Original Article
ISSN (Online): 3048-894X

Journal of Digital Security and Forensics
July-December 2025 2(2), 144–157

FINDINGS OF FORENSIC ARTIFACTS FROM APPLE SMARTWATCH: IMPLICATIONS FOR DIGITAL EVIDENCE

Sonali Kumari [1], Sakshi Sharma [2]

[1] DFIR Analyst, eSec Forte Technologies Pvt. Ltd., Gurgaon, Haryana, Postal Code-122008, India
[2] Senior Forensic Analyst, eSec Forte Technologies Pvt. Ltd, Gurgaon, Haryana, Postal Code-122008, India

Received 18 October 2025
Accepted 21 November 2025
Published 27 December 2025

Corresponding Author

Sakshi Sharma,
sharma02sakshi14@gmail.com

DOI
10.29121/DigiSecForensics.v2.i2.2025.73

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

In the relentless pursuit of truth, the smartwatch has emerged as an unexpected, yet powerful, witness.

Smartwatches and other wearable technology are becoming essential sources of evidence data in the rapidly developing field of digital forensics. This study presents a case-based forensic analysis of a Apple Watch, wherein data extraction was performed using Smartwatch Forensic Software and tool. The tool facilitated the retrieval of extensive personal information and system- level information. The extracted data encompassed a wide array of digital artifacts which can serve as critical indicators in criminal investigations involving alibi verification or timeline reconstruction. A correlation-driven approach was also employed to examine relationships between various data types, enhancing their potential to validate or contradict user statements. These findings affirm that smartwatch data, when methodically extracted and analyzed, can provide rich investigative leads and significantly contribute to modern digital evidence workflows.

Keywords: Smartwatch Forensic, Apple Watch, IOT Forensics, Wearable Devices

Highlights

1) Smartwatches are vital sources of digital forensic evidence.
2) A case study on an Apple Watch used a dedicated forensic tool for data extraction.
3) Extracted user and system data aided in alibi verification and timeline analysis.
4) Correlation between data types enhanced evidence reliability.
5) Systematic smartwatch analysis provides valuable leads in investigations

1. INTRODUCTION

Digital forensics is a broad investigative discipline that includes specialized domains such as cloud forensics, mobile device forensics, network forensics, and computer forensics and Internet of Things (IOT) forensics, each targeting distinct digital evidence sources and environments. Smart IoT refers to IOT devices that incorporate AI. Wearable technology can be used to operate smart IOT devices. Wearable technology, like smartwatches and smart bands, uses sensors to gather personal data to provide consumers with a variety of services. Kim et al. (2023)

Smartwatches may be used as digital evidence repositories since they store a significant amount of personal data. Ignoring their possible involvement in criminal activity, smartwatches are only used as digital evidence storage devices Jeon et al. (2023). Each subdomain requires specific investigative processes and tools, and the field is characterized by diverse data sources and overlapping acquisition methodologies. Al-Dhaqm et al. (2021), Brown (2022).

In recent years, wearable devices- particulary smartwatches-have become integral to daily life, offering continuous monitoring of health, activity, and location through embedded sensors such as accelerometers, gyroscopes, barometer, and GPS modules Rey et al. (2022), Kheirkhahan et al. (2019), Bouillet and Grandclément (2024). These compact yet powerful devices gather extensive personal data, making them not just fitness tools but potential digital evidence carriers in forensic investigations. The significance of this data becomes apparent when extracted using specialized forensic tools which allow investigators to retrieve structured information such as health metrics, sleep patterns, physical activity, and communication logs Fozoonmayeh et al. (2020), Odom et al. (2019). This kind of evidence can be instrumental in criminal cases, especially for validating alibis, reconstructing timelines, or identifying behavioral inconsistencies. Despite analysis of extracted smartwatch data can provide critical insights into an individual's health status, daily routines, and even psychological behavior. By accessing and analyzing this raw sensor data, practitioners can develop advanced applications for real-time assessment, mobility tracking, and forensic analysis. These capabilities make smartwatches a potent source of digital evidence, particularly as they sometimes store more data than the user's mobile phone Van et al. (2023), Kheirkhahan et al. (2019). However, extracting and handling this data introduces challenges regarding privacy and security. Smart watches have the potential to improve health in daily life by allowing self-monitoring of personal activity, offering feedback based on activity measures, enabling in-situ surveys to identify behavioural patterns, and facilitating bidirectional communication with family members and healthcare providers. However, since smart watches are a relatively new technology, research on them is still in their early stages. Reeder and David (2016)

2. OVERVIEW OF SMARTWATCH FORENSICS

Smartwatch Forensics is the branch of forensic science which mainly deals with the study of smartwatch evidence with respect to solving any criminal investigation. This field is an ongrowing field which impacts their importance day by day in human life. Smartwatches contain sensitive data and encrypting their backups is crucial to protect personal information Smartwatches contain personal data such as contacts, text messages, calendar information, emails, photos, and wallet details, all of which can serve as important evidence for forensic investigators. Al-Sharrah et al. (2018). It can offer a wide range of digital evidence directly from their internal storage, such as emails, contacts, events, notifications, health and fitness information, and communications Baggili et al. (2015).

3. METHODOLOGY

3.1. SWDGE GUIDELINES FOR IOT DEVICES EXTRACTION:

The Scientific Working Group on Digital Evidence (SWGDE) outlines a systematic process for handling IOT and digital evidence, including smartwatches for forensic examination. As depicted in their guidelines, the process begins with

identification and collection, followed by preservation, analysis, and finally reporting for legal proceedings.

Figure 1

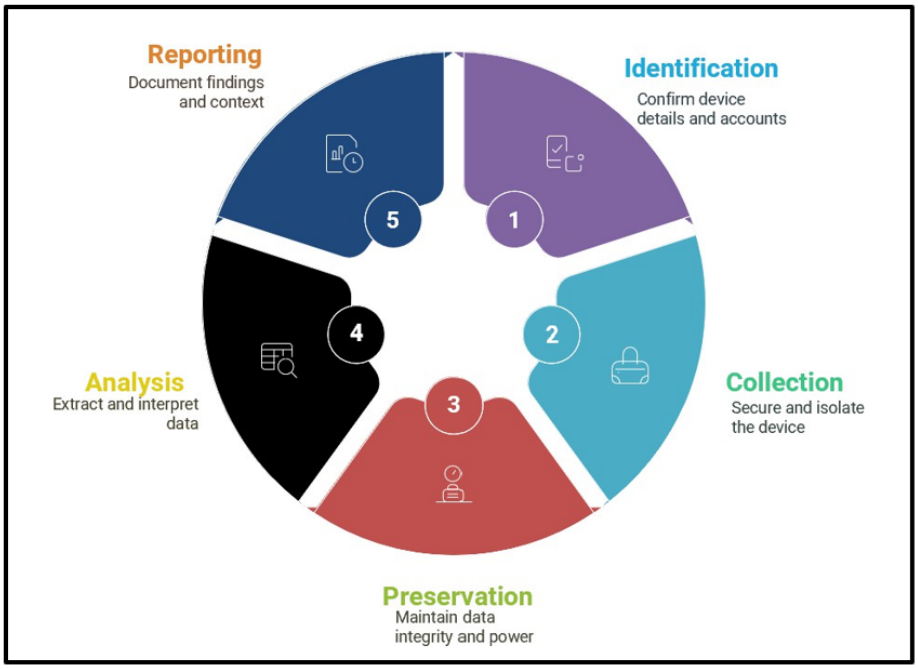


Figure 1 Steps of Investigation of Digital Evidence Provided by SWDGE

3.2. DEVICE AND SETUP

Smartwatch Infromation used in the Experiment:

Manufacturer	Product Name	Serial Number	System Version	HW Revision
Apple	Watch SE 44mm	G99*********	10.6.1_Firmware: iBoo t-1015 1.140.19_Build:21U580	N140bAP, Model:MYDT2

4. TOOLS

4.1. MOBILEDIT FORENSIC VERSION 9.1.0.25120

Forensic analysis of smartwatch data primarily relies on specialized tools like Mobile edit, with its effectiveness varying based on the smartwatch model and the chosen extraction technique. In our study we do extraction with the help of Mobile edit Forensic Version 9.1.0.25120. This mobile forensic tool was chosen because forensic analysts frequently utilize it to conduct their forensic investigations. Additionally, Because of its superiority in recovering a variety of data from mobile devices, including deleted data, the MOBILedit program was selected. Because of this feature, investigators can retrieve vital evidence from smartphones and tablets that might not otherwise be available. In cybersecurity situations, legal litigation, and criminal investigations, its value is immeasurable Akintola (2025). MOBILedit Forensic Express effectively extracts 0.75% of evidence from Android smartphones in body shaming cases Safitri et al. (2023) Mobile edit Forensic Pro (with the Smartwatch Kit) was used for data extraction. This tool supports Apple Watch Series 0–5 and SE (1st/2nd gen) via a specialized micro-USB adapter Compelson Labs (2025). For Series 5, we used the Series 4/5 adapter cable.

4.2. MOBILEDIT SMARTWATCH KIT

Mobile edit Smartwatch toolkit was used in the evidence samples of this research to extract data from various smartwatch models, including Apple Watch (Series 0 to Series 6), Samsung, and Garmin devices. The use of dedicated readers and diagnostic connectors facilitated structured data acquisition and supported forensic analysis throughout the study.

5. ANALYSIS

5.1. EXAMINATION OF APPLE SMARTWATCH EVIDENCE WITH MOBILEDIT FORENSIC

This research involves analyzing data from the Apple Smartwatch using MOBILedit Forensic and the Smartwatch Kit tools. We connected the Apple watch physically to the forensic Workstation using the specialized diagonstic reader provided in the MOBILedit Smartwatch Kit. In reader having, different Generational Series Ports. These ports correspond to various device series and sizes, including S1/S2/S3 (38mm), S2/S3 (42mm), S4/S5/SE (40mm), and S4/S5/S6/SE (44mm). The target Apple Watch is connected to the port that matches its specific model and size to ensure accurate and secure physical linkage for successful data acquisition. For extraction of data we install the iTunes Backup Service in forensic Workstation, it is necessary component to establish communication with Apple Devices, as apple watch accesss relies on Apple's backup protocols for logical extraction. This utility was downloaded and installed on the system to enable the process. For connecting Apple Watch is physically connected to the MOBILedit Smartwatch Reader through the diagnostic Port located beneath the watch strap connector. This adapter was then connected via USB to a forensic Workstation configured with the MOBIledit Forensic Software. The tool prompted the connection and identification of the smartwatch and here iTunes Backup Service established communication with Apple Watch and provide access relies on Apple's backup protocols for logical extraction. After getting access, the software interface displayed a preview of the connected Apple watch with a option having browse content which contain model, OS and other information of the smartwatch. Once the device was successfully recognized, we proceed with Next Option by clicking on it.

Figure 2

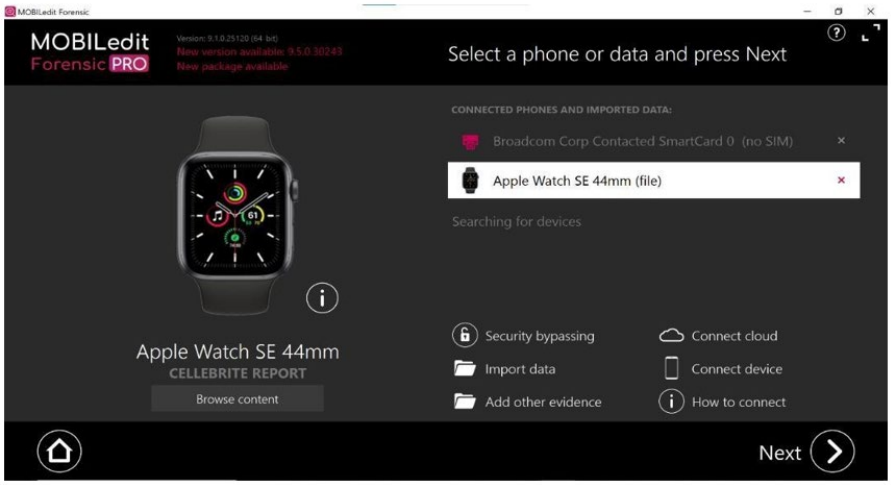


Figure 2 Apple Watch SE 44mm Connected to Mobile edit Software

The software provides us two options : Logical Extraction & Camera and Screen Capture. We click on the Logical Extraction method, which is the good approach for modern apple watches. In the extraction configuration step, the option " Full Content " we selected to ensure comprehensive acquisition across all supported artifact categories.

Figure 3

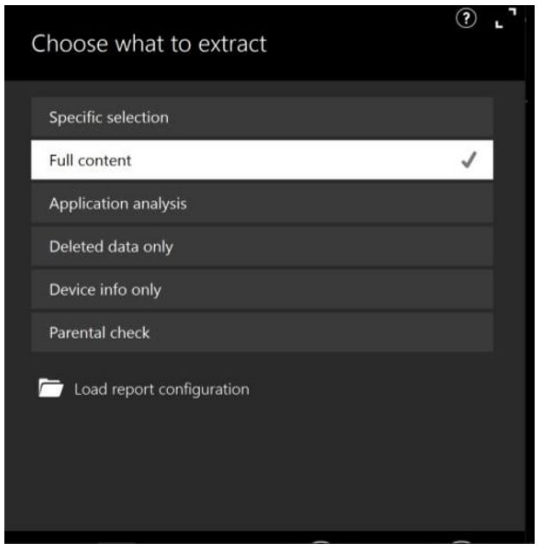


Figure 3 Full Content Logical Extraction by Mobile edit Software

At the end we prepare a report of all data, wherein the software provides the desired output format (PDF/HTML/MOBILedit Backup etc.) and entered relevant investigator and case details as required by forensic reporting standards. Finally, the extraction process completed successfully, and a structured forensic report was generated containing all accessible data categories retrieved from the Apple Watch. This included user-level, system-level, and application-specific data, now available for analysis within the digital forensic workflow.

Figure 4

Figure 4 Logical Extraction of Apple Smartwatch: Running Process

5.2. FINDINGS AND RESULTS

The forensic Examination of the Apple watch SE using MOBIledit Forensic Version 9.1 provides extensive data and useful artifacts. In Report we found important information regarding the apple watch. Figure 5 shows the recovered Smartwatch details which includes, Smartwatch manufacturer details (Apple), model and hardware revision (N140bAP, MYDT2), and Software Version (10.6.1). System identifiers such as device name (*******Apple Watch) serial number (********Q07Y).

Figure 5

Figure 5 Recovered Smartwatch Details

Figure 6

Packages	
App Downgrade	2023-08-08-0817
Bluetooth	2024-01-11-0944
Cell Towers	2023-10-03-0522
Clouds	2024-11-22-0778
File exclude list	2024-08-22-0839
Image processing	2023-06-19-0857
Malware detection	2024-08-16-0512
Rooting	2024-10-16-0793
Scripts	2025-01-15-0647
Security bypassing	2025-02-13-0576
iOS screenshots support	2023-10-19-0521

Figure 6 Packages Detail Found on Report

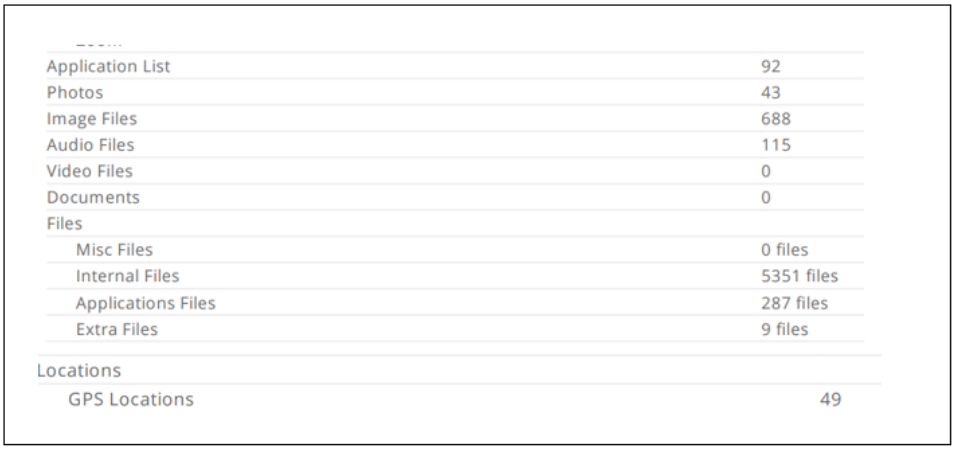
Figure 7

Device Properties	
Manufacturer	Apple
Product	Watch SE 44mm
HW Revision	N140bAP, Model:MYDT2
Platform	Apple
SW Revision	10.6.1 Firmware:iBoot-10151.140.19_Build:21U580
SW Revision extended	[redacted]ware:iBoot-10151.140.19_Build:21U580
Device Name	[redacted] Apple Watch
Serial Number	G99G4D3EQ07Y
Device Unique ID	00008006-0014D2300A63402E
Device Time	29-04-2025 11:26:03 (UTC+5:30)
Time Zone	Asia/Kolkata
Wi-Fi MAC Address	E8:1C:D8:B0:DC:9E
Bluetooth Address	E8:1C:D8:AE:C5:6F
Ethernet Address	E8:1C:D8:A8:C9:0F
Jailbroken	No
Communication Type	Apple Mobile Device Service
Device Type	Watch
SIM Card	No
Total Storage	29.8 GB
Used Storage	10.2 GB

Figure 7 Device Properties found on Apple Smartwatch

Figure 6, Package log table was extracted during the Apple smartwatch data acquisition process, listing multiple system-related modules. These include components such as App Downgrade, Bluetooth, Cell Towers, Malware Detection, and iOS Screenshot Support, each tagged with a timestamp indicating last activity or update. This metadata is valuable in forensic analysis as it helps in determining user behavior, system changes, and potential anomalies. Figure 7, shows the device properties of Apple Smartwatch including Wi-Fi MAC address, Bluetooth and Ethernet addresses, were also accessible, suggesting the device's ability to interface across multiple networks and communication environments. The report shows the absence of a SIM card, confirming the device was not cellular enabled. Time-specific parameters such as device time and time zone (Asia/Kolkata) were also recorded, essential for temporal mapping of activities. Storage metrics revealed a total capacity of 29.8 GB, of which 10.2 GB was in use.

Figure 8



Application List	92
Photos	43
Image Files	688
Audio Files	115
Video Files	0
Documents	0
Files	
Misc Files	0 files
Internal Files	5351 files
Applications Files	287 files
Extra Files	9 files
Locations	
GPS Locations	49

Figure 8 Artifacts Evidence Recovered

In terms of user content Figure 8 shows, the device contained 92 installed applications, 43 photos, 688 image files, 115 audio files, 5351 internal files, 287 application-specific files, and 9 miscellaneous extra files. Location-related data included 49 distinct GPS coordinates and one geolocation configuration store, underscoring the device's mobility tracking capabilities. Table 1, shows the 92 applications list which we found on the smartwatch during analysis.

Table 1

Table 1 92 Applications List Evidence found on Extracted Apple Smartwatch Data

Accessibility UI Server	Activity	Alarms	App Store
Apple Store	AppStoreTrampoline	Audiobooks	BluetoothUIService
Calculator	Calendar	Calendar	Camera Remote
Carousel	Check In	ClockFace	CompanionServices Alert
Compass	Contacts	Control Nearby Devices	CSViewService
CTKUIService	Cycle Tracking	DataMigrationMonitor	Diagnostics
DiagnosticsService	Find Devices	Find Items	Find People
FitnessNotifications	Flightradar24	Forest	Google Maps
Handwashing	Heart Rate	Home	iCloud
Keynote	Mail	Mail	Maps
Medications	Memoji	Messages	Mindfulness
MTLReplayer	Music	NanoCompassAlertUI	NanoDemo
NanoMessageUIViewService	NanoNowPlayingViewService	NanoSettingsViewService	NanoSharing
NanoTextSizeViewService	News	Nike Training	Noise
Now Exercising	Now Playing	OneNote	Outlook
Phone	Photos	Podcasts	PreBoard
QuickboardViewService	ReBoard	Reminders	Remote
Renpho Health	Safari	SessionAlertUI	Settings
Setup	Shortcuts	ShortcutsActions	Sleep
Stocks	Stopwatch	StoreKitUIService	Timers
Tips	Voice Memos	VoiceOverTouch	Walkie-Talkie
Wallet	Weather	Wi-Fi	WidgetRenderer_Default
Windy	Workout	World Clock	Zoom

6. CO-RELATION ANALYSIS OF PHOTOS & GPS LOCATION DATA

Figure 9 shows the photos recovered from Apple Smartwatch by analyzing the image metadata, such as File Name, path , size and when image is created, modified and accessed Some important information which includes Date of Generation & Digitization and information of Time when picture was Clicked from Phone (2023-07-15 18:41:55 (UTC +5:30). During analysis of Photos and GPS Location evidence, extracted metadata of apple smartwatch revealed the critical metadata within the image files, included the Position (Google Maps or GPS coordinates) (Latitude: 27.06737°, Longitude: 75.88012°), along with the date and time of image captured.

By clicking on Google Maps , these coordinates correspond to a physical location and by mapping the data which is extracted from GPS Data onto Google Maps, the exact geographical position from where image was captured is identified in Figure 10, shows the visual characteristics of the site in Google Street view were consistent with the content found in the image, which confirmed the correlation between the Image evidence and actual location from where picture clicked. It helps us to do the cross-verification of Image evidence found on Smartwatch. It also demonstrates that such data can pinpoint the origin of photographs and strengthens the evidential weight of location -based digital artifacts in forensic investigations, supporting accurate reconstruction of events and user activity through GPS Data.

Figure 9

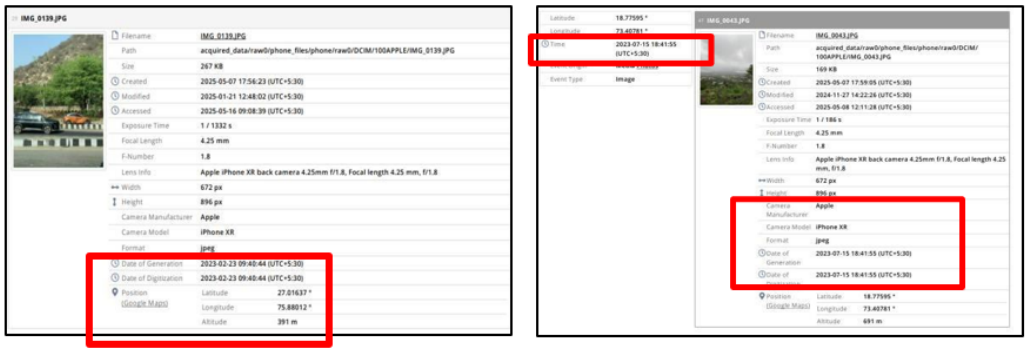


Figure 9 Photos & GPS Location Evidence Data Founds on Extracted Apple Smartwatch

Figure 10

Figure 10 Position from Google Maps showing from where Picture is Being Captured

Figure 11

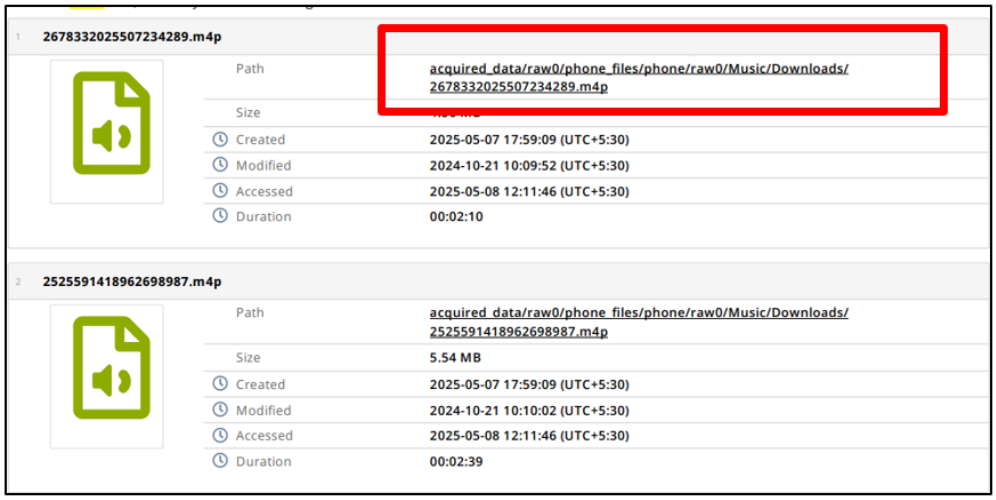
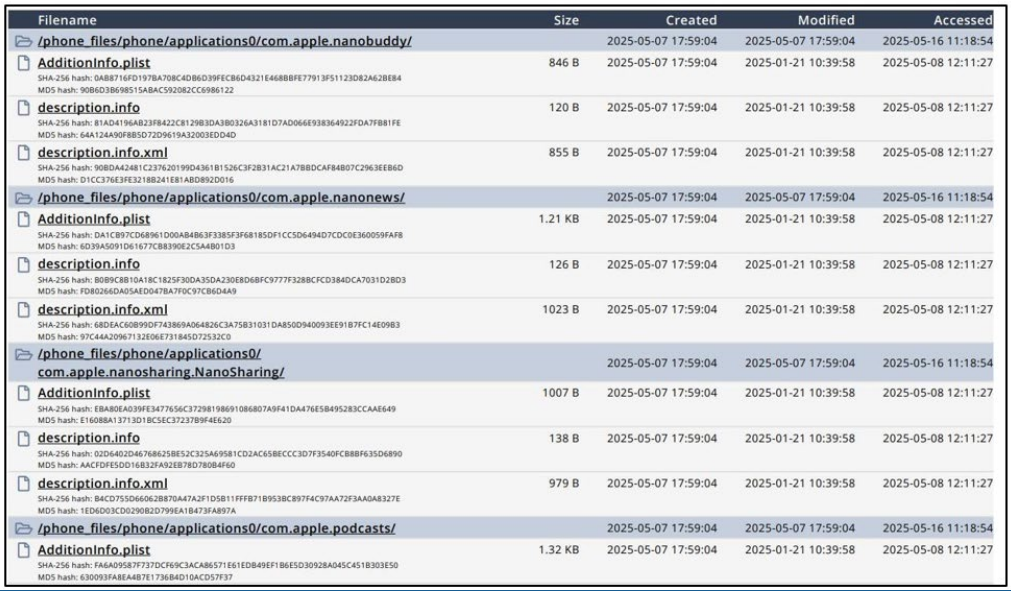


Figure 11 Audio Files Evidence Found in Apple Watch Report

Figure 12



Filename	Size	Created	Modified	Accessed
/phone_files/phone/applications0/com.apple.nanobuddy/		2025-05-07 17:59:04	2025-05-07 17:59:04	2025-05-16 11:18:54
AdditionInfo.plist	846 B	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27
description.info	120 B	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27
description.info.xml	855 B	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27
/phone_files/phone/applications0/com.apple.nanonews/		2025-05-07 17:59:04	2025-05-07 17:59:04	2025-05-16 11:18:54
AdditionInfo.plist	1.21 KB	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27
description.info	126 B	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27
description.info.xml	1023 B	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27
/phone_files/phone/applications0/com.apple.nanosharing.NanoSharing/		2025-05-07 17:59:04	2025-05-07 17:59:04	2025-05-16 11:18:54
AdditionInfo.plist	1007 B	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27
description.info	138 B	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27
description.info.xml	979 B	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27
/phone_files/phone/applications0/com.apple.podcasts/		2025-05-07 17:59:04	2025-05-07 17:59:04	2025-05-16 11:18:54
AdditionInfo.plist	1.32 KB	2025-05-07 17:59:04	2025-01-21 10:39:58	2025-05-08 12:11:27

Figure 12 Internal Files Recovered from Smartwatch

Furthermore, in Figure 11, represents the Audio Files found in the Report of Smartwatch which also have Path information, by clicking on it we can also download the Audio file. It also gives us information of Size of Audio File, Created, Modified, Accessed and Duration of the audio. This evidence also strengthens the credibility and admissibility of smartwatch derived data in Forensic investigations. Figure 12, Represents the internal files which is found during extraction also contains the size of the file.

7. DISCUSSION

Data collected from Apple Smartwatches has been extracted, examined, and analyzed. especially with forensic tools like MOBILedit, which are quite efficient. We

provide a concise overview of every data type found throughout the extraction process in table 3. We also get the most data from the Apple Watch's logical extraction. Photo evidence with GPS included to prove the accuracy of the data, metadata and time-stamped audio proof were readily taken out of the report and examined. Using Google Maps and Street View, the image-GPS data correlation was successfully confirmed. This data gives investigators an understanding of where the photo was taken or confirms the user's location and actions. Audio Evidence indirectly helps us to synchronize temporal metadata with other data sources and beneficial for event reconstruction Safitri et al. (2023). These findings also reinforce the border applicability of Smartwatch Forensic in real-world casework like missing person, location-based alibi verification. The ability to extract and validate data from wearable devices contributes not only to factual accuracy but also the evidentiary admissibility under legal standards.

7.1. Significance of Data found on Apple Smartwatch Forensic Examination

In Table 2, extracted data from the Apple Watch SE 44mm provides crucial forensic insights and key identifiers such as device model, serial number, and hardware/software revisions confirm the device's authenticity and integrity. Storage details, application count, and media files offer a snapshot of user activity. Network addresses (Wi-Fi, Bluetooth, Ethernet) and GPS data help investigator to trace connectivity and physical movements. The absence of jailbreaking ensures the data's reliability, while timestamps and timezone settings support accurate event timeline reconstruction. Overall, this metadata is vital for user profiling, activity analysis, and digital evidence correlation in forensic investigations.

Table 2

Table 2 Data Found on Apple Smartwatch During Examination

S.NO.	DATA TYPE	INFORMATION FOUND
1	Manufacturer Details	Apple
2	Product	Watch SE 44mm
3	HW Revision	N140bAP, Model:MYDT2
4	Platform	Apple
5	SW Revision	10.6.1_Firmware:iBoot-1015 1.140.19_Build:21U580
6	Device Name	*******Apple Watch
7	Jailbroken	NO
8	Serial Number	G99**********
9	SIM Card	NO
10	SW Revision Extended	10.6.1_Firmware:iBoot-10151.140.19_Build:21U580
11	Device Unique Id	00008006-0014D2300A63402E
12	Device Time	29-04-2025 11:26:03 (UTC+5:30)
13	Time Zone	Asia/Kolkata
14	Wifi MAC Address	E8:1C:D8:B0:DC:9E
15	Bluetooth Address	E8:1C:D8:AE:C5:6F
16	Ethernet Address	E8:1C:D8:A8:C9:0F
17	Communication Type	Apple
18	Device Type	Watch
19	Total Storage	29.8GB

20	Used Storage	10.2GB
21	Applications	92
22	Photos	43
23	Image Files	688
24	Audio Files	115
25	Internal Files	5351
26	Application Files	287
27	Extra Files	9
28	GPS Location	49
29	Geolocation Config Store	1

8. CONCLUSION

Smartwatches have become integral to our daily lives, meticulously recording personal, health, and sleep data. This research aimed to forensically examine the logical extraction of data from an Apple Watch using a specialized tool. Our goal was to demonstrate the utility of smartwatch evidence in criminal investigations by revealing the depth of personal information these devices can provide. Our findings indicate that MOBILedit Forensic Tool is highly effective, offering accurate data extraction and facilitating critical correlation analyses, such as linking GPS locations to specific image evidence. We successfully recovered a wide array of data, including media files, application lists, GPS locations, internal files, audio files, and comprehensive device information like Wi-Fi and Bluetooth MAC addresses. This study provides valuable insights for investigators seeking to extract crucial data from smartwatches.

AUTHOR CONTRIBUTION

Sonali Kumari designed the research framework Finding Forensic Artifacts on Smartwatches, developed the analytical models, and prepared the initial draft of the manuscript. Vaibhav Sakhare contributed to data acquisition, interpretation, and assisted in refining different sections of the paper. Both authors reviewed and approved the final manuscript for submission. The other contributors supported the review and provided critical feedback to enhance the quality of the work.

ABBREVIATIONS

GPS: Global Positioning System MAC: Media Access Control SW: Software

UTC: Coordinated Universal Time HW: Hardware

IoT: Internet of Things AI: Artificial Intelligence

SWDGE: Smart Wearable Device and Gadget Ecosystem

USB: Universal Serial Bus

OS: Operating System

iOS: iPhone Operating System SIM: Subscriber Identity Module

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Akintola, G. B. (2025). Evaluating the Security Vulnerabilities of Selected Mobile Forensic Applications. International Journal of Scientific Research in Multidisciplinary Studies, 11(2).

Al-Dhaqm, A., & others. (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. IEEE Access, 9, 152476–152502. https://doi.org/10.1109/ACCESS.2021.3124262

Al-Sharrah, M., Salman, A., & Ahmad, I. (2018, March). Watch Your Smartwatch. In 2018 International Conference on Computing Sciences and Engineering (ICCSE) (pp. 1–5). IEEE. https://doi.org/10.1109/ICCSE1.2018.8374228

Baggili, I., Oduro, J., Anthony, K., Breitinger, F., & McGee, G. (2015, August). Watch What You Wear: Preliminary Forensic Analysis of Smart Watches. In 2015 10th International Conference on Availability, Reliability and Security (pp. 303–311). IEEE. https://doi.org/10.1109/ARES.2015.39

Bouillet, J., & Grandclément, C. (2024). Sufficiency, Consumption Patterns and Limits: A Survey of French Households. Buildings and Cities, 5(1), 675–691. https://doi.org/10.5334/bc.454

Brown, E. K. (2022). Digital Forensic and Distributed Evidence. Research Nexus IT, Law, Cyber Security & Forensics, 1(1), 357–362. https://doi.org/10.22624/AIMS/CRP-BK3-P57

Compelson Labs. (2025). Introduction to MOBILedit Forensic. In MOBILedit Forensic User Guide.

Fozoonmayeh, D., Le, H. V., Wittfoth, E., & others. (2020). A Scalable Smartwatch-Based Medication Intake Detection System Using Distributed Machine Learning. Journal of Medical Systems, 44(76). https://doi.org/10.1007/s10916-019-1518-8

Jeon, S., Chung, J., & Jeong, D. (2023). Watch Out! Smartwatches as Criminal Tool and Digital Forensic Investigations. Arxiv Preprint arXiv:2308.09092.

Kheirkhahan, M., Nair, S., Davoudi, A., Rashidi, P., Wanigatunga, A. A., Corbett, D. B., Mendoza, T., Manini, T. M., & Ranka, S. (2019). A Smartwatch-Based Framework for Real-Time and Online Assessment and Mobility Monitoring. Journal of Biomedical Informatics, 89, 29–40. https://doi.org/10.1016/j.jbi.2018.11.003

Kim, M., Shin, Y., Jo, W., & others. (2023). Digital Forensic Analysis of Intelligent and Smart IOT Devices. Journal of Supercomputing, 79(2), 973–997. https://doi.org/10.1007/s11227-022-04639-5

Odom, N. R., Lindmar, J. M., Hirt, J., & Brunty, J. (2019). Forensic Inspection of Sensitive User Data and Artifacts from Smartwatch Wearable Devices. Journal of Forensic Sciences, 64(6), 1673–1686. https://doi.org/10.1111/1556-4029.14109

Reeder, B., & David, A. (2016). Health at Hand: A Systematic Review of Smartwatch Uses for Health and Wellness. Journal of Biomedical Informatics, 63, 269–276. https://doi.org/10.1016/j.jbi.2016.09.001

Rey, B., Lee, B., Choe, E. K., & Irani, P. (2022). Investigating in-Situ Personal Health Data Queries on Smartwatches. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 6(4), Article 179, 19 pages. https://doi.org/10.1145/3569481

Safitri, Y., Riadi, I., & Sunardi, S. (2023). Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework. MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, 22(3), 651–664. https://doi.org/10.30812/matrik.v22i3.2987

Van Dijk, R. M. K., Gawehns, D., & van Leeuwen, M. (2023). WEARDA: Recording Wearable Sensor Data for Human Activity Monitoring. Journal of Open Research Software, 11(1), 13. https://doi.org/10.5334/jors.454