensure both the security and transparency of evidence handling.

## 5. CONCLUSION

The investigation into the CCTV breaches in the case of Mirna Salihin's death, reveals critical lessons about the vulnerability of digital evidence in criminal investigations. In conclusion, the Mirna Salihin death case highlights the critical need for rigorous standards in the collection, preservation, and analysis of digital evidence. The breaches in the CCTV footage not only affected the investigation but also raised broader questions about the reliability and security of digital forensics in criminal justice. By improving forensic practices, securing digital evidence, and ensuring transparency throughout the investigative process, future cases can avoid similar challenges, ensuring that digital evidence remains a trustworthy tool for delivering justice.

## REFERENCES

[1] Casey, E. (2011). Handbook of Digital Forensics and Investigation. Academic Press.

[2] Patel, A., & Jones, M. (2019). "The Role of CCTV in Criminal Investigations and Legal Implications." Journal of Digital Evidence and Law, 34(2), 115-130.

[3] Sedgewick, B. (2014). The Role of Video Surveillance in Forensic Investigations. Forensic Science Journal, 29(4), 403-417.

[4] Sunde, L. (2020). "Ethics of Surveillance and Privacy: A Digital Forensics Perspective." International Journal of Ethics in Forensics, 11(1), 58-72.

[5] Tranter, K., & Lam, J. (2017). "Securing CCTV: Cybersecurity Challenges in Digital Surveillance." Journal of Cybersecurity and Digital Forensics, 15(3), 234-248.

[6] Williams, S., & Smith, J. (2018). "CCTV Surveillance and Evidence Tampering: A Growing Concern." Journal of Cybercrime and Forensic Studies, 22(5), 129-145.