Trauma-Informed Digital Evidence Collection: A Design Inquiry into Evidence Practices for Technology-Facilitated Abuse in Intimate Partner Violence

Sophie Stephenson
Computer Sciences
University of Wisconsin–Madison
Madison, Wisconsin, USA
sophie.stephenson@cs.wisc.edu

Naman Gupta
Computer Sciences
University of Wisconsin–Madison
Madison, Wisconsin, USA
n@cs.wisc.edu

Kyle Huang
Computer Sciences
University of Wisconsin–Madison
Madison, Wisconsin, USA
kkhuang@wisc.edu

David Youssef
Computer Sciences
University of Wisconsin–Madison
Madison, Wisconsin, USA
dyoussef@wisc.edu

Kayleigh Cowan
Disability Rights Wisconsin
Madison, Wisconsin, USA
kayleighc@dwri.org

Rahul Chatterjee
Computer Sciences
University of Wisconsin–Madison
Madison, Wisconsin, USA
rahul.chatterjee@wisc.edu

Abstract

Technology-facilitated abuse (TFA) is a widespread and harmful dimension of interpersonal violence. Documenting TFA can unlock mitigative actions for survivors such as legal orders of protection, but existing documentation tools are insufficient. This paper considers whether a trauma-informed design approach could yield more effective methods for documenting TFA and how, concretely, to approach *trauma-informed digital evidence collection.* Toward this goal, we use trauma-informed methods to design a new tool, Sherloc, that helps identify and document TFA within tech clinic interventions. We evaluated Sherloc in feedback sessions with legal experts, then in a small pilot program in the U.S. From our design inquiry, we present novel guidelines for trauma-informed digital evidence collection. We call on HCI researchers to build on our work to envision trauma-informed methods of documenting TFA.

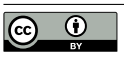
CCS Concepts

• **Security and privacy** → Human and societal aspects of security and privacy; • **Applied computing** → Evidence collection, storage and analysis.

Keywords

technology-facilitated abuse, clinical computer security, digital evidence, trauma-informed computing

ACM Reference Format:
Sophie Stephenson, Naman Gupta, Kyle Huang, David Youssef, Kayleigh Cowan, and Rahul Chatterjee. 2026. Trauma-Informed Digital Evidence Collection: A Design Inquiry into Evidence Practices for Technology-Facilitated Abuse in Intimate Partner Violence. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3772318.3790296



This work is licensed under a Creative Commons Attribution 4.0 International License.
CHI '26, Barcelona, Spain
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3790296

1 Introduction

Millions of people are affected by technology-facilitated abuse (TFA), which can include hate and harassment, image-based sexual abuse, and interpersonal surveillance [71, 104]. Documenting TFA can be a critical part of survivors' safety and healing, enabling them to seek legal recourse, reconfigure devices and accounts, and share their experiences with support systems [61, 100]. At present, a number of off-the-shelf apps [4, 13, 16, 18, 20, 26, 29] and forensic tools [8, 19, 64, 77] exist that can help survivors document TFA. Furthermore, HCI researchers have proposed methods for documenting TFA, such as Sultana et al. [102] and Goyal et al. [60]'s tools for documenting online harassment.

Unfortunately, existing methods for documenting digital evidence fall short of survivors' needs. Sophisticated investigative tools are rarely accessible to individual survivors [92, 100], and academic prototypes are not publicly available [60, 77, 102]. Survivor-facing apps mainly serve as repositories for evidence, requiring that survivors identify and record TFA on their own—a burdensome and potentially re-traumatizing undertaking [59, 78, 100].

We argue that an underlying limitation of the available documentation methods is that they are not *trauma-informed.* For research on digital safety, trauma-informed approaches can help minimize harm—and maximize benefits—for both survivors and researchers [40, 41]. For example, researchers have built trauma-informed *tech clinics* [64, 85, 86, 107] where survivors meet with trained technology experts to address their TFA concerns. However, to our knowledge, no prior work has used trauma-informed lenses to design *documentation methods* for TFA. Therefore, in this work, we propose and test a trauma-informed approach for designing digital evidence collection frameworks for TFA. More precisely, this work has two key contributions:

(1) Using a trauma-informed approach, we design and evaluate a framework to collect evidence of TFA in tech clinic consultations.
(2) We reflect on the use of trauma-informed methods to design TFA documentation tools, providing guidance for future work.

To design our evidence collection tool, we undertook a community-engaged design inquiry [111] focusing on TFA in the context of intimate partner violence (IPV) [55, 59, 78, 109]. Based on prior work [64, 100] and our own experiences volunteering at a tech clinic, we identified tech clinic consultations as a unique opportunity to document TFA without adding to survivors' burden, since much evidence of TFA is already uncovered during these consultations. Therefore, we designed Sherloc,[1] an evidentiary framework designed to identify, capture and document TFA within tech clinic consultations (Section 5).

We evaluated Sherloc in two stages. In the first round of evaluation, we sought feedback from legal experts on an initial prototype (Section 6). We performed interviews and focus groups with 19 legal support providers, ranging from attorneys and law clinicians to a police officer, and distributed a feedback survey to 12 judges. Feedback from these legal experts identified minor changes that could strengthen Sherloc—for example, ways to improve the readability of the evidence produced by Sherloc—while giving us the assurance to begin using Sherloc in practice.

Now, in the second stage of evaluation, we have partnered with the Madison Tech Clinic in Wisconsin, U.S., to pilot Sherloc in consultations (Section 7). Thus far, three pilot consultations have validated the usefulness of Sherloc, with a positive response from survivors and advocates so far. The pilot has also shown us opportunities to improve Sherloc's effectiveness by, e.g., removing noisy technical details that do not add to the report's robustness. We plan to continue the pilot program long-term, iterating and improving on Sherloc as we gather more data.

This design inquiry has helped us to understand what it takes to document TFA through a trauma-informed lens. To this end, we leave the reader with guidelines for *trauma-informed digital evidence collection* (Section 8). In sum, we recommend a focus on (i) survivor safety, (ii) early, situated iteration, (iii) flexible functionality and modality, (iv) evidence interpretability (even at the expense of technical sophistication), and (v) long-term maintainability. We put forward these guidelines to guide HCI researchers and designers to envision documentation methods that are safer, clearer, and more impactful for TFA survivors.

2 Background

To begin, we provide background information on technology-facilitated abuse (TFA), clinical computer security interventions for TFA, documenting TFA, and challenges to documenting TFA.

2.1 Technology-Facilitated Abuse

TFA refers to the use of digital technology to exercise control [55, 59, 78, 109]. It is an umbrella term encompassing behaviors like image-based sexual abuse [36, 37, 44, 65, 65–68, 82, 83], device and account compromise [75, 78], surveillance with spying applications [35, 46, 89] or smart devices [45, 76, 81, 94, 98, 99, 103], harassment and impersonation [78, 104], and financial abuse [33, 38, 39, 42]. Unfortunately, TFA is common in today's digital environment. A recent survey found that one in two respondents had experienced online abuse [104], and SPARC reported that at least one in four women in the U.S. have been stalked using technology [12].

[1] Sherloc = **S**oftware to **H**elp with **E**vidence **R**etrieval and **L**og **O**nline **C**yberabuse.

Our design inquiry focuses on TFA in intimate partner violence (IPV). IPV is estimated to affect nearly one in three women globally [10] and nearly half of U.S. residents [74]. Although IPV can happen to anyone, it disproportionately affects women, LGBTQ+ people, and people of color [10, 47, 88, 95]. Often, a large component of IPV is *coercive control*: a pattern of behavior (including physical, sexual, or psychological abuse) meant to exert power and control over survivors [97]. Digital technologies are one mechanism that abusers use to extend coercive control in IPV [55, 59, 62, 78].

2.2 Clinical Computer Security Interventions

To address TFA in IPV, Havron et al. [64] proposed the *clinical computer security* model. This model introduces *tech clinics*, where trained *technology consultants* provide trauma-informed TFA support in *consultations* with survivors of IPV (referred to as *clients*). The original tech clinic is in New York, U.S., and continues to evolve with ongoing research [2, 85, 106, 108]. To our knowledge, there are now three additional tech clinics in Washington, U.S. [50–52], Wisconsin, U.S. [24], and British Columbia, Canada [7].

Tech clinics often follow an Understand–Investigate–Advise model [64]. After learning about a client's technological concerns and priorities, a tech consultant investigates the client's digital devices and online accounts to identify potential compromise. Most investigations are done manually, but multiple clinics also use a tool called ISDi (IPV Spyware Discovery) [64] to scan clients' devices for malicious apps. Finally, tech consultants advise the client on actions that could mitigate TFA, noting any potential safety implications.

2.3 Documenting Technology-Facilitated Abuse

There are many reasons survivors of TFA might want to document that abuse. Documentation could be helpful in legal proceedings like restraining order hearings or custody and placement decisions, which survivors often undertake [59, 64, 100]. They may want to post evidence the abuse publicly to shame the abuser and warn others [102]. More broadly, documenting abuse may help survivors validate their experiences, since TFA is often invisible or ignored [57, 61, 64, 93]. Broadly, documentation can be a part of survivors' healing process.

It is useful to consider the necessary steps to documenting TFA. Generally, evidence documentation follows five stages: Identification (identifying abuse and sources of data), Collection (gathering the data), Examination (filtering relevant information), Analysis (drawing conclusions from data), and Reporting (presenting findings) [53, 70], as shown in Fig. 1.

Survivors face many challenges when attempting to document TFA. For example, evidence may not exist at all [100] or may disappear or be deleted from platforms [58, 59, 87, 100]. Collecting evidence is burdensome, as it may involve hundreds of screenshots [59, 100] or deeply traumatizing content such as non-consensual intimate images [59, 78, 100]. Proving an abuser is the one perpetrating TFA can be fruitless, and platforms provide little help to de-anonymize abusers [59, 66, 100]. Finally, TFA is not specifically included in most legal statutes, leaving it up to judges—who may have limited knowledge of tech, abuse, and TFA—to decide whether evidence of TFA meets the burden of

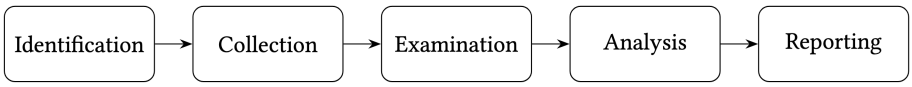


Figure 1: Steps to document evidence of tech abuse, from NIST [70] and Darrington [53].

proof [57, 59, 100].

3 Related Work

We now review existing tools for documenting TFA and identify limitations of these tools. We then introduce trauma-informed computing, our grounding framework, and discuss related work implementing a trauma-informed lens.

3.1 Existing Tools for Documenting TFA

While screenshots remain the state-of-the-art for documenting TFA [59, 100], various tools evidence documentation, TFA investigation, and evidence storage.

3.1.1 Most relevant: Tools meant for documenting TFA. There are three academic works that aim to help survivors document TFA. These works' designs were greatly informed by engagement with the affected communities.

First, Goyal et al. [60] prototyped a harassment documentation tool for female journalists. Their design aggregates data from multiple social media accounts, enabling journalists to compile evidence of harassment, analyze the data, and create a shareable report. The design uniquely enables survivors of abuse to identify, collect, examine, analyze, and report evidence of harassment in one application—an idea we draw on in this work.

Two additional tools aim to create "communities of accountability" [43, p. 5] by helping survivors share their experiences of TFA with online support networks. One, Unmochon [102], is a tool to capture, authenticate, and share screenshots of harassing Facebook Messenger threads. Creators Sultana et al. incorporated an authentication mechanism for screenshots, which works by comparing the Facebook account number reported by the user and the account number collected from the URL of the captured page.[2]

Similarly, Hate and Hope Tracker [16] (formerly HeartMob) is a private online community where survivors can record stories of online (or offline) harassment and community members can provide support. Survivors can submit text descriptions as well as screenshots or additional documentation of the abuse. Research focused on HeartMob [43] and its predecessor, Hollaback! [54], found that these tools substantially helped harassment survivors validate and understand their experiences in the context of the supportive community.

3.1.2 Tools to facilitate TFA investigations. A number of tools exist to help survivors investigate their devices for evidence of TFA, with a potential secondary use case of documentation.

Three tools—TinyCheck [8], ISDi [64], and WARNE [77]—were designed to help survivors of IPV identify stalkerware on their devices. TinyCheck, developed by Kaspersky, uses a Raspberry Pi to scan device traffic and identify interactions with known stalkerware-related sources. ISDi scans the list of apps on a mobile device and uses a list of known stalkerware, plus natural language heuristics, to identify potentially suspicious apps. While TinyCheck and ISDi are designed to be subtle and undetectable to an abuser, WARNE exploits vulnerabilities in spyware apps to gather information about abusers' account credentials, which they note "could raise an abuser's suspicion" [77, p. 8].

Sophisticated forensic tools can also help investigators identify, and potentially document, broader forms of TFA. As summarized by Shute et al. [92], forensic tools range from data aggregators, which scrape public websites for data related to an investigation [22, 23]; tools such as Cellebrite [19] that extract and analyze data from malicious devices; tip lines to gather information from the public [3, 21]; network capture tools [6]; tools for screen capturing websites [30]; systems to extract data from cloud-based storage [32]; and tools to help search through large volumes of evidence [31]. Law enforcement can also supplement social media investigations by reaching out to platforms for data preservation. These tools are generally unavailable for use by independent individuals.

3.1.3 Co-parenting applications. OurFamilyWizard [26] and CoTrackPro [20] are co-parenting apps with documentation capabilities. Both apps have messaging features that keep a detailed, court-admissible record of in-app conversations between co-parents. Additionally, CoTrackPro promotes sub-applications that detect and document cyberbullying (its "Cyber" app) and help parents document custody violations (its "Legal" app).[3]

3.1.4 Evidence storage applications for abuse survivors. Finally, there are several available applications that broadly help abuse survivors *store* evidence of abuse, which might include TFA. Survivor-facing apps Bright Sky U.S. [13], SafeYou [29], Document The Abuse [4], and VictimsVoice [18] provide survivors with a place to store journal entries, audio, photos, and/or videos that capture their experiences. Some of these apps allow survivors to share evidence with trusted contacts [18, 29] or law enforcement [4, 18], and two are built with legal admissibility in mind [4, 18]. As an analog alternative, NNEDV offers printable technology abuse logs for survivors to fill out [17].

In academia, Cho et al. [49] defined a digital evidence framework for survivors of IPV ("DEF-IPV"). Through interviews with advocates, they identified three requirements for digital evidence collection: invisibility, anti-leakage, and continuity. They then proposed an app, disguised as a calculator, which uses encryption, steganography, and access controls to allow survivors to securely

[2]Despite the goals of this authentication feature, we note that the method would not prevent a user from creating harassing threads from a faked account.

[3]At the time of writing CoTrackPro appears to be pre-release—all apps are listed as "Coming soon."

log abuse incidents. To our knowledge, the design is a prototype only and is not available to survivors.

3.2 Limitations of Existing Tools

Despite the breadth of available tools that could support documenting TFA, there are several limitations of these tools that hinder their usefulness to survivors.

3.2.1 Limited support for evidence identification, examination, and analysis. One key limitation of existing documentation tools is that they do not facilitate all steps in the evidence collection process (Fig. 1). These tools help survivors *collect* and occasionally *report* evidence, but leave survivors with the burden of *identifying*, *examining*, and *analyzing* the evidence. Identifying evidence of TFA is non-trivial, as survivors may not even realize they are being surveilled, much less know how to prove it [100]. Further, examining and analyzing evidence requires technical expertise, including the ability to express conclusions with precision and detail.

3.2.2 Quality of documentation. On the other hand are the tools that facilitate TFA investigations (Section 3.1.2). Although investigation capabilities are important, these tools do not robustly support survivors in *reporting* so they can leverage that evidence for healing (e.g., share with online support networks, or use toward a court case). Ideally, documentation tools would support survivors in all five stages of evidence collection.

3.2.3 Limitations in scope. Four tools—CoTrackPro [20], OurFamilyWizard [26], Unmochon [102], and Goyal et al.'s tool for journalists [60]—provide support for all stages of evidence collection. However, they collect only certain types of evidence of TFA and/or support only one way for survivors to use the evidence. For instance, CoTrackPro and OurFamilyWizard can only capture evidence of harassing in-app message or custody violations, and Goyal et al.'s proposal is specifically for harassment on social media. Unmochon only captures evidence of harassment over Facebook Messenger and only allows survivors to post the evidence of the harassment on a Facebook Group. There is a need for documentation tools that cover a wider range of TFA and support a variety of use cases for the evidence.

3.2.4 Legal robustness. One use case that is under-considered by existing tools is the use of evidence for legal proceedings. While some of these tools are designed with legal robustness in mind [4, 18], it is difficult to find information on how the evidence has been received in real-world legal proceedings. SafeYou [29] and WARNE [77] can share data directly with law enforcement, but make no claims about whether that evidence will be legally admissible. Several tools [13, 60, 102] make no claims about admissibility. Even some forensic tools "may be difficult to defend in court" [92, p. 20]. For survivors who want to use evidence in court, these documentation tools may not be sufficient.

3.2.5 Availability. The final limitation of existing tools is availability. Forensic tools often require significant resources or explicit connections to law enforcement agencies, making them inaccessible to many survivors [92, 100]. TinyCheck [8] and ISDi [64] are open-source, but are not recommended for use by individual survivors (nor are they designed for this use case). Academic works like Unmochon [102], WARNE [77], and Goyal et al.'s proposal for journalists [60] are not publicly available to survivors. And an accessibility issue exists with survivor-facing apps, too. Since the start of this project, three survivor-facing evidence collection apps—Arc [9], HeHop [11], and NNEDV's DocuSAFE [14]—are no longer usable, indicating a maintainability problem plagues survivor-facing apps for documenting TFA.

In summary. There is a need for TFA documentation tools that enable collecting, identifying, examining, analyzing *and* reporting evidence; that have the flexibility to document a variety of forms of TFA; that support multiple use cases for the evidence, including use in legal proceedings; and that are readily-available to survivors. Designing such a tool is one of the main contributions of this work.

3.3 Trauma-Informed Design Approaches

Through the design of a novel digital evidence collection tool for TFA survivors, we aim to answer a broader question: how *should* frameworks for digital evidence collection be designed? Inspired by prior work, we propose a trauma-informed approach for designing digital evidence collection frameworks.

3.3.1 Trauma-informed computing. Trauma-informed computing is defined by Chen et al. as "an ongoing commitment to improving the design, development, deployment, and support of digital technologies by explicitly acknowledging trauma and its impact, recognizing that digital technologies can both cause and exacerbate trauma, and actively seeking out ways to avoid technology-related trauma and retraumatization" [48, p. 7]. In brief, trauma-informed computing encompasses six key principles: safety, trust, peer support, collaboration, enablement, and intersectionality.

A number of researchers in HCI, digital safety, and family violence digital safety have emphasized the importance of using trauma-informed lenses in research with at-risk groups like survivors of abuse [40, 41, 73], and specifically in the realm of digital evidence collection [78, 84]. For instance, Rajan et al. argued that when designing incident logging tools for sexual violence, "A trauma-informed technical design with data privacy at its core is essential" [84, p. 4]. In one of the first HCI papers studying TFA, Matthews et al. called for technological methods "balancing the need to capture digital evidence of abuse while minimizing emotional trauma" [78, p. 2198].

3.3.2 Prior HCI work leveraging a trauma-informed approach. Despite calls for using trauma-informed lenses in the realm of digital evidence, to our knowledge, no academic work has taken on the challenge. However, a trauma-informed approach has been successfully operationalized in the context of abuse and violence.

For example, trauma-informed approaches have been applied in design studies related to sex and sexual violence. In their aforementioned study, Zheng and Walquist et al. [110] designed Ube, a data donation platform for sexual experiences related to online dating. Ahmed et al. [34] used trauma-informed principles to envision sociotechnical interventions for people affected by forced marriage. Outside of academia, the tool MediCapt [25]—designed to capture and securely share forensic medical evidence of sexual violence—was designed using trauma-informed co-design methods [69]. Researchers have also applied trauma-informed approaches to other

topics, like content moderation [91] and algorithmic influences in the child welfare system [90].

Most relevant to this study, though, is a suite of prior work addressing TFA with a trauma-informed lens. Specifically, a number of works used trauma-informed lenses to study and extend tech clinic interventions for survivors of TFA in IPV [64]. For instance, Ramjit and colleagues studied traumatic stress within tech clinic consultations [86] and designed methods for trauma-informed coordination between tech clinics and advocacy partners [85]. Other related works include the paper that introduced tech clinics [64], a project examining remote tech clinic services during the pandemic [107], and a study on TFA in human trafficking and the potential adaptation of tech clinics for this context [101]. Adding to these works, we explore *trauma-informed digital evidence collection* via a design inquiry situated within IPV tech clinic interventions. Through the lens of trauma-informed computing, we aim to design an evidence collection tool that addresses the limitations of existing documentation tools.

4 Designing an Evidence Collection Tool for Technology-Facilitated Abuse

In this work, we conducted a design inquiry [111] in the context of TFA in IPV. Our goal was to design a tool to help survivors of TFA document the abuse in a legally-admissible format. This section reviews our positionality and motivation for this design, our trauma-informed design process, and the design requirements we defined for our evidence collection tool.

4.1 Positionality and Design Motivation

Two authors are women and four are men. The authors represent South Asian, Chinese, Arabic, and White racial/ethnic backgrounds. The lead author and interviewer (Section 6.1) is a White woman, like most of the legal support providers we interviewed. Five of six authors are associated with a Computer Sciences department at an academic research institution; the remaining author is an attorney.

Perhaps more importantly, all authors have experience directly serving survivors of TFA. Five authors volunteer with the Madison Tech Clinic and have collectively helped nearly 100 survivors uncover and mitigate TFA on their devices or accounts. Three of these authors also form the core leadership team of the Madison Tech Clinic. The remaining author, K.C., is an attorney who has supported survivors of TFA in various legal proceedings, and who has previously referred clients to the Madison Tech Clinic. The motivation for this study is, in large part, born from interactions with Madison Tech Clinic clients who sought evidence of their experiences with TFA, but did not have sufficient tools to help them document them.

Given our embeddedness in the Madison Tech Clinic, it was impossible for us to ignore the tech clinic's potential to facilitate evidence documentation without adding to survivors' burden. Tech clinic consultants often find indicators of compromise during appointments, such as suspicious account logins, recovery contact information set to the abuser's contact information, or tracking apps installed on their devices; documenting these findings robustly is a natural next step. We also recognized that our deep connections with the tech clinic would help us roll out our tool quickly—providing earlier benefits for survivors—and would support our goal of a highly-engaged pilot program. Finally, we saw that anchoring evidence collection within the tech clinic would promote long-term sustainability—something that has eluded previous tools for documenting TFA.

Furthermore, we observed that a tech-clinic-based evidence collection tool would be inherently aligned with trauma-informed principles. For example, tech clinics support *trust* because they partner with existing victim service providers for referral and service provision. Similarly, in-person consultations are typically held at a victim service provider, a physically and emotionally *safe* space. Tech clinic consultations also foster *collaboration* and *enablement*: tech consultants work together with survivors to investigate technology and safety plan, and ultimately survivors choose what to do with the information they learn in the consultation (and, now, the evidence generated in that consultation). And tech clinic consultants, and advocates from partnering victim service providers, are trained in trauma-informed care.

Therefore, echoing calls from prior work [64, 100], we chose to design an evidence collection procedure situated within tech clinic consultations. We envisioned a tool that would allow tech consultants to document all investigations from the consultation in a standardized format, which would then be handed off to the client to use as they wish. In designing this tool, we therefore focused on documenting the types of TFA that are handled in the tech clinic, leaving other forms of TFA—such as harassment via text messages—for future work.

The next several sections describe the design and evaluation of our evidence collection tool, which we call Sherloc.

Table 1: Overview of our four-stage design process.

Stage	Design Activities	Section
Stage 1	**Identifying design requirements** informed by proxies, prior work, trauma-informed principles, and our experiences.	§ 4.3
Stage 2	**Design of an initial prototype** that best meets our design requirements.	§ 5
Stage 3	**Feedback sessions with proxies** to minimize risk and maximize benefit to survivors, followed by design updates.	§ 6
Stage 4	**Iterative, long-term pilot program** within an existing tech clinic.	§ 7

4.2 Trauma-Informed Design Process

Our design involved four key stages, depicted in Table 1. In short, we identified trauma-informed design requirements (Section 4.3), designed an initial prototype (Section 5), conducted extensive feedback sessions with proxies (Section 6), and finally embarked on a long-term pilot program within an existing tech clinic (Section 7).

This trauma-informed design process was inspired by four prior works: Chen et al. [48] and Zheng and Walquist et al. [110], who discussed how to do trauma-informed research in HCI, and papers

from Bellini et al. [40] and Bhalerao et al. [41] regarding safe computer security research with at-risk populations. We incorporated several of their suggestions into our methodology. For example, the first stage of our research aimed to define design requirements that adhere to trauma-informed principles [110]. By relying on proxies in the formulation of these design requirements, as well as first-round feedback, we minimized the risks to survivors of TFA at this stage while gaining rich insights from legal experts, including many people who directly support survivors [40, 41, 48, 110]. We also assessed existing applications to help identify design requirements [110] (Section 3.1).

4.3 Design Requirements

The first stage in our design process was to identify requirements for Sherloc. To begin, we reviewed the existing tools that could be used for documenting TFA and their limitations (Section 3.1). We observed that the key limitations of existing tools are all related to **(i) survivor enablement**: the tools do not properly enable survivors to identify, collect, examine, analyze, *and* report varied forms of TFA, nor do they enable survivors to use evidence flexibly depending on their needs. Thus, our primary design goal was to build a tool that supports survivor enablement.

To support survivor enablement, we want to build a tool that supports flexible use cases for evidence of TFA. One common use case is as evidence in legal proceedings, meaning that a truly flexible design must consider legal admissibility and effectiveness to enable legal use cases. This observation led us to our second high-level goal, **(ii) legal robustness**.

4.3.1 Design requirements to support survivor enablement. Next, we defined specific design requirements that would support our high-level goals. To define these requirements, we reviewed Chen. et al's suggestions related to survivor enablement [48] and reviewed prior work on this topic, particularly Stephenson et al.'s work on the barriers survivors face when using legal evidence of TFA [100]. We also relied on our experiences interacting with survivors of TFA to inform these requirements. In all, we defined six requirements to support survivor enablement:

(1) **Privacy-Preserving**: The tool, and the evidence produced by the tool, should not cause any additional risk to the survivors' privacy. The evidence produced by the tool may be used in public court proceedings and therefore viewed by an abuser; thus, privacy leaks could harm a survivor's safety.
(2) **Clear**: The evidence produced by the tool should be easy-to-understand for a wide range of viewers, including survivors, judges, lawyers, advocates, with varying technical expertise.
(3) **Concise**: The evidence produced by the tool should be as brief as possible, while still meeting other requirements. Large volumes of evidence may not be possible to review in shorter proceedings such as restraining orders (which are sometimes capped at 30 minutes [100]).
(4) **Safety-Enhancing**: The tool, and the evidence produced by the tool, should help survivors enhance their digital and/or physical safety in some way. It should not detract from survivors' experiences in the tech clinic consultation, which is often an important place for survivors to seek safety and healing.
(5) **Reassuring**: The tool, and the evidence produced by the tool, should provide reassurance to survivors regardless of whether any compromise was found using the tool.
(6) **Maintainable**: The tool should be designed in a manner that supports its continued use and accessibility to survivors.

4.3.2 Design requirements to support legal robustness. Secondly, we defined requirements to support legal robustness. To generate these requirements, we held discussions with legal experts to understand the broad requirements for evidence to be used in legal proceedings. We also reviewed legal statutes for Wisconsin. This research led us to six requirements for legal robustness:

(1) **Accurate**: The tool must provide an accurate representation of the survivor's devices and accounts at the time of the consultation. It must "support a finding that the item is what the proponent claims it is" [28].
(2) **Legally-Relevant**: The evidence produced by the tool must be relevant, meaning it "has any tendency to make a fact more or less probable than it would be without the evidence" and "the fact is of consequence in determining the action" [27]. Specifically, it must connect to the relevant legal statutes, and it should (as much as possible) provide some evidence connecting the abuse to the abuser.
(3) **Authentic**: It must also be able to be argued that the evidence has not been modified or tampered with since creation.
(4) **Trustworthy**: The evidence produced by the tool must be trustworthy, with a good reputation and evidence to back up its robustness. Judges and other legal decisionmakers are more likely to admit evidence that comes from a source they trust [100].
(5) **Properly-Formatted**: The evidence produced by the tool must be formatted in a way that is admissible in a variety of courts, or it may be rejected.
(6) **Complete**: The evidence produced by the tool must not omit any key contextual information that is necessary to understand the information presented, or it may be challenged by opposing attorneys.

We used these requirements to guide the design of the tool and its evaluation (Sections 5–7).

5 Sherloc: An Evidence-Collection Framework for Survivors of TFA

Toward our goals, we designed Sherloc, an evidentiary framework encompassing all of the five steps of evidence collection [53, 70]. Sherloc is a Python program with a Flask [80]-based user interface that runs on a designated clinic laptop. It is designed to be used during a tech clinic consultation and run primarily by the tech clinic consultant, in close collaboration with the client. The code for Sherloc is open-sourced on GitHub.[4]

Sherloc has two primary components: **investigation**, encompassing the Identification, Collection, and Examination steps of ICEAR (Section 5.1) and **documentation**, which enacts the Analysis and Reporting steps of ICEAR (Section 5.2). In short, Sherloc facilitates and captures data from the investigations that happen during the consult, then compiles the data into an investigation

[4] https://github.com/sophiestephenson/sherloc

report. Sherloc is designed to capture both technical details and survivors' experiences in one cohesive report, providing context and illustrating the impact of the TFA captured.

Some components were added after we sought feedback from legal experts (Section 6). Table 4 in the Appendix summarizes the updates made in each iteration of Sherloc. The key additions at this stage were (1) a page capturing responses to a technology assessment questionnaire and (2) automated explanations of the types of risks identified during the consultation. We note updates with `Update #`.

5.1 Investigation Components

Sherloc supports the main investigation steps that are typically followed during a consultation. These steps include a technology assessment questionnaire, or TAQ (which helps us assess technology risks); scanning the client's devices for malicious apps or rooting; and performing account security investigations.

5.1.1 Technology assessment questionnaire (`Update 1.1`). Usually, consultations begin by taking a client through the TAQ, adapted from Havron et al. [64]. This questionnaire is meant to assess the client's technology use and the different risks the technology consultants should consider in an investigation. For instance, the TAQ asks whether the person of concern has ever had physical access to the client's technological devices. Sherloc's TAQ page, shown in Fig. 4, contains several dropdown sections containing questions from the TAQ. At any point, the consultant can save the TAQ responses and return to the home page.

5.1.2 Device scanning with ISDi. Often, the next step of a consultation is scanning the client's devices. Sherloc's scanning functionality comes from the IPV Spyware Discovery (ISDi) tool,[5] another Python program used in tech clinics since 2018 [64]. To initiate a scan, the consultant plugs in the client's device and asks the client to unlock it. Sherloc then details the apps installed on the device and an assessment of whether the device is jailbroken. Apps may be accompanied by tags, such as "system-app", "dual-use",[6] or "spyware." The consultant and the client discuss this list and select apps to investigate further.

The last phase of the scan is the investigation page, which displays each app selected for investigation. For each selected app, Sherloc shows all known details about the app, then prompts the consultant to answer questions about the app's installation and data sharing behaviors. The client and consultant can enter open notes about each app for additional context, and the consultant can also take a screenshot from the device.

5.1.3 Manual device investigations. We learned from Madison Tech Clinic partners that an ISDi scan is not always possible. This could be due to tampering with the device, or more mundane issues like the device OS being too out of date. If the scan fails, Sherloc enables consultants to enter details from a manual investigation of the device. Consultants can enter details like the device manufacturer, model, version, and serial number (or UDID) and then record their assessment of whether the device is jailbroken and why. Finally, the consultant can add the names of any apps they find suspicious, then record investigations of these apps as they would in a normal ISDi scan. When the information from the scan is saved, it is labeled as a manually-inputted scan.

5.1.4 Account investigations. The third, and often most important, piece of consultations is account security checkups. Sherloc guides consultants through these checks in a dedicated account investigation page. After entering the platform and username of the account they are investigating, the consultant and the client can go through several groups of questions to investigate the account for compromise. If relevant, the consultant can add screenshots from the client's device or leave overall notes about an account.

5.1.5 Home page. Consultants can navigate through these various investigative steps from the home page, shown in Fig. 3. The home page has buttons to add new investigations in any order, edit previous investigations, and view or delete any screenshots taken so far. The home page is also where consultants and clients can enter notes on the overall consultation.

5.2 Creation of an Investigation Report

The second key function of Sherloc is documentation: compiling the findings of the consultation to create a comprehensive investigation report. To do this, consultants simply enter the name their client wants to put on the document, then click a button to generate the report PDF, which will open in the browser when ready. In practice, we print this document for the client because printed evidence is most likely to be accepted in every court (Section 7). Appendix **??** shows examples of some of the pages of an investigation report.

5.2.1 Report structure. The report has three main parts, starting with a cover page. The cover page titles the document as "Investigation Report: Prepared by the Madison Tech Clinic" and includes the tech clinic logo and the UW–Madison logo. It lists the client name as they entered it and the timestamp indicating when the report was generated. Finally, it includes a paragraph describing this project: "This report describes the findings of a Madison Tech Clinic consultation. The report was created using Sherloc [version], an investigative tool developed by the Madison Tech Clinic. Source code for Sherloc is available at [url]. Please see [clinic website] or contact [clinic email] for more information about the Madison Tech Clinic, Sherloc, or this report." At the bottom is a space for the lead consultant to sign the investigation report (`Update 1.6`).

After the cover page is a summary page which highlights the main actions and findings from the investigation. It details any concerns found through the TAQ; the devices scanned, and if any rooting or malicious devices were identified; and the accounts investigated along with any compromise that was identified. The summary page also shows the overall notes on the consultation inputted by the consultant and the client. On this page, and going forward, we label data either as "human-entered" or "system-captured" to differentiate the two data sources.

The rest of the report details each investigation performed. First, it outlines all questions of the TAQ along with the client's responses. Then, it shows each scan performed, detailing the device nickname,

[5] https://github.com/stopipv/isdi

[6] The term "dual-use" refers to apps that are intended for a benign purpose, but are known to be repurposed by abusers for surveillance [46].

manufacturer, model, version, serial or UDID, along with assessments of whether the device is rooted. For each app that was investigated, the report details all information collected about that app and shows the responses to the questionnaires about the app's installation and data leakage. Finally, it displays all of the questions and responses for each account investigation.

Screenshots are also included throughout the report, placed immediately after the relevant data. Alongside each screenshot is simple metadata: the file size, modify date, access date, and file type.

5.2.2 Automated descriptions of risks (`Update 1.2` *).* To help with interpretability, peppered throughout the report are automated descriptions of the risks that were identified. For example, say that a client indicates that the person of concern has physical access to their devices. Sherloc would generate and show an associated risk called "Physical access to devices" with the description "A person with physical access to devices might be able to install apps, adjust device configurations, and access or manipulate accounts logged in on that device."

The potential risks, their descriptions, and the data that indicates each risk are pre-defined. To define them, we went through each question in the TAQ and account investigations, along with the different potential results of a device scan, and identified which answers or scan results indicate different kinds of risks. For example, consider the aforementioned risk from physical access to devices. In the TAQ, one can identify a risk from physical access to devices if the client responds affirmatively to any of the following questions: "Do you live with the person of concern?"; "Did the person of concern purchase and/or set up any of your devices?"; and "Has the person of concern had physical access to your devices at any point in time?" Similar logic is written for all risks we could identify.

When the consultant initiates the generation of a report, Sherloc uses this predefined logic to identify and inject risks into the report. The risks are highlighted in yellow and accompanied by a warning icon. These risks are shown both on the summary page and in the detailed findings from each investigation performed, as shown in Fig. 6 and Fig. 7.

5.3 Implementation of Sherloc

As previously mentioned, Sherloc is a locally-run Flask application written in Python. To scan devices for spyware and jailbreaking, Sherloc builds on ISDi. ISDi relies on Android Debug Bridge (`adb`) [1] for Android devices and `pymobiledevice3` [56] for iOS devices. At a high level, these packages enable Sherloc to communicate with the phone and gather information about installed apps and other data relevant to assessing jailbreaking. Then, Sherloc analyzes this data to determine malicious apps and look for evidence of jailbreaking. Please refer to Havron et al. [64] for more details on how ISDi performs device scans. We assume that ISDi is reliable and rely on prior work for the accuracy of the implementation. We note that ISDi has been successfully used in tech clinics (including Madison Tech Clinic) for years.

Sherloc enables consultants to easily take a screenshot on the client's device and save it as a file on the computer running Sherloc. For Android devices, we use `adb`'s `screencap` command; for iOS devices, we use the `screenshot` command from `pymobiledevice3`. This method of screenshotting on iOS devices requires the device to be in Developer Mode and Sherloc to be run using `sudo`. When creating the report, we gather screenshot metadata using `exiftool` [63].

Data from the consults is stored temporarily in JSON files in the project directory. We use the `FileLock` [105] package to prevent race conditions during file access. The report is generated using `pdfkit` [96] and `wkhtmltopdf` [72]. Sherloc compiles the consultation data and enters it into an HTML template. Then, `pdfkit` creates a PDF from the resulting HTML.

5.4 Operational Details and Limitations

We designed Sherloc for use inside the Madison Tech Clinic.

5.4.1 Data storage. Madison Tech Clinic is not protected from subpoena. Therefore, to protect clients from unwanted disclosure of their data, we do not retain any information about consultations or clients. All data, including generated reports, is deleted manually after every consultation. We make it clear to survivors that the printed report we give them is the only copy of the report that will persist. The only data we keep from consultations is research data, which includes survey responses and manually anonymized consultant notes (Section 7).

5.4.2 Reliability and legal considerations. It is possible that an error in Sherloc could prevent clients from benefiting from the system. A main concern is that the ISDi scan could (i) fail or (ii) miss a spyware app installed on a device. Since the rest of the data captured by Sherloc is human-entered, the other source of error is human error.

In the event that Sherloc fails, tech clinic consultants can simply revert to the original consultation procedure; clients would miss out on Sherloc, but would still receive tech clinic services. If any legal concerns become relevant, Madison Tech Clinic relies on its partner victim service providers to handle that legal liability.

5.4.3 Accessibility. Sherloc is written in English and generates English investigation reports. Madison Tech Clinic does not typically support languages other than English, requiring external language services to assist clients in other languages. This limits Sherloc's accessibility for some survivors and we plan to offer multiple languages in future versions of Sherloc.

6 Evaluation With Legal Experts

Once we had designed an initial prototype of Sherloc, we sought feedback from legal experts in Wisconsin. In this early stage of evaluation, the legal experts served as proxies to minimize the risks to survivors [40]. Our goal was twofold: (i) to understand the feasibility of Sherloc's success in legal settings, and (ii) to ensure Sherloc minimizes harm to survivors. Toward these goals, we first held feedback sessions with legal support providers (Section 6.1). Then, we used surveys to solicit additional feedback from judges (Section 6.2). Both efforts were approved by our Institutional Review Board (IRB).

6.1 Sessions with Legal Support Providers

First, we held feedback sessions with 19 legal support providers who help survivors of TFA prepare for their legal endeavors. We were interested in their feedback since they could provide insight

Table 2: Aggregate demographics for the 41 legal experts who gave us feedback on Sherloc. The experts may fall into multiple categories for roles and race/ethnicity. Six participating experts (one from the feedback sessions, five from the surveys) chose not to fill out our demographic form.

	Role(s)		Age		Gender		Race/Ethnicity	
Feedback Sessions	Madison Tech Clinic partner	10	18-24 years	3	Woman	16	White	16
	Program lead	8	25-34 years	6	Man	2	Asian	2
	Legal advocate	5	35-44 years	5			Black or African American	1
	Attorney	4	45-54 years	2				
	Law clinician	4	55-64 years	2				
	Judge	1						
	Police officer	1						
	Sexual assault nurse examiner	1						
Surveys	Judge	22	35-44 years	2	Man	9	White	16
			45-54 years	5	Woman	6	Asian	1
			55-64 years	7			Other	1
			65-74 years	3				

into both the legal aspects of our work and the survivor-safety considerations.

We offered both individual interviews (N=9) and focus groups made up of people from the same organization (N=3). The sessions were held between November 2024 and March 2025. Two focus groups occurred in-person at the participants' organization, with the rest of the sessions over Zoom.

6.1.1 Recruitment. We recruited legal support providers mainly through direct contact, often leveraging existing connections. We also shared a recruitment notice on a statewide advocacy email list and posted fliers in public places. We offered legal support providers $20 for participating. To participate, they had to be at least 18 years old and be living and working in Wisconsin.

In this phase, we spoke with 19 legal support providers (Table 2). Their roles included program leadership, legal advocates, attorneys, and law clinicians, as well as one judge, one police officer, and one sexual assault nurse examiner. They work at 12 different organizations in 9 counties of Wisconsin. 10 out of 19 legal support providers work with Madison Tech Clinic, the tech clinic for which we designed Sherloc. Most of the participants are White women.

6.1.2 Session procedures. We first shared the consent form and asked for consent to participate. We also asked if we could audio-record each session, to which all agreed. Then, we explained Sherloc and provided a simulated demo. Specifically, we showed images of Sherloc's user interface, described the steps of using Sherloc, and provided a sample investigation report that Sherloc might produce. Then, we assessed what they liked about our idea, what they found concerning, and their suggestions for updates.

6.1.3 Data analysis. After each session, the first author listened to the recording and cleaned the auto-generated transcript, fixing errors and removing any potentially identifying information (such as locations). She then uploaded the transcript to a secure repository accessible only to the researchers and deleted the audio recording.

To analyze the data, we began using deductive structural coding. We were interested in three structural codes: (i) ways they envision clients might use the evidence we produce; (ii) positive comments about Sherloc; and (iii) concerns and constructive feedback. After familiarizing themselves with the data, five authors collaborated to define the structural codes and apply them to the session transcripts. At least two authors coded each transcript.

Then, the first author combed through each structural code to inductively generate sub-codes. For instance, the concerns structural code (the richest in our data) yielded sub-codes like interpretability, the weight of the evidence, and expert witnessing. The subsections in Section 6.3 map to the subcodes we generated.

6.2 Feedback Survey for Judges

Next, we sought feedback from one specific type of legal support provider: judges. Judges can provide particularly valuable insight given that they would be the people interpreting the evidence Sherloc creates. However, they are also very busy and difficult to recruit for studies. Although we were able to interview one judge in the previous sessions, we undertook an additional effort to get judges' feedback on our proposal.

6.2.1 Recruitment. In September and October 2025, we collaborated with the Office of Court Operations in Wisconsin to provide three judges' trainings on evidence of TFA.[7] We leveraged this opportunity to recruit the judges to give feedback on Sherloc. At the end of each 75-minute training, we took 10 minutes to describe Sherloc, providing the judges with a printed example of an investigation report generated by Sherloc. Then, we invited them to take a survey about the tool, either on paper or online using Qualtrics.

In all, 22 judges took our survey (Table 2). They were primarily White men between the ages of 45 and 64.

6.2.2 Survey materials. The survey exclusively focused on the investigation report, as this is the part of Sherloc that the judges would eventually come into contact with. The survey is similar to ones we would end up using in our pilot program (Section 7).

[7]Readers may notice that these trainings began one month after we started our pilot program. After receiving feedback from the legal support providers, we felt the tool had been vetted enough that it was safe to pilot before getting this additional feedback from judges.

We began by asking about the judges' broad impressions of the investigation report. Then, we had them evaluate the document according to our design requirements (Section 4.3) on five-point Likert scales with an "I don't know" option. We omit the Maintainable requirement, which is not relevant to Sherloc users.

6.2.3 Data analysis. We used descriptive statistics to synthesize the judges' Likert scale ratings for each of our design requirements. Additionally, the first author coded all (brief) qualitative responses using the codebook from the legal support provider sessions (Section 6.1).

6.3 Findings from Expert Feedback

Here, we synthesize findings from a total of 41 legal experts (LE-01—LE-41). We made several changes to Sherloc's design to account for their feedback, summarized in Table 4.

6.3.1 Broadly positive response. In general, the legal experts thought our proposal was "*very well done*" (LE-25). In our survey results, judges on average ranked the investigation report as at least "Moderately" meeting all of our design requirements. We'd like to highlight the following quotes:

> *If a client walked out of a tech clinic appointment with something like this, that was an automatic paper documentation of the TFA that they've experienced, I could see that carrying a lot of weight. (LE-04)*

> *Well, this is awesome, first of all...I think there's tremendous value in it.. I think it's protective, and also, it could lead to the ability to the client to actually get evidence in front of the court, too. (LE-19)*

> *It seems more than appropriate for what we see in our injunction cases. (LE-27)*

The legal experts spoke of the potential for Sherloc to help clients "*better provide educated testimony*" (LE-19) and to give support providers a starting point for further investigation. LE-13, a police officer, agreed "*That's good evidence. It gives you your basis to stand on.*" They also emphasized the value of Sherloc to help survivors find safety in whatever way they choose:

> *A person who's not involved in a court case wanting to know if their partner is doing this, and walking away with that, like, it's just as much of a useful document....So it's to the benefit of the user, and to the benefit of the judge if it is being used as evidence. (LE-12)*

6.3.2 Credibility and expert testimony. While overall positive about Sherloc, legal experts cautioned that expert testimony may be required to explain "*Why this is legit, what does it say*" (LE-02). Judge LE-24 believed, "*This would not be admitted in court without testimony from the author,*" noting that without expert testimony the report is "Not at all" authentic or trustworthy.

One reason for expert testimony is that Sherloc is not (yet) widely known—"*this would be such a new tool for many judges to think about that you'd still need a person to explain it at the end of the day*" (LE-12). On these lines, LE-11 asked, "*Does the court system know who you are? And what it is? Because I am concerned about presenting this at an injunction hearing, and a court commissioner saying, 'Well, it's a third party, so it's a he-said-she-said situation.'*" Expert testimony would, therefore, be required to show that Sherloc is trustworthy.

The legal experts gave us some ideas for how to reduce the chance that expert testimony will be requested. Producing the investigation report as part of the normal course of business—i.e., using Sherloc at every consultation—"*would help lend a lot more credibility to the document in the eyes of the law, and it would help kind of skate over hearsay objections*" (LE-12). We plan to do this going forward (Update 1.9). Some like proposed creating a guide or website describing how Sherloc works, then asking a judge to take judicial notice[8] of that guide. As a short-term solution, we added a cover page (shown in Fig. 5) that names our partner tech clinic (Section 7) and our university and describes how the investigation report was generated (Update 1.7). Alternatively, LE-18 recommended we embrace expert witnessing as "*an opportunity to educate the court on what TFA is and how to identify it.*"

6.3.3 Interpretability. Another common concern was interpretability. One suggestion was to add more technical details from the investigation. As LE-07 said, "*especially with tech, the more information you can give people the better.*" For example, "*login locations, login times, if it's unique*" (LE-18). Other providers wanted to see "*details of the suspicious logins and unrecognized devices [which] could be very helpful evidence and tie the abuser to 'breaches'*" (LE-28) or "*the number of times they were accessing certain things...where in this invasion of privacy is this fellow spending his time*" (LE-07) on that account. One reason to add this information is that "*information supplied by the victim themselves is not persuasive, in my opinion, from a legal standpoint*" (LE-28). Unfortunately, much of this information is not currently available on user interfaces. Where possible, though, we added relevant technical details such as metadata showing the creation time of all screenshots (Update 1.3).

They also suggested we add more interpretive information on top of the investigation details, to "*highlight problematic info*" (LE-31). For example, if a spyware app was found on the device, LE-08 would like to see details on "*How likely is it that this was user error, rather than something malicious from the respondent?*" Others asked for more information on what happens during a consultation. LE-13 said we could add more information on the client's technical habits—for example, "*Do you allow your significant other to use your cell phone?*" and "*do you allow him to download things on your cell phone?*"—to give more context on how compromise may have occurred. Accordingly, we updated Sherloc to record the client's answers to a technical assessment questionnaire (asking about their technological habits and risks) (Update 1.1) and add highlights describing any concerns identified during the consultation (Update 1.2).

At the same time, some felt that there was already *too much* information in the report; for example, LE-22 felt that the report was already "*too long, too complicated.*" However, given the number of people who wished for more information, we opted to begin with more detail and trim back later if needed.

[8] When a court takes judicial notice, it accepts a fact as true without the need for formal evidence [15].

Finally, LE-09 suggested we "*change the language to just say 'the respondent' instead of 'your partner.' ...partner is too collegial, somehow.*" We updated Sherloc to use "person of concern" rather than "your partner" (Update 1.8).

6.3.4 Weight of the evidence. Because some investigative details are difficult to capture, legal experts worried the evidence might not carry weight. For example, judge LE-05 said, "*Do I think that something like this is going to come in just all by itself? Probably not*", indicating that the report would not be sufficient without other supporting evidence to back it up.

One reason is that "*It would be hard if there wasn't more specific proof of who was doing this*" (LE-16). If the abuser can't be attributed, "*then the client is saying 'I had no idea this was on my phone' and the respondent's also saying, 'Okay, I don't know either'*" (LE-09). In cases of account compromise, it's also hard to show how an abuser *used* their access to the account. "*There's evidence that their ex partner can access this account...But were they actually doing it, or just that they had the capability of doing it?*" (LE-16).

Unfortunately, we may not be able to capture information definitively attributing an abuser or showing malicious activity. As noted by Stephenson et al. [100], tech platforms need to surface more internal data to enable us to capture that information. We plan to assess whether account data exports could provide additional information to this end, as suggested by Nonnenkamp et al. [79].

6.3.5 Anonymity and privacy. Legal experts raised concerns about violating the privacy of survivors. The concerns arose because the investigation report generated by Sherloc could be viewed by the abuser, in court or if otherwise found. Specific concerns were the client's name, contact information, and address.

We discussed various ways of preventing privacy leaks. One idea was redacting the information, either digitally or on paper: "*Then the client could explain that it was their number but they're not comfortable saying what that is*" (LE-01). LE-08 also suggested "*Maybe just use the last two digits? ... Like XXX-XX89. And then, someone would say, 'Well, yeah, my phone number does end in 8-9'*". We plan to encourage clients to manually redact any information they wish not to share (Update 1.10). In general, we learned that printing the exact details of survivors' accounts and contact information is not crucial, "*as long as you're able to say like, 'These are the [survivor's] accounts,' it'll effect enough*" (LE-10). We thus updated Sherloc to omit private details that are not relevant (such as un-compromised contact information) (Update 1.5).

Tech clinic consultants' privacy was also a concern, since the consultant's name was printed on the investigation report. "*The respondent would have a copy of this. So I don't know if you want them to know your names*" (LE-01). We therefore removed the consultant's name from the investigation report to protect their privacy (Update 1.4).

6.3.6 Admissibility. The legal experts anticipated that we might get the objection that "*anybody could make something that looks like this*" (LE-08). Thus, they suggested ways to help authenticate the document. For example, LE-19 offered that there may be "*exceptions of why we can rely on something without having somebody testify to how it was created. So there may be something with the rules of evidence could be helpful.*" Alternatively, LE-08 explained the value of using physical markers of authenticity such as a stamp or initials: "*Even if it's just something like this, with just initials and the date in pen—just to say, "This is when it was done." with like a stamp or something. . . . I just think it helps*" (LE-08). We took this idea and added space for the consultant's signature on the cover page of the investigation report (Fig. 5) (Update 1.6).

6.3.7 Training and awareness. One police officer, LE-13, emphasized the importance of raising awareness of Sherloc and teaching legal experts how to interpret the evidence. The trainings could potentially reduce the need for expert testimony, as previously mentioned. LE-13 described how training would help officers feel more equipped to interpret the evidence: "*We're not always going to understand what we're looking at. And maybe having a how-to helps point it out.*" (LE-13). Accordingly, we have undertaken efforts to inform legal experts in our region about Sherloc (Update 1.11). One of these efforts was the training during which we recruited judges for feedback (Section 6.2).

6.3.8 Added burden on survivors. Finally, LE-12 worried that Sherloc could place extra burden on survivors. Specifically, they thought survivors may face additional scrutiny about their tech knowledge when trying to present Sherloc-generated evidence. "*If there's not the consultant available, I could see a client not knowing how to interpret this, and it being used to make them seem less credible on the stand*" (LE-12). To help prevent this, we plan to carefully review investigation reports with survivors to ensure they feel comfortable with the reports' contents and meaning (Update 1.12).

6.3.9 Final thoughts: A need for in-situ assessment. There are some challenges we can only learn and mitigate once we start using Sherloc in practice:

> *It's going to probably be a lot of trial and error once it even goes into play...It may not be working right away. But we know the challenges, and we know the challenges that would be successful against it. And then we could say, 'Okay, how can we fix it?' (LE-08)*

7 Sherloc Pilot Program: Documenting TFA at the Madison Tech Clinic

After getting feedback from legal support providers and updating Sherloc accordingly, we collaborated with Madison Tech Clinic to pilot Sherloc. Going forward, all in-person Madison Tech Clinic consultations will use Sherloc; survivors do not need to participate in the research to receive support including the use of Sherloc.

At the time of writing, we have used Sherloc in three consultations and received feedback from six individuals: two survivors, two advocates, and two tech clinic consultants who are not on the research team. This is an ongoing, IRB-approved pilot program.

7.1 Briefing Advocates

Before piloting, we received permission from the leadership of Madison Tech Clinic and its partner organizations and met with advocates to introduce Sherloc. We reviewed the motivation for the project, explained how Sherloc works, provided a sample investigation report, outlined the procedure for pilot consultation, and

explained the methods we would use to evaluate Sherloc. We gave the advocates a chance to ask questions and raise any concerns.

7.2 Procedure for Pilot Consultations

All pilot consultations are held in-person at an advocacy organization. As with all Madison Tech Clinic consultations, an advocate is required to be present. The first author serves as the tech clinic consultant for all pilot consultations. In some consultations, there are other tech clinic consultants present to assist with the investigation; in addition to helping with investigation, these consultants are instructed to observe how Sherloc impacts the consultation.

7.2.1 Consultation flow. At the start of each pilot consultation, we assure the survivor (the client) that the consultation is private and will be taken at their pace. Then, we briefly describe Sherloc, explaining that it is a new piece of software that we use to guide the consultation and produce an investigation report. If needed, we turn on Developer Mode on the client's devices. We then proceed with the consultation.

Once the consultation has wrapped up, we create the investigation report and email it to the advocate for printing. We then walk the client through the printed report, highlighting the key parts relevant to their situation. We also sign the cover page of the report. Finally, we delete all consultation data from the clinic laptop and turn off Developer Mode if needed.

7.2.2 Study recruitment. Then, we invite the client, advocate, and any additional consultants who were present to participate in our research study. We pass out printed consent forms and invite them to participate by (i) allowing us to analyze anonymous notes from the consultation for our research and (ii) taking a survey to provide feedback on the investigation report and the consultation broadly. For clients, we also ask if we may reach out to them in 3 weeks with a follow-up survey. We emphasize that participation is optional.

7.3 Evaluation Methods

During the pilot program, we are using several methods to evaluate Sherloc. We aim to collect feedback from anyone who comes into contact with Sherloc or the evidence it produces. The first author is the primary coder for all pilot data. Survey responses, notes, and memos are coded using the list of design requirements as codes.

7.3.1 Anonymized consultation notes. With consent from everyone present, we collect the consultants' anonymized notes from each pilot consultation. These notes are initially typed by each consultant in a Google Doc specifically for tech clinic notes. The lead researcher copied the notes, manually redacted any potentially private information, and stored the notes in a dedicated, secure repository for the study. These notes can capture subtle ways that Sherloc impacted the consultation and help us remember what happened during the consultation, such as the types of investigations that were performed.

7.3.2 Post-consultation feedback surveys for clients, advocates, and consultants. Immediately following each pilot consultation, we invite all present to take a feedback survey about the consultation and the investigation report. Each survey takes around 5-10 minutes.

The surveys focus mainly on the investigation report. We ask open-ended questions about their thoughts on the investigation report. Then, we ask them to evaluate the document on our design requirements, and then to evaluate the importance of the requirements. As with the judges' survey (Section 6.2), we omit the Maintainable requirement from this evaluation. Next, we ask about how clients think they will use the document and we ask advocates how they think their client will use the document. Finally, we ask about how the use of Sherloc impacted the consultation.

We also ask advocates and consultants to fill a short demographic form. We do not collect demographic information for clients.

We offer surveys in multiple formats, including on paper, online using the clinic laptop or on a personal device, or as an interview. Since Sherloc is only available in English, all study materials are also provided in English. We are working to translate all materials into other languages to extend support as the pilot goes on.

7.3.3 Follow-up surveys with clients. To learn how clients use the document, we ask their permission to share a follow-up survey 3 weeks after their consultation. This survey is a bit longer than the post-consultation survey, taking around 15–20 minutes to complete. We offer clients a $10 Walmart gift card for their participation.

The first part of the survey covers how the client has used the investigation report since their consultation. We ask how they've used it, their motivation for using it in that way, and in what ways the document was helpful and not helpful. We also ask which uses were most important. If they have not used the document, we ask why they have not used it.

If they have used the document in legal proceedings, we ask several follow-up question about this. For instance, we ask what type of legal proceeding it was, in what ways they used the document for this proceeding (e.g., as evidence, showing it to their attorney, etc.), whether the document was admitted, and, if it wasn't admitted, the reasons it was not admitted. We end this section by asking about the document's formatting and how they stored it.

The second part of the survey repeats the same evaluation on the design requirements as we used in the post-consultation survey. Our aim is to see whether their opinion of the evidence document has changed in the weeks since they first received it.

We do not collect the contact information of clients in our study. Therefore, to send follow-ups, we email a link to the Qualtrics survey to their advocate, and ask the advocate to forward the survey to them. We use the date and time of the pilot consultation to reference the client we wish to follow up with. To compensate the client, we meet with the advocate to give them a physical gift card, asking them to pass it on to the client.

7.4 Status of the Pilot Program

We began the pilot program at the start of August, 2025. At the time of writing, we have conducted three[9] pilot consultations at three different victim service organizations partnered with Madison Tech Clinic. We found evidence of compromise in one pilot consultation, including compromised email and streaming accounts.

[9]We used Sherloc in a fourth pilot consultation, but we chose not to ask for research participation as it felt inappropriate to do so (see Section 8.1.5). Thus, we omit this consultation from the findings.

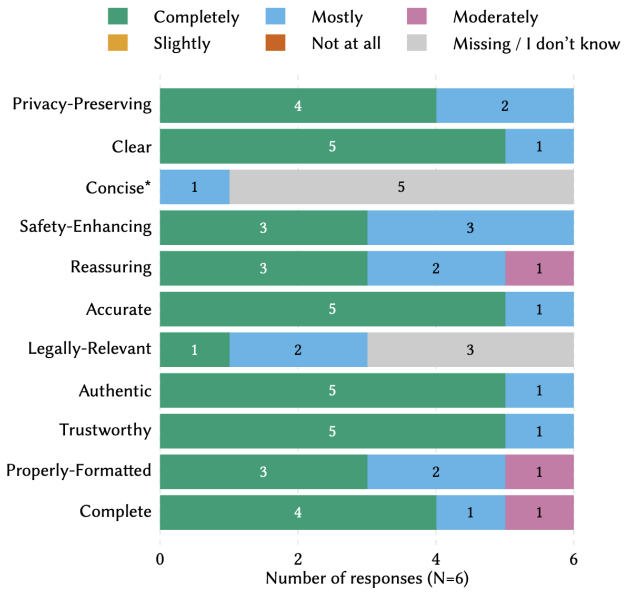


Figure 2: How survivors (N=2), advocates (N=2), and consultants (N=2) rated Sherloc's investigation report on our design requirements (Section 4.3). *Note that the Concise requirement was mistakenly omitted in the feedback surveys for the first two consults.

From the three pilot consultations, we received post-consultation feedback on Sherloc from two survivors (S-01, S-02), two advocates (A-01, A-02), and two non-researcher Madison Tech Clinic consultants (C-01, C-02). Three survivors gave consent for us to reach out later for follow-up, but we have not received any follow-up responses so far. We received consent to analyze the notes from two pilot consultations.

Since we are piloting Sherloc within Madison Tech Clinic, we cannot control how often we are able to test Sherloc. We also cannot control how survivors will use the document, and thus far, we have not been made aware of anyone using the document in legal proceedings (although one survivor said they planned to). This, in part, is why we are choosing to undertake a long-term pilot program, evaluating Sherloc slowly as consultations are scheduled.

7.5 Preliminary Findings

Initial feedback from the pilot program has been promising. We would like to highlight this quote from the first survivor we worked with: "*This document allows me to get the details I need to keep myself and family safe!*" (S-01). In this section, we share preliminary findings, including participants' ratings on each of the design requirements (Fig. 2).

7.5.1 Findings related to survivor enablement. Sherloc's investigation report was assessed on five survivor enablement characteristics: privacy-preserving, clear, concise,[10] safety-enhancing, and reassuring. In almost all cases, the survey respondents indicated that the investigation report "Completely" or "Mostly" fit each requirement. Qualitative responses matched; for example, S-02 wrote that the document was "*clear, made me feel safer,*" while C-02 said it was "*Really good, I think it will really help both consultants and the clients.*" Regarding clarity, C-01 noted that the document is "*Easy to read for non-technical audience*", and A-01 said the report "*helps w/ summarizing and visualizing (lots of) info for client.*" Survivors and advocates indicated that they might use the investigation reports in many different ways; for example, both survivors and both advocates believed survivors would talk about the report with an advocate, use it to remember what was done during the consultation, use it to help secure devices and accounts, and use it to help with legal action.

In addition to the document, we found that the use of Sherloc had a positive impact on the consultations without adding to consultation length, which supports safety and reassurance. The survivors indicated that their consultation was "Incredibly" and "Very" helpful in addressing their respective technology concerns. S-02 indicated that the investigation report enhanced the value of their consultation "A moderate amount," and advocates believed that the consultation was "Very effective" (A-01) and "Much more effective" (A-02) compared to consultations without Sherloc. C-01 agreed that Sherloc "*Kept complicated consultation (lots of vectors of compromise) on track & relatively prompt,*" and C-02 said "*I feel Sherloc is making the consultation more organized. In the past, we tended not to follow any order and conducted our investigation randomly.*"

While most feedback was positive, there were some opportunities to better support survivor enablement. For example, C-02 marked the investigation report as only "Moderately" reassuring because it does not include the consultant's recommendations for the client (e.g., to change an account password). Current practice at Madison Tech Clinic is to email the advocate a list of recommendations, separate from the investigation report. Going forward, we may seek to integrate these into the report.

The investigation report was ranked very highly on clarity, yet qualitative feedback indicated ways to improve its clarity further. Survey responses indicated that some of the technical details were noisy; e.g., "*not all the metadata for screenshots is necessary*" (C-01). A-01 added that they would like to see a "*slightly more 'dumbed down' or simpler format*", noting concerns such as "*somewhat technical/some jargon...could be simpler in some places*" (A-01). Therefore, we trimmed some of the technical details in the report (the permissions used by suspicious apps, plus some screenshot metadata) to reduce noise and improve interpretability (`Update 2.2`). Following a consultation where no device compromise was found, C-02 also suggested that we "*Maybe highlight the urgent things and make them more on the front*" because "*today's client is not having any critical things on the device.*" This indicates we may need to revisit how risks are highlighted and summarized, especially for consultations where no compromise is found.

Additionally, although the advocates and survivors agreed that the consultation was not at all disrupted by Sherloc, C-01 and the first author noticed a couple of disruptions. In two cases, Sherloc sparked conversations that briefly distracted from the consultation's goals. One such moment was at the start of the consultation,

[10] Due to an error in our survey, we also accidentally omitted the Concise requirement for the first two consults.

when the first author asked S-01 what name they would like to put on the report—a question requiring more thought than we had anticipated. We moved this question to the end of the consultation, to prevent the name decision from slowing down the consultation (Update 2.4). The second question asked about legal custody of children and started a larger, troubling conversation for the client. Our goal with this question was to identify risks from children's devices, so we rephrased the question to focus on children's devices instead of legal custody (Update 2.1).

Additionally, in S-02's consult, we encountered a bug when scanning their old iPhone which required the first author to live-debug the ISDi scanning code (Update 2.3). However, we got the scan working quickly, and confirmed that the client's phone had no malicious apps installed (their main concern). This client wrote that "*Some of the errors were worrisome at first, thank you for talking through it*" (S-02).

Finally, S-02 pointed out that our evaluation materials ask how the investigation report "violates" our design requirements, terminology which can be triggering to violence survivors. Thus, we quickly updated the wording of our heuristic evaluation to ask how the investigation report "does not fit" criteria (Update 2.5).

7.5.2 Findings related to legal robustness. Thus far, we have not received follow-up surveys from any survivors, so we have not been informed whether they have used their investigation report in legal proceedings (or other use cases). This limits our ability to assess legal robustness at this time. However, most survey responses indicated that the investigation report "Completely" or "Mostly" fits the six requirements we defined for legal robustness: accuracy, legal relevance, authenticity, trustworthiness, proper formatting, and completeness. Qualitative responses indicated it was "*thorough; a nice summary of everything discussed during consult, very detailed*" (A-01). C-02 said "*The overall structure is clear and matches what I heard during the consultation.*"

Proper formatting received the lowest ratings (although still relatively high). We received suggestions for how to structure the report for more legibility. For example, C-01 noted that it has "*a ton of whitespace. Index would be helpful or table of contents*" (C-01). We are currently working to address these formatting concerns.

To help with completeness, the survey respondents also noted some data that we could add to the investigation report, including "*metadata on unknown or concerning devices accessing client's devices and/or accounts*" (A-01), "*potentially photos*" (S-02, referring to non-consensual intimate imagery), or "*some kind of graph visualizing the connection between recovery methods*" (C-01). C-02 also said "*Maybe also have the recommendation (if it is not sent separately).*" We are planning to explore such additions to Sherloc as we iterate long-term (Section 8.3).

Additionally, survey respondents had some trouble assessing legal relevance. Half of the respondents—A-01, A-02, and S0-2—rated the report as "Mostly" or "Completely" legally-relevant; three respondents did not answer or selected "I don't know." Since legal relevance depends on statutes and specific case details, it is not surprising that this question was hard to answer.

8 Discussion: Trauma-Informed Digital Evidence Collection

Through the design of Sherloc, we explored how a trauma-informed lens can be applied to digital evidence collection frameworks. In this section, we review challenges we faced in designing Sherloc and six guidelines we derived for trauma-informed digital evidence collection. We then propose future directions for Sherloc.

8.1 Challenges Faced in Designing Sherloc

While designing, vetting, and piloting Sherloc, we encountered challenges illustrating the tensions inherent in documenting TFA.

8.1.1 Supporting survivor enablement often conflicted with legal robustness. In earlier sections, we defined two primary goals for Sherloc: *survivor enablement* and *legal robustness*. Often, these goals worked in tandem; for example, interpretability is important toward both goals. Unfortunately, at many times during the design process, enablement and legal robustness were at odds. For example, a more detailed investigation report helped to provide legal context and completeness, but increased the potential for privacy issues and retraumatization. Situating documentation within tech clinics provided higher robustness in court—but only for those who can access tech clinics. Potential upgrades, like online evidence storage or a client-led option (Section 8.3), might increase accessibility for survivors but could harm legal robustness. Protecting consultant privacy can also conflict with the need for legal robustness; in our case, requiring consultants to sign investigation reports strengthens their evidentiary value, but it also reduces consultant anonymity.

8.1.2 Evidence had to be interpretable, concise, and complete all at once. Deciding on the content and presentation of the investigation report was one of the more difficult design tasks of this study. We learned that the report must be easily-interpreted by a diverse set of people—judges, law enforcement, advocates, and survivors themselves—with varying degrees of technical expertise. To be most interpretable, and have the best chance of being reviewed in legal proceedings, the document should also be concise. Yet at the same time, the investigation report must contain all relevant context (for admissibility) and provide technical information to assure the reader that the findings are trustworthy.

Making matters more complicated, evidence of TFA is elusive. Often, there are technical details we would like to include in the report—e.g., installation times for spyware apps—that are simply not available to capture. This lack of information makes it more difficult to create documentation that is comprehensive and compelling. On the other hand, the information that *is* accessible requires explanation for non-experts to understand. For example, laypeople may not be aware that an abuser could log into an account using access to the account recovery information. Overall, balancing completeness, conciseness, and interpretability is a tension we are still grappling with as we improve and iterate on Sherloc.

8.1.3 Survivors' goals and experiences varied greatly. When designing Sherloc, and in tech clinic consultations more broadly, we must consider that survivors have wide-ranging concerns, situations, and goals regarding TFA. For example, some survivors may want to collect evidence for a specific legal proceeding, while others

mainly want to document what was discussed in the tech clinic for their own memory. For some, evidence may be a key priority, but others may place a higher value on the discussions that occur in the tech clinic consultation. And of course, the TFA we help to address can take a number of forms and involve many kinds of modern technology. Thus, a key challenge when designing Sherloc was accounting for this variety in both the modality of the service and the format/content of the evidence we provide.

8.1.4 Sherloc's effectiveness was difficult to assess without using it in practice. As noted by the legal experts we interviewed in Section 6, we could not be sure of Sherloc's effectiveness without real-world implementation in a pilot program. One reason is that the letter of the law can be different from how the law plays out in real legal proceedings—for example, court rules may be enforced with varying degrees of strictness, and individual judges and juries can vary greatly in how they interpret evidence. Furthermore, it was difficult to assess how Sherloc would help survivors, since every survivor has unique needs and wishes regarding documentation.

8.1.5 Challenges doing trauma-informed design in the real world. Finally, there were certain challenges to implementing a trauma-informed approach in practice. One ongoing challenge is that being trauma-informed can limit opportunities to collect pilot data. For example, since we are minimizing the information collected about clients, it can be difficult to follow up with them to see how they use the investigation reports in practice. Even within the pilot consultations, we use our best judgment to evaluate whether it is appropriate to ask for research participation. In one consultation, for instance, our client and their advocate began another pressing conversation right after the consultation was finished; we chose not to disrupt this important discussion to ask for feedback on Sherloc. Thus, being trauma-informed at a low level—i.e., within individual consultations—sometimes conflicts with our overall trauma-informed goal of a highly-engaged pilot program.

More broadly, using a trauma-informed approach requires a number of real-time judgment calls. Researchers must not only decide when it is appropriate to request research participation, but also determine when the prototype is ready for piloting, respond appropriately to survivors' and advocates' needs during interactions, and assess which design suggestions from advocates and survivors should be implemented immediately versus deferred to later upgrades. All of these choices rely on the researchers' situational judgments and as a result, similar situations may be handled differently by different researchers. We see this as an inherent characteristic of implementing trauma-informed design in practice: trauma-informed research prioritizes situational responsiveness, sometimes at the expense of methodological consistency.

8.2 Guidelines for Trauma-Informed Digital Evidence Collection

Informed by these challenges and our overall experience designing Sherloc, we share guidelines for trauma-informed digital evidence collection. The guidelines are summarized in Table 3. We encourage designers to use our guidelines as a complement to prior work from Chen et al. [48], Zheng and Walquist et al. [110], Bellini et al. [40], and Bhalerao et al. [41] on which this study is built.

8.2.1 Center survivor safety from the start of a project. Any effort to support trauma-informed digital evidence collection must, from its inception, prioritize survivor safety. The ultimate goal of this type of work is to help survivors gain back their digital safety. Therefore, throughout the process, designers should think critically about how their design might unintentionally harm survivors and seek feedback from survivor advocates to avoid harm.

8.2.2 Build in continuous, situated iteration. We recommend that designers pilot new digital evidence collection tools in practice as soon as it is safe and feasible to do so. Designers should first create a minimum viable product that provides at least *some* evidence-collection capability, then begin to offer it to survivors. Further upgrades and iterations should occur in the context of this real-world pilot. The outcome of this early-stage implementation is twofold: (i) survivors can benefit from the design sooner and (ii) designers can receive real-world feedback and iterate earlier.

However, it is absolutely crucial that these early prototypes are still thoroughly vetted before being piloted with survivors. Premature deployments could be unhelpful (at best) or could create additional barriers to safety (at worst). To balance the importance of in situ assessment with a need to protect survivor safety, early prototypes must be carefully assessed by proxies (e.g., survivor advocates and legal experts) to confirm that they are likely to bring more benefit than harm overall. Only then should they be offered to survivors. Care should also be taken to work with advocates who support a deployment to minimize the additional burden on them (e.g., to explain a new tool to survivors).

8.2.3 Support a variety of evidentiary goals and priorities. As discussed, tools for documenting TFA must meet survivors where they are. To support flexibility, we recommend that designers implement multiple options in their documentation tools that support differing priorities. For example, one survivor might prefer the current version of Sherloc, but another might benefit more from a version of Sherloc that allows them to document TFA on their schedule, even if that evidence may have lower legal robustness. Overall, when there are two design options representing two conflicting priorities, opt to provide *both* options and let survivors choose the best option for them. Importantly, designers must be transparent with survivors about the benefits and limitations of each option so they can make an informed choice.

8.2.4 Consider how technical sophistication may harm the interpretability of evidence. A key insight was that interpretability was crucial to the success of documentation, even more so than technical richness. Although we predicted that more technical sophistication could improve legal robustness, the additional complexity in fact appeared to *reduce* legal robustness by reducing interpretability. Thus, we caution designers against building the most technically-sophisticated solution on the first attempt. Instead, we recommend designers focus on documentation that would be easily-interpreted by a wide audience. Then, further along in the design process, designers can assess whether the benefits of additional technical sophistication could override effects on interpretability (and consider making more technically-sophisticated functionality optional).

8.2.5 Begin any design effort with a high level of engagement. It is tempting to design documentation tools for a wide audience from

Table 3: Guidelines for trauma-informed digital evidence collection.

Guideline	Description
Safety Focus	Prioritize survivor safety from the outset of the project.
Situated Iteration	Build in continuous iteration in collaboration with people affected by digital harm.
Flexibility	Support a variety of evidentiary goals and priorities.
Interpretability	Consider how technical sophistication may harm the interpretability of evidence.
Early Engagement	Begin any design effort with a high level of engagement.
Maintanability	Build in long-term maintainability from the outset.

the outset. For example, the survivor-facing documentation apps mentioned in the background are all accessible to anyone with a mobile device. However, to ensure effectiveness, we recommend that designers start with a smaller-scale, highly-engaged pilot program. By starting with a version of Sherloc situated in one tech clinic, we were able to closely scrutinize the usefulness of Sherloc, observe any potential drawbacks, and assess whether a larger-scale or more hands-off option would be useful.

8.2.6 Prioritize long-term maintainability. Our final recommendation is to prioritize maintainability from the outset. We observed that several survivor-facing tools for documenting TFA were obsolete after a few short years. A sustainable, reliable tool is going to be more beneficial to survivors. In designing Sherloc, we prioritized maintainability by situating Sherloc within an existing tech clinic service and setting up scaffolding for its long-term maintenance. Other designers could promote sustainability by anchoring documentation tools to victim service providers, nonprofit organizations, or university departments. Importantly, the tools should not hinge upon continued funding; even if resources are low, they should be able to remain operational with minimal software maintenance.

8.3 The Future of Sherloc

With these guidelines in mind, we plan to continue iterating on Sherloc with both short-term and long-term enhancements.

8.3.1 Short-term enhancements to Sherloc. We plan to implement a number of minor changes in the coming months to strengthen Sherloc and its investigation report. Many planned updates center on the report's interpretability, with plans to add a glossary and test different structures of the report to ease readability. We also hope to upgrade Sherloc's flexibility by better enabling consultants to record miscellaneous, less-common checks performed during the consultation, such as investigating a client's laptop computer. Similarly, we would like to test functionality to record any mitigative actions taken during a consultation (e.g., changing a password) and the reasons for those actions, as well as recommendations actions to take after the consultation.

8.3.2 Long-term directions for Sherloc. In the long term, we would like to further expand the flexibility and comprehensiveness of Sherloc. Toward comprehensiveness, we plan to explore other sources of data for Sherloc to analyze and report. For example, prior work has pointed out the potential for account data exports, such as Google Takeouts [5], as a tool for investigating TFA [79]—we plan to explore ways to analyze and incorporate data exports into Sherloc.

Toward flexibility, we plan to explore several optional modalities and procedures. One option is to enable automated scans of account security interfaces. However, it may be retraumatizing for some clients to provide access to their accounts or account credentials. We would like to explore offering both automated and manual account scans as part of Sherloc. Another idea is offering secure evidence storage and retrieval with cryptographic authenticity guarantees, which may increase accessibility for clients and add cryptographic tamper prevention—but may cause chain-of-custody issues. More broadly, we plan to work toward a version of Sherloc that is client-led, generalizable outside of Wisconsin, and accessible to the many survivors who cannot access tech clinics. Our ultimate goal is to offer both consultant-led and client-led options to survivors so they are able to make the best choice for their situation.

Acknowledgments

We are very thankful to all who collaborated with us on this work, including the survivors and advocates who have engaged with Sherloc in tech clinic consultations; the legal experts who gave us feedback and early support; and the volunteers of the Madison Tech Clinic. In particular, we would like to acknowledge the late Jessa Nicholson Goetz, an attorney who helped guide this work early on. We would also like to thank the anonymous reviewers, whose feedback made this paper stronger.

We acknowledge funding from the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice (Grant # 15POVC-23-GK-01414-NONF). The opinions, findings, and conclusions or recommendations expressed in this paper are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

References

[1] [n. d.]. Android Debug Bridge (ADB). Android Developers. https://developer.android.com/tools/adb
[2] [n. d.]. Clinic to End Tech Abuse. https://www.ceta.tech.cornell.edu/
[3] [n. d.]. Complaint Form - Internet Crime Complaint Center (IC3). Federal Bureau of Investigation. https://complaint.ic3.gov/
[4] [n. d.]. Document The Abuse. https://documenttheabuse.org/
[5] [n. d.]. Google Takeout. https://takeout.google.com
[6] [n. d.]. NetworkMiner - The NSM and Network Forensics Analysis Tool. NETRESEC AB. https://www.netresec.com/?page=NetworkMiner
[7] [n. d.]. Services. Tech Safe BC. https://techsafe.bcsth.ca/services/
[8] [n. d.]. tinycheck. Kaspersky. https://tiny-check.com
[9] 2019. Arc App. Domestic Violence Resource Centre Victoria. URL no longer available.
[10] 2021. Devastatingly pervasive: 1 in 3 women globally experience violence. World Health Organization Joint News Release, https://www.who.int/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence.

[11] 2021. HeHop - Help for Hope. https://play.google.com/store/apps/details?id=com.mco.hehop&hl=en&gl=FR

[12] 2022. Technology-Facilitated Stalking: Fact Sheet. Stalking Prevention, Awareness, and Resource Center (SPARC). https://www.stalkingawareness.org/wp-content/uploads/2022/12/SPARC-Stalking-Techology-Fact-Sheet.pdf

[13] 2023. Bright Sky US. Women's Center and Shelter of Greater Pittsburgh. https://apps.apple.com/us/app/bright-sky-us/id1667028531

[14] 2023. DocuSAFE Documentation and Evidence Collection App. Safety Net Project, National Network to End Domestic Violence (NNEDV). https://www.techsafety.org/docusafe

[15] 2023. Judicial Notice. Legal Information Institute, Cornell University. https://www.law.cornell.edu/wex/judicial_notice

[16] 2024. Hate and Hope Tracker. Right to Be. https://hateandhope.righttobe.org/

[17] 2025. Sample Technology Abuse Log. Safety Net Project, National Network to End Domestic Violence (NNEDV). https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/68effc214c5c6e3f5e9ee68c/1760558113407/Sample+Documentation+Log_2025.pdf

[18] 2025. VictimsVoice – Giving victims a legal voice. VictimsVoice. https://victimsvoice.app/

[19] 2026. Cellebrite | End-to-End Digital Investigations Software & Platform. https://cellebrite.com/en/home/

[20] 2026. Co-Track Pro: AI-Powered Family Safety & Cyberbulling Protection. https://cotrackpro.com/

[21] 2026. CyberTip Report. National Center for Missing and Exploited Children (NCMEC). https://report.cybertip.org/

[22] 2026. Feedly: Track the topics and trends that matter to you. https://feedly.com/

[23] 2026. Intelligence X. https://intelx.io/

[24] 2026. Madison Tech Clinic. https://techclinic.cs.wisc.edu/

[25] 2026. MediCapt. Physicians for Human Rights. https://phr.org/issues/sexual-violence/medicapt/

[26] 2026. OurFamilyWizard - Best Co-Parenting App for Child Custody. https://www.ourfamilywizard.com/

[27] 2026. Rule 401. Test for Relevant Evidence. Legal Information Institute, Cornell Law School. https://www.law.cornell.edu/rules/fre/rule_401

[28] 2026. Rule 901. Authenticating or Identifying Evidence. Legal Information Institute, Cornell Law School. https://www.law.cornell.edu/rules/fre/rule_901

[29] 2026. Safe YOU. Impact Innovations Institute. https://safeyou.space/en

[30] 2026. WebPreserver: Website Screen Capture & Evidence Tool. https://www.pagefreezer.com/webpreserver/

[31] 2026. XAMN Viewer — Mobile Forensic Data Recovery & Extraction. MSAB. https://www.msab.com/product/analyze/xamn-viewer/

[32] 2026. XRY Cloud - Cloud data extraction forensic tool. MSAB. https://www.msab.com/product/xry-extract/xry-cloud/

[33] Adrienne E. Adams, Angela K. Littwin, and McKenzie Javorka. 2020. The Frequency, Nature, and Effects of Coerced Debt Among a National Sample of Women Seeking Help for Intimate Partner Violence. *Violence Against Women* 26, 11 (Sept. 2020), 1324–1342. doi:10.1177/1077801219841445

[34] Nimra Ahmed, Anton Fedosov, and Elaine M. Huang. 2024. 'Women just have to accept it when the man wants it': An Investigation of the Practice of Forced Marriage and the Potential for Design Interventions. In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction* (Uppsala, Sweden) *(NordiCHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 36, 14 pages. doi:10.1145/3679318.3685371

[35] Majed Almansoori, Andrea Gallardo, Julio Poveda, Adil Ahmed, and Rahul Chatterjee. 2022. A Global Survey of Android Dual-Use Applications used in Intimate Partner Surveillance. *Proceedings on Privacy Enhancing Technologies* 1 (2022), 20. doi:10.56553/popets-2022-0102

[36] Ashwaq Alsoubai, Jihye Song, Afsaneh Razi, Nurun Naher, Munmun De Choudhury, and Pamela J. Wisniewski. 2022. From 'Friends with Benefits' to 'Sextortion:' A Nuanced Investigation of Adolescents' Online Sexual Risk Experiences. *Proceedings of the ACM on Human-Computer Interaction* (2022), 411:1–411:32. doi:10/gsjrvg

[37] Amna Batool, Mustafa Naseem, and Kentaro Toyama. 2024. Expanding Concepts of Non-Consensual Image-Disclosure Abuse: A Study of NCIDA in Pakistan. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24)*. Association for Computing Machinery, New York, NY, USA, 1–17. doi:10.1145/3613904.3642871

[38] Rosanna Bellini. 2023. Paying the Price: When Intimate Partners Use Technology for Financial Harm. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–17. doi:10/gr8rpz

[39] Rosanna Bellini, Kevin Lee, Megan A. Brown, Jeremy Shaffer, Rasika Bhalerao, and Thomas Ristenpart. 2023. The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 87–104. https://www.usenix.org/conference/usenixsecurity23/presentation/bellini

[40] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. 2024. SoK: Safer Digital-Safety Research Involving At-Risk Users. In *IEEE Symposium on Security and Privacy (S&P 2024)*. doi:10.1109/SP54263.2024.00071

[41] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M Redmiles, and Angelika Strohmayer. 2022. Ethical Practices for Security Research with At-Risk Populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 546–553. doi:10.1109/EuroSPW55150.2022.00065

[42] Arkaprabha Bhattacharya, Kevin Lee, Vineeth Ravi, Jessica Staddon, and Rosanna Bellini. 2024. Shortchanged: Uncovering and Analyzing Intimate Partner Financial Abuse in Consumer Complaints. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–20. doi:10.1145/3613904.3642033

[43] Lindsay Blackwell, Jill Dimond, Sarita Schoenebeck, and Cliff Lampe. 2017. Classification and Its Consequences for Online Harassment: Design Insights from HeartMob. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 24 (Dec. 2017), 19 pages. doi:10.1145/3134659

[44] Natalie Grace Brigham, Miranda Wei, Tadayoshi Kohno, and Elissa M. Redmiles. 2024. "Violation of my body:" Perceptions of AI-generated non-consensual (intimate) imagery. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Philadelphia, PA, 373–392. https://www.usenix.org/conference/soups2024/presentation/brigham

[45] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Sneaky Spy Devices and Defective Detectors: The Ecosystem of Intimate Partner Surveillance with Covert Devices. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 123–140. https://www.usenix.org/conference/usenixsecurity23/presentation/ceccio

[46] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. In *2018 IEEE Symposium on Security and Privacy (SP)*. 441–458. doi:10.1109/SP.2018.00061

[47] Jieru Chen, Mikel L Walters, Leah K Gilbert, and Nimesh Patel. 2020. Sexual violence, stalking, and intimate partner violence by sexual orientation, United States. *Psychology of violence* 10, 1 (2020), 110.

[48] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 544, 20 pages. doi:10.1145/3491102.3517475

[49] Kyungsuk Cho, Kyuyeon Choi, Yunji Park, Minsoo Kim, Seoyoung Kim, and Doowon Jeong. 2025. DEF-IPV:A Digital Evidence Framework for Intimate Partner Violence Victims. *Forensic Science International: Digital Investigation* 54 (Oct. 2025), 301979. doi:10.1016/j.fsidi.2025.301979

[50] Dana Cuomo. 2019. Gender-Based Violence and Technology-Enabled Coercive Control in Seattle: Challenges & Opportunities. TECC Whitepaper Series. (2019).

[51] Dana Cuomo, Nicola Dell, Lana Ramjit, and Thomas Ristenpart. 2023. The Technology Abuse Clinic Toolkit. (2023). https://www.techabuseclinics.org/the-toolkit

[52] Dana Cuomo and Natalie Dolci. 2022. The TECC Clinic: An innovative resource for mitigating technology-enabled coercive control. *Womens. Stud. Int. Forum* 92 (May 2022), 102596. https://www.sciencedirect.com/science/article/pii/S0277539522000371

[53] Jeff Darrington. 2023. The Phases of the Digital Forensics Investigation Process. https://graylog.org/post/the-phases-of-the-digital-forensics-investigation-process/

[54] Jill P. Dimond, Michaelanne Dye, Daphne Larose, and Amy S. Bruckman. 2013. Hollaback! the role of storytelling online in a social movement organization. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work* (San Antonio, Texas, USA) *(CSCW '13)*. Association for Computing Machinery, New York, NY, USA, 477–490. doi:10.1145/2441776.2441831

[55] Jill P Dimond, Casey Fiesler, and Amy S Bruckman. 2011. Domestic violence and information communication technologies. *Interact. Comput.* 23, 5 (Sept. 2011), 413–421. http://dx.doi.org/10.1016/j.intcom.2011.04.006

[56] DoronZ. [n. d.]. pymobiledevice3. https://pypi.org/project/pymobiledevice3/1.6.8/

[57] Asher Flynn, Anastasia Powell, and Sophie Hindes. 2023. Policing Technology-Facilitated Abuse. *Policing and Society* 33, 5 (May 2023), 575–592. doi:10.1080/10439463.2022.2159400

[58] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3173574.3174241

[59] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 46 (Dec. 2017), 22 pages. doi:10.1145/3134681

[60] Nitesh Goyal, Leslie Park, and Lucy Vasserman. 2022. "You Have to Prove the Threat Is Real": Understanding the Needs of Female Journalists and Activists to Document and Report Online Harassment. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–17. doi:10.1145/3491102.3517517

[61] Naman Gupta, Kate Walsh, Sanchari Das, and Rahul Chatterjee. 2024. "I really just leaned on my community for support": Barriers, Challenges, and Coping Mechanisms Used by Survivors of Technology-Facilitated Abuse to Seek Social Support. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 4981–4998. https://www.usenix.org/conference/usenixsecurity24/presentation/gupta

[62] Bridget A Harris and Delanie Woodlock. 2019. Digital coercive control: Insights from two landmark domestic violence studies. *The British Journal of Criminology* 59, 3 (2019), 530–550. doi:10.1093/bjc/azy052

[63] Phil Harvey. [n. d.]. ExifTool. https://exiftool.org

[64] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical Computer Security for Victims of Intimate Partner Violence. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 105–122. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[65] Nicola Henry and Asher Flynn. 2019. Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support. *Violence Against Women* (2019), 1932–1955. doi:10/gpbtwr

[66] Nicola Henry, Asher Flynn, and Anastasia Powell. 2018. Policing Image-Based Sexual Abuse: Stakeholder Perspectives. *Police Practice and Research* (2018), 565–581. doi:10/gn7zhh

[67] Nicola Henry and Anastasia Powell. 2018. Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, & Abuse* (2018), 195–208. doi:10/gddz8g

[68] Nicola Henry and Rebecca Umbach. 2024. Sextortion: Prevalence and Correlates in 10 Countries. *Computers in Human Behavior* (2024), 108298. doi:10/gt6s43

[69] Katy Johnson, Lindsey Green, and Suzanne Kidenda. 2020. Novel Research Methods that Avoid Retraumatizing Survivors. Physicians for Human Rights. https://phr.org/our-work/resources/novel-research-methods-that-avoid-retraumatizing-survivors/

[70] K Kent, S Chevalier, T Grance, and H Dang. 2006. *Guide to Integrating Forensic Techniques into Incident Response* (0 ed.). Technical Report NIST SP 800-86. National Institute of Standards and Technology, Gaithersburg, MD. NIST SP 800–86 pages. doi:10.6028/NIST.SP.800-86

[71] Nikolaos Koukopoulos, Madeleine Janickyj, and Leonie Maria Tanczer. 2026. Defining and Conceptualizing Technology-Facilitated Abuse ("Tech Abuse"): Findings of a Global Delphi Study. *Journal of Interpersonal Violence* 41, 1-2 (2026), 249–275. doi:10.1177/08862605241310465 PMID: 39825713.

[72] Ashish Kulkarni and Jakob Truelsen. [n. d.]. wkhtmltopdf. https://wkhtmltopdf.org

[73] Shanti Kulkarni. 2019. Intersectional Trauma-Informed Intimate Partner Violence (IPV) Services: Narrowing the Gap between IPV Service Delivery and Survivor Needs. *J. Fam. Violence* 34, 1 (Jan. 2019), 55–64. doi:10.1007/s10896-018-0001-5

[74] R. W. Leemis, N. Friar, S. Khatiwada, M. S. Chen, M. Kresnow, S. G. Smith, S. Caslin, and K. C. Basile. 2022. *The National Intimate Partner and Sexual Violence Survey: 2016/2017 Report on Intimate Partner Violence.* Technical Report. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, Atlanta, GA. https://www.cdc.gov/nisvs/documentation/NISVSReportonIPV_2022.pdf

[75] Roxanne Leitão. 2021. Technology-Facilitated Intimate Partner Abuse: A Qualitative Analysis of Data from Online Domestic Abuse Forums. *Human–Computer Interaction* 36, 3 (2021), 203–242. doi:10.1080/07370024.2019.1685883

[76] Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. 2019. 'Internet of Things': How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly* 63 (2019), 22–26. doi:10.2139/ssrn.3350615

[77] Philippe Mangeard, Bhaskar Tejaswi, Mohammad Mannan, and Amr Youssef. 2024. WARNE: A Stalkerware Evidence Collection Tool. *Forensic Science International: Digital Investigation* 48, 301677. doi:10.1016/j.fsidi.2023.301677

[78] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 2189–2201. doi:10.1145/3025453.3025875

[79] Julia Nonnenkamp, Naman Gupta, Abhimanyu Dev Gupta, and Rahul Chatterjee. 2025. Hidden in Plain Bytes: Investigating Interpersonal Account Compromise with Data Exports. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security* (Taipei, Taiwan) *(CCS '25)*. Association for Computing Machinery, New York, NY, USA, 4304–4318. doi:10.1145/3719027.3765147

[80] PalletsProjects. [n. d.]. Flask. PyPI. https://pypi.org/project/Flask/

[81] Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. 2020. Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse. In *Proceedings of the New Security Paradigms Workshop* (San Carlos, Costa Rica) *(NSPW '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. doi:10.1145/3368860.3368861

[82] Anastasia Powell and Nicola Henry. 2019. Technology-Facilitated Sexual Violence Victimization: Results From an Online Survey of Australian Adults. *Journal of Interpersonal Violence* (2019), 3637–3665. doi:10/gfttwz

[83] Anastasia Powell, Adrian Scott, Asher Flynn, and Nicola Henry. 2020. *Image-Based Sexual Abuse: An International Study of Victims and Perpetrators*. doi:10.13140/RG.2.2.35166.59209

[84] Anjana Rajan, Lucy Qin, David W. Archer, Dan Boneh, Tancrede Lepoint, and Mayank Varia. 2018. Callisto: A Cryptographic Approach to Detecting Serial Perpetrators of Sexual Misconduct. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies* (Menlo Park and San Jose, CA, USA) *(COMPASS '18)*. Association for Computing Machinery, New York, NY, USA, Article 49, 4 pages. doi:10.1145/3209811.3212699

[85] Lana Ramjit, Nicola Dell, and Dana Cuomo. 2025. Trauma-Informed Organizational Coordination in Clinical Computer Security. *Proc. ACM Hum.-Comput. Interact.* 9, 7, Article CSCW502 (Oct. 2025), 28 pages. doi:10.1145/3757683

[86] Lana Ramjit, Natalie Dolci, Francesca Rossi, Ryan Garcia, Thomas Ristenpart, and Dana Cuomo. 2024. Navigating Traumatic Stress Reactions During Computer Security Interventions. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 2011–2028. https://www.usenix.org/conference/usenixsecurity24/presentation/ramjit

[87] Michaela M Rogers, Colleen Fisher, Parveen Ali, Peter Allmark, and Lisa Fontes. 2022. Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. *Trauma Violence Abuse* (May 2022), 15248380221090218. doi:10.1177/15248380221090218

[88] André B Rosay. 2016. Violence against American Indian and Alaska Native Women and Men. *NIJ Journal* 277 (Sept. 2016). https://scholarworks.alaska.edu/handle/11122/7030

[89] Kevin A. Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy. 2020. The Many Kinds of Creepware Used for Interpersonal Attacks. In *2020 IEEE Symposium on Security and Privacy (SP)*. 626–643. doi:10.1109/SP40000.2020.00069

[90] Devansh Saxena, Karla Badillo-Urquiola, Pamela Wisniewski, and Shion Guha. 2020. Child Welfare System: Interaction of Policy, Practice and Algorithms. In *Companion Proceedings of the 2020 ACM International Conference on Supporting Group Work* (Sanibel Island, Florida, USA) *(GROUP '20)*. Association for Computing Machinery, New York, NY, USA, 119–122. doi:10.1145/3323994.3369888

[91] Carol F Scott, Gabriela Marcu, Riana Elyse Anderson, Mark W Newman, and Sarita Schoenebeck. 2023. Trauma-Informed Social Media: Towards Solutions for Reducing and Healing Online Harm. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 341, 20 pages. doi:10.1145/3544548.3581512

[92] Rebecca Shute, Emily Vernon, Rick Satcher, Michelle Verastegui-Sanchez, Molly O'Donovan Dix, and Michael Planty. 2021. *Landscape Study of Digital Tools to Identify, Capture, and Analyze Digital Evidence in Technology-Facilitated Abuse Cases.* Technical Report. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. https://cjtec.org/files/612cdd7c2dd0c Prepared by RTI International for CJTEC.

[93] Julia Slupska and Angelika Strohmayer. 2022. Networks of Care: Tech Abuse Advocates' Digital Security Practices. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 341–358. https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-networks

[94] Julia Slupska and Leonie Maria Tanczer. 2021. Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited. doi:10.1108/978-1-83982-848-520211049 arXiv:https://www.emerald.com/book/chapter-pdf/8984583/978-1-83982-848-520211049.pdf

[95] Sharon G. Smith, Xinjian Zhang, Kathleen C. Basile, Melissa T. Merrick, Jing Wang, Marcie jo Kresnow, and Jieru Chen. 2018. The National Intimate Partner and Sexual Violence Survey (NISVS): 2015 Data Brief – Updated Release. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, https://www.cdc.gov/violenceprevention/pdf/2015databrief508.pdf.

[96] Golovanov Stanislav. [n. d.]. pdfkit. PyPI. https://pypi.org/project/pdfkit/

[97] Evan Stark. 2007. *Coercive control: How men entrap women in personal life*. Oxford University Press.

[98] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. 2023. "It's the Equivalent of Feeling Like You're in Jail": Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 105–122. https://www.usenix.org/conference/usenixsecurity23/

presentation/stephenson-lessons

[99] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 69–86. https://www.usenix.org/conference/usenixsecurity23/presentation/stephenson-vectors

[100] Sophie Stephenson, Naman Gupta, Akhil Polamarasetty, Kyle Huang, David Youssef, Kayleigh Cowan, and Rahul Chatterjee. 2025. Legal Evidence of Technology-Facilitated Abuse in Wisconsin: Surfacing Barriers Within and Beyond the Courtroom. *Proceedings of the ACM on Human-Computer Interaction* 9, 7, Article CSCW441 (Nov. 2025), 32 pages. doi:10.1145/3757622

[101] Sophie Stephenson, Lana Ramjit, Thomas Ristenpart, and Nicola Dell. 2025. Digital Technologies and Human Trafficking: Combating Coercive Control and Navigating Digital Autonomy. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 832, 21 pages. doi:10.1145/3706598.3713544

[102] Sharifa Sultana, Mitrasree Deb, Ananya Bhattacharjee, Shaid Hasan, S.M.Raihanul Alam, Trishna Chakraborty, Prianka Roy, Samira Fairuz Ahmed, Aparna Moitra, M Ashraful Amin, A.K.M. Najmul Islam, and Syed Ishtiaque Ahmed. 2021. 'Unmochon': A Tool to Combat Online Sexual Harassment over Facebook Messenger. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–18. doi:10.1145/3411764.3445154

[103] Leonie Maria Tanczer, Isabel López-Neira, and Simon Parkin. 2021. 'I Feel like We're Really behind the Game': Perspectives of the United Kingdom's Intimate Partner Violence Support Sector on the Rise of Technology-Facilitated Abuse. *Journal of Gender-Based Violence* 5, 3 (2021), 431–450. doi:10.1332/239868021X16290304343529

[104] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. 2021. SoK: Hate, Harassment, and the Changing Landscape of Online Abuse. In *2021 IEEE Symposium on Security and Privacy (SP)*. 247–267. doi:10.1109/SP40001.2021.00028

[105] tox. [n. d.]. filelock. PyPI. https://pypi.org/project/filelock/

[106] Emily Tseng, Rosanna Bellini, Yeuk-Yu Lee, Alana Ramjit, Thomas Ristenpart, and Nicola Dell. 2024. Data Stewardship in Clinical Computer Security: Balancing Benefit and Burden in Participatory Systems. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 39, 29 pages. doi:10.1145/3637316

[107] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. 2021. A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 71, 17 pages. doi:10.1145/3411764.3445589

[108] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care Infrastructures for Digital Security in Intimate Partner Violence. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 123, 20 pages. doi:10.1145/3491102.3502038

[109] Delanie Woodlock. 2017. The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women* 23, 5 (2017), 584–602. doi:10.1177/1077801216646277 PMID: 27178564.

[110] Wenqi Zheng, Emma Walquist, Isha Datey, Xiangyu Zhou, Kelly Berishaj, Melissa Mcdonald, Michele Parkhill, Dongxiao Zhu, and Douglas Zytko. 2024. "It's Not What We Were Trying to Get At, but I Think Maybe It Should Be": Learning How to Do Trauma-Informed Design with a Data Donation Platform for Online Dating Sexual Violence. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 743, 15 pages. doi:10.1145/3613904.3642045

[111] John Zimmerman, Jodi Forlizzi, and Shelley Evenson. 2007. Research through Design as a Method for Interaction Design Research in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, San Jose California USA, 493–502. doi:10.1145/1240624.1240704

Table 4: Updates made to Sherloc during each iteration of our design process. The update number `Update X.Y` represents the design stage X and the specific change Y. Design stages can be Stage 1 (expert feedback, § 6) or Stage 2 (pilot, § 7).

Category	Update		Reasoning
Content and Functionality	`Update 1.1`	Add TAQ section	Interpretability
	`Update 1.2`	Add automated risk descriptions	Interpretability
	`Update 1.3`	Add technical details to report	Interpretability
	`Update 1.4`	Remove consultants' names	Anonymity & privacy
	`Update 1.5`	Reduce private information	Anonymity & privacy
	`Update 2.1`	Tweak wording of certain TAQ questions	Avoiding retraumatization
	`Update 2.2`	Trim technical details in the report	Interpretability
	`Update 2.3`	Fix bug in scan code	Data collection
Presentation	`Update 1.6`	Support consultant signature	Admissibility
	`Update 1.7`	Add cover page	Credibility & expert testimony
	`Update 1.8`	Formalize language in the report	Interpretability
Procedures	`Update 1.9`	Use Sherloc at every consultation	Credibility & expert testimony
	`Update 1.10`	Encourage survivors to redact data	Anonymity & privacy
	`Update 1.11`	Undertake outreach efforts	Training & awareness
	`Update 1.12`	Go through report with clients	Interpretability
	`Update 2.4`	Ask for client's name near the end	Enabling normal consultation flow
	`Update 2.5`	Remove "violates" from survey	Avoiding retraumatization

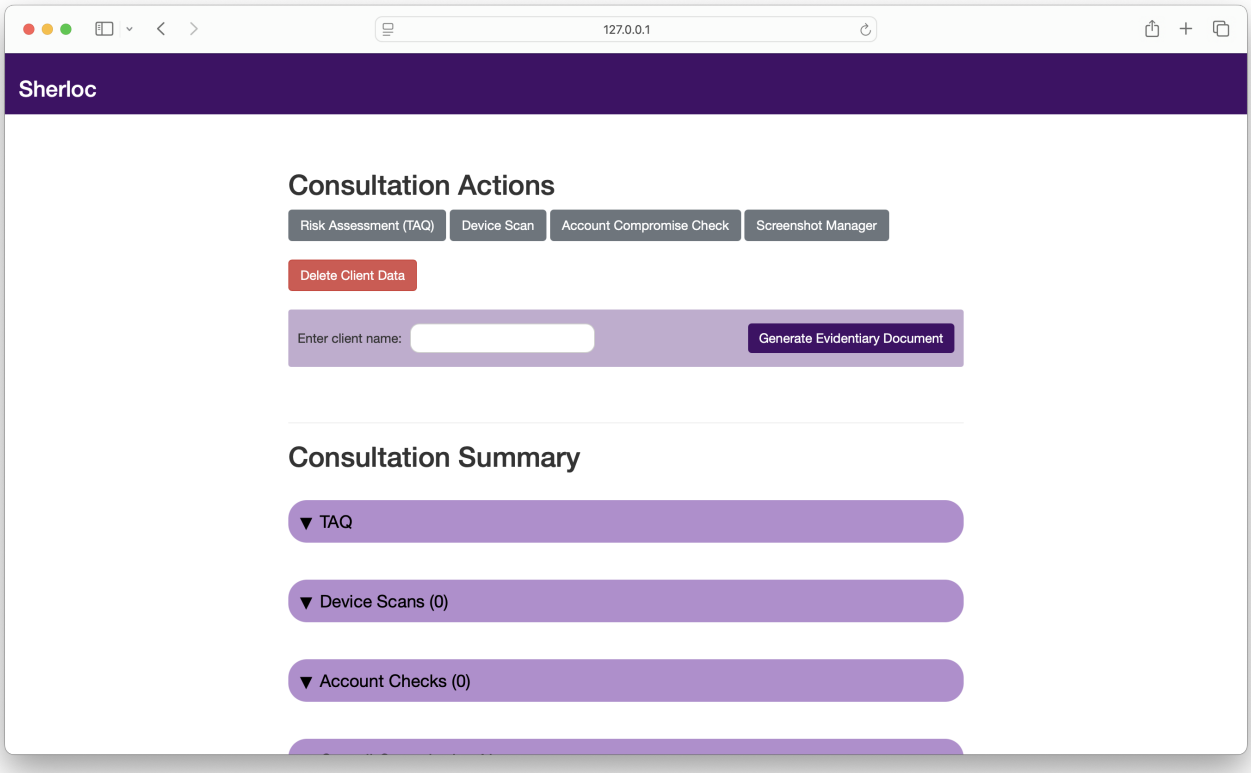


Figure 3: Sherloc's homepage.

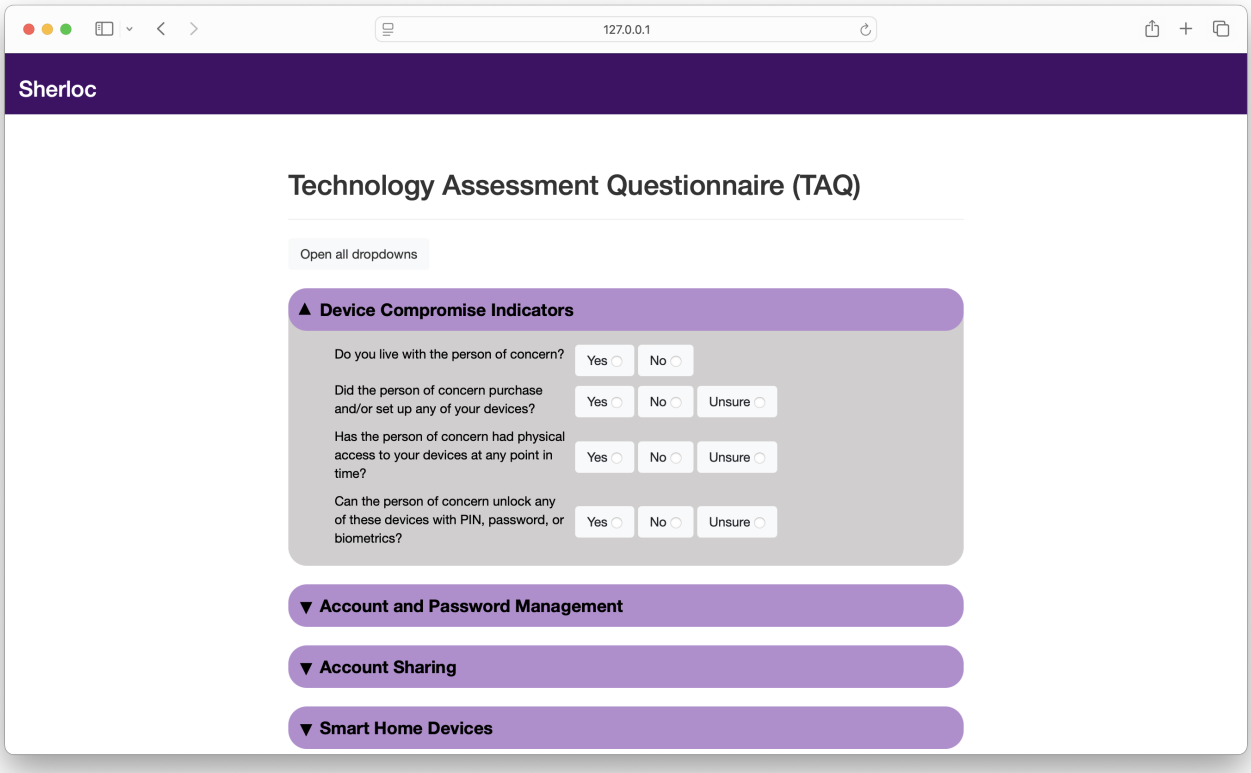


Figure 4: The Technology Assessment Questionnaire (TAQ) page of Sherloc.

Investigation Report

Prepared by the Madison Tech Clinic

Client Name: Sophie Stephenson

Consultation Start Time: 2026/01/23 15:21:31

This report describes the findings of a Madison Tech Clinic consultation. The report was created using Sherloc 1.1.4, an investigative tool developed by the Madison Tech Clinic. Source code for Sherloc is available at https://github.com/sophiestephenson/ips-evidence-collector/releases.

Please see https://techclinic.cs.wisc.edu or contact techclinic.madison@gmail.com for more information about the Madison Tech Clinic, Sherloc, or this report.

Consultant Signature: _____

Figure 5: The cover page of a Sherloc investigation report.

Summary of Findings

The following are automated summaries generated deterministically from the content of this report.

Technology Assessment Questionnaire

The following risks were identified based on the client's responses to the Technology Assessment Questionnaire:

- ⚠ **Physical access to devices** : A person with physical access to devices might be able to install apps, adjust device configurations, and access or manipulate accounts logged in on that device.
- ⚠ **Shared phone plan** : A shared phone plan may leak a variety of information, possibly including call history, message history (but not message content), contacts, and sometimes location. The account administrator of the client's phone plan has even more privileged access to this information.
- ⚠ **Physical access to children's devices** : A person with physical access to children's devices might be able to install apps, adjust device configurations, and access or manipulate accounts logged in on that device. These changes could allow monitoring of the parent, for example by tracking the children's location when they are with their parent.
- ⚠ **Shared phone plan (child)** : A shared phone plan may leak a variety of information, possibly including call history, message history (but not message content), contacts, and sometimes location. This could include information about the parent, such as their phone number and location when with the children. The plan administrator has even more privileged access to this information.

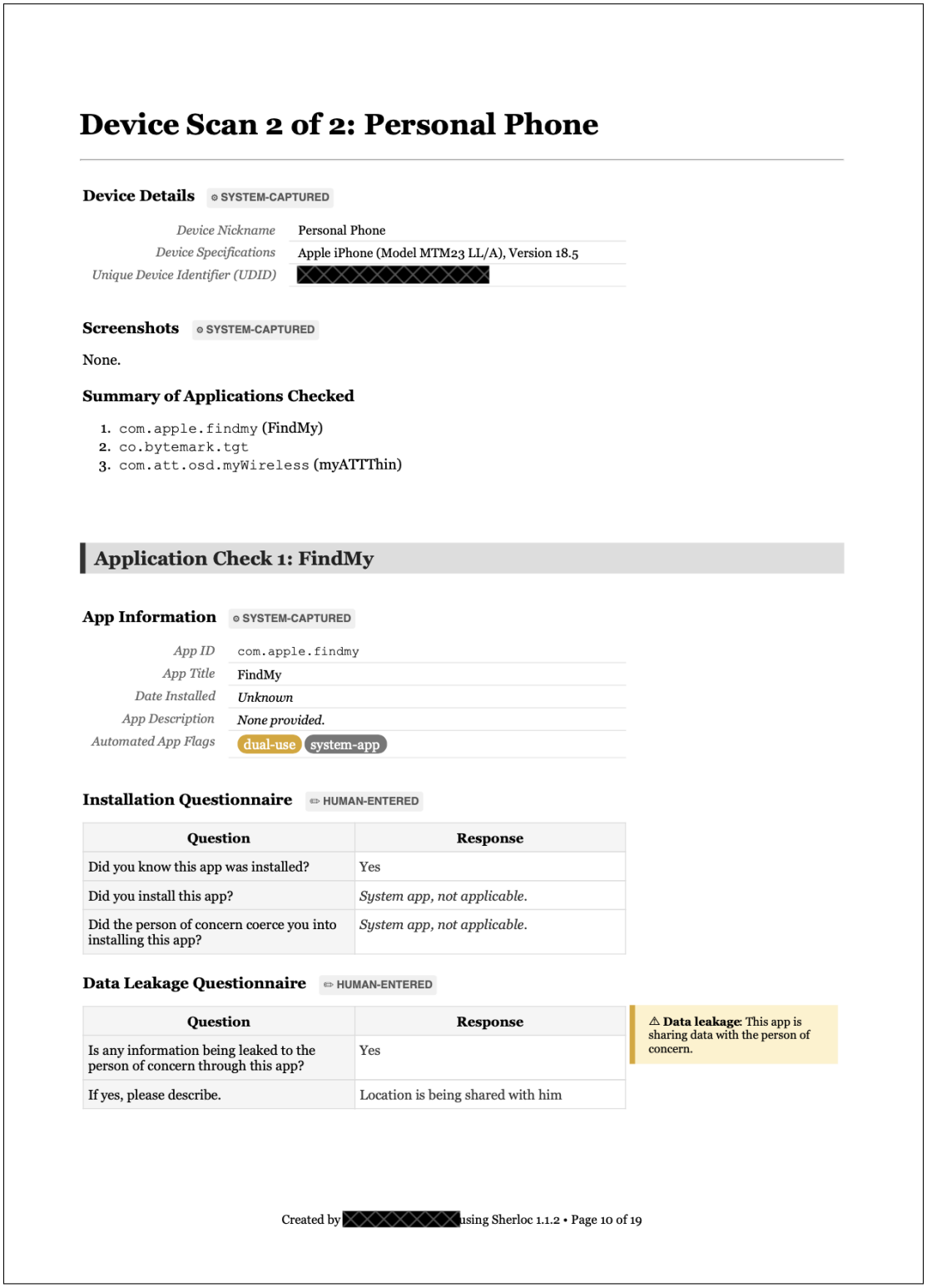
2 Devices Scanned

Device	Risks Identified
Google Pixel 2, Version 11 (Nickname: Work Pixel)	No risks identified.
Apple iPhone (Model MTM23 LL/A), Version 18.5 (Nickname: Personal Phone)	• ⚠ **Risk from app: FindMy** : Risks identified: Data leakage.

4 Accounts Checked for Compromise

Account	Risks Identified
Google (Nickname: Personal Google)	• ⚠ **Unrecognized devices** : There are unrecognized devices currently logged into this account. • ⚠ **Suspicious logins** : There are suspicious logins to this account that do not appear to have come from the client. • ⚠ **Compromised recovery information** : With access to the recovery contact information, someone can access an account without knowing the password using the 'Forgot password' option. • ⚠ **Compromised second factor** : If someone has access to the second authentication factor, they only need the account password to log into the account. They could also intercept and delete login notifications. • ⚠ **Guessable security questions** : The client believes the person of concern knows the answers to security questions, which could allow them an easy way to log into the account.

Figure 6: The summary page of a sample Sherloc investigation report.



Device Scan 2 of 2: Personal Phone

Device Details ⚙ SYSTEM-CAPTURED

Device Nickname	Personal Phone
Device Specifications	Apple iPhone (Model MTM23 LL/A), Version 18.5
Unique Device Identifier (UDID)	[redacted]

Screenshots ⚙ SYSTEM-CAPTURED

None.

Summary of Applications Checked

1. `com.apple.findmy` (FindMy)
2. `co.bytemark.tgt`
3. `com.att.osd.myWireless` (myATTThin)

Application Check 1: FindMy

App Information ⚙ SYSTEM-CAPTURED

App ID	`com.apple.findmy`
App Title	FindMy
Date Installed	*Unknown*
App Description	*None provided.*
Automated App Flags	dual-use system-app

Installation Questionnaire ✏ HUMAN-ENTERED

Question	Response
Did you know this app was installed?	Yes
Did you install this app?	*System app, not applicable.*
Did the person of concern coerce you into installing this app?	*System app, not applicable.*

Data Leakage Questionnaire ✏ HUMAN-ENTERED

Question	Response
Is any information being leaked to the person of concern through this app?	Yes
If yes, please describe.	Location is being shared with him

⚠ **Data leakage**: This app is sharing data with the person of concern.

Created by [redacted] using Sherloc 1.1.2 • Page 10 of 19

Figure 7: The start of a device scan section in a sample Sherloc investigation report.