DEF-IPV: Digital Evidence Framework for Intimate Partner Violence victims

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

성균관대학교
SUNG KYUN KWAN UNIVERSITY(SKKU)

Outline

1. Overview
2. Background
3. Related Works
4. Expert Interview
5. DEF-IPV Architecture
6. Evaluation & Limitation
7. Conclusion

Overview

- **Goal**: Enabling victims to safely collect digital evidence under surveillance.
- **Scope**
  - Assumption: The victim has minimal independent access to their device.
  - Abuser’s Control Range:

Category	Description	Included
Physical Access	The abuser can physically access the victim’s mobile device.	✅ Included
Application-Level Access	The abuser can access applications installed on the victim’s device	✅ Included
Advanced Technical Control	The abuser performs forensic analysis or system log inspection.	❌ Excluded

- **3Methods**
  - Literature Review: Analysis of prior technical approaches and existing evidence-collection services.
  - Qualitative Research: Identification of essential requirements through expert interviews.
  - Framework Design and Evaluation: Design of the digital evidence framework followed by comparative evaluation.

Background

- **Global Trends in IPV**
  - France: Reports increased by 15% in 2022
  - Germany: IPV-related crimes rose by 9% in 2023
  - Canada: Continuous increase observed from 2015–2021
  - South Korea: IPV-related femicide and attempted femicide cases nearly doubled (311 → 650, 2022–2024).

- **Key Characteristics of IPV**
  - IPV victims are usually closely connected to their abusers physically and psychologically.
  - This close relationship allows abusers to **easily monitor and control** the victim.
  - Abusers often **isolate victims** by disrupting their social relationships and **checking or restricting mobile device use.**

Related Works - Academic Research

- **Digital Control in Adolescent Relationships**

  Research shows frequent device and social media monitoring and password demands among adolescent IPV cases. Digital control is becoming commonplace within youth romantic relationships (Torp et al., 2023)[3].

- **Technology-Facilitated Abuse**

  Recent work documents how abusers exploit mobile and IoT devices to surveil and exert control over partners (Stephenson et al., 2023)[4]; (Freed et al., 2018)[5].

- **Security and Forensic Interventions**

  Studies propose victim-centered security practices and advisory workflows (Havron et al., 2019)[6] and forensic tools for collecting evidence of stalkerware (Mangeard et al., 2024)[7].

Related Works - Existing Services

- 🇬🇧 **BrightSky:** Allows victims to store evidence and send it to a pre-designated email.
- 🇩🇪 **No Stalk**: Evidence stored in-app, but viewing requires a decryption code on another device.
- 🇺🇸 **VictimsVoice:** Ensures HIPAA compliance and chain-of-custody integrity for legal validity.
- 🇺🇸 **Seek Then Speak:** Provides guidance on how and where to locate evidence.

Category	Features	BrightSky	No Stalk	Victims Voice	Seek then Speak
Evidence Collection	Incident Log Recording	O	O	O	O
	Photo Upload	X	X	O	X
	Photo Capture	O	O	O	O
	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 Functions	Report Generation	X	X	O	O

IPV Expert Interview

- **Interview Design**
  - Semi-structured Interviews followed by thematic Analysis
- **Participants**

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 sexual crimes	Legal and counseling support

* WHRDs : Women's Human Rights Defenders

IPV Expert Interview - Interview Finding

We identified three essential requirements for a digital evidence framework:

- **Invisibility:** Both the act of collecting evidence and the stored evidence files must remain hidden.

  "*Many abusers routinely monitor messenger conversations and often retain victims' financial credentials and passwords, allowing them unfettered access to personal data. (P4)*"
- **Anti-Leakage**: Sensitive images (e.g., containing the victim's body) must be protected against unauthorized exposure.

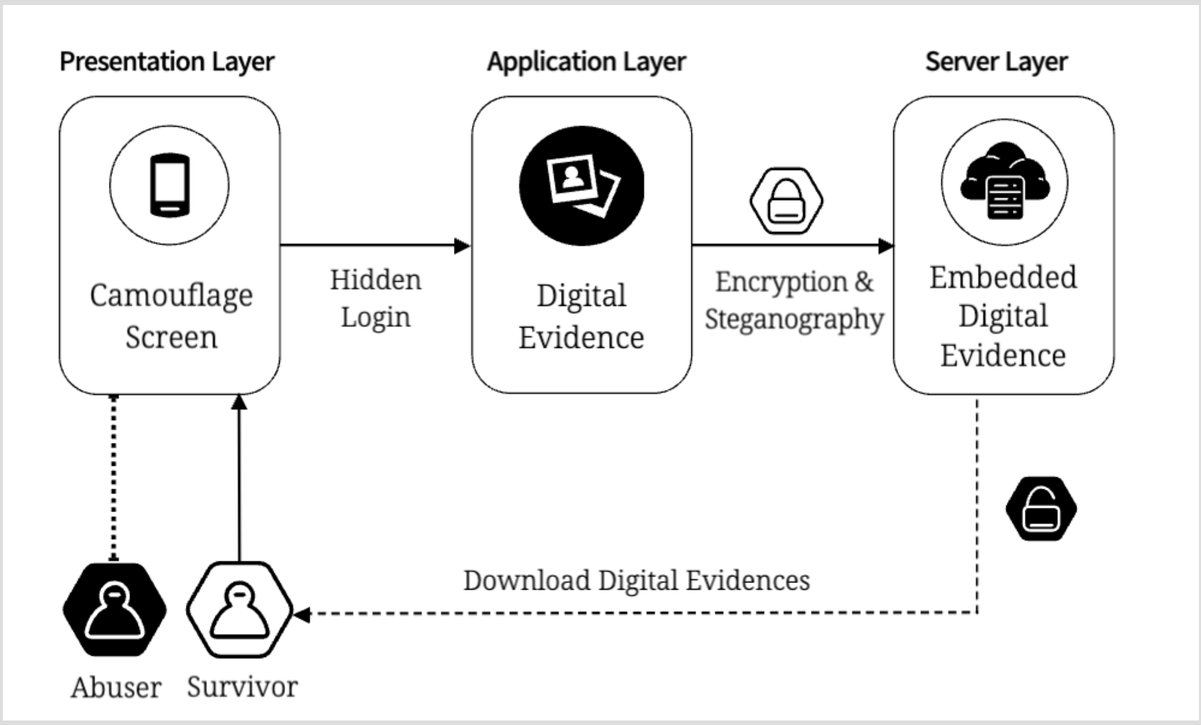
  "*Many victims expressed deep concern over the possibility that someone might view the files, regardless of their evidentiary value. Some repeatedly asked whether any men were present at the counseling center or who would be able to see the evidence files if submitted. (P5)*"
- **Continuity**: The sequence of events should be captured and presented in a clear, continuous timeline.

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

DEF-IPV Framework

- **The Definition of ‘Digital Evidence Framework’**
  - 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.

- **Core Technologies of DEF-IPV**



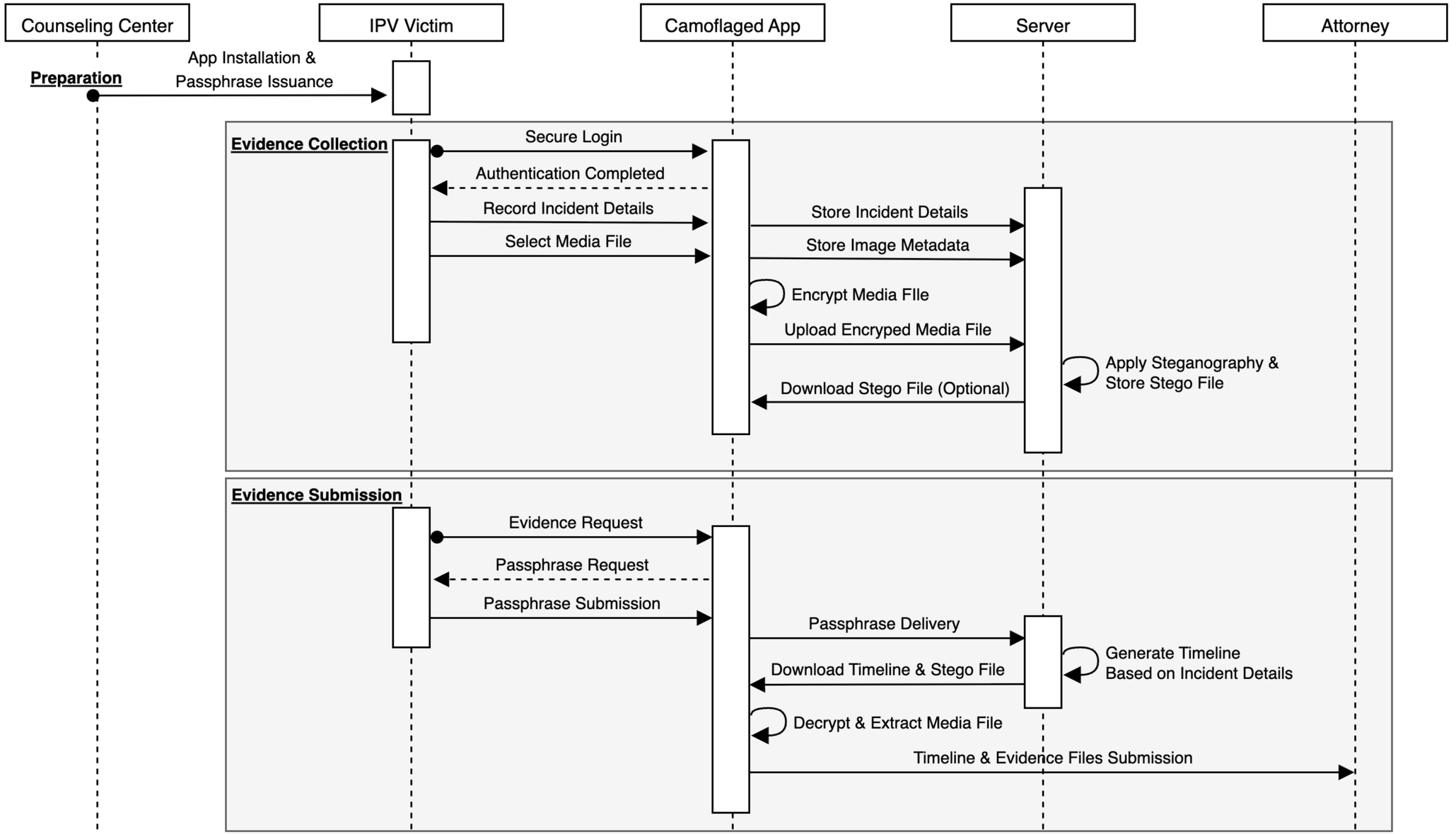
- Camouflaged application
- Dual-Layer Media File Encryption
  - Device-Specific Key Encryption (e.g., Android Keystore)
  - Steganographic Embedding

DEF-IPV Framework

- **Functional Layers of DEV-IPV**
  - Presentation Layer *(Key Requirement: Invisibility)*
    - Victims interact with **a camouflaged application** that appears as an everyday utility (e.g., calculator).
  - Application Layer *(Key Requirement: Anti-Leakage)*
    - Victims can record diary entries and upload media evidence.

      A dual-layer security process is applied:
    - **Client-side encryption** using a device-specific key
    - **Steganographic embedding**
  - Server Layer *(Key Requirement: Continuity)*
    - Encrypted files are steganographically embedded into cover images and **stored with chronological metadata**. The server cannot decrypt the files (no key access), ensuring end-to-end confidentiality — only the victim's device can decrypt the evidence.

DEF-IPV Framework - Sequence Diagram

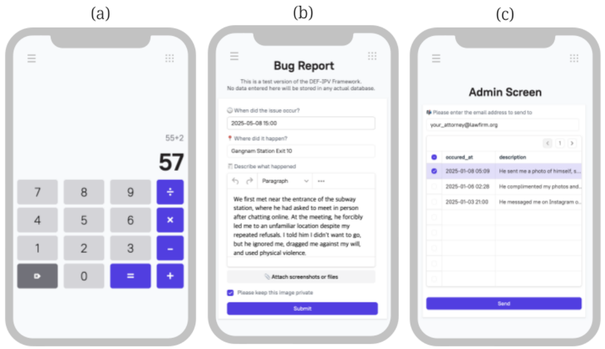


Evaluation & Limitation

- **Prototype**

  Designed a calculator-style camouflage prototype implementing core DEF-IPV functions.

  Demo stores no real data. Enter 123456 for recording, 456789 and passphrase “You can raise your voice” for evidence review.



- **Criteria and Results**

Category	Features	BrightSky	No Stalk	Victims Voice	Seek then Speak	DEF-IPV
Invisibility	Activity Stealth	X	X	O	△	O
	Evidence Stealth	△	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

Evaluation & Limitation — Post Submission Update

- **Usability Test**
  - Conducted based on HCI usability evaluation practices
  - Sample size: 5 participants, following Nielsen's guideline that 3–5 users can reveal most usability issues (J Nielsen, 1994)
  - Participants: 3 women in their 30s, 2 women in their 40s
  - Duration: September 20–21, 2025 (2 days)
  - Device: Prototype installed on a test smartphone (Galaxy)
- **Key Research Question**
  - Can users successfully and discreetly upload evidence using the DEF-IPV prototype in realistic coercive-control scenarios?
- **Evaluation Metrics**
  - Effectiveness: Task success rate
  - Efficiency: Average time per task
  - Satisfaction: Subjective user rating (7-point Likert scale)

Evaluation & Limitation — Post Submission Update

- **Scenario Setting**
  - Participants were asked to simulate discreetly uploading evidence to avoid detection by an abuser.
  - To induce situational tension, tasks were performed in a quiet corner space, although no real surveillant was present.

- **Results**

Task	Effectiveness	Efficiency (Avg. Seconds)	Satisfaction
Access the Evidence Upload screen	100%	33.4	5
Upload Evidence	100%	193	
Access the Evidence Download screen	100%	56.4	
Download Evidence	100%	11.8	

Avg. 3 min 7 sec to access & upload evidence

If the user can handle the device unobserved for ~4 minutes, they can safely conceal evidence via DEF-IPV.

Evaluation & Limitation

- **Potential Beneficiaries**
  - Employees under employer-imposed digital monitoring

    In such contexts, victims also need discreet documentation and secure preservation of digital evidence.

- **Limitation**
  - Manual evidence collection
  - Dependence on external/institutional support
  - Limited media format support (Currently image-only, video not supported)
  - No validation against malicious misuse
  - Legal admissibility of evidence not yet evaluated

Conclusion

DEF-IPV is a secure and covert digital evidence framework designed to help IPV victims safely collect, store, and submit 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**.

- **Future Work**
  - Automated evidence capture (reduce manual burden)
  - Support for additional media types (e.g., video)
  - Flexible deployment models not reliant on institutions
  - Legal admissibility validation for formal evidentiary use

Thank you