DEF-IPV: A digital evidence framework for intimate partner violence victims

By:
Kyungsuk Cho, Kyuyeon Choi, Yunji Park, Minsoo Kim, Seoyoung Kim, Doowon Jeong

From the proceedings of
The Digital Forensic Research Conference
DFRWS APAC 2025
Nov 10-12, 2025

Forensic Science International: Digital Investigation 54 (2025) 301979

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS APAC 2025 - Selected Papers from the 5th Annual Digital Forensics Research Conference APAC

DEF-IPV:A digital evidence framework for intimate partner violence victims

Kyungsuk Cho, Kyuyeon Choi, Yunji Park, Minsoo Kim, Seoyoung Kim, Doowon Jeong *

Dept. of Forensic Sciences, Sungkyunkwan University, 25-2 Sungkyunkwan-ro, Jongno-gu, Seoul, 03063, South Korea

ARTICLE INFO

Keywords:
(IPV)
Intimate partner violence
Secure evidence collection
Digital victim support
Digital evidence
Digital forensics framework

ABSTRACT

Intimate partner violence (IPV), involving abuse by current or former partners, is a growing global concern. Victims often face serious barriers not only in escaping abusive situations but also in securely collecting and preserving evidence, due to the proximity and control exerted by perpetrators. Storing photos, videos, or audio recordings directly on personal devices increases the risk of discovery—especially when abusers have access to the victim's digital environment. While several support services for IPV survivors have been developed, many remain unsuitable for use in high-risk or surveillance-heavy situations. In this study, we propose the Digital Evidence Framework for IPV (DEF-IPV), a technological solution that enables victims to collect and store digital evidence even under surveillance by their abuser. To identify the essential requirements, we conducted expert interviews with IPV support professionals. Based on these insights, DEF-IPV was designed to combine a camouflaged application with steganographic techniques, ensuring that both the evidence and the act of evidence collection remain undetectable. A detailed process model was constructed, and a proof-of-concept prototype was implemented to validate its technical feasibility. This work lays the foundation for future research on real-time and survivor-centered support in high-risk environments.

1. Introduction

Intimate partner violence (IPV)—defined as abuse committed by a current or former partner—is increasingly recognized as a critical global issue. In France, reports of IPV increased by more than 15 % in 2022 compared to the previous year. Similarly, Germany saw a 9 % rise in IPV-related crimes in 2023, while Canada reported a steady increase in cases between 2015 and 2021 (IMPRODOVA, 2023; Statistics Canada, 2023). These statistics highlight the growing prevalence of IPV across countries and underscore the urgent need for effective intervention strategies.

IPV is characterized by the close emotional and physical proximity between abusers and victims, as it is rooted in a pre-existing intimate relationship. Particularly within romantic relationships, this proximity often leads to the normalization or justification of digital control. In the case of adolescent IPV victims, studies have reported frequent occurrences of controlling behaviors, such as monitoring a partner's device or social media activity and demanding access to passwords (Torp Løkkeberg et al., 2023). Intimate partner violence (IPV) is increasingly facilitated through the use of advanced technologies, including mobile and IoT devices. Consequently, there has been growing attention to IPV within the security and digital forensics communities. Prior research has examined how abusers exploit technologies to surveil and control victims (Stephenson et al., 2023), while others have focused on proposing technical and procedural countermeasures (Freed et al., 2018; Havron et al., 2019; Mangeard et al., 2024).

In contrast to previous research that primarily analyzes the technological means employed by abusers, our study focuses on expanding the technological agency of victims. Specifically, we address the problem that victims often find it difficult to collect digital evidence themselves, due to the abuser's physical proximity and frequent access to or control over shared devices.

To this end, this study reviews existing victim support technologies and conducts expert interviews to identify the core challenges faced by IPV survivors in digital evidence collection. Based on the findings, we define three essential requirements—invisibility, anti-leakage, and continuity—that a digital evidence framework must satisfy. We then propose DEF-IPV, a secure and covert framework that integrates steganography and a camouflaged application to enable safe collection, storage, and submission of digital evidence. The framework's design, implementation process, and prototype evaluation are presented to demonstrate its feasibility and comparative advantages over existing

* Corresponding author.
E-mail addresses: kninami@skku.edu (K. Cho), cky0312@skku.edu (K. Choi), yun.jiggle@skku.edu (Y. Park), pinggoo001@gmail.com (M. Kim), pangkz@skku.edu (S. Kim), doowon@skku.edu (D. Jeong).

https://doi.org/10.1016/j.fsidi.2025.301979

Available online 3 November 2025

solutions.

2. Background

2.1. Intimate partner violence (IPV)

IPV refers to violence that occurs within intimate relationships. Its conceptual definitions and legal scope vary significantly across jurisdictions. These differences primarily relate to two dimensions: the definition of a partner and the recognized forms of violence (European Institute for Gender Equality, 2019).

For instance, South Korea's *Act on Special Cases Concerning the Punishment of Crimes of Domestic Violence* defines domestic violence as physical, psychological, or property-related harm inflicted among family members. The law includes current or former spouses, and direct lineal ascendants or descendants of oneself or one's spouse within its definition of "family."

In contrast, several European countries—such as Belgium, France, Sweden, Finland, and Slovakia—adopt broader definitions of intimate partnerships. These jurisdictions recognize various relationship configurations, including current and former, cohabiting and non-cohabiting, registered and informal partners. As a result, the legal scope of "intimate partner" differs significantly by region.

Similarly, recognized forms of IPV vary. UN Women (UN Women) defines IPV as physical, sexual, or psychological abuse by a current or former partner, and highlights the emerging threat of technology-facilitated abuse, such as deepfakes. The European Institute for Gender Equality (European Institute for Gender Equality, 2019) further categorizes IPV into five types: physical, psychological, sexual, economic violence, and femicide—with each encompassing more specific subcategories such as property destruction or non-payment of alimony.

Despite these jurisdictional variations, a common thread remains: IPV encompasses abuse occurring within current or former intimate relationships and includes physical, sexual, and psychological violence.

2.2. Victim support services

Several tools have been developed to support IPV victims, including Bright Sky, No Stalk, VictimsVoice, and Seek Then Speak. Table 1 summarizes key features across these services.

Bright Sky is a mobile app developed by UK-based charity Hestia (Hestia). Available on Android and iOS, it provides a risk assessment tool that enables victims to gauge the danger of their situation ("Am I at Risk?"), a location-based directory of nearby support agencies ("Nearby Support"), and a journaling feature for recording audio and photographic evidence ("My Journal"). Uploaded media is forwarded to a designated email address rather than stored locally.

Table 1
Feature comparison of victim support services.

Category	Features	Bright Sky	No Stalk	Victims Voice	Seek Then Speak
Evidence Collection	Journal Entry	O	O	O	O
	Photo Upload	X	X	O	X
	Photo Capture	O	O	O	X
	Audio Recording	O	O	X	X
	Video Recording	O	O	O	X
Evidence Storage	Remote Storage	X	O	O	X
	Evidence Encryption	X	X	O	X
Other Features	Report Form Generation	X	X	O	O

Rating Scale: O = Feature is supported; X = Feature is not supported.

No Stalk, developed by the German nonprofit Weisser Ring, is an Android app that includes encryption and an in-app lock (Weisser Ring,). Users receive a complex passphrase—e.g. "kaufen inhaltlich insofern befürchten Server Ganze"—at registration, which is required to download saved evidence. Evidence files cannot be viewed directly on the device and must be accessed by logging into the No Stalk website on a PC. The app supports recording, photographing, and adding contextual notes to evidence, and offers emergency call and SMS features connecting users to local authorities such as nearby police stations and support organizations.

VictimsVoice is a web application developed in the U.S. and offered as a progressive web app (PWA) (Victims Voice), which users access through a browser without installation, leaving no trace of app usage on the device. It includes a "Safe Exit" feature that allows users to instantly redirect to an unrelated, innocuous website and simultaneously clears the browser history of the current session—preventing the use of the Back button to return to VictimsVoice if the activity is discovered by the perpetrator. VictimsVoice helps users collect legally admissible evidence by guiding them through structured documentation. It ensures chain-of-custody integrity and complies with HIPAA standards (U.S. Department of Health and Human Services), which are designed to protect individuals' health information while allowing its use for healthcare delivery and public health purposes. The app is subscription-based, but users who cannot afford the fee can apply for hardship waivers.

Seek Then Speak is a web-based resource operated by End Violence Against Women International (EVAWI) in the U.S. (EVAWI), intended to help victims of sexual violence secure evidence immediately after an assault. It offers step-by-step instructions (e.g., "place the clothing you were wearing in a sealed plastic bag") and collects detailed responses to generate police report forms.

2.3. Steganography

Technologies used to support victims often overlap with anti-forensic techniques in that they aim to conceal and preserve digital evidence. Harris (2006) defines anti-forensics as any action taken to corrupt, conceal, or undermine evidence during the forensic process. Methods include deleting evidence, hiding it, preventing its creation, and falsifying existing data. Anti-forensic technologies enable these behaviors. Traditionally viewed as tools for evading law enforcement, these techniques can also serve to protect victims and their evidence.

Steganography is a widely used anti-forensic technique that embeds hidden data within digital media—such as images or audio files—so that the existence of the concealed data is not perceptible (Evsutin et al., 2000). The cover file, which appears to be a normal file (e.g., a photo), is subtly modified to carry the hidden information. Common steganographic techniques include the Least Significant Bit (LSB) method, which embeds hidden data by modifying the least significant bits of pixel values, and the Pixel Value Differencing (PVD) method, which increases embedding capacity while maintaining image fidelity. More advanced methods, such as adaptive image steganography, have been proposed to further reduce the detectability of hidden content (Laishram and Tuithung, 2018).

The main objective of steganography is to hide the existence of the data itself. However, if an attacker identifies a file as a potential cover file, they may extract hidden data using publicly available tools. To mitigate this risk, it is common to first encrypt the data before embedding it into the cover image (Haider, 2021). In this study, steganography is applied not to obstruct forensic analysis, but to enable IPV victims to collect and store digital evidence in a secure and undetectable manner.

3. Expert interviews

3.1. Interview design

This section describes the expert interviews conducted to explore the characteristics of IPV crimes, the types of violence experienced by victims, and specific traits of the victims themselves. A semi-structured interview approach was adopted. This qualitative method involves preparing a thematic interview protocol in advance while allowing flexibility in follow-up questions based on participants' responses (Hanna et al., 2016). It is especially suitable for exploring emergent ideas, investigating complex social behaviors, and understanding practical strategies for service implementation (Adeoye-Olatunde and Olenik, 2021).

The interviews focused on understanding the circumstances of IPV victims and collecting expert insights on technologies that could effectively assist them. The aim was to identify specific technical and operational requirements for the digital evidence framework for IPV victims.

The interview protocol provided to participants included an overview of the study and a structured questionnaire. The questionnaire covered: (1) forms and challenges of IPV victimization; (2) methods and risks associated with evidence collection; (3) technical and institutional requirements for a digital evidence framework; and (4) considerations related to usability, accessibility, and real-world application. Participants were informed that their responses might be directly quoted in the study and were asked for consent to audio recording and use of their input for research purposes. Interviewers honored participants' requests to avoid specific case descriptions that might reveal victim identities. The interviews were conducted over four sessions between March and July 2025, each lasting approximately 2 h. A detailed interview guide is provided in Appendix A.

3.2. Interview participants

Participants included professionals who support both IPV survivors and victims of digital crimes against women. Recruitment was intentionally balanced based on participants' institutional affiliations and professional roles. The sample consisted of two counselors, one attorney, and two Women Human Rights Defenders (WHRDs). Table 2 presents participant details.

P1 and P2 work at institutions that primarily support adolescents under the age of 19. In most cases, abuse is reported by schools or family members, who refer the victims to these institutions. While some adult clients also receive counseling, they are usually individuals who began receiving support as adolescents.

By contrast, P3 and P4 work at institutions that primarily support adults. Although they do not exclude adolescent clients, their services are not specifically tailored to this group, and adolescent representation is minimal. P5 works primarily with victims of digital sexual crimes, providing support for the removal of non-consensual videos. Given the similarity between digital sexual crimes and IPV—particularly the prevalence of sensitive images involving victims' bodies—the interview focused on the collection and management of sensitive digital evidence.

The institutions represented by P1, P2, and P4 offer medical support, including access to gynecological and surgical services. Legal support includes connecting victims with attorneys for reporting and legal proceedings. P3, a practicing attorney, provides legal representation and litigation services through referrals from support centers.

Table 2
Interview participants and their organizations' victim support Activities.

Number	Affiliation	Position (Years)	Support Target	Support Program
P1	NGO	WHRDs (26)	Adolescent victims of IPV	Legal, medical, and counseling support
P2	Public Counseling Center	Counselor (11)		Legal, career, and counseling support
P3	Law Firm	Attorney (7)	Adult victims of IPV	Legal service provision
P4	NGO	Counselor (11)		Legal, medical, and counseling support
P5	NGO	WHRDs (9)	Victims of digital crimes	Legal and counseling support

3.3. Interview findings

Thematic analysis was employed to examine interview data, identifying and interpreting semantically meaningful patterns (Braun and Clarke, 2006). Through the interviews, we identified the types of evidence typically collected by IPV victims, along with the challenges they face in doing so. From these insights, three essential requirements for a digital evidence framework were derived: invisibility, anti-leakage, and continuity. These themes were analyzed in relation to the nature of IPV and represent key features necessary to enable secure and effective evidence collection by victims.

3.3.1. Types of evidence collected by victims

Table 3 summarizes the types of evidence victims collect and submit to investigative authorities. This includes both digital and non-digital artifacts retained by victims. Such evidence helps not only to substantiate incidents but also to support victims in recalling and articulating specific circumstances and timelines.

Non-digital evidence includes diaries, medical certificates, police reports, and counseling records. These are often issued in physical form and may be time-sensitive—emergency call logs, for example, may be unrecoverable after one year, and medical documents can become inaccessible if institutions close or relocate.

Among digital evidence, all interviewees emphasized screenshots of messaging apps as particularly significant. These often contain multimedia files and threatening or coercive messages. Conversely, the absence of such data poses a major barrier to substantiating victims' accounts.

> *Support services routinely advise victims to preserve message histories, but many exit chat rooms or block abusers to reduce psychological distress, inadvertently deleting crucial evidence. (P2)*

> *Some victims even delete their messenger accounts altogether, further precluding later retrieval. The relational complexity of IPV often delays reporting until more severe incidents occur, by which point the pertinent data have typically been lost and forensic recovery must be recommended. (P3)*

> *Although practitioners emphasize exporting conversation logs or capturing screenshots to ensure evidentiary integrity, these interventions are frequently rendered moot if performed only after the communication channels have already been deleted. (P4)*

While it is possible to collect additional evidence through counseling centers, this is rare, as many victims prioritize separating from the

Table 3
Types of evidence.

Type	Example
Non-digital Evidence	Diary
	Medical Certificate
	Police incident confirmation letters
	Counseling Certificate
Digital Evidence	Image File
	Video File
	Voice File

perpetrator over engaging in post-incident documentation. On the other hand, an excess of preserved evidence has at times led to suspicion from investigators.

Although evidence collection is crucial, using dedicated services can bias investigators—victims with extensive records are often asked how they gathered so much evidence while still experiencing abuse. (P3)

When large volumes of evidence are submitted, some investigators suspect fabrication. (P4)

These findings illustrate that while evidence is critical, both its absence and overabundance can negatively affect its perceived credibility. Therefore, creating a system that enables discreet and reliable collection is essential for supporting victims' claims and ensuring their safety.

3.3.2. Invisibility

Interviewees consistently emphasized that abusers often monitor and control victims' personal devices. This control includes deleting content and inspecting apps, photo galleries, and message histories.

Abusers often require victims—especially adolescents—to share passwords and install tracking apps. They inspect and delete conversations regularly. (P1)

In extreme cases, abusers even hire private forensic firms to recover deleted data and then entrap the victim. (P3)

Many abusers routinely monitor messenger conversations and often retain victims' financial credentials and passwords, allowing them unfettered access to personal data. (P4)

Given this, any collected evidence must remain imperceptible. If abusers discover evidence, they may destroy it or escalate abuse. Thus, invisibility must apply not only to the data itself but also to the act of collecting it.

In cases where adolescents are the victims, abusers are almost always adults. Owing to the age gap and the adult's superior access to information and technical know-how, victims face significant challenges when gathering evidence. Such evidence must be collected covertly, as any obvious action, such as pressing a phone's recording button, would be immediately detected by the abuser. (P1)

In the worst-case scenario, if an abuser discovers that evidence is being collected, the victim may face even greater danger. Thus, evidence must be obtained without the abuser's awareness, or disguised so that it remains unintelligible even if seen. (P3)

In particular, participants emphasized that invisibility must encompass not only the stored evidence itself but also the entire act of evidence collection. They expressed strong concerns about the design of foreign applications reviewed in Section 2.2, which rely on in-app cameras and recorders rather than the device's native functionality. This approach, while intended to isolate evidentiary functions, was seen as impractical in high-risk situations. When victims are under real-time surveillance, opening a separate, unfamiliar application to initiate recording could easily trigger suspicion or retaliation from the abuser. In light of this, participants unanimously stressed that secure and imperceptible storage takes precedence over collection features.

3.3.3. Anti-leakage

Among IPV victims, the fear of retaliatory harm—ranging from counter-litigation to the non-consensual distribution of intimate media—was repeatedly identified as a major barrier to reporting or seeking support. Adolescent victims, in particular, often refrained from disclosing abuse due to threats that evidence would be shared with their parents or school officials. Even in the absence of active threats, many victims lived with persistent anxiety that private recordings or images could be leaked before any formal legal proceedings had begun.

Adolescents often fear the potential distribution of sexual exploitation images to parents more acutely than the prospect of further violence. Consequently, abusers leverage this anxiety to blackmail their victims. (P2)

Although many victims understand the evidentiary value of digital media they record themselves, these files are frequently deleted due to psychological distress and fear of exposure.

In cases of digital sexual violence, evidence is often absent because victims delete recordings out of fear of dissemination. (P3)

Even when technically secure systems are used, concerns about the remote storage of intimate media persist. Victims worry that, if a breach occurs, unauthorized parties could access or distribute the files. (P4)

Many victims expressed deep concern over the possibility that someone might view the files, regardless of their evidentiary value. Some repeatedly asked whether any men were present at the counseling center or who would be able to see the evidence files if submitted. (P5)

Victims of digital sexual crimes—particularly those whose bodies were exposed in distributed videos or images—often showed a strong reluctance to store or transmit digital evidence. Due to intense fear and anxiety about further distribution, they tended to avoid submitting such files to counselors or law enforcement, even when required as evidence. According to P5, some victims tended to avoid using digital devices such as mobile phones or computers altogether after experiencing image-based abuse.

These accounts underscore the importance of implementing robust anti-leakage mechanisms in any digital evidence framework for IPV victims. Such mechanisms must address both unauthorized external access and the victim's internal hesitation to retain sensitive files. In addition to technical robustness, interviewees emphasized that such technologies must also enable victims to feel safe on an intuitive, emotional level—not merely understand safety in a rational or abstract sense. They highlighted the need for systems that not only ensure technical security, but also foster a tangible sense of safety for the user.

3.3.4. Continuity

IPV often arises from ongoing relational dynamics between the victim and the perpetrator, rather than from isolated incidents. As such, abuse tends to persist over time and may escalate gradually. This nature of IPV was repeatedly emphasized by interview participants, particularly in cases involving adolescent victims.

Adolescent IPV cases frequently begin through online contact. Perpetrators initiate conversations via social media or messaging platforms, cultivate emotional intimacy, and gradually escalate interactions toward sexual content or physical encounters.

Playful online chats often lead to offline sexual abuse and digital exploitation. (P1)

Adolescents form false intimacy online, then face in-person sexual violence. (P2)

In contrast, adult victims typically have pre-existing offline relationships with the perpetrator, making the onset of abuse more difficult to identify. Prolonged and repeated abuse often blurs the timeline of events, which in turn hinders victims' ability to report incidents clearly.

Prolonged domestic violence hinders reporting, as its onset and severity become unclear. (P4)

For these reasons, establishing a clear chronological record of incidents is critical. Many adolescent victims struggle to sequence events or identify specific details related to time and place. Support centers often assist by organizing messaging logs, retrieving synchronized image backups from cloud services, or cross-referencing diary entries and witness accounts to reconstruct the timeline of abuse.

Adolescents often don't know what counts as evidence, so counselors help them record incidents chronologically. (P1)

Because domestic violence can last years, key evidence like medical reports often gets lost, making long-term preservation difficult. (P4)

The need to maintain continuity extends beyond the preservation of isolated artifacts. Victims must be able to consistently store and later retrieve evidence across the full timeline of the abusive relationship. This includes maintaining both temporal continuity—the ability to preserve and organize evidence in chronological order—and contextual continuity, which involves retaining metadata and surrounding information (e.g., capture dates, device data, locations) to support the interpretability of each record.

3.4. Framework Necessity

A synthesis of the interview data revealed broad consensus among participants regarding the critical role of digital evidence in substantiating IPV claims. While journals, media files, and audio recordings were all cited as valuable, digital conversation records—particularly screenshots and exported chat logs—were described as the most frequently used and effective forms of evidence. However, interviewees consistently highlighted significant challenges in both timely acquisition and long-term retention of such materials.

One particularly acute issue is that victims often delete image or video files—especially those involving intimate or compromising content—due to anxiety over potential exposure or retaliation. As a result, victim support professionals frequently receive requests from clients to store evidence on their behalf, reflecting the need for external systems that can safeguard sensitive data.

Despite unanimous support for the idea of a digital evidence framework tailored to IPV victims, interviewees expressed several concerns regarding its implementation. These include: (1) the risk of unauthorized leakage of stored media through system breaches; (2) skepticism or bias from investigative authorities regarding the validity of both the victim and the evidence; and (3) the possibility that the abuser could detect the evidence collection process, leading to escalation of violence.

When asked to prioritize framework features, all participants emphasized invisibility—the ability to conceal both the evidence and the act of collecting it—and anti-leakage mechanisms that prevent any unauthorized disclosure. In addition, timeline visualization tools were recommended to help victims chronologically reconstruct and communicate the progression of abuse to investigators or legal representatives.

Given the wide demographic range of IPV victims—from adolescents to older adults—participants also underscored the importance of usability. The framework must be intuitive and accessible, even to individuals with limited digital literacy. Ensuring that victims can safely and independently engage with the system was seen as a prerequisite for its real-world viability.

In summary, the interview findings confirm a strong demand for a digital evidence support system tailored to IPV victims. However, they also highlight that the system must be designed with careful consideration of the surveillance risks, psychological vulnerabilities, and institutional challenges these victims face. A successful framework must therefore incorporate technical safeguards that ensure privacy, protect against data breaches, minimize the risk of abuser detection, and preserve survivable access to evidence over time.

4. Digital evidence framework for IPV victims

4.1. Architecture

The digital evidence framework proposed in this study comprises a comprehensive technical architecture and set of functional components that enable IPV victims to collect, store, and submit digital evidence using their personal devices, such as smartphones. The framework was designed based on the specific risks and needs of IPV victims, as identified through expert interviews. Accordingly, we propose a digital evidence framework for intimate partner violence victims (DEF-IPV).

To minimize the risks to victims, DEF-IPV integrates two core protective technologies: a camouflaged application and steganographic encoding. While various methods exist for hiding files—such as utilizing slack space in file systems or storing them in the cloud—this study adopts a combination of camouflage and steganography due to their accessibility, effectiveness in alleviating victims' anxiety, and suitability for real-life scenarios.

Using the camouflaged application, victims can document incidents discreetly and at any time. Media files are not only encrypted but also processed through steganography before being uploaded to a remote server. Victims may optionally choose to store the steganographic file (stego file) locally on their device. Because the files are embedded within seemingly innocuous images, they are less likely to be detected by abusers compared to conventionally encrypted files. Even if a stego file is discovered and forcibly deleted by an abuser, a backup remains on the remote server, allowing the victim to recover it later. The encryption key used for securing the media is stored only on the victim's device; therefore, the stego file stored on the remote server cannot be decrypted by others unless accessed through the victim's device.

The framework consists of three functional layers: presentation, application, and server.

- Presentation Layer: Victims interact with the system through a camouflaged application that appears as a benign utility (e.g., a calculator). When a specific numeric pattern is entered, the app reveals a hidden interface that enables evidence collection. Even if app usage is discovered, it remains impossible to determine what functions were accessed.
- Application Layer: Victims can record text-based diary entries and upload media files. To meet the anti-leakage requirement, DEF-IPV applies a dual-layer security mechanism in which encryption occurs on the client side and steganographic encoding is performed server-side. Based on expert interviews, many victims tend to delete sensitive images out of fear of unauthorized access or distribution. In this framework, uploaded media files are encrypted locally using a device-specific key stored securely on the victim's device (e.g., via the Android Keystore). The encrypted file is then transmitted to the server for further processing.
- Server Layer: The server receives encrypted media files and performs steganographic embedding into preselected cover images. The resulting stego files are securely stored and indexed alongside the victim's diary entries and incident metadata via a timeline file (see Fig. 1). This structure allows reviewers to understand the chronological sequence and context of each piece of evidence. Optionally, the stego files can be transmitted back to the victim's device upon request, enabling personal retention or offline backup. Importantly, the server holds no decryption key and cannot access the original media. To submit evidence, the stego file must be downloaded to the

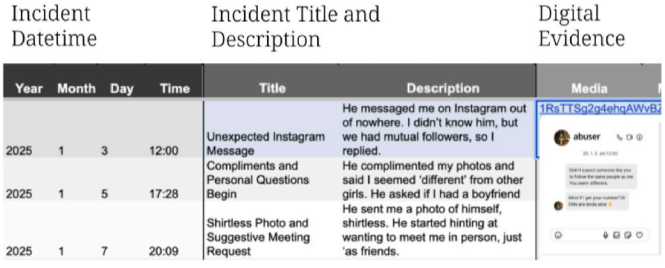

Fig. 1. Underlying data structure of the timeline file, showing chronological organization of incident details and links to media evidence.

victim's original device for decryption. This client-side-only model ensures end-to-end confidentiality, keeping all content inaccessible to the server or third parties unless explicitly decrypted by the victim.

4.2. Process

This section outlines the procedural flow by which IPV victims interact with the DEF-IPV framework—from initial setup to final submission of evidence. To contextualize its structure, the proposed process is contrasted with the conventional digital forensic model.

The traditional digital forensic process, as defined by the DFRWS model, consists of six investigator-driven phases: identification, preservation, collection, examination, analysis, and presentation. It is primarily designed for post-incident evidence recovery from seized devices.

In contrast, the DEF-IPV process is victim-driven, designed for real-time evidence collection under conditions of ongoing surveillance or coercion. While it shares a general structure with the conventional model—comprising preparation, evidence collection, and submission—it excludes phases such as seizure and forensic analysis. Instead, it incorporates technical safeguards to ensure that both the evidence and the act of collecting it remain hidden from the abuser.

The DEF-IPV framework prioritizes discreet acquisition, invisibility, and continuity of evidence, rather than in-depth forensic examination. It consists of three operational stages: Preparation, Evidence Collection, and Evidence Submission. At each stage, protective mechanisms are embedded to reduce the risk of discovery or retaliation.

Fig. 2 illustrates the full procedural sequence between the victim, the disguised application, and the DEF-IPV server. The diagram visualizes the integration of core technical components—such as passphrase issuance, encryption, steganographic embedding, and remote storage—within the victim's user experience, providing an end-to-end overview of the framework's functionality.

The DEF-IPV process comprises three main stages: Preparation, Evidence Collection, and Evidence Submission.

- Preparation Stage: A victim support organization consults with the victim to assess the applicability of DEF-IPV. If appropriate, the organization assists in installing the camouflaged application, creating an account, and generating a passphrase. As part of the setup, a device-specific encryption key is securely stored on the victim's device to enable local encryption of media files. The passphrase modeled after the No Stalk natural language password approach serves as an additional authentication factor during the submission stage. It is required when downloading the steganographically embedded file from the server to the victim's device.
- Evidence Collection Stage: Victims can discreetly collect evidence using the disguised application interface. The system supports the capture and upload of media files—including photos, screenshots, and images of official documents—using a dual-layer security approach: encryption followed by steganographic embedding. The files are backed up to the DEF-IPV server, with an option for the victim to download and store the steganographically embedded version on their device.
- Evidence Submission Stage: When the victim deems it safe, they may use their passphrase to download the steganographically embedded file from the server to their device. The file is then decrypted locally and can be submitted to trusted entities, such as legal representatives or investigative authorities.

This end-to-end process ensures that not only individual evidence items but also the overall act of documentation and submission remains covert and survivable. It is specifically designed to address the operational constraints and psychological needs of IPV victims operating under surveillance or coercion.

5. Evaluation

5.1. Criteria

In Section 3, three essential requirements for assisting IPV victims in digital evidence collection were identified: invisibility, anti-leakage, and continuity. For evaluation purposes, each of these was further divided into two functional components.

Invisibility refers to the characteristic of preventing the abuser from seeing both the act of evidence collection and the collected evidence itself. This requirement is divided into two aspects: *Activity Stealth* and *Evidence Stealth*. Activity stealth evaluates whether the victim's behavior—such as launching an application or collecting media—can be detected by the abuser through residual traces like browser usage, search history, or application logs. Evidence stealth refers to the ability to prevent the abuser from discovering evidence files stored on the device, which can be achieved by hiding or remotely storing them so that no residual data remains locally.

Anti-Leakage addresses the risk of unauthorized access or distribution of sensitive evidence files. It is evaluated based on *Access Control* and *Media Security*. Access control refers to the implementation of authentication mechanisms that block unauthorized access to stored evidence. Media security evaluates whether the media files themselves are encrypted or otherwise protected to prevent misuse or exposure.

Continuity refers to the consistent documentation of evidence in both content and format to demonstrate the persistence of harm and enhance the legal validity of the evidence. This requirement is evaluated through timeline generation and metadata preservation. Timeline generation refers to the system's ability to chronologically organize and continuously maintain collected evidence. Metadata preservation helps support the admissibility of evidence by ensuring that key attributes—such as capture date, device information, and other file-specific properties—are properly retained.

These evaluation criteria serve as the basis for the technical comparison between DEF-IPV and existing victim support services.

5.2. Prototype of DEF-IPV

To demonstrate the technical feasibility of DEF-IPV, we developed a prototype simulating its key functionalities.[1] While the camouflage interface can take various forms—such as games or note-taking apps—the prototype adopts a calculator–style interface to enable discreet and intuitive use in everyday environments.

The prototype includes several core components: a disguised home screen (calculator interface), an evidence recording interface, a passphrase input screen, and a review screen for transmitting stored evidence. These are illustrated in Fig. 3.

Collected evidence is encrypted locally on the user's device and then transmitted to the server, where it is embedded into a cover image using steganography. The resulting stego file is securely stored on the server. To retrieve the file, the victim uses the previously issued passphrase to authorize download. Decryption is performed locally on the device where the encryption key is stored, ensuring that the server cannot access the original content.

5.3. Comparative analysis

To evaluate the relative effectiveness of DEF-IPV, we conducted a comparative analysis against four existing victim support services introduced in Section 2.2: Bright Sky, No Stalk, VictimsVoice, and Seek Then Speak. The evaluation is based on the six sub-criteria outlined in

[1] https://tinyurl.com/def-ipv-prototype, Demo stores no real data. Enter 123456 for recording, 456789 and passphrase "You can raise your voice" for evidence review.

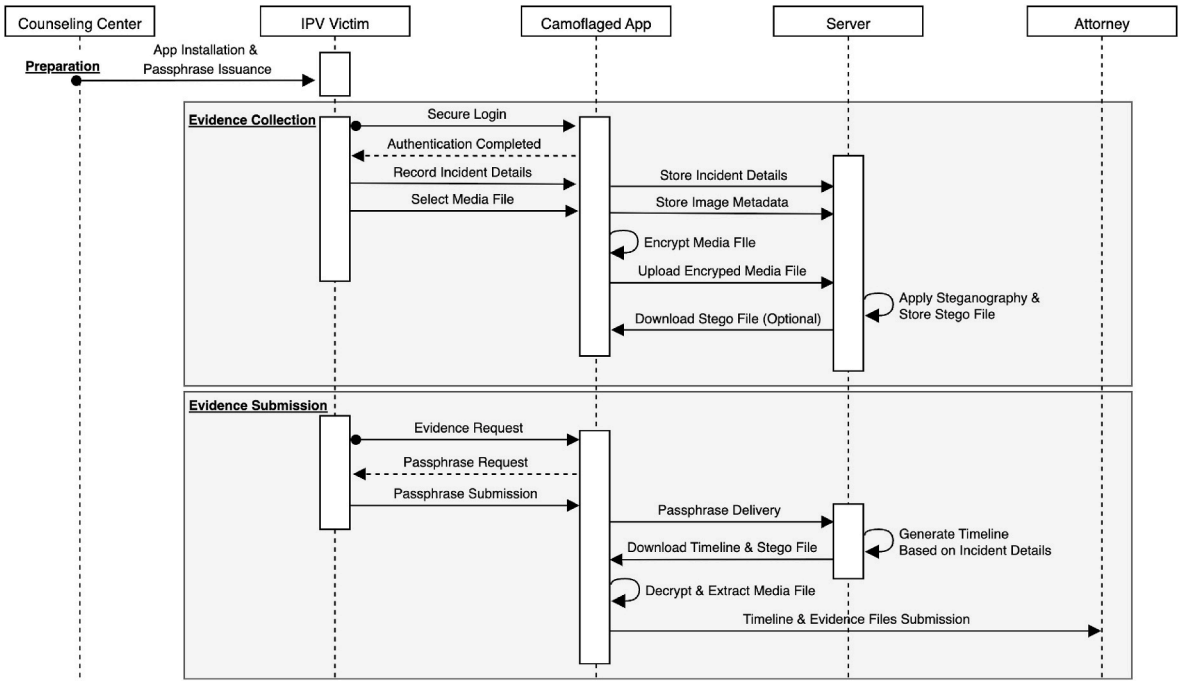

Fig. 2. Sequence diagram illustrating the integration of procedure and framework in DEF-IPV.

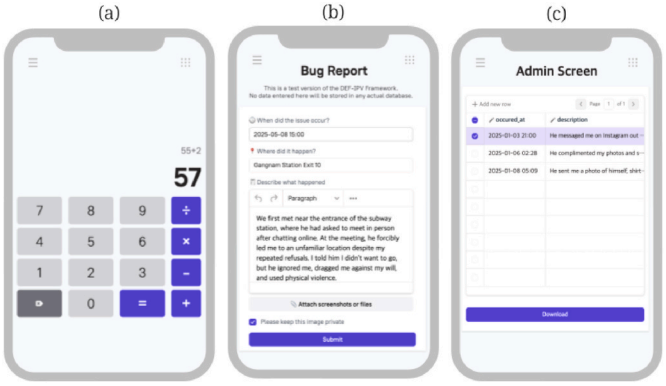

Fig. 3. Key interface screenshots of DEF-IPV prototype: (a) Camouflaged screen, (b) Evidence recording, (c) Evidence List.

Section 5.1. The results are summarized in Table 4.

5.3.1. *Invisibility: activity and evidence stealth*

DEF-IPV satisfies both activity stealth and evidence stealth. For activity stealth, the camouflaged application allows users to access evidence collection features through an innocuous calculator interface. No app name or icon indicative of victim support is shown. In contrast, BrightSky and No Stalk use clearly labeled apps that may raise suspicion if discovered. Seek Then Speak partially supports stealth by offering a "Safe Exit" button, which clears browser history only if the user activates it before exiting.

In terms of evidence stealth, DEF-IPV ensures that collected files do not remain on the device. Media files are encrypted, steganographically embedded, and then uploaded to the server, leaving no local traces. VictimsVoice and No Stalk also support evidence storage on a remote server or in restricted environments, meeting this criterion. However, Seek Then Speak generates a downloadable report file after form submission, which remains on the user's device. BrightSky sends evidence to a user-designated email address, making the presence of evidence visible within the user's email client or outbox.

5.3.2. *Anti-leakage: media security and access control*

DEF-IPV satisfies both media security and access control. It encrypts media files before embedding them in cover images using steganography. This two-layered protection not only mitigates the technical risk of evidence exposure, but also reassures victims that their files cannot be accessed by others, effectively reducing the anxiety of potential leakage. In contrast, BrightSky, VictimsVoice, and No Stalk do not implement encryption or obfuscation techniques for media files. Seek Then Speak similarly lacks any file-level protection.

In terms of access control, DEF-IPV requires a passphrase to retrieve and download stored evidence. This phrase is issued at the preparation stage. No Stalk also uses a strong passphrase-based authentication method. VictimsVoice offers login-based access control, but it does not prevent stored media from being viewed locally if the login is compromised. BrightSky and Seek Then Speak do not include any access control

Table 4
Comparative analysis of DEF-IPV framework and existing solutions.

Dimension	Subcategory	BrightSky	No Stalk	VictimsVoice	Seek Then Speak	DEF-IPV
Invisibility	Activity Stealth	X	X	O	Δ	O
	Evidence Stealth	Δ	O	O	X	O
Anti-Leakage	Media Security	X	X	X	X	O
	Access Control	X	O	O	X	O
Continuity	Timeline Generation	X	O	O	O	O
	Metadata Preservation	O	O	O	X	O

Rating Scale: O = Completely satisfies the requirement; Δ = Partially satisfies the requirement; X = Does not satisfy the requirement.

mechanisms within their apps or platforms.

5.3.3. Continuity: timeline and metadata preservation

DEF-IPV supports both timeline generation and metadata preservation. It automatically generates a timeline file that organizes the collected evidence in chronological order and links media files to the corresponding entries. This file is exported in XML format and includes metadata such as capture time, device information, and file path, which is preserved during encryption and steganographic embedding.

No Stalk and VictimsVoice provide partial support for continuity. VictimsVoice allows users to enter detailed information per entry and structures it in a form that can be exported for court submission, while No Stalk enables annotation of each file. However, neither system offers full metadata export or automatic timeline generation. Seek Then Speak supports some degree of narrative continuity by guiding users through a structured questionnaire but does not preserve timestamps or raw media metadata. BrightSky allows evidence submission with simple date input but lacks time sequencing, metadata preservation, or export functionality.

5.4. Discussion

The comparative analysis demonstrates that DEF-IPV effectively addresses the three core requirements identified for digital evidence collection in IPV contexts: invisibility, anti-leakage, and continuity. Unlike existing solutions, which tend to focus on documentation or support provision, DEF-IPV provides a comprehensive technical response to the unique risks IPV victims face when attempting to preserve digital evidence covertly.

Its strengths lie in the integrated application of encryption and steganography, a camouflaged user interface, and a server-side architecture that prevents local evidence retention. Together, these features provide a high degree of activity and evidence stealth, minimizing the risk of detection by abusers. Additionally, the system's ability to generate a time-ordered, metadata-rich timeline strengthens evidentiary continuity and supports later investigative or legal processes.

In addition to IPV-specific use cases, the applicability of DEF-IPV extends to other high-risk environments characterized by surveillance and coercive control. For instance, migrant workers facing exploitative labor conditions or individuals monitored through employer-imposed digital surveillance may also benefit from a system that enables discreet documentation and preservation of digital evidence (Shin, 2025).

In situations where immediate separation from a perpetrator or controlling entity is not feasible, the ability to securely and invisibly collect digital evidence can play a critical role in accelerating exit and access to institutional protection. This study contributes to that broader aim by offering a technically grounded, survivor-centered foundation for protective interventions.

Despite these advantages, several limitations must be acknowledged.

- Manual evidence collection: The current version of DEF-IPV requires victims to manually capture and upload evidence. While the interface is designed to be discreet, this still poses a risk of discovery for those under intensive surveillance. Future versions may benefit from incorporating automated capture mechanisms, such as keyword-triggered screenshots or background message logging.
- Dependency on institutional support: The framework assumes that victims can install and initialize the system in collaboration with support organizations. However, in many real-world situations, access to such support may be limited or entirely absent. This highlights the need for more autonomous onboarding and authentication methods.
- Limited media support: The current implementation only supports image-based evidence. Although screenshots are among the most common formats submitted by victims, the inability to handle audio, video, or documents restricts the framework's applicability in broader cases.
- Lack of user and legal validation: The evaluation presented here focuses on functionality and comparative criteria. Usability testing and expert validation—particularly regarding perceived safety and legal admissibility—remain as essential next steps. While the framework attempts to preserve evidentiary integrity through metadata retention, its lack of involvement in the original media production process poses inherent limitations for legal admissibility.

6. Conclusion

This study proposed DEF-IPV, a secure and covert digital evidence framework designed to assist victims of intimate partner violence in safely collecting, storing, and submitting digital evidence. Unlike existing support tools, which often lack protection against discovery or unauthorized access, DEF-IPV incorporates technical safeguards that directly address the operational threats IPV victims face—particularly under conditions of surveillance or coercion.

Drawing upon expert interviews, we identified three essential requirements for a victim-centered evidence framework: invisibility, anti-leakage, and continuity. Based on these, we designed a three-layer architecture incorporating a camouflaged user interface, dual-layer media protection using encryption and steganography, and a timeline-based evidence structuring system. A prototype was implemented and evaluated against four existing support services. The results showed that DEF-IPV meets all six sub-criteria under the three main requirements, demonstrating advantages in both technical functionality and alignment with victim needs.

As discussed in Section 5.4, future work will focus on improving the framework in several key areas. These include integrating automated evidence capture mechanisms, expanding support for diverse media types, and developing more flexible deployment methods that can operate without institutional assistance. In addition, usability testing and legal admissibility validation will be necessary to ensure that the system is both practically effective and formally recognized within evidentiary procedures.

Ultimately, DEF-IPV contributes to bridging the gap between victim advocacy and digital forensics by offering a technically grounded, user-centered approach to evidence preservation in IPV contexts. It provides a foundation upon which more resilient and survivor-friendly forensic technologies can be developed.

Acknowledgements

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No.RS-2024-00398745, Proofs and responses against evidence tampering in the new digital environment).

Appendix A. Expert Interview Guide

Prior to the interview, participants were provided with a brief overview of the study's purpose and scope. The following is the structured questionnaire used in the interviews.

Section 1. Characteristics of Victimization

1. Could you describe the main types of violence experienced by victims (e.g., physical violence, emotional abuse, economic coercion, digital abuse, etc.)
2. What are the most common difficulties victims report when attempting to report or disclose their experiences?
3. How do victims usually collect evidence of the violence they experience, and what risks are involved in this process?

4. Are there cases in which perpetrators monitor or control the victim's digital devices? If so, what forms does this control typically take?

Section 2. Evidence Collection and Preservation

1. How frequently do victims preserve evidence of their experiences? If they do, what methods or platforms do they typically use?
2. Do you provide guidance to victims on how to collect or store digital evidence? If so, what kind of information or recommendations do you offer?
3. Have you ever referred a victim's device for digital forensic analysis? What was the purpose, and what were the positive or negative aspects of that process?

Section 3. Digital Evidence Framework for IPV victims

1. In your opinion, what is the most important feature a digital evidence framework should have?
2. What essential functions do you believe such a framework must include?
3. What technical or institutional support do you think is necessary to help victims safely collect and store digital evidence?
4. What factors should be considered to ensure the victim's safety during the process of evidence collection?

Section 4. Accessibility and Usability

1. Are most IPV victims generally proficient in using digital devices?
2. If shelters or counseling centers are to introduce such digital systems, what technical or institutional support would be necessary?
3. How should digital evidence systems be integrated with existing victim support services to ensure effective delivery?

Section 5. Case-Based Reflections

1. Have you encountered a case where effective evidence collection played a critical role in providing support or protection to the victim?
2. Have there been cases where the inability to collect evidence hindered the provision of appropriate legal or institutional support?

Section 6. Additional Comments

1. Are there any additional suggestions, concerns, or issues you would like to raise regarding digital evidence framework for IPV victims?

References

Adeoye-Olatunde, O.A., Olenik, N.L., 2021. Research and scholarly methods: semi-Structured interviews. J. Am. Coll. Clin. Pharm. 4, 1358–1367.

Braun, Virginia, Clarke, Victoria, 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101.

European Institute for Gender Equality, 2019. Understanding intimate partner violence in the eu:the role of data. https://eige.europa.eu/publications-resources/publications/understanding-intimate-partner-violence-eu-role-data.

EVAWI. Seek then speak. URL: https://seekthenspeak.app.

Evsutin, O., Melman, A., Meshcheryakov, R., 2000. Digital steganography and watermarking for digital images: a review of current research directions. IEEE ASME J. Microelectromech. Syst. 8, 166589–166611.

Freed, Diana, Palmer, Jackeline, Minchala, Diana, Levy, Karen, Ristenpart, Thomas, Dell, Nicola, 2018. "a stalker's paradise": how intimate partner abusers exploit technology. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery.

Haider, Th, 2021. Alrikabi and Haitham Tuama Hazim. Enhanced data security of communication system using combined encryption and steganography. International Journal of Interactive Mobile Technologies (iJIM) 15 (16), 144–157.

Hanna, Kallio, Pietilä, Anna-Maija, Johnson, Martin, Kangasniemi, Mari, 2016. Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. J. Adv. Nurs. 72 (12), 2954–2965.

Harris, R., 2006. Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem. In: Digital Forensic Research Workshop. Elsevier.

Havron, Sam, Freed, Diana, Chatterjee, Rahul, McCoy, Damon, Dell, Nicola, Ristenpart, Thomas, 2019. Clinical computer security for victims of intimate partner violence. In: 28th USENIX Security Symposium (USENIX Security 19). USENIX Association.

Hestia. Bright sky. URL: https://bright-sky.org.

IMPRODOVA, 2023. Data and Statistics on Domestic Violence.

Laishram, Debina, Tuithung, Themrichon, 2018. A survey on digital image steganography: current trends and challenges. In: 3rd International Conference on Internet of Things and Connected Technologies.

Mangeard, Philippe, Tejaswi, Bhaskar, Mannan, Mohammad, Youssef, Amr, 2024. Warne: a stalkerware evidence collection tool. Forensic Sci. Int.: Digit. Invest. 48 (Suppl. ment).

Shin, Daeun, 2025. Tulsi Spent 4 Years Dreaming of Life in Korea. Within 6 Months of Arrival, He Was Dead. The Hankyoreh.

Statistics Canada, 2023. Family Violence in Canada: a Statistical Profile, 2022 – Chart 1. Rate of police-reported Intimate Partner Violence, Canada, 2009 to 2022.

Stephenson, Sophie, Almansoori, Majed, Emami-Naeini, Pardis, Huang, Danny Yuxing, Chatterjee, Rahul, 2023. Abuse vectors: a framework for conceptualizing IoT-Enabled interpersonal abuse. In: 32nd USENIX Security Symposium (USENIX Security 23). USENIX Association.

Torp Løkkeberg, Stine, Ihlebæk, Camilla, Brottveit, Gudrun, Busso, Lilliana Del, 2023. Digital violence and abuse: a scoping review of adverse experiences within adolescent intimate partner relationships. Trauma Violence Abuse 25 (3), 1954–1965.

UN Women. Types of violence against women and girls. URL: https://www.unwomen.org/en/articles/faqs/faqs-types-of-violence-against-women-and-girls.

U.S. Department of Health and Human Services. Hipaa Privacy Rule and Sharing Information, n.d.

Victims Voice. Victims voice. URL: https://victimsvoice.app.

Weisser Ring. No stalk.https://nostalk.de.