Digital Forensic Readiness of Regulated Medical Devices: An Empirical Study of the GE Venue Ultrasound System

Muhammad Shaharyar Yaqub[a], Wooyeon Jo[a], Tamer Nadeem[a], Erdem Topsakal[b] and Irfan Ahmed[a]

[a]Department of Computer Science, Virginia Commonwealth University, Richmond, VA, USA
[b]Department of Electrical and Computer Engineering, Virginia Commonwealth University, Richmond, VA, USA

ARTICLE INFO

Keywords:
Digital forensic readiness
Memory forensics
Point-of-care ultrasound (POCUS)
Medical device security
Protected health information (PHI)
Windows Embedded systems
Healthcare Forensics

ABSTRACT

Medical devices increasingly operate as networked computing platforms, yet incident response remains difficult because many regulated systems restrict logging, execution, and evidence collection. Point-of-care ultrasound (POCUS) devices are especially challenging: they are workflow-driven, safety-adjacent, and often run embedded, vendor-managed Windows stacks that handle patient-associated data while limiting investigator access. This paper, to our knowledge, presents the first end-to-end forensic readiness and physical-memory forensics study of a POCUS ultrasound platform, using the GE Venue Ultrasound system as a case study.

We introduce URSA, a volatile-first readiness workflow for constrained ultrasound devices, and operationalize it with a UI-state-driven acquisition design that ties memory collection to observable clinical modes. Across seven full physical memory dumps captured before and after controlled scan-and-review interactions, we demonstrate repeatable acquisition under segmented storage and restrictive execution boundaries. Memory analysis reconstructs the clinical launch chain and yields both security-relevant artifacts and clinical exposure artifacts, including structured patient-associated logs and renderable diagnostic images recovered from RAM, with persistence characterized across states and time offsets. We complement volatile results with targeted disk-side context to quantify permission boundaries and corroborate selected findings. These findings provide practical guidance for improving forensic readiness and privacy-aware response on regulated ultrasound platforms.

1. Introduction

Medical imaging devices sit at the intersection of safety-critical care and general-purpose computing. The increasing connectivity of medical devices through hospital networks, cloud services, and remote monitoring systems further expands their attack surface [1, 2, 3]. Ultrasound systems, in particular, support rapid bedside diagnosis and are deployed widely across emergency departments, intensive care units, operating rooms, and inpatient wards. Modern point-of-care ultrasound (POCUS) platforms increasingly connect to hospital networks, exchange data with Picture Archiving and Communication System (PACS) and Electronic Health Record (EHR) infrastructure, and store or cache patient-associated content. At the same time, many platforms run embedded configurations of mainstream operating systems and commodity software components, inheriting familiar weaknesses in authentication, update cadence, and telemetry coverage.

This combination creates a high-value target. Healthcare and similar kind of environments face persistent pressure from ransomware, credential theft, and supply-chain abuse [4, 5]. When an incident is suspected, responders must answer practical questions quickly: what executed on the device, what patient-associated content was present, and whether device operation or data handling deviated from expected clinical workflow. On managed workstations, teams rely on EDR, centralized logs, and standardized collection interfaces. Regulated medical devices often provide limited host visibility and restrict execution and file-system access to preserve stability and certification posture. These constraints reduce forensic readiness: even authorized responders may be unable to perform disk-first triage, capture comprehensive logs, or reconstruct timelines reliably.

A recurring obstacle in clinical incident response is therefore a *forensic blind spot*. Many medical devices lack responder-accessible, tamper-evident logging and restrict access to the underlying OS. Storage is frequently segmented into vendor-controlled partitions, and executable launch can be constrained by policy. Even when disk access is possible, critical evidence may never be written to persistent storage. Attackers can also reduce durable traces by operating primarily in memory. As a result, volatile memory becomes a first-order evidence source. Physical memory can contain process structures, module mappings, runtime configuration, credential material, network state, and cached application data. For imaging devices, memory may also contain patient-associated metadata and diagnostic image content created during scanning, review, and export workflows.

Despite its evidentiary value, memory acquisition on clinical devices is operationally sensitive. Investigators must minimize disruption to patient care, bound their footprint, preserve integrity and provenance, and document collection conditions precisely. These constraints motivate a conservative, reproducible workflow that treats memory acquisition as the foundation of investigation rather than an optional enhancement.

In this paper, we study the digital forensic readiness of a commercial POCUS ultrasound platform using the GE Venue system as a case study. We operationalize readiness through a volatile-first workflow *(URSA)* and a UI-state-driven acquisition design that ties memory collection to

observable clinical modes (e.g., Scan, Post-capture, Review). This design provides two benefits. First, it enables reproducible acquisition labeling without relying on undocumented internal triggers. Second, it grounds interpretation of recovered artifacts in the clinical workflow state at the time of capture, reducing ambiguity when estimating persistence and exposure.

Grounded in the above challenges, we address the following research questions:

1. **RQ1** What types of Protected Health Information (PHI) and system telemetry persist in volatile memory on POCUS devices, and are they recoverable?
2. **RQ2** How does volatile memory acquisition enhance forensic readiness for both patient-specific exposure assessment and administrative reconstruction in POCUS systems?
3. **RQ3** Can volatile memory analysis be leveraged to bypass device hardening and expose high-privilege authentication artifacts?
4. **RQ4** Can a digital forensic readiness workflow be used not only for incident response but also to uncover latent security vulnerabilities and architectural weaknesses in medical imaging platforms?

1.1. Contributions

There are three contributions.

1. We propose and operationalize URSA, a volatile-first digital forensic readiness workflow tailored to embedded ultrasound systems with constrained execution and segmented storage.
2. We present an empirical seven-dump study (two baseline, five post-interaction) that characterizes the recoverability and persistence of both security-relevant artifacts (execution chains, extracted binaries, privileged authentication material) and privacy-relevant artifacts (patient logs and diagnostic images) across UI-defined states and time offsets.
3. We complement memory results with targeted disk-side context to characterize permission boundaries and to demonstrate how memory-derived privilege can expand access to persistent clinical artifacts under an authorized examiner model.

1.2. Threat Model and Examiner Model

We separate two capabilities that are often conflated in medical device security and forensic studies: an authorized examiner model and an adversary model.

Examiner model. We assume an authorized investigator with physical access to the device in a controlled environment (e.g., biomedical engineering staff or an incident response team operating under written policy). The investigator's goal is evidence acquisition and interpretation with minimal operational disruption. The investigator documents all actions, bounds persistent writes, preserves integrity via hashing and manifests, and performs analysis offline on verified copies. Where privileged access is required to enumerate or corroborate artifacts, we treat the feasibility of obtaining such access as a forensic readiness property and report it as such.

Adversary model. We consider a physical-access attacker who can interact with pre-login and local interfaces (keyboard/screen access and, where permitted, removable media). Such an attacker may attempt to abuse local execution pathways or accessibility mechanisms to gain unauthorized control and extract patient-associated data. We treat the existence of these pathways as security-relevant because they reduce the effort required to compromise a device, even if the same pathways can also be leveraged by authorized responders during acquisition.

This distinction matters for interpretation. Our empirical results demonstrate what artifacts are recoverable and how acquisition can expand visibility under authorization. We do not claim remote exploitation capability, continuous compromise detection, or fleet-wide prevalence beyond the studied configuration.

2. GE Venue Ultrasound System

We evaluate a commercial POCUS platform, the GE Venue Ultrasound system (Figure 1). The device combines a proprietary clinical imaging application stack with a general-purpose operating system and commodity compute hardware. This architecture enables UI-driven workflows and interoperability with hospital infrastructure, but it also implies that the platform inherits forensic and security properties typical of mainstream endpoints, including OS-level process structures, credential subsystems, and application-layer caching behavior.

Our experiments were conducted under an authorized examiner model in a controlled environment and not during patient care. The examined device runs an embedded Windows configuration and executes a vendor-managed application stack that mediates clinical workflow through stable loader and UI components. These properties matter for forensic readiness because (i) OS build family and kernel behavior determine which memory artifacts exist and how reliably standard parsing assumptions hold, and (ii) the vendor application stack determines how clinical states (Scan, Post-capture, Review) map to memory-resident artifacts such as image buffers, cached frames, and patient-associated metadata.

To ground the platform characterization, Table 1 summarizes key configuration properties observed in our environment. These fields are used later to justify analysis choices and to delimit the scope of the claims to the studied configuration.

The platform also exposes a segmented storage layout and restrictive execution boundaries typical of regulated clinical devices. While these constraints limit conventional disk-first triage, they are also part of the forensic readiness

Table 1
Observed system configuration of the evaluated GE Venue ultrasound platform.

Field	Value
Device model	GE Venue Ultrasound
OS edition	Windows 10 Enterprise 2016 LTSB
OS version	10.0.14393 (Build 14393)
Architecture	x64
BIOS	American Megatrend Inc. 1.10.10.GE03 (2017)
Compute base	ADLINK-manufactured GE computing base (observed)

Figure 1: The GE Venue ultrasound device evaluated in our forensic-readiness and memory-acquisition experiments.

problem: collection feasibility and investigator footprint depend on which volumes are writable and whether executables can be launched from removable media or only from approved paths. We characterize these boundaries in detail in Section 7 and incorporate them into the acquisition design described in Section 5.

Finally, the Venue application stack includes a loader-driven launch pathway that is stable across captures and provides a practical anchor for baseline-driven interpretation. In our memory analysis, this stability enables consistent reconstruction of expected process lineage and supports deviation analysis when investigating suspected compromise or misconfiguration (Section 6).

3. Forensic Readiness of Ultrasound Systems

Forensic readiness is the operational capacity of a system to support timely, defensible investigation when a security or safety incident is suspected. In clinical environments, readiness must be defined under constraints that differ materially from enterprise incident response. Ultrasound platforms are safety-adjacent systems that must maintain high availability, operate under conservative change control, and often restrict investigator access to preserve stability and vendor supportability. At the same time, they process highly sensitive patient-associated information and may connect to hospital networks and external peripherals. These realities create a tension: the systems most in need of rapid, trustworthy forensic visibility are often the least prepared to provide it through conventional logs and endpoint telemetry.

This work treats forensic readiness as an evidentiary problem rather than a compliance checklist. For embedded ultrasound systems built on general-purpose operating systems, readiness hinges on a documented and minimally invasive procedure for acquiring and validating high-value evidence under restrictive execution and storage policies. In practice, this requires a volatile-first strategy. Execution traces, transient configuration, authentication material, and cached clinical artifacts can exist only in memory and can be overwritten quickly. Disk artifacts, when present, may be incomplete, rotated, or inaccessible without vendor tooling. A readiness posture that defers memory acquisition risks losing the most informative evidence and underestimating potential exposure of patient-associated content.

3.1. URSA: Ultrasound Readiness and Security Assurance Framework

To systematize readiness for embedded ultrasound platforms, we propose URSA (Ultrasound Readiness and Security Assurance), a forensic readiness framework tailored to devices that operate as embedded Windows endpoints with vendor-managed application stacks and constrained execution environments. URSA is designed for authorized hospital incident response teams and biomedical engineering staff operating under policy. It does not assume invasive instrumentation, continuous endpoint agents, or vendor-exclusive tooling. Instead, it structures readiness around four investigation-aligned phases: *Prepare*, *Preserve*, *Acquire*, and *Interpret*. Each phase defines concrete activities and outputs, and together they provide a repeatable method for evidence collection and analysis that remains defensible under operational constraints. Table 2 summarizes the four URSA phases and their primary outputs.

URSA is intentionally scoped to scenarios in which an authorized examiner can obtain physical access to the device under controlled conditions (e.g., during a maintenance window or a controlled investigation). It does not assume remote-only acquisition, fleet-scale continuous monitoring, or malware attribution without corroborating behavioral evidence. The goal is to ensure that core evidence classes can be collected reliably and interpreted conservatively, with explicit handling of PHI.

3.2. Forensic objectives

Consistent with digital forensic readiness principles that derive collection strategy from explicit readiness objectives [6], URSA defines readiness for ultrasound systems in terms of six measurable objectives that reflect both security and clinical realities.

Table 2
URSA phases.

Phase	Purpose / key outputs
Prepare	Baseline (process lineage/module set), pinned acquisition kit, PHI governance.
Preserve	Provenance: action log, timestamps, cryptographic hashes; bound writes and footprint.
Acquire	Volatile-first RAM capture, then minimal runtime context and targeted disk corroboration.
Interpret	Cross-validated parsing; evidence-tier reporting; privacy exposure summary.

O1: Evidence availability under embedded constraints. Authorized responders should be able to obtain core evidence classes using an approved method that does not require installing agents or modifying vendor binaries.

O2: Volatile-first capture of high-value artifacts. Memory acquisition should occur as early as possible because execution traces, secrets, and clinically sensitive buffers can be overwritten quickly.

O3: Integrity and provenance. Evidence must be verifiable through hashing, timestamp discipline, and detailed action logging that bounds the examiner footprint.

O4: Operational safety and minimal invasiveness. Acquisition must minimize disruption and avoid impacting patient care; persistent writes should be bounded to the minimum required for staging and should be documented.

O5: Privacy-aware handling and reporting. Because volatile memory may contain PHI, readiness must include encryption, controlled access, retention limits, and reporting formats that separate privacy exposure assessment from security conclusions.

O6: Baseline-driven interpretation. Expected baselines for process lineage, loader chains, and core module sets reduce ambiguity and support deviation analysis when logging is sparse.

These objectives convert readiness from an aspiration into a capability that can be evaluated empirically. In this study, we operationalize O2 through a seven-dump, UI-labeled acquisition design; we evaluate O6 through stable reconstruction of the clinical launch pathway; and we evaluate O5 by quantifying the recoverability of patient logs and diagnostic images from RAM across states and time offsets.

3.3. Scope and assumptions

URSA targets embedded ultrasound platforms that share three properties: a general-purpose OS foundation, a vendor application stack that mediates clinical workflow through stable loader and UI processes, and restrictions that constrain typical endpoint investigations. The framework assumes that evidence collection is conducted under authorization and governance, with explicit rules for PHI handling. URSA's scope includes memory acquisition, reconstruction of process and module artifacts, extraction of memory-resident executables and clinical artifacts, and targeted disk context collection to corroborate memory findings and characterize permission boundaries.

URSA excludes remote-only forensic acquisition without physical access, continuous monitoring deployments that require persistent agents or vendor integration, and formal attribution of malicious intent based solely on third-party reputation signals. These exclusions are deliberate. In many hospitals, capabilities that depend on kernel drivers, long-lived agents, or deep vendor cooperation are difficult to deploy during a real incident. URSA instead focuses on procedures that can be executed reliably under realistic constraints and interpreted conservatively under review.

4. User Interface as a Forensic State Surface

Embedded ultrasound platforms often provide limited responder-accessible host telemetry and restrict conventional incident response actions. In this setting, the clinical user interface (UI) provides a practical and semantically meaningful surface for structuring forensic acquisition and interpretation. We treat the UI as a *forensic state surface* for three reasons.

First, the UI exposes workflow mode (e.g., Scan versus Review), which is directly coupled to the imaging pipeline and to the artifacts resident in memory. Second, UI-visible mode transitions correspond to operational events (Freeze, Store/Capture, Review navigation) that change caching and retention behavior and therefore affect the persistence of diagnostic images and metadata in volatile memory. Third, UI state labeling is reproducible in practice: investigators can recreate states without relying on undocumented internal triggers, enabling repeatable acquisition schedules and defensible comparisons across memory dumps.

Figure 2 shows a representative GE Venue scanning screen used in our study. The figure is included solely to illustrate the UI elements used to define state and does not disclose patient identifiers. Depending on deployment configuration, the UI may display study context or patient fields; when present, such UI elements motivate privacy-aware acquisition and reporting because corresponding strings may also exist in process memory at capture time.

4.1. UI-defined investigation states

We define four investigation states based on observable UI modes and operator actions. These states are used to label memory dumps, interpret artifact persistence, and support workflow-grounded exposure assessment.

S0: Baseline idle. The device is booted and allowed to stabilize without initiating a scan workflow. The UI remains in a steady idle condition (e.g., home/ready screen). This state captures background execution and long-lived vendor components independent of recent clinical activity.

S1: Active scan. The device enters Scan mode using a fixed probe/preset configuration. Live acquisition runs continuously, implying rapid turnover of frame buffers and real-time rendering state. This state is expected to maximize transient buffer activity while limiting persistence unless explicit capture actions occur.

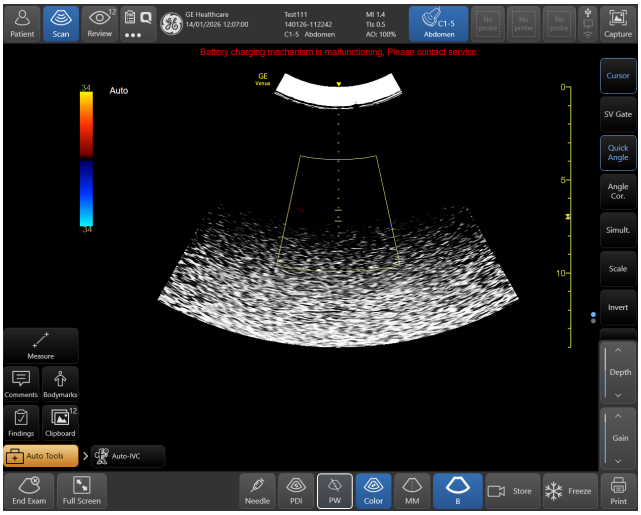

Figure 2: Representative GE Venue scanning interface used to define UI-anchored investigation states. UI modes and operator actions (e.g., Scan/Review, Freeze/Store/Capture) provide reproducible state labels for volatile acquisition and contextual anchors for interpreting memory-resident clinical artifacts.

S2: Post-capture retention. While remaining in the scan workflow, a controlled capture sequence is executed (e.g., Freeze followed by Store/Capture), after which the UI is left in a stable post-capture condition. This state is designed to increase the likelihood that frames, thumbnails, measurements, or derived objects remain resident beyond the live acquisition window.

S3: Review. The device transitions to Review mode and, study navigation is performed. This state is expected to induce additional caching (e.g., thumbnails, preview images, navigation metadata) and to increase persistence of diagnostic imagery and workflow metadata in UI and application memory.

State recording for reproducibility. At the moment each memory dump was initiated, we recorded (i) the state identifier (S0–S3), (ii) the device-local UI time displayed on-screen when available, and (iii) a de-identified photograph of the UI showing the active mode. These records provide a defensible link between acquisition time, operational state, and later interpretation of memory-resident artifacts.

4.2. Interpretation implications

UI state labeling reduces ambiguity in two recurring forensic tasks. First, it improves execution interpretation: process lineage and module sets can be evaluated relative to expected baseline behavior for the state at capture time. Second, it improves exposure assessment: the presence or absence of patient logs and diagnostic images in memory can be interpreted as workflow-conditioned outcomes rather than as random recoverability. This discipline is used throughout the analysis in Section 6 to characterize when patient-associated artifacts appear, how they persist across time offsets, and how acquisition timing affects what can be recovered.

5. Methodology

This section describes a reproducible, volatile-first protocol for evaluating forensic readiness on a constrained POCUS platform. The protocol is designed for an authorized examiner operating under policy-controlled conditions and emphasizes minimal footprint, integrity and provenance, and conservative interpretation. We operationalize URSA (Section 3.1) using UI-defined investigation states (Section 4.1) and evaluate feasibility and artifact yield through a seven-dump study. We established an acquisition-capable execution context using a software-based approach. Specifically, we leveraged the Sticky Keys accessibility exploit (Section 8.3) to obtain a command shell at the pre-login screen, from which a pinned acquisition toolchain could be launched from removable media. Memory was acquired via a software-based RAM imaging tool executed within this context; no direct hardware readout (e.g., JTAG or chip-off) was performed, although such techniques may be feasible in other scenarios. Full physical memory images were captured while labeling each acquisition with the observable UI state (S0–S3) at the time of collection. After RAM capture, we collected minimal disk-side context to characterize storage/permission boundaries and, where feasible, corroborate selected memory-observed components. All parsing, extraction, and validation were performed offline on hash-verified copies. The analysis targets three artifact classes aligned with the research questions: (i) execution artifacts for runtime reconstruction and baseline comparison, (ii) authentication artifacts reported categorically to characterize privilege exposure without disclosing sensitive values, and (iii) clinical exposure artifacts (patient logs and diagnostic images) validated conservatively and reported with de-identification.

5.1. Acquisition schedule and experimental design

We conducted a seven-dump acquisition study consisting of two baseline captures and five post-interaction captures. Baseline dumps (D1–D2) were collected in the S0 state to characterize stable background execution independent of clinical workflow interactions. Post-interaction dumps were collected after the controlled workflow, with D3–D4 in S2 and D5–D7 in S3. Post-interaction captures were intentionally spaced at multiple time offsets (t_1–t_5) to characterize persistence and decay of volatile artifacts, including both execution evidence and patient-associated content. This design supports direct comparison of pre and post-interaction artifact yields and enables state- and time-conditioned exposure assessment.

5.2. Integrity and footprint accounting

To preserve evidentiary defensibility, we applied integrity and footprint controls at each acquisition.

Action logging and bounded writes. We maintained an examiner action log that recorded commands executed, files copied, and directories touched on the device. Persistent writes were bound to the minimum necessary for tool staging and output storage and were restricted to documented

Table 3
Research questions (RQs), evaluated items, primary artifacts, and where evidence is reported.

RQ	What is evaluated	Primary artifacts / signals	Section(s)
RQ1	Volatile persistence and recoverability of PHI and telemetry using standard forensic techniques.	Patient logs (CSV), exam records/identifiers, diagnostic images (JPG), process and UI caches.	6.5
RQ2	Forensic readiness gains from volatile acquisition for patient exposure assessment and operational reconstruction.	Cross-dump artifact yield (D1–D7), UI-state conditioning (S0–S3), workflow/admin traces, runtime reconstruction.	5.1, 6.6
RQ3	Exposure of high-privilege authentication artifacts and potential hardening bypass.	Credential artifacts in RAM, `RID 500` attribution, offline feasibility testing (categorical), credential-enabled directory access.	6.4, 7.2
RQ4	Use of the readiness workflow to uncover latent weaknesses beyond incident response.	Ambiguous-provenance binaries (e.g., `echoloader.exe`), local execution pathways, corroboration limits.	6.3, 10

locations. We did not modify vendor executables or system configuration as part of the experimental protocol.

Evidence transfer and storage. Captured memory images and derived artifacts were transferred to evidence media and analyzed offline. Access to evidence was restricted, and PHI-bearing outputs were handled under the privacy controls described in Section 9.

5.3. Research question mapping

We structured the analysis around the research questions (Section 3). Table 3 summarizes how each research question is evaluated, which artifact classes are used, and where evidence is reported in the paper.

6. Memory Analysis of the GE Venue Ultrasound System

This section reports volatile artifacts recovered from seven full physical memory acquisitions collected under the URSA procedure (Section 5). We interpret artifacts using the UI-defined investigation states (Section 4.1) and the acquisition schedule (D1–D7). The objective is to characterize the evidence that can be practically recovered from RAM on a constrained ultrasound platform and how that evidence changes as a function of the clinical workflow state and time. We organize results into three artifact classes aligned with the research questions: (i) execution artifacts (runtime reconstruction), (ii) authentication artifacts (privilege exposure), and (iii) clinical exposure artifacts (patient-associated metadata and diagnostic imagery).

6.1. Memory Dump set and analysis validity

We analyzed seven full physical memory dumps acquired from the same platform. Two dumps (D1–D2) were collected in the baseline idle state (S0) prior to any scan-and-review interaction. Five dumps (D3–D7) were collected after a controlled workflow sequence spanning states S1–S3 and were intentionally spaced at multiple time offsets (t_1–t_5) to evaluate persistence and decay of volatile artifacts.

All analysis was performed offline. Before artifact extraction, we performed validity checks to reduce the risk of reporting parser artifacts as findings. These checks included confirming (i) correct OS profile selection consistent with the observed build family, and (ii) internal consistency of core kernel structures used by process and handle enumeration. Only dumps that passed these checks were used for downstream claims.

6.2. Execution artifacts and the ultrasound application runtime

Memory analysis consistently supported reconstruction of the clinical runtime environment. Process enumeration and lineage reconstruction revealed a stable vendor launch pathway in which `StartLoader.exe` initiates the clinical environment and transitions into the primary ultrasound application runtime. We also observed `EchoLoaderUI.exe` early in the launch chain, consistent with UI initialization. This stability is readiness-relevant because it provides a baseline anchor: responders can compare observed process trees and parent-child relationships against expected lineage for a given UI state.

Beyond the launch chain, we observed a set of long-lived vendor processes and services that remained present across both baseline and post-interaction dumps. We refer to the dominant, state-driving user-space process as the *EchoLoader.exe*. This process was consistently present in post-interaction captures and exhibited state-dependent memory surfaces that align with clinical workflow: during the Scan state, it is associated with live rendering and rapid buffer turnover; during the Post-capture and Review states, it is associated with increased caching and retention. These observations motivate the clinical artifact analysis in Section 6.5.

6.3. In-memory executable extraction and provenance

We extracted memory-resident executables and UI assets from selected processes to support provenance assessment and to demonstrate the evidentiary value of volatile acquisition under restrictive disk conditions. Extraction outputs were validated structurally (e.g., PE header consistency and section layout) prior to any enrichment or interpretation.

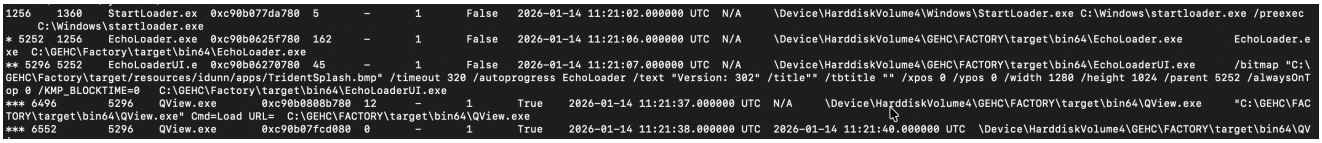

Figure 3: Process lineage reconstructed from memory illustrating the clinical launch pathway (i.e., `StartLoader.exe` → main ultrasound application runtime (`Echoloader.exe`)→ UI/Loader components).

This validation step is critical for avoiding false positives caused by partial dumping or parsing errors.

As a concrete example of UI-linked recovery, we extracted a splash-screen bitmap (`TridentSplash.bmp`) associated with the UI initialization pathway. Such assets provide verifiable anchors for correlating observed UI transitions with in-memory artifacts without relying on disk paths that may be access-restricted.

We also recovered a binary artifact labeled `echoloader.exe` via in-memory extraction. We treat this as an *ambiguous provenance artifact*. Its significance is operational: volatile acquisitions can surface binaries and runtime components that are not easily explained by responder-accessible disk telemetry in embedded environments. Under URSA, ambiguous artifacts are handled conservatively by (i) validating extraction correctness, (ii) evaluating recurrence across dumps and UI states, and (iii) seeking disk-side corroboration where feasible (Section 7). We avoid attributing intent without corroborating behavioral evidence.

6.4. Authentication artifacts and privilege exposure

We evaluated the dump set for authentication artifacts to assess whether privileged credential material is recoverable from RAM under the studied configuration. Findings are reported as risk characterization rather than disclosure. In our analysis, we recovered authentication artifacts, as shown in Figure 4, sufficient to identify a high-privilege account context and to evaluate feasibility under controlled offline conditions.

To interpret the impact of privilege without disclosing sensitive values, we used standard Windows account semantics. The recovered account identifier corresponded to `RID 500`, which denotes the built-in Windows *Administrator* account [7]. This mapping matters because it distinguishes a generic local user from the highest-privilege built-in principal, thereby elevating the security implications of recoverability.

Offline feasibility testing was performed solely to characterize risk. Specifically, we used John the Ripper [8] to evaluate whether recovered hash material could be dehashed under controlled conditions. We do not report any credential values and avoid operational details that could enable misuse. The readiness implication is that privileged authentication artifacts may be present in volatile memory and should be handled as sensitive evidence; from a security perspective, recoverability weakens hardening assumptions and can expand both the defender's and the adversary's capabilities.

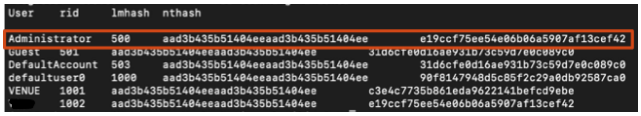

Figure 4: Authentication artifact extraction from memory. The account context corresponds to `RID 500` (built-in Admin).

6.5. Clinical exposure artifacts: patient logs and diagnostic images

The most operationally sensitive artifacts recovered from volatile memory were PHI-bearing metadata and diagnostic imagery. These artifacts are central to incident response because they inform both forensic reconstruction and privacy exposure assessment. They also illustrate why a volatile-first strategy is necessary: such artifacts can exist primarily in memory and can be shaped by workflow actions that are not reliably reflected in disk telemetry.

Structured logs and records. We recovered structured patient-associated logs in CSV form from volatile memory using standard memory-assisted recovery techniques. Across the post-interaction series, later captures yielded richer, more structured logs than earlier ones. In particular, the latest dump (D7) contained the most detailed patient log representation observed in our study, indicating that workflow progression and caching can increase metadata richness over time. This result implies that a single snapshot may understate exposure: as workflow continues, additional identifiers, timestamps, and administrative metadata may remain resident in memory even without additional explicit user actions.

Diagnostic images. We also recovered diagnostic images in standard image formats (i.e., JPG) from volatile memory. Recovered images were conservatively validated through renderability checks and basic file consistency tests. The presence of renderable diagnostic content in RAM, particularly in post-capture and review states, supports the conclusion that imaging workflows can leave clinically meaningful content resident beyond the immediate live-acquisition window.

These findings address **RQ1** by demonstrating recoverability of PHI-bearing artifacts and system telemetry using standard forensic techniques, and they address **RQ2** by showing that volatile acquisition enables exposure assessment and workflow reconstruction even when disk-first telemetry is limited.

6.6. Reproducibility across seven dumps

Comparing artifacts across D1–D7 revealed consistent state dependence aligned with clinical workflow expectations. Baseline captures (D1–D2) primarily supported platform characterization and process-level reconstruction,

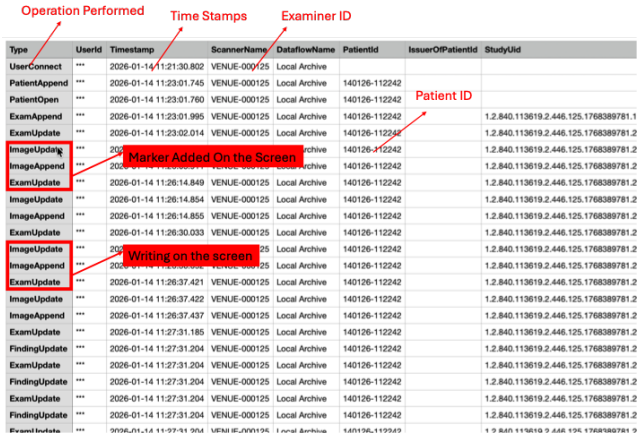

Figure 5: Patient-associated log recovered from memory

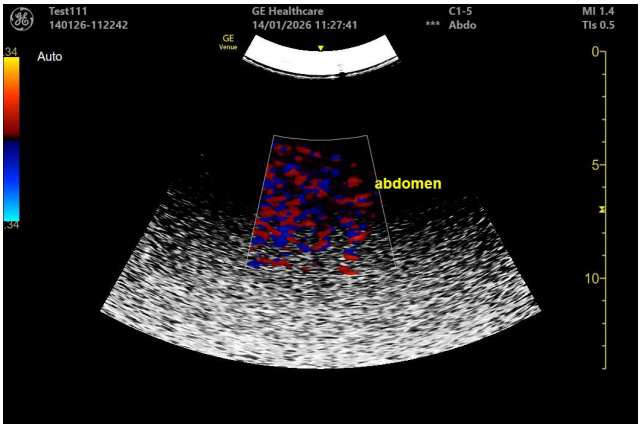

Figure 6: Diagnostic image recovered from volatile memory .

Table 4
Artifact yield across seven memory samples. Counts reflect recovered patient-log CSV lines and extracted JPG artifacts; D7 contains the most detailed patient log.

Dump	Condition	Offset	CSV	JPGs
D1	Pre-interaction	Baseline	0	0
D2	Pre-interaction	Baseline	0	0
D3	Post-interaction	$t_1 \approx 5$ min	18	0
D4	Post-interaction	$t_2 \approx 30$ min	24	0
D5	Post-interaction	$t_3 \approx 60$ min	36	1
D6	Post-interaction	$t_4 \approx 120$ min	66	1
D7	Post-interaction	$t_5 \approx 150$ min	**96**†	1

†Most detailed (richer) patient log observed in this dump.

with minimal recovery of patient-associated artifacts. Post-interaction captures (D3–D7) yielded substantially richer clinical artifacts, including structured logs and recoverable images.

To summarize artifact yield, Table 4 reports counts of recovered patient-log CSV lines and extracted diagnostic images across the seven dumps. This table provides a compact, reviewer-friendly view of the key reproducibility claim: post-interaction captures consistently yielded clinical artifacts, and the latest capture produced the richest structured log.

6.7. Summary

In summary, volatile acquisition on the GE Venue platform yielded four readiness-relevant outcomes. First, it enabled stable reconstruction of the clinical launch pathway and runtime baseline anchors. Second, it supported the extraction of in-memory executables and UI assets, including ambiguous provenance artifacts that require conservative handling and corroboration. Third, it revealed privileged authentication artifacts associated with the built-in Administrator principal (`RID 500`) under the studied configuration, motivating both defensive mitigation and privacy-aware evidence handling. Fourth, it demonstrated the recoverability of PHI-bearing structured logs and diagnostic images from RAM, with artifact richness increasing after workflow interaction and with the latest dump yielding the most detailed patient log. Together, these findings support URSA's volatile-first readiness principle and motivate repeated, UI-labeled acquisition when estimating exposure and reconstructing activity on constrained ultrasound platforms.

7. Disk Analysis of the GE Venue Ultrasound System

This section reports disk-side context and explains how persistent observations corroborate and constrain the volatile findings in Section 6. On embedded ultrasound platforms, disk analysis is often incomplete due to segmented storage, restrictive permissions, and vendor-managed telemetry. Nevertheless, targeted disk context remains useful to (i) characterize responder-relevant boundaries (where writes and execution are permitted), (ii) corroborate selected memory observed components, and (iii) scope persistent clinical exposure surfaces.

7.1. Storage layout and permission boundaries

The device exposes multiple volumes with uneven permissions and execution constraints. In our environment, several vendor-controlled locations were not suitable for arbitrary tool execution, and writable-executable locations were limited. These boundaries directly affect forensic readiness by constraining where acquisition tools can be staged and what disk artifacts can be collected without modifying the clinical stack. From both a defensive and investigative perspective, any writable-executable staging paths are dual-use and should be treated as high-value: responders must footprint-account for writes, and defenders should consider hardening controls that reduce unnecessary write/execute surfaces.

7.2. Credential-enabled access expansion and persistent clinical artifacts

Disk-side visibility increased after the volatile authentication findings (Section 6.4). Using the recovered administrative credentials under an authorized examiner model, we were able to traverse additional directories via `cmd.exe` and Windows Explorer. This enabled the identification of saved ultrasound scan images stored on disk, confirming a persistent exposure surface beyond RAM. We report this finding

in a privacy-preserving manner and do not disclose patient identifiers, filenames, or operational directory structures. The readiness implication is that volatile acquisition can unlock corroborating disk context, while the security implication is that recoverable privileged authentication artifacts can materially expand access if obtained by an adversary.

7.3. Summary

In summary, disk analysis primarily served as constrained corroboration and boundary characterization. It documented storage and permission constraints that limit disk-first response and confirmed that diagnostic images may persist on disk once access is available, complementing the volatile exposure evidence recovered from memory.

8. Related Work and Comparative Analysis

Digital forensics on regulated medical devices remains underdeveloped relative to enterprise endpoints. Prior work has largely emphasized vulnerability discovery, network exposure, and risk modeling in the Internet of Medical Things (IoMT) ecosystem, while comparatively fewer studies provide end-to-end, evidence-driven investigation procedures that can be executed under realistic clinical constraints [9]. This section situates our work across three themes: (i) forensic readiness for medical devices, (ii) volatile memory forensics on embedded and specialized platforms, and (iii) interpretation challenges introduced by vendor opacity and legacy components.

Existing efforts fall into two broad categories that each leave significant gaps when applied to high-complexity clinical systems. Prior medical device forensic frameworks [10, 11, 12, 13, 14, 15, 16, 17, 18] were designed for constrained embedded targets, such as ECG monitors or industrial controllers, and do not account for the hybrid OS environment, rich patient data exposure, or supply chain ambiguity present in modern imaging platforms. Conventional Windows forensic practice, by contrast, assumes privileged access, persistent logging infrastructure, and disk-first acquisition strategies that are incompatible with vendor-locked clinical deployments.

Table 5 compares both categories against URSA across eight investigative dimensions. The differences from conventional Windows forensics are structural rather than parser-level: URSA applies the same underlying tooling (Volatility 3) but reorganizes acquisition priority, labeling, and evidence handling around embedded clinical constraints. The differences from prior medical device frameworks are more fundamental, addressing device complexity, PHI exposure, and supply chain opacity that simpler targets do not encounter. Taken together, these comparisons support the central argument of this work: the primary gap in medical device forensics is *procedural* rather than technical, and existing tools can be made effective through a domain-appropriate readiness framework.

8.1. Forensic Framework for Medical Devices

The security of medical devices has been extensively surveyed, with focus often placed on network-level vulnerabilities and encryption deficits. Newaz et al. [4] and recent industry reports [25] confirm that a significant majority of clinical devices harbor known vulnerabilities. However, these studies primarily focus on prevention rather than investigation.

Prior forensic frameworks have successfully targeted simpler embedded systems. Grispos et al. [10] proposed methods for ECG devices, and Rais et al. [11] developed models for industrial controller memory. While foundational, these frameworks address devices with constrained data models and limited OS functionality.

Unlike the lightweight approaches suitable for ECGs or PLCs, our proposed framework addresses the hybrid nature of modern ultrasound systems, which function as both safety-critical firmware and general-purpose workstations (Windows Embedded). Existing generic IoMT frameworks fail to account for the convergence of high-fidelity patient imagery, hospital infrastructure integration (PACS/EHR), and complex OS file systems [12, 26, 27, 28]. Our framework fills this gap by defining specific readiness criteria for hybrid artifacts, integrating system logs with clinical application data, which we validated through the successful reconstruction of patient workflows on the real-world POCUS system.

8.2. Volatile Memory Forensics

Memory forensics is established as a standard discipline for enterprise systems, using frameworks such as Volatility [29]. However, its application to proprietary medical devices has historically been viewed as challenging due to non-standard hardware and restricted environments. While recent studies, such as Mishra et al. [30], have successfully demonstrated the applicability of Volatility in the broader IoMT domain, there remains a lack of validation on high-complexity, real-world medical imaging platforms like the GE Venue.

Our investigation validates that standard forensic tooling remains highly effective for these complex clinical devices without requiring custom kernel modules. By applying the Volatility plugin ecosystem to the acquired memory image, we confirmed the feasibility of extracting critical artifacts from a locked-down medical OS: Plugins such as `pslist` and `psscan` successfully mapped the proprietary application stack, distinguishing between OS services and clinical executables. The use of `dumpfiles` and `memdump` allowed for the extraction of non-file-system-bound data, which is critical in medical devices where local disk storage is often encrypted or restricted.

This finding demonstrates that entirely bespoke tooling is not a prerequisite for medical device forensics, but rather that the primary challenge lies in the acquisition strategy and the interpretation of domain-specific data structures.

8.3. Addressing Supply Chain Opacity

A critical finding from our framework's application is the opacity of the medical software supply chain, which

Table 5
Comparison of prior medical/IoMT forensic frameworks, conventional Windows memory forensics, and the URSA workflow.

Dimension	Prior Medical/IoMT Frameworks	Conventional Windows Forensics	URSA (This Work)
Target platform	Constrained embedded devices (ECG, PLC, infusion pump) with limited OS functionality [10, 11].	General-purpose Windows workstation with full OS and application stack assumed [19, 20, 21].	Hybrid clinical platform: Windows Embedded with a proprietary imaging layer (§ 2).
Execution environment	Physical or vendor-assisted access, often platform-specific.	Full admin access assumed; agents and tools install freely [21, 22].	No persistent agents; accessibility workaround and removable media staging (§ 5).
Acquisition priority	Device log or firmware extraction with memory not prioritized [13].	Disk-first with memory acquisition optional [23].	Volatile-first; RAM before disk (§ 3).
Acquisition labeling	None or timestamp-based with no clinical workflow context.	Timestamp-based with no application-layer context.	UI-state-driven: captures tied to clinical modes (S0–S3) (§ 4.1).
Artifact interpretation	Matched against device-specific known states or vendor specifications.	Compared against OS baselines, golden images, or threat intelligence feeds [24].	Clinical launch chain and vendor process lineage as baseline (§ 6).
PHI handling	Not addressed; devices assumed to hold minimal patient data [12].	General PII policies with no domain-specific controls.	Explicit readiness objective (O5): PHI-aware acquisition and reporting (§ 3.2).
Supply chain opacity	Not addressed; constrained targets have transparent firmware stacks.	Not a primary concern; OS and application provenance generally traceable.	Legacy vulnerabilities and proprietary behavioral ambiguity (§ 6, § 8.3).
Tooling assumption	Custom or platform-specific tools with limited cross-device transferability.	EDR, centralized logs, and standard forensic suites available.	Volatility 3 offline on hash-verified images, no EDR (§ 5).

manifests in two distinct *forms*: the persistence of unpatched legacy components and the behavioral ambiguity of proprietary vendor software.

The first *form* creates a *legacy vulnerability* landscape due to the failure to manage upstream dependencies. Our analysis revealed that the device was susceptible to the Sticky Keys exploit, a commodity Windows vulnerability [31]. The presence of this decade-old vector in a modern medical device highlights a significant failure in the supply chain lifecycle, vendors often ship frozen OS configurations to maintain certification, inadvertently preserving known vulnerabilities. While we leveraged this for forensic acquisition, it fundamentally represents a security lapse inherent to the medical supply chain.

Beyond legacy flaws, the proprietary software layer introduces interpretation challenges [32]. Our analysis of the `echoloader.exe` binary revealed legitimate medical software exhibiting behaviors indistinguishable from "dropper" malware, such as:

- Dynamic Loading: The use of `mscoree.dll` and dynamic assembly loading obscures static analysis.
- Telemetry vs. C2: The `Idunn` telemetry packages bear structural similarities to malicious Command and Control (C2) traffic.

These characteristics strongly resemble dropper-style or loader malware designed to quietly introduce second-stage payloads or siphon data. By leveraging external threat intelligence platforms, specifically *VirusTotal* and *CrowdStrike*, we correlated these behaviors with known malware patterns, confirming overlaps in C2 IP addresses and library signatures.

Our framework addresses this opacity by enforcing dynamic memory analysis as a requisite step to distinguish between vendor-sanctioned anomaly and genuine compromises.

9. Ethical handling and privacy controls

Because our analysis recovers PHI-bearing artifacts (e.g., patient logs and diagnostic images) from volatile memory, we applied privacy and governance controls throughout acquisition, analysis, and reporting. All work was performed under an authorized examiner model in a controlled setting and not during patient care. Evidence was handled in accordance with data-minimization principles: we characterized artifact classes, recoverability, and persistence trends without collecting or disclosing identifiers beyond what was necessary for validation.

Memory images and derived artifacts were transferred to encrypted evidence media and analyzed offline on restricted

systems. Access was limited to authorized personnel, and PHI-bearing intermediate outputs were retained only long enough to validate results. All screenshots, logs, and images included in the paper are de-identified and redacted; we avoid publishing patient identifiers, file paths, filenames, or operational directory structures that could identify patients. Dual-use considerations were addressed by reporting access-enabling conditions at a high level and focusing on defensive implications rather than operational instructions. External enrichment services, when used, are treated as a triage context rather than as proof of compromise.

10. Discussion and Recommendations

Our results indicate that forensic readiness on embedded ultrasound platforms is limited less by the absence of evidence than by the ability to acquire and interpret evidence under restrictive execution and storage policies. Volatile memory provided the highest-yield source for both incident scoping (runtime reconstruction and authentication context) and privacy exposure assessment (recoverable logs and diagnostic images). Because PHI-bearing artifacts were state- and time-dependent and became richer in later post-interaction dumps, responders should treat memory acquisition as a primary step and label captures by observable UI state; where feasible, repeated captures at controlled offsets improve defensibility.

Baseline-driven interpretation is also critical when logs are sparse. Hospitals can improve readiness by capturing known-good baselines during maintenance windows (e.g., process trees for idle and scanning states and hashes of core vendor executables) and using them to interpret deviations during investigations. Given the observed recoverability of privileged authentication artifacts and the expansion of disk visibility under administrative context, mitigations should prioritize reducing local privilege exposure, tightening write/execute boundaries on staging paths, and enforcing removable-media and pre-login access controls within vendor- and certification-constrained environments. Incident response reporting should include a privacy exposure assessment that inventories PHI-bearing artifact classes observed and summarizes how recoverability varies by state and time.

Limitations. This study evaluates one platform configuration and a controlled workflow; persistence will vary with software versions, settings, and clinical usage. Broader validation across models is required to generalize quantitative estimates.

11. Conclusion

This paper presents a volatile-first forensic readiness study of a commercial POCUS ultrasound platform using the GE Venue system as a case study. We introduced URSA, a readiness workflow for constrained ultrasound devices, and operationalized it with UI-defined acquisition states to support reproducible evidence collection and interpretable analysis.

Across seven full physical memory dumps (two baseline and five post-interaction), we demonstrated repeatable acquisition and offline analysis using standard forensic techniques. Memory analysis reconstructed the clinical runtime baseline and recovered both security-relevant artifacts (execution lineage, extracted components, and high-privilege authentication artifacts) and privacy-relevant artifacts (structured patient logs and diagnostic images). Artifact richness increased after workflow interaction, and the latest dump contained the most detailed patient log observed in our study. Targeted disk context characterized permission boundaries and corroborated selected results, and administrative access enabled identification of stored ultrasound images, confirming a persistent exposure surface beyond RAM.

Overall, our results show that volatile acquisition is central to incident scoping and PHI exposure assessment on embedded ultrasound systems, and that readiness improves when acquisition is state-labeled, integrity-preserving, and privacy-aware. Future work should validate these findings across additional models and software configurations.

Acknowledgment

This work is partially supported by the National Science Foundation under Grant Award Number 2212424 and the CCI Central Virginia Node.

References

[1] C. Li, A. Raghunathan, N. Jha, Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system, in: 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2011, 2011, pp. 150–156. doi:10.1109/HEALTH.2011.6026732.

[2] D. Halperin, T. Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, W. Maisel, Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses, Security and Privacy, IEEE Symposium on 0 (2008) 129–142. doi:10.1109/SP.2008.31.

[3] N. Ellouze, S. Rekhis, N. Boudriga, M. Allouche, Cardiac implantable medical devices forensics: Postmortem analysis of lethal attacks scenarios, Digital Investigation 21 (2017) 11–30. doi:https://doi.org/10.1016/j.diin.2016.12.001.
URL https://www.sciencedirect.com/science/article/pii/S1742287616301426

[4] A. I. Newaz, A. K. Sikder, M. A. Rahman, A. S. Uluagac, A survey on security and privacy issues in modern healthcare systems: Attacks and defenses, ACM Transactions on Computing for Healthcare 2 (3) (2021) 1–44.

[5] Y. Forihat, C. Taylor, R. A. Awad, I. Ahmed, Security assessment of an lbp16-protocol-based computer numerical control machine, in: International Conference on Critical Infrastructure Protection, Springer, 2024, pp. 65–84.

[6] M. Elyas, A. Ahmad, S. B. Maynard, A. Lonie, Digital forensic readiness: Expert perspectives on a theoretical framework, Computers & Security 52 (2015) 70–89.

[7] J. Kävrestad, M. Birath, N. Clarke, Fundamentals of digital forensics: A guide to theory, research and applications, Springer Nature, 2024.

[8] The Openwall Project, John the Ripper Password Cracker, https://github.com/openwall/john, accessed: 2026-02-06 (2025).

[9] M. Ahsan, B. Najarro-Blancas, J. T. Ebode, N. Lewinski, I. Ahmed, 3d bioprinter firmware attacks: Categorization, implementation, and impacts, in: 2025 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), IEEE, 2025, pp. 99–110.

[10] G. Grispos, F. Tursi, W. Mahoney, A digital forensic analysis of an electrocardiogram medical device: A first look, Wiley Interdisciplinary Reviews: Forensic Science 6 (2) (2024) e1535.
[11] M. H. Rais, R. L. Asmar-Awad, J. L. Jr., I. Ahmed, Memory forensic analysis of a programmable logic controller in industrial control systems, Forensic Science International: Digital Investigation 40 (2022) 301339, supplement.
[12] B. Shanmugam, S. Azam, Risk assessment of heterogeneous iomt devices: a review, Technologies 11 (1) (2023) 31.
[13] V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, S. Katsikas, A forensics-by-design management framework for medical devices based on blockchain, in: 2019 IEEE world congress on services (SERVICES), Vol. 2642, IEEE, 2019, pp. 35–40.
[14] C. DeVoe, S. Rahman, Incident response plan for a small to medium sized hospital, arXiv preprint arXiv:1512.00054 (2015).
[15] N. Ameen, R. Vijayakanthan, A. Ayub, A. Ali-Gombe, I. Ahmed, Wavesleuth: Retrospective plc memory for anomaly detection in industrial control systems, in: 2025 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), IEEE, 2025, pp. 170–181.
[16] H. Jahankhani, J. Ibarra, Digital forensic investigation for the internet of medical things (iomt), Journal of Forensic, Legal & Investigative Sciences 5 (2) (2019) 1–6, article 029 (publisher lists it as 100029). doi:10.24966/FLIS-733X/100029.
URL https://www.heraldopenaccess.us/openaccess/digital-forensic-investigation-for-the-internet-of-medical-things-iomt
[17] M. Ahsan, I. Ahmed, Wattshield: A power side-channel framework for detecting malicious firmware in fused filament fabrication, in: 2025 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), IEEE, 2025, pp. 438–449.
[18] M. Ahsan, E. Pak, K. Jackson, M. H. Rais, B. Najarro-Blancas, N. Lewinski, I. Ahmed, Biosafe: Bioprinting security framework for detecting sabotage attacks on printability and cell viability, in: 2024 Annual Computer Security Applications Conference (ACSAC), IEEE, 2024, pp. 271–287.
[19] B. Carrier, File System Forensic Analysis, Addison-Wesley Professional, 2005.
[20] H. Carvey, Investigating Windows Systems, Academic Press, 2018. doi:10.1016/C2017-0-00408-3.
[21] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition, Academic Press, 2011.
[22] K. Kent, S. Chevalier, T. Grance, H. Dang, Guide to integrating forensic techniques into incident response, Tech. Rep. SP 800-86, National Institute of Standards and Technology (2006). doi:10.6028/NIST.SP.800-86.
[23] S. L. Garfinkel, Digital forensics research: The next 10 years, Digital Investigation 7 (2010) S64–S73. doi:10.1016/j.diin.2010.05.009.
[24] M. H. Ligh, A. Case, J. Levy, A. Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, John Wiley & Sons, 2014.
[25] A. Das, Infusion pump vulnerabilities: Common security gaps, Unit 42, Palo Alto Networks, accessed July 23, 2025 (Mar. 2022).
URL https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/
[26] L. Dzamesi, N. Elsayed, A review on the security vulnerabilities of the iomt against malware attacks and ddos, arXiv preprint arXiv:2501.07703 (2025).
[27] V. Schmitt, Medical device forensics, IEEE Security & Privacy 20 (1) (2022) 96–100.
[28] M.-H. Maras, A. S. Wandt, State of ohio v. ross compton: Internet-enabled medical device data introduced as evidence of arson and insurance fraud, The International Journal of Evidence & Proof 24 (3) (2020) 321–328. arXiv:https://doi.org/10.1177/1365712720930600, doi:10.1177/1365712720930600.
URL https://doi.org/10.1177/1365712720930600
[29] A. Walters, N. L. P. Jr., Volatools: Integrating volatile memory forensics into the digital investigation process, in: Black Hat DC, 2007.
[30] A. Mishra, P. Bagade, Digital forensics for medical internet of things, in: 2022 IEEE Globecom Workshops (GC Wkshps), IEEE, 2022, pp. 1074–1079.
[31] MITRE, Accessibility features (att&ck technique t1546.008), https://attack.mitre.org/techniques/T1546/008/, accessed 2025 (2025).
[32] G. HealthCare, EchoPAC Connect Product, https://www.gehealthcare.com/products/ultrasound/vivid/echopac.

A. Supplementary Evidence Artifacts

This appendix provides additional evidence of artifacts referenced in the main text. All outputs are de-identified and redacted in accordance with the privacy controls described in Section 9. These materials are included to strengthen the transparency and reproducibility of the reported findings.

A.1. Diagnostic Images Recovered from Disk

Figure 7 presents six representative images recovered from vendor-managed directories accessible only after administrative authentication. Patient identifiers and file paths have been redacted.

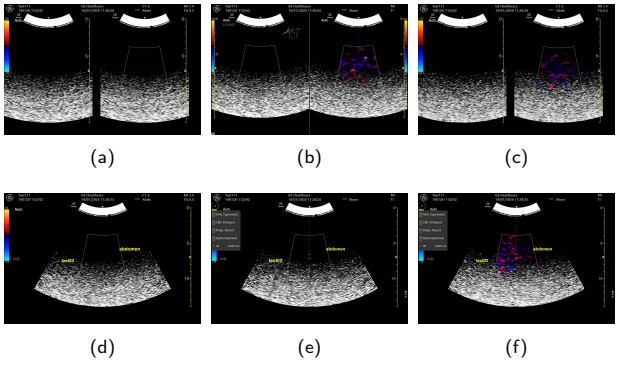

Figure 7: Diagnostic images recovered from persistent storage after credential-enabled access expansion. Images (a)–(f) are saved scan outputs found on vendor-managed disk partitions, accessible only after administrative authentication.

A.2. Representative Patient-Log Field Structure

Table 6 describes the field structure observed in structured patient-associated logs recovered from volatile memory (Section 6.4). Field names are reported as observed; all sample values shown are synthetic examples used solely to illustrate data types and are not drawn from actual patient records.

Table 6: Representative field structure of patient-associated CSV logs recovered from volatile memory.

Field	Data Type	Synthetic Example
Operation Type	String	`ExamUpdate`
User ID	String	`user_001`
Timestamp	DateTime	`2026-01-14 11:28`
Scanner Name	String	`VENUE-00XXX`
Data Store Name	String	`Local Archive`
Patient ID	Numeric	`XXXXXX`
Issuer of Pat. ID	OID String	`X.X.XXX.X. . .`
Study ID	Numeric	`X`