

Research Article

Forensic Analysis of Residual Bluetooth Artefacts in Android-Based Smartphones Before and After Device Unpairing

Dave Drashti¹ , Kashyap Joshi^{2,*} , Kapil Kumar¹ 

¹Department of Biochemistry & Forensic Science, Gujarat University, Ahmedabad, India

²School of Management Studies, National Forensic Sciences University (NFSU), Gandhinagar, India

Abstract

Bluetooth technology is the most popular method of wireless communications in mobile phones, wearables, and Internet of Things devices. Bluetooth makes device connectivity and information transfer easy, and thus Bluetooth-related information can be useful digital forensic evidence. Research looking into the persistence of Bluetooth artefacts in Android smartphones after devices are unpaired is lacking. This study was designed to look into possible residual Bluetooth artefacts persistence and assess their forensic importance. A controlled experiment using Android devices was designed for the inclusion of Bluetooth artefacts through the pairing, connecting, and transferring of files. This was followed by manual device unpairing by the experimenter. Afterwards, Android Debug Bridge (ADB) was used to perform a logical acquisition of the paired Android device and extract paired Bluetooth information along with Bluetooth device identifiers, Bluetooth device MAC addresses, connection information, file information, and system information. Persistence of Bluetooth artefacts in the system before and after the unpairing of Bluetooth devices was assessed through a comparative analysis. The results of the study showed that unpairing Bluetooth devices does remove the bonding information, but residual artefacts still exist in the system. Evidence of user activities that includes transferred files, file information, and device identifiers was found to remain after the unpairing of the Bluetooth device. The transferred files along with the file information retained user file timestamps and showed a complete absence of changes, and thus provided evidence that the unpairing of the Bluetooth device did not remove all information connected to Bluetooth. Forensic evidence was found to be still available even after the active pairing(s) of the Bluetooth devices had been removed. These results are significant for forensic studies because they show how Bluetooth artefacts help to show how devices were used, what other devices were paired to, and what communication may have taken place. One of the contributions of this study to mobile and digital forensics is the understanding that the unpairing of Bluetooth devices is, in fact, not the full removal of evidence, but only the partial removal of evidence. This shows that forensic investigators should focus on the unpairing of Bluetooth devices to evidence.

Keywords

Bluetooth Forensics, Android Smartphones, Digital Forensics, Bluetooth Artefacts, Device Unpairing, Mobile Forensics

*Correspondence: Kashyap Joshi (kashyapjoshi.it@gmail.com)

Received: 5 June 2026; **Accepted:** 18 June 2026; **Published:** 29 September 2026



Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Bluetooth is a short-range wireless technology originally designed for replacing cables between nearby devices, now embedded in phones, wearables, laptops, vehicles, and many IoT sensors [1]. It operates in the 2.4 GHz ISM band and emphasises low cost, low power, and ease of use. Bluetooth was introduced in the late 1990s as a cable-replacement protocol for personal devices, based on frequency-hopping spread spectrum in the 2.4 GHz band [2]. References in this manuscript are consecutively numbered as they appear in the text using numerals in square brackets (e.g., [1-3] or [4-7]).

1.1. Bluetooth Technology in Mobile Devices

1.1.1. Overview of Bluetooth Communication

Originally meant to replace cables, Bluetooth connects nearby personal devices such as phones, computers, and peripherals using wireless technology within the 2.4 GHz band,

ranging over short distances and using low power and low-cost links. Bluetooth Classic uses frequency-hopping spread spectrum to increase resistance to interference and operates at 1 Mbps and 1600 hops/s using Gaussian frequency shift keying (GFSK) modulation [3].

1.1.2. Bluetooth Classic and Bluetooth Low Energy (BLE)

Although Classic Bluetooth and Bluetooth Low Energy (BLE) share the same frequency band, they have different functions and protocols [4]. Bluetooth Classic is intended for continuous, real-time, higher-throughput applications (such as audio streaming), while BLE is designed for quick, intermittent, and low-throughput transmissions typical of IoT-based sensors and wearables.

Table 1. High-level comparison of Classic Bluetooth and BLE design and usage.

Aspect	Bluetooth Classic (BR/EDR)	Bluetooth Low Energy (BLE)
Design goal	Continuous, higher data rate	Ultralow power, short bursts
Compatibility	Separate from BLE	Separate from Classic; dual-mode chips support both
Energy use	Higher; not ideal for coin-cell multi-year operation	Much lower; coin-cell battery can last years
Typical apps	Audio, keyboards, legacy peripherals	IoT sensors, wearables, beacons, smart cities

1.2. Artefact Persistence and Data Remanence

Data remanence is the phenomenon whereby digital information persists on a device even after an individual attempts to erase or delete it. There are several technical explanations within the Android operating system that account for the persistence of Bluetooth artefacts [4].

1.3. Literature Review

Bluetooth technology emerged in the late 1990s as a protocol for cable replacement and is now a communication standard used across many device categories, including smartphones, laptops, wearables, automobiles, and IoT devices. This technology has become a valuable source of digital forensic evidence. Harte (2004) established the technical specifications of Bluetooth Classic by describing its use of frequency-hopping spread spectrum (FHSS) with GFSK modulation at a transmission rate of 1 Mbps [5].

From a forensic standpoint, the difference between Bluetooth Classic (BR/EDR) and BLE is substantial. Bluetooth

Classic handles high-volume continuous data streams such as audio, while BLE was designed for low-volume, low-energy data bursts typical of IoT devices and wearables (Heydon, 2012). Because both variants exist in the same dual-mode chips, they produce different forensic evidence profiles in the Android OS, necessitating different forensic approaches [6]. Becker (2019) demonstrated the importance of examining low-level system architecture in digital forensics; BLE advertisements generate persistent entries in Android logs, highlighting their digital forensic significance [7].

The Android OS saves Bluetooth artefacts in several locations, most critically the /data/misc/bluetooth/ directory, which stores configuration files including bt_config.conf—containing device names, MAC addresses, link keys, and connection timestamps. Anglano (2014) noted the persistence of bonding records in this directory and their ability to survive user-initiated application deletions, providing investigators with a reliable source of historical device connection data. Access to this directory is restricted on non-rooted devices, a limitation that later studies addressed using ADB logical acquisition and memory forensics [8].

The Android Debug Bridge (ADB) is the primary tool for

logical forensic acquisition on Android. Lessard and Kessler (2010) were among the first to describe ADB forensic capabilities in detail, demonstrating how the command `adb shell dumpsys bluetooth_manager` retrieves active and historical Bluetooth communication data without requiring root access [9]. Cusack and Tug (2012) carried out controlled experiments pairing and unpairing Android devices, confirming the recovery of MAC address and timestamp information from system files post-unpairing.

2. Materials and Methods

2.1. Aim

To analyse and recover residual Bluetooth artefacts in Android smartphones before and after device unpairing for forensic investigation purposes.

2.2. Objectives

- 1) To study how Bluetooth Classic and BLE store device information in Android systems.
- 2) To identify Bluetooth artefacts generated during pairing and connection.
- 3) To examine the persistence of Bluetooth artefacts after device unpairing.
- 4) To recover forensic artefacts such as MAC addresses, device names, and connection logs.
- 5) To evaluate the forensic significance of recovered Bluetooth artefacts.

2.3. Experimental Setup and Device Selection

Android smartphones were selected as the primary test devices due to their widespread use and flexible access to system-level data for forensic analysis. Devices were chosen based on practical usability and availability, ensuring they reflected real-world usage settings. Each device was used to carry out specific tasks including uploading data, associating with another device via Bluetooth, and subsequently unpairing the devices. An identical set of procedures was applied to every device to ensure uniformity. Furthermore, all chosen devices supported ADB access, which was required to collect internal data pertaining to Bluetooth activities.

2.4. Performing Bluetooth Pairing and Communication Activities

Following device selection, Bluetooth pairing and communication tasks were performed to generate relevant artefacts for analysis. This step was critical to replicating real-world usage and observing how Bluetooth data is generated and stored within the devices. The activities included initiating Bluetooth

discovery, pairing between devices, and transferring test files to simulate normal operational interactions.

2.5. Simulating Device Unpairing Scenarios

Device unpairing scenarios were simulated after completing Bluetooth communication exercises in order to examine the ongoing existence of Bluetooth artefacts. The Android smartphones' Bluetooth settings were used to manually unpair previously paired devices under typical user circumstances. The unpairing process was repeated using the same method on each of the chosen devices to guarantee consistency [8, 10].

2.6. Logical Forensic Acquisition

A logical forensic acquisition procedure was employed to gather Bluetooth-associated data from the chosen Android smartphones after the unpairing scenarios were simulated. Android Debug Bridge (ADB) was used to carry out the extraction procedure via a controlled interface. Commands were executed to obtain Bluetooth-related information including system logs, MAC addresses, paired device records, and connection details, while maintaining data integrity throughout [11].

2.7. Artefact Analysis

Once logical acquisition was completed, the extracted data was assessed for Bluetooth artefacts. Analysis focused primarily on configuration files and system-level data captured by ADB commands [12]. The first phase reviewed retrieved Bluetooth configuration settings to locate device identities, MAC addresses, and previously paired device records. Bluetooth-related directories (e.g., `/data/misc/bluetooth/`) received particular attention, as connection and device data are typically stored there. System-level outputs from commands such as `adb shell dumpsys bluetooth_manager` were also analysed to observe connected device lists, connection settings, and other Bluetooth-related parameters.

3. Results

3.1. Bluetooth Artefacts Identified Before Device Unpairing

Prior to unpairing the Android devices, Bluetooth-related artefacts were analysed using ADB-based logical acquisition. The investigation confirmed the presence of Bluetooth-related evidence in accessible storage following successful pairing and file transfer. The command `adb shell dumpsys bluetooth_manager` was used to check Bluetooth functionality and confirmed that pairing and file transfer operations had occurred at the device level. The output showed that Bluetooth was functional during the experiment.

```
C:\platform-tools>adb devices
List of devices attached
UGQSR8IRCEHMPZGM    device
```

Figure 1. Connected Devices before Unpairing.

```
C:\platform-tools>adb devices
List of devices attached
UGQSR8IRCEHMPZGM    device
```

Figure 2. Connected Devices after Unpairing.

It should be noted that efforts to access Bluetooth system directories (e.g., /data/misc/bluetooth) were restricted by permission limitations common to non-rooted devices, preventing examination of configuration and deep pairing data [13].

3.2. Bluetooth Artefacts Identified After Device Unpairing

Further analysis was performed after Bluetooth devices were unpaired using ADB-based logical acquisition. The command `adb shell dumpsys bluetooth_manager` confirmed that the pairing connection had been removed at the system level, showing no bound devices remaining.

However, files previously transferred during the pairing phase remained in the `sdcard/Download/` folder, retaining the default name associated with the Bluetooth transfer. This confirms that file-level artefacts were not deleted during the unpairing process. As in the pre-unpairing phase, access to system directories such as `/data/misc/bluetooth` remained restricted due to the absence of root access, leaving low-level configuration data unexamined [8].

3.3. Comparative Analysis of Artefact Persistence

A comparative analysis was performed on Bluetooth artefacts before and after device unpairing using ADB-based logical acquisition. The analysis reveals that certain system-level indicators are removed post-unpairing; however, user-level artefacts largely persist.

```
beryl:/ $ stat /sdcard/Download/BT_TEST_04_072508.jpg
File: /sdcard/Download/BT_TEST_04_072508.jpg
Size: 291202  Blocks: 576    IO Blocks: 512  regular file
Device: 80h/128d    Inode: 290313  Links: 1      Device type: 0,0
Access: (0770/-rwxrwx---)  Uid: (10263/ u0_a263)  Gid: ( 1023/media_rw)
Access: 2026-02-15 19:25:10.912293040 +0530
Modify: 2026-02-15 19:25:12.960293040 +0530
Change: 2026-02-15 19:25:13.056293040 +0530
beryl:/ $ |
```

Figure 3. File Information before Unpairing.

```
beryl:/ $ stat /sdcard/Download/BT_TEST_04_072508.jpg
File: /sdcard/Download/BT_TEST_04_072508.jpg
Size: 291202  Blocks: 576    IO Blocks: 512  regular file
Device: 80h/128d    Inode: 290313  Links: 1      Device type: 0,0
Access: (0770/-rwxrwx---)  Uid: (10263/ u0_a263)  Gid: ( 1023/media_rw)
Access: 2026-02-15 19:25:10.912293040 +0530
Modify: 2026-02-15 19:25:12.960293040 +0530
Change: 2026-02-15 19:25:13.056293040 +0530
beryl:/ $ |
```

Figure 4. File Information after Unpairing.

Bluetooth activity on the device prior to unpairing remains evidenced through recovered file artefacts. The retention of user-level artefacts is more complete than that of system-level artefacts, indicating that the unpairing process constitutes only partial deletion rather than complete removal [9].

3.4. ADB Commands Used for Bluetooth Artefact Analysis

The following ADB commands were used to extract and compare Bluetooth artefacts before and after device unpairing:

Table 2. ADB commands used in forensic artefact extraction.

Stage	Command	Key Result
ADB Setup	adb start-server & adb devices	Server started; device listed as authorised
Shell Access	adb shell	Entered Android device shell (/ \$)
BT Manager (Before)	dumpps bluetooth_manager grep -i "Sender Device Name"	Full MAC address of connected device displayed; device in paired condition confirmed
Storage Navigation	cd /sdcard/Download	Accessed download directory; test files present
File Listing	ls /sdcard/Download	All files including transferred file displayed
File Metadata	stat /sdcard/Download/Filename.jpg	File size, access/modify/change timestamps, and ownership (UID/GID) confirmed
Hash Verification	sha256sum /sdcard/Download/Filename.jpg	Unique hash value generated for integrity baseline
BT Manager (After)	dumpps bluetooth_manager grep -i "Sender Device Name"	Partial MAC address shown; device confirmed as unpaired

Note: System-level Bluetooth directories (/data/misc/bluetooth) were inaccessible without root access, representing a significant limitation for forensic investigation on non-rooted devices.

3.5. Identification of Stored Device Information

The forensic examination identified artefacts related to MAC addresses, device names, connection timestamps, and Bluetooth configuration files.

```

beryl:/ $ ls -lt /sdcard/Download
total 28393
-rwxrwx--- 1 u0_a263 media_rw 291202 2026-02-15 19:25 BT_TEST_04_072508.jpg
-rw-rw---- 1 u0_a263 media_rw 8948 2026-02-04 13:58 OWASP_Top_10_2021_Detailed_Professional.pdf
-rw-rw---- 1 u0_a263 media_rw 7121 2026-02-04 13:44 OWASP_Top_10_Beginner_Guide.pdf
-rw-rw---- 1 u0_a263 media_rw 1584709 2026-01-03 21:28 Penetration\ Testing\ Methodology.pdf
-rw-rw---- 1 u0_a263 media_rw 1205081 2026-01-01 18:04 Forensic\ Recruitment\ Notice.pdf
-rw-rw---- 1 u0_a263 media_rw 97393 2025-12-30 20:16 DLRL\ Walkin.pdf
-rwxrwx--- 1 u0_a263 media_rw 121237 2025-12-27 16:41 Paytm_QRcode_1766833885808.png
-rw-rw---- 1 u0_a263 media_rw 2282 2025-12-26 01:00 invite.ics
-rw-rw---- 1 u0_a263 media_rw 27978 2025-12-18 09:13 PoojaSharma_InternshalaResume.pdf
-rwxrwx--- 1 u0_a263 media_rw 100786 2025-12-10 17:05 Paytm_QRcode_1765366519316.png
drwxrws--- 3 u0_a263 media_rw 3452 2025-12-02 15:39 TeraBox
-rwxrwx--- 1 u0_a263 media_rw 2222652 2025-11-20 22:18 b0940179-9b79-4962-900e-6132961ec9fc
-rw-rw---- 1 u0_a263 media_rw 100786 2025-11-11 22:41 Paytm_QRcode_1762881101389.png
-rw-rw---- 1 u0_a263 media_rw 7748515 2025-11-08 05:39 \ Ethical\ Hacker\ (CEH)\ Study\ Guide-2.pdf
-rw-rw---- 1 u0_a263 media_rw 7748515 2025-11-08 05:39 \ Ethical\ Hacker\ (CEH)\ Study\ Guide-1.pdf
-rw-rw---- 1 u0_a263 media_rw 7748515 2025-11-08 05:39 \ Ethical\ Hacker\ (CEH)\ Study\ Guide.pdf
drwxrws--- 2 u0_a263 media_rw 3452 2025-11-01 10:20 downloaded_rom
drwxrws--- 2 u0_a263 media_rw 3452 2025-11-01 09:48 downloaded_apex
beryl:/ $

```

Figure 5. Storage Location before Unpairing.

```

l|beryl:/ $ ls -lt /sdcard/Download
total 28393
-rwxrwx--- 1 u0_a263 media_rw 291202 2026-02-15 19:25 BT_TEST_04_072508.jpg
-rw-rw---- 1 u0_a263 media_rw 8948 2026-02-04 13:58 OWASP_Top_10_2021_Detailed_Professional.pdf
-rw-rw---- 1 u0_a263 media_rw 7121 2026-02-04 13:44 OWASP_Top_10_Beginner_Guide.pdf
-rw-rw---- 1 u0_a263 media_rw 1584709 2026-01-03 21:28 Penetration\ Testing\ Methodology.pdf
-rw-rw---- 1 u0_a263 media_rw 1205081 2026-01-01 18:04 Forensic\ Recruitment\ Notice.pdf
-rw-rw---- 1 u0_a263 media_rw 97393 2025-12-30 20:16 DLRL\ Walkin.pdf
-rwxrwx--- 1 u0_a263 media_rw 121237 2025-12-27 16:41 Paytm_QRcode_1766833885808.png
-rw-rw---- 1 u0_a263 media_rw 2282 2025-12-26 01:00 invite.ics
-rw-rw---- 1 u0_a263 media_rw 27978 2025-12-18 09:13 PoojaSharma_InternshalaResume.pdf
-rwxrwx--- 1 u0_a263 media_rw 100786 2025-12-10 17:05 Paytm_QRcode_1765366519316.png
drwxrws--- 3 u0_a263 media_rw 3452 2025-12-02 15:39 TeraBox
-rwxrwx--- 1 u0_a263 media_rw 2222652 2025-11-20 22:18 b0940179-9b79-4962-900e-6132961ec9fc
-rw-rw---- 1 u0_a263 media_rw 100786 2025-11-11 22:41 Paytm_QRcode_1762881101389.png
-rw-rw---- 1 u0_a263 media_rw 7748515 2025-11-08 05:39 \ Ethical\ Hacker\ (CEH)\ Study\ Guide-2.pdf
-rw-rw---- 1 u0_a263 media_rw 7748515 2025-11-08 05:39 \ Ethical\ Hacker\ (CEH)\ Study\ Guide-1.pdf
-rw-rw---- 1 u0_a263 media_rw 7748515 2025-11-08 05:39 \ Ethical\ Hacker\ (CEH)\ Study\ Guide.pdf
drwxrws--- 2 u0_a263 media_rw 3452 2025-11-01 10:20 downloaded_rom
drwxrws--- 2 u0_a263 media_rw 3452 2025-11-01 09:48 downloaded_apex
beryl:/ $ |

```

Figure 6. Storage Location after Unpairing.

MAC addresses uniquely identify devices within the Bluetooth environment, while device names provide contextual information that may assist investigators in associating a device with a specific user.

3.6. Partial Deletion Vs. Complete Removal Analysis

This analysis examines whether Bluetooth unpairing removes all artefacts or results only in superficial deletion.

```
C:\platform-tools>adb shell
beryl:/ $ dumpsys bluetooth_manager | grep -i "vivo y56 5g"
A8:05:56:02:EA:96 [ DUAL ] vivo Y56 5G
shim::legacy::record 004 xx:xx:xx:xx:ea:96 DUAL cod:0x0c025a remote_info:10-00000-00070 sm4:0x11 SecureConn:T name:"vivo Y56 5G"
shim::legacy::btm 2026-02-15 19:24:58.439 CBACK Ssp request : xx:xx:xx:xx:ea:96 name:"vivo Y56 5G" just_works:F pin:482683
beryl:/ $ |
```

Figure 7. Before Unpairing.

```
C:\platform-tools>adb shell
beryl:/ $ dumpsys bluetooth_manager | grep -i "vivo y56 5g"
shim::legacy::btm 2026-02-15 19:24:58.439 CBACK Ssp request : xx:xx:xx:xx:ea:96 name:"vivo Y56 5G" just_works:F pin:482683
beryl:/ $ |
```

Figure 8. After Unpairing.

The evidence indicates that unpairing triggers partial deletion at the system level, while user-accessible file artefacts, partial connection identifiers, and metadata remain intact.

3.7. Correlation and Validation of Artefacts

Bluetooth artefact correlation and validation involved cross-examination of data from different sources, including logs and configuration files. Core data elements such as device identifiers, timestamps, MAC addresses, and device names were examined for consistency.

```
beryl:/ $ sha256sum /sdcard/Download/BT_TEST_04_072508.jpg
a3bcfe678b69ef2d4d8bb64cc06075a421c88cb9649308c0698225dd046337b3 /sdcard/Download/BT_TEST_04_072508.jpg
beryl:/ $
```

Figure 9. Hash value before Unpairing.

```
beryl:/ $ sha256sum /sdcard/Download/BT_TEST_04_072508.jpg
sha256sum: /sdcard/Download/BT_TEST_04_072508.jpg: No such file or directory
1|beryl:/ $ sha256sum /sdcard/Download/BT_TEST_04_072508.jpg
a3bcfe678b69ef2d4d8bb64cc06075a421c88cb9649308c0698225dd046337b3 /sdcard/Download/BT_TEST_04_072508.jpg
beryl:/ $ |
```

Figure 10. Hash value after Unpairing.

Data validation reduces the risk of misinterpretation and confirms the reliability and integrity of the data. This process adds evidentiary value and ensures that forensic conclusions derived from artefacts are sound [14].

4. Discussion

The findings of this study demonstrate that Bluetooth artefacts on Android smartphones exhibit varying degrees of persistence depending on the level of storage (system-level vs.

user-level) and the type of artefact. At the system level, unpairing results in the removal of bonding records from the active Bluetooth manager output, suggesting that the operating system carries out some cleanup upon unpairing. However, the restricted access to /data/misc/bluetooth on non-rooted devices limits the completeness of system-level forensic examination, a challenge widely documented in the literature [8, 9].

At the user-accessible storage level, the persistence of transferred files is particularly notable. Files received via Bluetooth remained in the sdcard/Download/ directory with

their original metadata intact including file size, timestamps, and hash values after the unpairing event. This finding is consistent with Cusack and Tug (2012), who also observed that Bluetooth file transfers produce persistent artefacts independent of the pairing relationship. The unchanged hash values confirm that file integrity was maintained, and no tampering occurred post-unpairing, reinforcing the evidentiary value of these artefacts.

The transition from full MAC address visibility to partial MAC address display in `dumppsys bluetooth_manager` output post-unpairing represents a significant forensic indicator. While the full bonding record is removed, the partial MAC address suggests that residual Bluetooth activity data is retained in system buffers or logs accessible without root. This partial persistence supports the hypothesis that Android's Bluetooth stack does not perform a complete purge of all device interaction records upon unpairing [13].

This study aligns with other studies of Bluetooth and mobile device forensics. Previous literature has shown that information related to Bluetooth can still be found within Android systems in cases where the user unpaired the device, or erased device associations. A study by Cusack and Tug in (2012) showed that device-related information persisted after Bluetooth-related activities. This study supports their work by showing that even though records of the active bond were purged after unpairing, user-level artefacts, such as transmitted files and metadata, as well as partial device identifiers, were still found onboard. These results also suggest that Bluetooth artefacts have a crucial role in forensics in reconstructing how the device was used and in the history of the device's communications.

The dual-nature of artefact persistence partial system-level removal versus complete user-level retention has meaningful implications for forensic investigators. Investigators should not assume that a device's Bluetooth history is inaccessible simply because no paired devices appear in the settings menu. Both ADB-accessible storage and, where root access permits, low-level configuration directories should be systematically examined.

5. Conclusions

5.1. Major Observations Regarding Bluetooth Artefact Persistence

Several important observations were made regarding the persistence of Bluetooth artefacts on Android smartphones. Bluetooth-related data, including device names, MAC addresses, and connection timestamps, are generated during the pairing and communication processes and persist at varying levels after device unpairing [12]. System-level bonding records are partially removed, while user-accessible artefacts particularly transferred files and file metadata remain fully intact.

5.2. Forensic Value of Recovered Artefacts

The Bluetooth artefacts recovered in this study demonstrate considerable importance to the field of digital forensics. Artefacts such as MAC addresses, device names, pairing records, and connection timestamps enable forensic examiners to link devices, identify previously connected devices, and reconstruct user behaviour [13]. The persistence of file artefacts with unchanged hash values further confirms the integrity and evidentiary reliability of these data points.

5.3. Implications for Digital Forensic Investigations

The findings demonstrate that Bluetooth unpairing does not constitute a complete erasure of device interaction history. Bluetooth-related artefacts enable insight into proximity-based communications and device associations that would not be recoverable through standard user-interface examination alone. Mobile forensic investigators should treat Bluetooth artefact analysis as a standard component of Android device examination [14].

5.4. Limitations of the Research

This study examined only a small number of Android devices, restricting the range of hardware, device models, and Android OS versions. The impact of the different Android versions, in combination with the manufacturers' customizations, leave room for possible variance in the storage, availability, and persistence of Bluetooth artefacts. This may impact the study's findings. The study also included only Android Debug Bridge (ADB) based logical extractions. Because the devices could not be rooted, the study was constrained in its ability to examine the Bluetooth system's file, `/data/misc/bluetooth`, and gain access to low-level system files and bonding files. Neither advanced forensic extraction tools nor rooting techniques were used in this study. The Bluetooth artefacts were also only partially analyzed. Further studies on this field may explore a wider range of techniques and methods and consider the persistence of artefacts across a wider range of Android devices and versions and Bluetooth Low Energy (BLE) artefacts. This will provide a more comprehensive forensic evaluation of the Android operating system.

Abbreviations

ADB	Android Debug Bridge
BLE	Bluetooth Low Energy
BR/EDR	Basic Rate/Enhanced Data Rate (Bluetooth Classic)
FHSS	Frequency-Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
IoT	Internet of Things
MAC	Media Access Control

OS Operating System

Author Contributions

Dave Drashti: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Writing – original draft

Kashyap Joshi: Methodology, Project administration, Supervision, Validation, Writing – review & editing

Kapil Kumar: Resources, Supervision, Validation, Writing – review & editing

Data Availability Statement

The data supporting the outcome of this research work has been reported in this manuscript.

Conflicts of Interest

The authors declare no conflicts of interest.

References

- [1] Neyaz, A., Shashidhar, N. USB artifact analysis using windows event viewer, registry and file system logs. *Electronics* (Switzerland). 2019, 8(11). <https://doi.org/10.3390/ELECTRONICS8111322>
- [2] Anathi, M., Vijayakumar, K. An intelligent approach for dynamic network traffic restriction using MAC address verification. *Comput. Commun.* 2020, 154, 559-564. <https://doi.org/10.1016/j.comcom.2020.02.021>
- [3] Teing, Y. Y., Dehghantanha, A., Choo, K. K. R., Dargahi, T., Conti, M. Forensic Investigation of Cooperative Storage Cloud Service: Symform as a Case Study. *J. Forensic Sci.* 2017, 62(3), 641-654. <https://doi.org/10.1111/1556-4029.13271>
- [4] Ahmed, A. A., Farhan, K., Ninggal, M. I. H., Alsawi, G. Retrieving and Identifying Remnants of Artefacts on Local Devices Using Sync.com Cloud. *Sensors.* 2025, 25(1). <https://doi.org/10.3390/S25010106>
- [5] OWASP Top 10 - OWASP Developer Guide. Available from: <https://devguide.owasp.org/en/02-foundations/05-top-ten/> (accessed 10 April 2026).
- [6] Gomez, C., Oller, J., Paradells, J. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors* (Switzerland). 2012, 12(9), 11734-11753. <https://doi.org/10.3390/s120911734>
- [7] Naik, A. G., Kuwelkar, S., Magdum, V. Energy and Current Consumption Analysis for Classic Bluetooth and Bluetooth Low Energy (BLE). *Emerging Research in Computing, Information, Communication and Applications: ERCICA* 2015. 2015, 87-95. https://doi.org/10.1007/978-81-322-2550-8_9
- [8] Natgunanathan, I., Fernando, N., Loke, S. W., Weerasuriya, C. Bluetooth Low Energy Mesh: Applications, Considerations and Current State-of-the-Art. *Sensors.* 2023, 23(4). <https://doi.org/10.3390/s23041826>
- [9] Garc á-Ortiz, J. C., Silvestre-Blanes, J., Sempere-Pay á V. Experimental application of bluetooth low energy connectionless in smart cities. *Electronics* (Switzerland). 2021, 10(22). <https://doi.org/10.3390/electronics10222735>
- [10] Murugalakshmi, S. Evolution and performance analysis of bluetooth low energy 5.0. *i-manager's Journal on Mobile Applications and Technologies.* 2023, 10(2), 31. <https://doi.org/10.26634/jmt.10.2.20436>
- [11] Yang, J., Poellabauer, C., Mitra, P., Neubecker, C. Beyond beaconing: Emerging applications and challenges of BLE. *Ad Hoc Networks.* 2020, 97. <https://doi.org/10.1016/j.adhoc.2019.102015>
- [12] Raj, U. Bluetooth Low Energy: A Comprehensive Wireless Technology. *International Journal of Advance Research and Innovation.* 2021, 9(3), 64-69. <https://doi.org/10.51976/ijari.932110>
- [13] Liu, C., Zhang, Y., Zhou, H. A comprehensive study of bluetooth low energy. *J. Phys. Conf. Ser.* 2021, 2093(1). <https://doi.org/10.1088/1742-6596/2093/1/012021>
- [14] Hoddie, P., Prader, L. Bluetooth Low Energy (BLE). *IoT Development for ESP32 and ESP8266 with JavaScript.* 2020, 185-220. https://doi.org/10.1007/978-1-4842-5070-9_4