Seeing the Evidence: A Forensic Framework for Analyzing Ray-Ban Meta AI Smart Glasses

Shishir Panta[a,b], Ruba Alsmadi[a,b], Ibrahim Baggili[a,b]

[a] *Baggili(i) Truth (BiT) Lab, Center of Computation & Technology, Baton Rouge, LA, USA*
[b] *Division of Computer Science & Engineering, Louisiana State University, Baton Rouge, LA, USA*

Abstract

Meta's Ray-Ban smart glasses, paired with the Meta AI mobile application, are part of a rapidly growing class of generative AI-enabled wearable devices, with over two million units sold by early 2025. As adoption increases, these devices are becoming increasingly relevant to civil and criminal investigations. However, the forensic landscape for these systems remains underexplored and is not yet supported by existing tools. This paper presents (i) a forensic methodology for acquiring and analyzing the Ray-Ban Meta ecosystem, (ii) a forensic framework that formalizes evidence distribution, correlation, and attribution across the glasses–companion–cloud ecosystem, and (iii) an open-source contribution that operationalizes these findings. Through privileged filesystem acquisition of the Android companion application and correlation with Meta cloud exports, we recover and validate account and device identifiers, media artifacts, geolocation traces, and AI interaction records. We further evaluate user-initiated anti-forensic actions, including deletion, unpairing, and factory reset, demonstrating that certain identifiers and traces persist across these attempts and that cloud exports retain complementary conversational evidence. We also develop a Meta AI Parser plugin for the Android Logs, Events, and Protobuf Parser (ALEAPP) to automate artifact extraction and timeline correlation, providing digital forensic practitioners with a practical workflow for investigating generative AI-enabled smart glasses.

Keywords: Digital Forensics, Wearable Forensics, Smart Glasses, Ray-Ban Meta, GenAI

1. Introduction

Wearable computing has evolved rapidly over the past decade, with smart glasses emerging as a consumer-ready yet forensically understudied device category. Unlike earlier prototypes such as Google Glass (Rongen and Geradts, 2017) or Snap Spectacles (VanPutte et al., 2022), which faced limited adoption, current-generation smart glasses have achieved significant market penetration. By early 2025, Meta had sold over two million units and announced plans to scale annual production to ten million units by 2026 (Heaney, 2026).

Modern smart glasses, such as the Meta Ray-Ban platform, integrate cameras, microphone arrays, and near real-time AI assistance within a discreet, everyday form factor (Meta, 2025). While this design enables hands-free media capture and AI interaction, it also introduces new challenges for privacy, surveillance, and digital forensics (Iqbal and Campbell, 2023; Gallardo et al., 2023), particularly by complicating detection and attribution compared to smartphones or traditional wearables.

The forensic relevance of these devices became apparent in January, 2025, when the FBI disclosed that the perpetrator of the New Orleans attack had used Meta Ray-Ban glasses for reconnaissance (Bacon, 2025). Academic studies have further demonstrated their surveillance potential; for example, Cox (2024) reported on a system built by AnhPhu Nguyen and Caine Ardayfio that combined smart glasses with facial recognition systems to identify individuals in real time. These cases highlight the growing likelihood that smart glasses will appear in criminal investigations and underscore the need for systematic forensic methodologies tailored to this device class.

This need is amplified by the rapid expansion of the smart glasses market. Counterpoint Research (2025) reported that global shipments rose 210% year-on-year in 2024 and projected compound annual growth of smart glasses sales above 60% through 2029. So, Generative AI (GenAI) enabled smart glasses are now transitioning from niche devices to mainstream consumer electronics.

From a forensic perspective, smart glasses with cloud-backed GenAI assistants introduce challenges that differ from those associated with smartphones and earlier wearables. First, they distribute evidentiary traces across devices, companion applications, and remote cloud services that mediate assistant interactions. Second, they generate assistant-specific artifacts such as voice interaction logs, conversational logs, and visual query metadata that were absent from earlier non-generative smart-glasses platforms. Existing work on mobile phone forensics (Alghafli et al., 2012), smartwatch analysis (Park et al., 2024), and

Email addresses: spanta6@lsu.edu (Shishir Panta), ralmsa1@lsu.edu (Ruba Alsmadi), baggili@gmail.com (Ibrahim Baggili)

IoT ecosystems (Kim et al., 2023) does not address this combination of cross-layer evidence distribution and generative AI interaction.

Prior forensic studies of smart glasses have primarily focused on device-specific artifact recovery. Rongen and Geradts (2017) rooted Google Glass to extract logs and media files, while VanPutte et al. (2022) analyzed the Snapchat companion application for Snap Spectacles, recovering thumbnails and device metadata. These studies predate the integration of conversational AI and cloud-assisted processing and therefore do not capture the forensic complexity of current GenAI-enabled smart glasses.

This gap motivates the present work. Rather than cataloging artifacts for a single device, we develop an empirically derived forensic framework for GenAI-enabled smart glasses that structures artifact categorization, event reconstruction, and anti-forensic analysis. We instantiate and evaluate this framework through forensic analysis of the Meta Ray-Ban smart glasses and their Android companion application. Two research questions guide this study:

- **RQ1:** What categories of forensic artifacts exist in GenAI-enabled smart glasses ecosystems, and how can they be organized into a generalizable framework?
- **RQ2:** How resilient are these artifacts to user-initiated anti-forensic actions, and what are the implications for forensic investigations?

To address these questions, we conducted controlled experiments across multiple acquisition stages using an Android device paired with Meta Ray-Ban glasses. Both privileged and non-privileged acquisitions were performed, and forensic as well as user-initiated anti-forensic actions were systematically evaluated. Based on these experiments, we developed a custom Meta AI parser that can be integrated into the ALEAPP framework (Brignoni, 2023). The main contributions of this work are: **(C1)** an empirically grounded forensic framework for GenAI-enabled smart glasses that formalizes artifact taxonomy, event reconstruction, and cross-layer attribution; **(C2)** an open-source ALEAPP plugin ("Meta AI Parser") that automates artifact extraction and timeline correlation from the Meta AI companion application; and **(C3)** a case study demonstrating how the framework supports forensic reconstruction under realistic conditions.

The remainder of this paper is organized as follows. Section 2 reviews prior work in wearable and AI application forensics. Section 3 describes the experimental methodology, followed by artifact findings in Section 4. Section 5 presents the derived forensic framework, which is applied in a case study in Section 7. Section 6 discusses implications and limitations, and Section 8 concludes the paper.

2. Background and Related Work

This section describes the architecture of the smart glasses ecosystem and situates this work within prior research on wearable and AI application forensics.

2.1. Forensic Access Model for Smart-Glasses Ecosystem

Current-generation smart glasses integrate on-device sensors with a cloud-connected companion application (Meta, 2025). Unlike standalone wearables such as fitness trackers, which primarily store data locally or synchronize with a single backend service, these devices operate within a three-layer ecosystem. The glasses capture media and support voice-driven interactions, the companion mobile application synchronizes data, and the cloud service supports AI processing and stores user interaction data (Grumeza et al., 2025; Dipert, 2025).

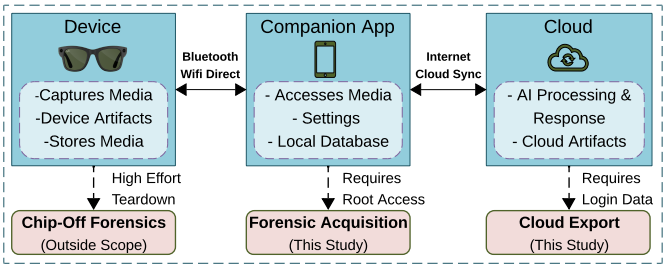

Figure 1: Three-layer forensic access model for GenAI smart glasses.

From a forensic perspective, this architecture distributes evidence across multiple layers, each presenting distinct acquisition challenges. As illustrated in Figure 1, evidentiary artifacts may reside at:

- **The Device Layer** *(Glasses)*: Responsible for media capture and voice input, with data stored temporarily in onboard flash memory. Access to this layer typically requires invasive physical acquisition techniques.
- **The Application Layer** *(Mobile Device)*: The companion application synchronizes content from the glasses and records interaction metadata. Artifacts at this layer are accessible through standard mobile forensic methods, often requiring elevated privileges.
- **The Cloud Layer** *(Cloud Servers)*: Stores AI conversation history, processed media, and account-level metadata. Access generally depends on user credentials or legal process.

This study focuses on the application and cloud layers, which are accessible through logical acquisition and do not require destructive hardware analysis. Direct physical extraction from the glasses themselves is outside the scope of this work and is left for future investigation.

2.2. Wearable Device Forensics

Early forensic research on wearable devices emphasized direct on-device acquisition. Rongen and Geradts (2017) analyzed Google Glass by rooting the device to recover logs, voice commands, and captured media, while Baggili et al. (2015) examined smartwatches to extract emails, fitness records, and voice memos. These studies demonstrated the evidentiary value of on-device storage but relied on invasive techniques that risk data modification.

As wearable hardware became more integrated and less accessible, forensic analysis increasingly shifted toward companion applications. For example, VanPutte et al. (2022) showed that although Snap Spectacles offered limited on-device access, the paired Snapchat application contained recoverable media and device-linkage metadata. Similar approaches have been applied to fitness trackers (MacDermott et al., 2019) and medical device ecosystems (Grispos et al., 2023), allowing recovery of GPS data, biometric information, and persistent identifiers.

Contemporary smart glasses further complicate direct hardware extraction due to tightly integrated components, often requiring destructive techniques such as chip-off analysis (Figure 2) (Dipert, 2025). As a result, application- and cloud-level artifacts have become the primary sources of forensic evidence.

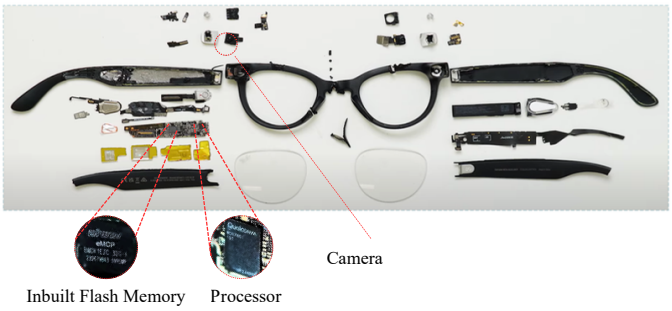

Figure 2: Teardown of Ray-Ban Meta glasses, illustrating integrated camera, storage, and sensor components (Dipert, 2025).

The integration of generative AI introduces additional forensic complexity. Studies of AI-driven applications, such as ChatGPT, have shown that evidentiary artifacts are distributed across local storage and cloud services (Dragonas et al., 2024; Tyagi et al., 2025; Kankanamge et al., 2025). Other work has explored forensic workflows for AI-enabled systems more broadly (Cho et al., 2025) but does not cover GenAI-based wearable devices.

Research Gap. Existing forensic studies of smart glasses do not include the integration of conversational AI, while current AI forensics focuses on standalone software without wearable hardware involvement. As a result, existing work does not examine devices that support covert audio-visual capture, near real-time cloud-based AI processing, and evidence distribution across wearable, mobile, and cloud layers. This work addresses this gap by developing a forensic framework for GenAI-enabled smart glasses and validating it through a controlled study of the Meta Ray-Ban ecosystem.

3. Methodology

This section describes the experimental setup and forensic workflow used to identify, acquire, and analyze artifacts generated by the Meta Ray-Ban smart glasses and their Android companion application. All experiments were conducted in a controlled environment summarized in Table 1.

Table 1: Hardware, software, and target application versions.

Component	Version
Hardware	
Samsung Tab A7 Lite (SM-T220)	Android 14
Ray-Ban Meta Wayfarer (Gen 1)	Firmware 21
MSI Pulse 15 B13VFK	Windows 11
Software	
Magisk	29.0
Android SDK Platform-Tools	36.0.0
Odin	3.13.1
Autopsy	4.22.1
ALEAPP	3.1.9
SQLite	3.46.1
Target Application	
Meta AI	258.0.0.15.167

3.1. Experimental Environment

The Android tablet was factory reset prior to experimentation to establish a known baseline state. The glasses were paired to a newly created Meta account to establish an equivalent baseline. This setup ensured the glasses were in a like-new state at the start of testing. System clocks on the host and mobile device were synchronized to UTC at the beginning and end of each experiment.

3.2. Experimental Procedure

The experimental workflow adapts the stimulus—acquisition—analysis methodology described by Dragonas et al. (2024) to the smart glasses ecosystem. Each experiment followed a controlled stimulus-–acquisition-–analysis loop (Figure 3), with differential analysis adapted from (Garfinkel et al., 2012). This full protocol was executed once. A baseline acquisition captured the system state prior to installation of the Meta AI application. Each subsequent experiment executed a predefined sequence of user interactions, referred to as an *Action Set*, followed by immediate data acquisition.

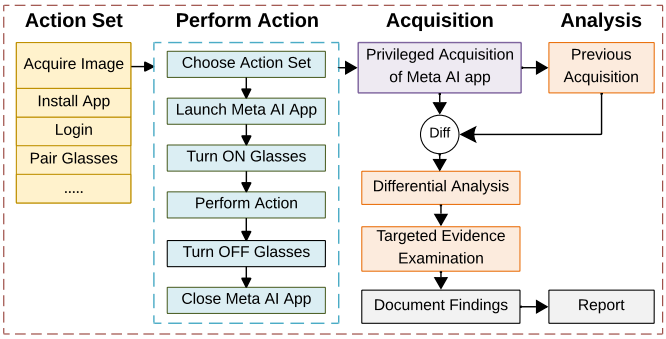

Figure 3: Controlled stimulus–acquisition-analysis workflow.

Across multiple Action Sets, a controlled set of user actions covering device setup, pairing lifecycle, media capture, AI interaction, anti-forensic manipulation, and cloud data export was performed. Table 2 summarizes the forensic actions used in the experimental design but excludes user-initiated anti-forensic actions listed in Table 6.

Table 2: User actions included in the experimental protocol.

Actions Performed		
Account Login	Pair Glasses	Take Photo (🎙)
Take Photo (✋)	Take Video (🎙)	Take Video (✋)
Hyperlapse (🎙)	Translate Text (🎙)	Change Voice
New Conversation (🎙)	New Conversation (⌨)	Continue Chat (⌨)
Set Reminder (🎙)	Connect Instagram	Connect Facebook
Connect Spotify	Connect WhatsApp	Enable Share Data
Post to Instagram Story (🎙)	Post Facebook Story (🎙)	Message on Messenger (🎙)
Connect Amazon Music	Link Phone and Messages	Enable Cloud Media
Export Cloud Data		

Legend: 🎙 Voice Command; ✋ Physical/Touch Input; ⌨ Text

3.3. Acquisition Strategy

Each Action Set was followed by three acquisition paths to evaluate artifact accessibility under different access conditions: (i) root-level logical extraction of the application sandbox (`/data/data/com.facebook.stella`) using `adb pull`; (ii) non-root logical acquisition using standard `adb backup`, with media extracted from SD-card storage; and (iii) cloud export via data export from Meta's Accounts Center at defined checkpoints. All collected artifacts were hashed using SHA-256 and verified prior to analysis.

3.4. Analysis

Analysis was conducted by comparing sequential acquisitions to identify file system and database additions, deletions, and modifications. This differential approach, following Garfinkel et al. (2012), allowed step-wise examination of artifacts while reducing analyst bias. Artifact categories, persistence behavior, and cross-layer correlations derived from this analysis are presented in Section 4.

4. Results

Our forensic analysis identified a distributed set of artifacts across the companion application sandbox (`/data/data/com.facebook.stella`), and the Meta cloud services. This section presents those findings.

4.1. Privileged vs. Non-Privileged Acquisition

A central practical question in this study is whether meaningful forensic analysis of the Meta AI companion application is possible without elevated privileges. To evaluate this, we performed both privileged and non-privileged acquisitions at multiple experimental stages and compared the resulting artifact coverage.

Table 3: Comparing privileged vs. non-privileged acquisition results.

Artifact Category	Non-Privileged	Privileged
User Identity (ID, username, profile)	✗	✓
Device Identity (serial, MAC, UUID)	✗	✓
Configuration Files	✗	✓
Media Files (photos, videos)	✓	✓
AI Conversation Logs	✗	✓
System Logs (FFLogger, errors)	✗	✓
Service Integrations (Spotify, etc.)	✗	✓

Legend: ✓ Acquired, ✗ Not Acquired

Non-privileged acquisition using standard `adb backup` produced a 47-byte file containing metadata headers. To examine this behavior, we decompiled the Meta AI APK using JADX and inspected `AndroidManifest.xml`, where the application specifies `android:allowBackup="false"`, which disables logical backup-based extraction. In contrast, privileged acquisition via `adb pull` yielded many files like SQLite databases, configuration files, cached media, and AI interaction logs.

As summarized in Table 3, non-privileged acquisition failed to recover artifacts across nearly all categories, whereas privileged acquisition provided comprehensive access to user identifiers, device configuration, media artifacts, AI conversations, and system logs.

These results indicate that the Meta AI application sandbox is not accessible through standard non-privileged acquisition methods. This observation is consistent with prior companion-application forensic studies on wearable devices (VanPutte et al., 2022), and is particularly relevant for GenAI-enabled smart glasses, where conversational artifacts and visual query metadata are stored within protected application storage. While cloud-based data exports provide partial visibility into user activity, privileged acquisition is necessary to recover the local artifacts required for detailed event reconstruction and evaluation of user-initiated anti-forensic actions.

4.2. User and Device Attribution

Establishing a reliable linkage between user activity, account identity, the companion application, and the physical smart glasses is an important requirement in forensic analysis. Our examination identified multiple identifiers that, when considered together, support attribution across the Meta Ray-Ban ecosystem.

At the account level, the companion application stores unique *Account ID* and *User ID* values (`account_id`, `user_id`) that associate recorded activity with a specific Meta account. The Account ID (e.g., `...830165636`) corresponds to the user's Meta identity and may be cross-referenced with linked services such as Facebook or Instagram when available. The User ID (e.g., `...19445281`)

Table 4: Key forensic artifacts in the Meta AI application sandbox organized by artifact category.

Category	Artifact Path	Artifacts
Identity	`databases/StellaDatabase -> user_profile`	User ID, username, account ID, profile picture
	`app_light_prefs/.../device_system_info_*`	Serial number, MAC addresses, frame type/color
	`databases/StellaDatabase -> device_assets`	Device UUID, Bluetooth MAC, pairing history
Media	`files/media/[ID]/*.jpg, *.mp4`	Photos (raw, processed, thumbnails), videos (raw, display)
	`files/media/[ID]/*.bin`	IMU data (accelerometer, gyroscope), video time metadata
	`databases/StellaDatabase -> capture`	Capture timestamps, device serial, pairing ID, media type
	`databases/StellaDatabase -> media_item_location`	GPS coordinates (latitude, longitude) for videos
AI Logs	`databases/interaction_log.db -> entries`	AI conversation states, response text, session UUIDs
	`cache/graphql_response_cache/.../P3%3a*`	User queries in plaintext, AI responses
	`files/assistantLogs/*.json`	Voice command metadata, interaction IDs, device states
	`databases/StellaDatabase -> multimodal_metadata`	Links AI visual queries to capture sessions and device serial
Configuration	`app_light_prefs/.../wearable_device_settings_*`	LED brightness, video stabilization, notification settings
	`app_light_prefs/.../app_privacy_consent_settings`	Privacy consent timestamps, data sharing preferences
	`files/media/.../SupernovaDeviceMediaSource_*`	Calibration files: camera, IMU, audio, LED, touch, ALS
System	`app_analytics/fflogger/FFLogger.sql -> event`	Assistant analytics, performance metrics, file transfers
	`app_errorreporting/.../systems_health_report.txt`	System health logs, device events, connectivity timestamps
	`databases/StellaDatabase -> update_log`	OTA firmware updates, version history
Integrations	`app_light_prefs/.../partner_app_settings`	Spotify, Amazon Music package names and configs
	`databases/StellaDatabase -> contacts_row_contact`	Synced messenger, instagram contacts
	`files/stella/general_files/aum_account_*`	Messenger account DB, Instagram account DB
AI Models	`files/media/aimodels/*.pte, *.ptl`	PyTorch models (Face Detection, Classifier, Occlusion)
	`files/mobileconfig/.../*.mctable`	LLM system prompts, AI configuration data, UUIDs

functions as a stable identifier within local databases and file paths, enabling consistent association of actions, media artifacts, and AI interactions.

At the hardware level, attribution is supported by the device serial number (`device_serial`). This identifier is physically engraved on the inner-left temple of the glasses and is also stored within the application sandbox and corresponding cloud records. In our experiments, the serial number extracted from the application (`..11H5300YH`) matched the value observed on the physical device, providing corroboration between digital artifacts and the associated hardware.

In addition to persistent identifiers, the system records a *Pairing ID* (`pairing_id`), corresponding to the MAC address used during pairing between the glasses and the companion device (e.g., `7C:86:52:3F:E0:19`). This identifier is used to log pairing and connection events and may change following unpairing or a factory reset of the glasses, as discussed in Section 4.5. Although not persistent, historical Pairing IDs remain useful for reconstructing prior device associations and connection timelines.

4.3. Android Application Artifacts

The primary source of locally accessible forensic evidence is the Meta AI application sandbox at `/data/data/com.facebook.stella`. Key artifacts identified during analysis are summarized in Table 4.

Core Databases: The `StellaDatabase` SQLite database represents the most forensically informative database identified in the Meta AI application sandbox. It supports reconstruction of capture events by correlating media artifacts with device identifiers, timestamps, and, where available, location data. Several tables were found to be particularly relevant:

- `capture`: Contains records linking captured media to the device serial number (`....11H5300YH`), Bluetooth MAC address (`7C:86:52:3F:E0:19`), and capture timestamps.
- `media_item`: Stores import timestamps, processing states, and media type information for captured photos and videos.
- `media_item_location`: Records GPS coordinates associated with video captures; location data was not observed for images in our experiments.
- `multimodal_metadata`: Associates AI visual query images with corresponding device identifiers, enabling attribution of image-based AI interactions (e.g., visual queries initiated via voice commands).

The `media_item_location` table stores precise GPS coordinates for video captures. Our analysis revealed an asymmetry: videos consistently include geolocation data, while photos do not. This finding has significant implications for reconstructing user movement patterns from glasses-captured evidence. The `interaction_log.db` database maintains the AI conversation history, but user

voice queries are redacted to `<redacted>` in this database and only the AI responses are accessible.

Configuration Artifacts: Device-specific configuration artifacts are stored in binary protobuf format within the `app_light_prefs/` directory. Files of the form `device_system_info_[MAC]` encode hardware and configuration attributes, including the device serial number, frame type (Wayfarer), frame color (Matte Black), lens type (Graphite Green Transitions), and software build information.

Analysis of these protobuf files showed that records associated with both the current Bluetooth MAC address (`7C:86:52:3F:E0:19`) and a previously observed MAC address (`72:97:5E:14:1D:F8`) remained present following factory reset and re-pairing in our experiments. This behavior provides supporting evidence for reconstructing device pairing history and prior associations between the glasses and the companion application.

AI-Specific Artifacts: The Meta AI companion application has on-device machine learning models. The `files/media/aimodels/` directory contains five PyTorch models. These models persist across all user deletion actions, including factory reset and logout. Their presence indicates that the application's AI processing models persist even when usage evidence has been deleted.

4.4. Cloud Artifacts

While on-device acquisition provides forensic detail, Meta's cloud data export - obtained through the Meta Accounts Center - offers a higher-level view of user activity. In our experiments, cloud artifacts persisted across device factory resets. The cloud export consists of HTML files organized by data category. Table 5 summarizes the most forensically relevant artifacts identified.

4.5. Anti-Forensic Analysis

This study explored anti-forensic artifacts and techniques available to a user of the Meta AI ecosystem. For this paper, we define anti-forensics as user-initiated actions intended to prevent the creation of evidentiary data or to remove existing data from the device and the cloud. It is important to clarify that these actions are not explicitly tied to malicious intent, as they can be performed to manage a user's digital footprint and privacy.

4.5.1. On-Device Artifact Persistence

Table 6 summarizes the persistence of critical forensic artifacts across these actions. Results indicate that the factory reset AF6 is a significant but incomplete method of obfuscation. While the reset forced the Pairing ID (MAC address) to change upon re-pairing (↻), the database records for media captured *prior* to the reset retained the original Pairing ID, preserving a historical link to the device's previous state. Furthermore, the Device Serial Number remained immutable across all actions.

Table 5: Summary of Meta AI cloud artifacts organized by artifact category.

Artifact Path	Forensic Value
Identity	
meta_ai_profile/your_meta_ai_profile.html	Username Account creation date Last update timestamp
Media	
meta_ai_app/meta_ai_media.ht	Links media items to device serial number and date.
posts/media/your_posts/	Image files used as visual input during AI conversations.
AI Logs	
meta_ai_profile/your_ai_ conversations.html	User prompts AI responses Conversation timestamps/dates
Configuration	
meta_ai_app/connected_devices html	Voice interaction metadata "Hey Meta" settings Device settings snapshot
meta_ai_app/app_settings.html	Records the user's last known configuration for the Meta AI application and paired devices.

Table 6: On-device artifact persistence across anti-forensic actions.**AF1**:Clear Cache, **AF2**:Unpair + Pair Glasses, **AF3**:Delete Media, **AF4**: Delete Voice Activity, **AF5**:Delete Conversation, **AF6**:Glasses Factory Reset + Pair Glasses, **AF7**:Logout, **AF8**:Uninstall App, **AF9**:Reinstall + Re-pair Glasses

Artifact	AF1	AF2	AF3	AF4	AF5	AF6	AF7	AF8	AF9
Identity Artifacts									
User ID	✓	✓	✓	✓	✓	✓	✗	✗	✓
Device Serial	✓	✓	✓	✓	✓	✓	✓	✗	✓
Device ID (UUID)	✓	✓	✓	✓	✓	↻	✓	✗	✓
Pairing ID (MAC)	✓	↻	✓	✓	✓	↻	↻	✗	↻
Media Artifacts									
Photos & Videos	✗	✓	✗	✓	✓	✓	✓	✗	✗
AI query images	✗	✓	✓	✓	✓	✓	✓	✗	✗
Geolocation (videos)	✓	✓	✗	✓	✓	✓	✓	✗	✗
AI & System Logs									
Interaction log	✓	△	✓	✓	✓	△	✓	✗	✗
GraphQL cache	△	✓	△	✓	✓	✓	✗	✗	✗
Assistant logs	✓	✓	✓	✓	✓	✓	△	✗	✗

Legend: AF= Anti Forensics, ✓ Persists/Returns, ✗ Deleted/Not Present, △ Partial/Modified, ↻ Changed/Regenerated

4.5.2. Cloud and Ecosystem Persistence

We further analyzed the impact of user actions on server-side data by comparing cloud exports generated before and after the anti-forensic sequence.

In a later export, the `meta_ai_media.html` file and the `posts/media/your_posts/` directory were successfully purged of all media requiring AI processing. This confirms that deleting media via the companion app triggers a synchronization event that removes the correspond-

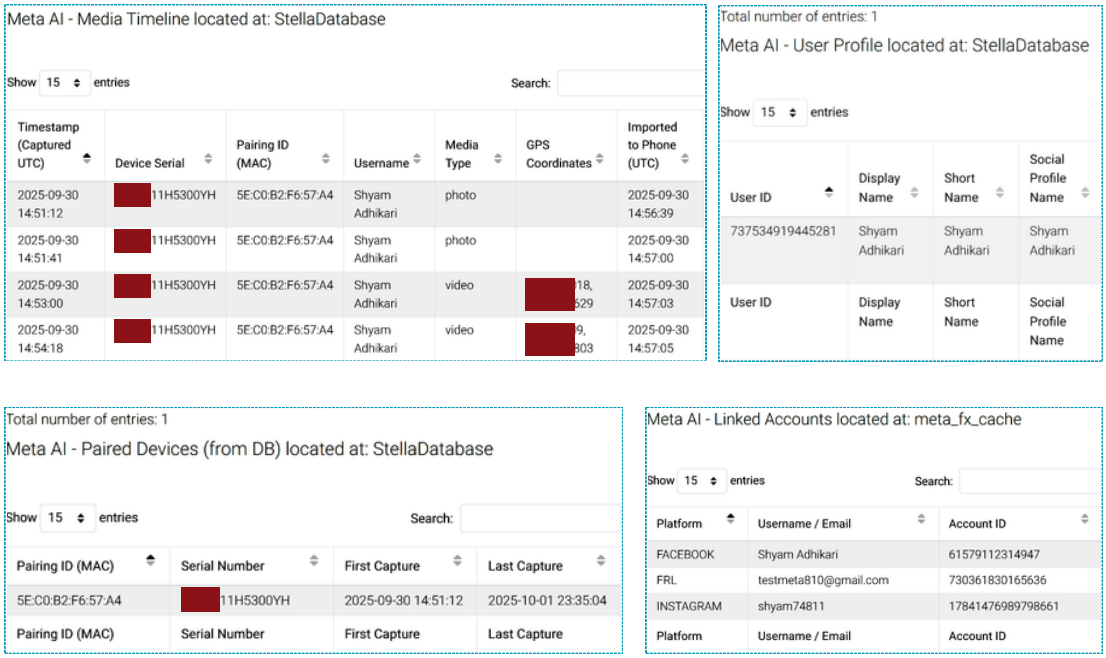

Figure 4: Report generated by the Meta AI parser.

ing cloud backup. Similarly, the "Delete Voice Activity" feature successfully removed conversation transcripts from the cloud archive. However, distinct data types showed varying persistence policies; for example, reminders created via the AI assistant persisted in `reminders.html` even after conversation logs were cleared and the glasses were reset. These artifacts required explicit deletion via the application interface to be removed.

4.6. Contribution to Free and Open-Source Software

At the beginning of this study, we evaluated existing digital forensic tools and found that the popular open-source framework ALEAPP did not parse Meta AI artifacts from companion application (`com.facebook.stella`).

This capability gap presents a significant hurdle for digital investigators. Without automated support, examiners are required to conduct a manual, file-by-file analysis of the application's complex data structures. This process is not only time-intensive but also increases the risk of overlooking subtle but critical pieces of evidence, particularly when investigators are operating under the immense pressure. Such omissions can lead to incomplete findings and are a known source of error in digital investigations.

In light of this challenge, the findings from this research were used to develop a dedicated parser for the Meta AI application and contribute it to the open-source community. More specifically, a comprehensive Python plugin was developed for the ALEAPP framework to automate the extraction and interpretation of the key artifacts identified in this study. Implementation details and code availability are presented in Section 8.

A sample of the collection of reports generated by the plugin is shown in Figure 4. The developed parser processes the central `StellaDatabase` to build a consolidated evidentiary timeline, correlates user and device identifiers from various Shared Preferences files, extracts AI interactions from JSON logs, and recovers transient media from the application cache. By joining data from over seven distinct database tables and multiple configuration files, the plugin transforms fragmented data landscape into a series of clear, actionable reports for forensic examiners. It also parses the cloud data to include the conversations with Meta AI and media stored in the cloud.

5. Forensic Framework for GenAI-Enabled Smart Glasses

Prior work on smart glasses and wearable forensics has largely focused on identifying recoverable artifacts on a specific device or companion application (e.g., logs, media, and synchronization traces) (Rongen and Geradts, 2017; VanPutte et al., 2022; Baggili et al., 2015; MacDermott et al., 2019). However, modern GenAI-enabled smart glasses operate as a distributed *glasses–companion–cloud* ecosystem, in which evidentiary traces are generated at the glasses, materialized within the companion application's protected storage, and selectively mirrored or summarized in cloud services. This architecture creates two recurring forensic challenges: (i) evidence is fragmented across layers with different retention and deletion semantics, and (ii) attribution and integrity often require cross-layer corroboration rather than relying on a single artifact source.

To address this, we present an empirically-derived forensic framework implemented on the Ray-Ban Meta ecosystem. The framework is not intended as a vendor-specific

Table 7: A multi-layered forensic taxonomy for GenAI-enabled smart glasses, categorizing artifacts by evidence source, acquisition type, and investigative utility.

Artifact Type	Layer			Acquisition		Forensic Value				
Identity										
User/Account Identifiers	▶	☁		👤⚙/ ⬇		🏷	⛓		🔒	
Device Serial Number	▶	☁	👓	👤⚙/ ⬇		🏷	⛓		🔒	
Wearable Pairing Identifier	▶	☁		👤⚙/ ⬇			⛓	🕐		
Media										
Raw Media Files (Photos/Videos)	▶	☁	👓	👤⚙/ ⬇/ 👤			⛓	🕐		📄
Geolocation Coordinates	▶			👤⚙			⛓	🕐		
AI Visual Query Images	▶	☁	👓	👤⚙/ ⬇		🏷	⛓	🕐		📄
AI Logs										
AI Conversation (User Prompts)		☁		⬇		🏷	⛓	🕐		📄
AI Conversation (AI Response)	▶	☁		👤⚙/ ⬇			⛓	🕐		📄
Assistant Logs	▶			👤⚙			⛓	🕐		
Configuration										
Wearable Device Settings	▶	☁		👤⚙/ ⬇			⛓	🕐		
Privacy Consent/Data Sharing Preferences	▶	☁		👤⚙/ ⬇				🕐	🔒	
Device Calibration	▶		👓	👤⚙		🏷			🔒	
Integrations										
Partner App Settings	▶			👤⚙			⛓			
Contacts/Social Linkage	▶			👤⚙			⛓			
Account Database Records	▶			👤⚙			⛓		🔒	

Legend. Layers: ▶ Companion App, ☁ Cloud, 👓 Evidence origin on glasses (not direct filesystem acquisition). **Acquisition:** 👤 Non-root logical, 👤⚙ Privileged filesystem extraction, ⬇ Cloud export. **Forensic Value:** 🏷 Attribution, ⛓ Correlation, 🕐 Timeline, 🔒 Integrity, 📄 Content, Context.

data map; rather, it captures repetitive forensic properties of GenAI-enabled smart glasses that rely on companion application and cloud-assisted AI processing.

Scope and acquisition assumptions.. In our study, the most information-rich artifacts were recovered from the companion application's protected sandbox via privileged filesystem extraction. Non-privileged acquisition was ineffective for accessing the application sandbox (Table 3). Cloud exports provide complementary evidence that persists across local anti-forensic actions and preserves plaintext user prompts that are redacted on-device. Throughout, the (👓) layer denotes the *evidence-origin* on the glasses; in practice, these traces are observed through app and cloud artifacts unless a separate glasses filesystem acquisition is available.

5.1. Artifact Taxonomy

Table 7 formalizes the multi-layer artifact taxonomy aligned with the artifact categories reported in Section 4. Each artifact type is characterized along three axes:

(1) Architectural layer: where the artifact is generated or observed (👓, ▶, ☁). **(2) Acquisition feasibility:** whether the artifact is accessible via non-privileged logical methods (👤), privileged filesystem extraction (👤⚙) or cloud export (⬇). **(3) Forensic value:** the investigative utility dimensions the artifact supports.

Forensic value dimensions: To operationalize investigative utility, we characterize each artifact type using six forensic value dimensions (Table 7). **Attribution (🏷)** reflects whether an artifact can reliably bind activity to a specific user account and/or a specific physical device. **Correlation (⛓)** captures whether an artifact provides join keys that link evidence across layers or datasets. **Timeline (🕐)** indicates that an artifact contains timestamps or ordering signals sufficient to reconstruct event sequences. **Integrity (🔒)** denotes that an artifact supports authenticity assessment or tamper-resistance through immutability, redundancy, or cross-layer corroboration. **Content (📄)** represents direct evidentiary payload such as media or conversation transcripts. **Context ()** captures surrounding state needed to interpret actions (e.g., settings, consent state, connectivity, or coarse location). These dimensions support systematic evidence prioritization and cross-layer validation, when single-layer artifacts are incomplete or user-modified.

5.2. Event Reconstruction

Using the taxonomy, investigators can reconstruct forensically relevant events by correlating to stable identifiers

(e.g., device serial number and account identifiers) and metadata across layers. In the examined ecosystem, recurring event families include: device lifecycle events (pairing/unpairing, factory reset), media capture events (photo/video creation and import), AI interaction events (voice or visual queries), and data management events (synchronization and deletion). Reconstruction is strengthened by corroboration between protected on-device records (e.g., `capture`, `multimodal_metadata`, `interaction_log.db`) and cloud exports that preserve prompts and high-level media linkage.

5.3. Artifact Correlation, Integrity, and Attribution

Attribution is challenging in GenAI-enabled smart glasses because user interaction often occurs through voice and the glasses typically lack strong on-device authentication. In our analysis, attribution is achieved by correlating persistent identifiers across layers, notably device serial numbers (hardware anchor), account identifiers (user anchor), and pairing identifiers (connectivity anchor). Integrity assessment relies on cross-layer consistency checks: for example, verifying that identifiers and timestamps in local databases align with cloud exports, and recognizing artifacts with higher resistance to local manipulation (e.g., cloud-retained conversation logs). Finally, the framework supports anti-forensic analysis by highlighting which artifact types are expected to persist after user actions (Table 6), enabling investigators to detect selective deletion and to prioritize acquisition from less-mutable layers.

6. Discussion

This section interprets the findings through the lens of the study's research questions.

RQ1: Organizing artifact categories in AI-enabled smart glasses ecosystems into a generalizable framework. Our results identify a set of artifact categories that repeat across modern AI-enabled smartglasses ecosystems: *Identity*, *Media*, *AI Logs*, *Configuration*, *System*, *Integrations*, and *AI Models* (Section 4). The framework operationalizes these categories by encoding three properties that matter during investigations: (i) layer of observation (glasses evidence-origin vs. companion protected storage vs. cloud), (ii) acquisition feasibility (non-privileged vs. privileged extraction vs. cloud export), and (iii) forensic value (Table 7). Two ecosystem-level patterns motivate the need for a framework rather than a flat artifact list. First, the companion application acts as the primary evidence layer: the most information-rich records are present inside protected app storage, making privileged acquisition necessary for completeness (Table 3). Second, cloud exports act as a semantic completion layer for GenAI activity: they preserve user prompts in cases where on-application sources may redact them.

RQ2: Resilience of artifacts to user-initiated anti-forensic actions. The user-initiated anti-forensic experiments (Section 4.5) demonstrate that artifact resilience is strongly layer-dependent and artifact-type dependent. Several identity links persist across user actions, most notably the device serial number, providing a stable hardware linkage even when pairing identifiers change after unpairing or factory reset. Conversely, certain high-value evidentiary content (e.g., media and conversation transcripts) can be selectively removed, with different effects on local versus cloud representations (Table 6). Importantly, anti-forensic actions do not uniformly erase evidentiary traces; instead they often create secondary evidence of deletion or reconfiguration, such as pairing-ID rotation, partial log modification, and inconsistencies between local records and cloud exports. These behaviors reinforce the framework's emphasis on correlation and cross-layer consistency checks as an integrity strategy.

Implications for Digital Forensics. This study shows that evidence related to GenAI-enabled smart glasses is not stored in a single location. Instead, meaningful analysis requires examining both the companion application and the cloud data, as relying on only one source can leave important gaps. The findings guide how such devices can be examined when they arise in forensic investigations.

Limitations. This study has several limitations. The analysis was limited to the Android version of the Meta AI companion application; artifact availability and storage locations may differ on iOS. In addition, although the potential value of physical acquisition was considered, no hardware teardown or chip-off analysis of the glasses was performed. Such analysis could reveal additional artifacts not accessible through application or cloud acquisition. The study also focused on the first-generation model of the Ray-Ban Meta smart glasses, and findings may not generalize to later hardware or firmware versions.

Future Work. An immediate next step is a comparative forensic analysis of the Meta AI companion application on iOS to assess platform-specific differences in artifact storage and accessibility. Further study of encrypted network traffic between the companion application and Meta's cloud services could provide additional insight into data synchronization and retention behavior. Finally, a deeper analysis of video metadata and associated sensor or telemetry data may support improved methods for validating recordings and reconstructing user activity.

7. Case Study

To validate the proposed forensic framework (Section 5) and our custom ALEAPP parser, we conducted a controlled covert recording scenario. In this study, two subjects discussed a fictional trade secret in a public laboratory at Louisiana State University, while a third subject (the suspect) recorded the conversation using Ray-Ban

Meta smart glasses on 2025-10-08. Law enforcement subsequently seized the suspect's glasses and the paired Android companion device. The case study was designed to evaluate the framework beyond simple artifact demonstration by exercising attribution, correlation, and integrity claims under realistic investigative conditions. The investigation workflow is summarized in Figure 5.

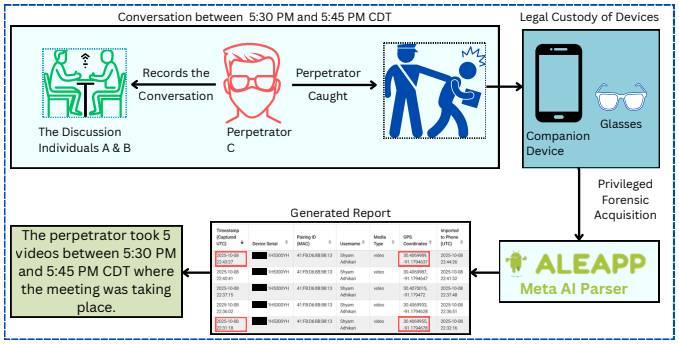

Figure 5: Visual overview of the covert recording case study findings.

7.1. Forensic Objectives

We structured the analysis around the forensic value dimensions defined in Table 7. Our primary objectives were to **(i)** attribute the recordings to a specific user and device, **(ii)** reconstruct the capture and import timeline, **(iii)** correlate media files across local and cloud artifacts, and **(iv)** assess the framework's resilience against anti-forensic deletion attempts. These objectives map directly to the attribution, timeline, correlation, and integrity dimensions of the proposed framework.

7.2. Data Acquisition

After confirming the device was powered on and accessible with privileged permissions, we executed a filesystem extraction of the Meta AI application sandbox (`/data/data/com.facebook.stella`) using `adb pull`. The data was then processed using the custom Meta AI parser. Privileged acquisition was required to access protected application storage and recover the full set of forensic artifacts relevant to this case study.

7.3. Evidence Reconstruction

Attribution (Account & Device): The parser successfully linked the recovered recordings to a single user account and a unique physical device via the glasses' serial number (`...11H5300YH`). This identifier appeared consistently in local `StellaDatabase.capture` records and was corroborated by available cloud linkage artifacts.

Timeline Analysis: Timestamps confirmed the recordings occurred between `22:31:18` and `22:43:27` UTC, aligning with the incident window. Subsequent "Imported to Phone" logs verified the successful transfer of evidence from the glasses to the mobile device.

Location & Context: Embedded GPS coordinates in the video metadata pinpointed the PFT, Louisiana State University laboratory building. Additionally, the analysis revealed two distinct pairing identifiers: the evidentiary videos were linked to MAC address `(41:FB:D6:8B:B8:13)`, while earlier logs referenced `(5E:C0:B2:F6:57:A4)`. This discrepancy indicates a factory reset and re-pairing event occurred on the day of the incident, establishing a critical timeline for device history.

8. Conclusion

GenAI-enabled smart glasses introduce a distributed *glasses–companion–cloud* evidence surface in which forensic traces are fragmented across layers with different access controls, retention policies, and deletion semantics. This work provides a structured response to that challenge through an empirical forensic examination of the Ray-Ban Meta ecosystem.

We identified and organized artifact categories produced by GenAI-enabled smart glasses into a multi-layer forensic framework. The proposed taxonomy characterizes artifacts by (i) architectural layer, (ii) acquisition feasibility, and (iii) investigative utility using six forensic value dimensions. We evaluated artifact resilience under user-initiated anti-forensic actions. Our results show that user-initiated anti-forensic actions can significantly reduce locally available evidence, but do not fully eliminate attribution anchors. In particular, certain identifiers persist in ways that enable reconstruction, while cloud exports provide complementary evidence that can survive local deletion.

To operationalize these findings, we contributed an open-source Meta AI parser to the ALEAPP framework that automates extraction and correlation of key artifacts and produces timelines suitable for practitioner workflows. The controlled case study demonstrates how the framework-guided approach can support attribution, timeline reconstruction, and cross-layer corroboration in an unauthorized recording scenario.

While this study provides a methodology and framework, several avenues for future work remain. Our analysis focused on the Android companion application and a specific device; artifact locations and persistence may vary across iOS, firmware versions, and future models.

Ethical Considerations

All experiments were conducted using researcher-owned devices and accounts, with no third-party data accessed. Recording tests were performed with explicit consent in a controlled laboratory setting and focused solely on evaluating forensic visibility and privacy implications.

Code Availability

The code is available at https://github.com/BiTLab-BaggiliTruthLab/Meta-AI-Parser.

References

Khawla Abdulla Alghafli, Andrew Jones, and Thomas Anthony Martin. Forensics data acquisition methods for mobile phones. In *2012 International Conference for Internet Technology and Secured Transactions*, pages 265–269. IEEE, 2012.

Auzinea Bacon. The New Orleans attacker wore Meta glasses. What can they be used for?, January 2025. URL https://www.cnn.com/2025/01/06/tech/meta-glasses-new-orleans-attack/.

Ibrahim Baggili, Jeff Oduro, Kyle Anthony, Frank Breitinger, and Glenn McGee. Watch what you wear: preliminary forensic analysis of smart watches. In *2015 10th International Conference on Availability, Reliability and Security*, pages 303–311. IEEE, 2015.

Alexis Brignoni. ALEAPP: Android logs, events, and protobuf parser, 2023. URL https://github.com/abrignoni/ALEAPP/releases/tag/v3.1.9. GitHub.

Kyungsuk Cho, Yunji Park, Jiyun Kim, Byeongjun Kim, and Doowon Jeong. Conversational AI forensics: A case study on ChatGPT, Gemini, Copilot, and Claude. *Forensic Science International: Digital Investigation*, 52, 2025.

Counterpoint Research. Global smart glasses market soars 210% YoY in 2024 driven by Ray-Ban Meta smartglasses, 2025. URL https://counterpointresearch.com/en/insights/post-insight-research-notes-blogs-rayban-meta-smart-glasses-drive-global-smart-glasses-market-surge-in-2024-fuelling-momentum-in-2025-with-projected-60-cagr-through-2029. Accessed: 2026-04-03.

Joseph Cox. Someone put facial recognition tech onto Meta's smart glasses to instantly dox strangers, 2024. URL https://www.404media.co/someone-put-facial-recognition-tech-onto-metas-smart-glasses-to-instantly-dox-strangers/. Accessed: 2026-01-11.

Brian Dipert. Ray-Ban Meta's AI glasses: A transparency-enabled pseudo teardown analysis, 2025. URL https://www.edn.com/ray-ban-metas-ai-glasses-a-transparency-enabled-pseudo-teardown-analysis/. Accessed: 2025-10-08.

Evangelos Dragonas, Costas Lambrinoudakis, and Panagiotis Nakoutis. Forensic analysis of OpenAI's ChatGPT mobile application. *Forensic Science International: Digital Investigation*, 50:301801, 2024.

Andrea Gallardo, Christopher Choy, Jaideep Juneja, Efe Bozkir, Camille Cobb, Lujo Bauer, and Lorrie Faith Cranor. Speculative privacy attitudes and concerns about AR glasses data collection. *Proceedings on Privacy Enhancing Technologies*, 2023(4):416–435, 2023.

Simson Garfinkel, Alex J. Nelson, and Joel Young. A general strategy for differential forensic analysis. *Digital Investigation*, 9:S50–S59, 2012. The Proceedings of the Twelfth Annual DFRWS Conference.

George Grispos, Kim-Kwang Raymond Choo, and William Bradley Glisson. Sickly apps: A forensic analysis of medical device smartphone applications on android and iOS devices. *Mobile Networks and Applications*, 28 (4):1282–1292, 2023.

Theodor-Radu Grumeza, Thomas-Andrei Lazăr, and Alexandra-Emilia Fortiş. A hybrid microservices architecture for smart glasses: integrating cloud-based LLMs, containerized services, and on-device functionalities. In *International Conference on Advanced Information Networking and Applications*. Springer, 2025.

David Heaney. Meta EssilorLuxottica discuss doubling or tripling smart glasses production. https://www.uploadvr.com/meta-essilorluxottica-discuss-doubling-smart-glasses-production/, January 2026. Accessed: 2026-02-02.

Muhammad Zahid Iqbal and Abraham G Campbell. Adopting smart glasses responsibly: potential benefits, ethical, and privacy concerns with Ray-Ban stories. *AI and Ethics*, 3(1):325–327, 2023.

Malithi Wanniarachchi Kankanamge, Nick McKenna, Santiago Carmona, Syed Mhamudul Hasan, Abdur R. Shahid, and Ahmed Imteaj. Digital forensic investigation of the ChatGPT windows application. *arXiv preprint arXiv:2505.23938*, 2025.

Jieon Kim, Jungheum Park, and Sangjin Lee. An improved IoT forensic model to identify interconnectivity between things. *Forensic Science International: Digital Investigation*, 44:301499, 2023.

Aine MacDermott, Stephen Lea, Farkhund Iqbal, Ibrahim Idowu, and Babar Shah. Forensic analysis of wearable devices: Fitbit, Garmin and HETP watches. In *2019 10th IFIP International Conference on New Technologies, Mobility and Security*, pages 1–6. IEEE, 2019.

Meta. Ray-Ban Meta wayfarer glasses. https://www.meta.com/ai-glasses/wayfarer-matte-black-clear-green-transitions/, 2025. Accessed: 2025-09-02.

Nam In Park, Ji Woo Lee, Seong Ho Lim, Oc-Yueb Jeon, Jin-Hwan Kim, Jun Seok Byun, Chanjun Chun, and Jung-Hwan Lee. Advanced forensic method to authenticate audio files from Tizen-based Samsung Galaxy watches. *Forensic Science International: Digital Investigation*, 48:301697, 2024.

J Rongen and Zeno Geradts. Extraction and forensic analysis of artifacts on wearables. *International Journal of Forensic Science and Pathology*, 5(1):312–318, 2017.

Sonali Tyagi, Yufeng Gong, and Umit Karabiyik. Forensic analysis and privacy implications of LLM mobile apps: A case study of ChatGPT, Copilot, and Gemini. *Forensic Science International: Digital Investigation*, 54:301974, 2025.

Logan VanPutte, Gokila Dorai, Andrew Clark IV, Rayna Mock, and Josh Brunty. Forensic analysis of the snapchat iOS app with spectacles-synced artifacts. In *IFIP International Conference on Digital Forensics*, pages 65–81. Springer, 2022.