# Security Issues in Bluetooth Network

Abhishek Rana, Kuldip Kumar

Department of Electronics & Communication Engineering, Chandigarh University (University Institute of Engineering), Mohali, Punjab, India

Corresponding author: Abhishek Rana, Email: ranaabhishek.a1@gmail.com

The Remote PANs are usually connected through Bluetooth. Data exchange across gadgets is exciting and challenging. The process begins with one device. It allows metered data transfer between multiple devices. Bluetooth transmits 1 Mbps. Bluetooth's security requirements are growing, which could compromise consumers' sensitive data. Devices must match to restrict secure correspondence. This study shows harmful threats inside devices that exchange data over Bluetooth. It also shows many Bluetooth development successes during information transfer.

**Keywords**: Bluetooth Security, organizing, destructive aggressors, the integrity of computer networks, and man-in-the-middle attacks (MIM)

in: *Advancements in Communication and Systems*. Ed. by Ashish Kumar Tripathi and Vivek Shrivastava. Computing and Intelligent Systems, SCRS, India., 2023, pp. 1–8. DOI: https://doi.org/10.56155/978-81-955020-7-3-1

## 1. Introduction

The Bluetooth helped switch alliances—a fast-make radio link with sturdy hitch and electronics. The current solid reach is 30 feet. We require programming and equipment upgrades. A radio chip is needed. As usual, product quality and security are tested. Bluetooth standardizes professional, adaptable long-distance communication. For many applications, the Bluetooth Technology SIG has reduced execution costs and accelerated its event.

Bluetooth needs three security partners: Verifying device reliability without Bluetooth addresses is necessary. Bluetooth does not verify client sight. Confidentiality limits data to permitted devices. Accepting means controlling assets with help before operating. Bluetooth groups can reach 10 meters with low power. Bluetooth uses IEEE 802.15 shows. New PAN works by touch or admission. Connect two parts without a cortical view. Device users are verified via 4-digit PINs. Matching customer PINs to device numbers protects connections. Two devices generate a development secret with uncontested confirmation numbers to connect. Bluesnarf steals vulnerable device data. Aggregating devices is possible with Bluetooth clients. Short battery life or man-in-the-middle attacks damage electronics. Data, device, and association disruption [3]. Speeding up Bluetooth transmissions of critical data and improving security are industry recommendations.

## 2. Presentation of Information Relating to the Devices

Text Helping Bluetooth devices protect data encourages cryptography. Preventing illegal access and use requires data privacy rules, administration, and regulation. Proper data puzzling uses these structures:

Certification of clients Giving a secret word is wrong. Explaining helps clients acquire info and accommodations. Distribute credentials securely. Bluetooth on/off When needed, enable Bluetooth respect. Switch off the organization after Bluetooth data transfer.

Bluetooth association decreases. Bluetooth devices should be closed. Pair Bluetooth devices in crowds with long, hard-to-decipher passkeys.

## 3. How does Bluetooth Compromise Security?

Pros and drawbacks of Bluetooth. We offer authentication, permission, and encryption. Two Bluetooth gadgets show characters. Granting something. Bluetooth connections cannot access device assets or relationships without permission. Eavesdropping is prohibited through plaintext encryption. Bluetooth decreases safety but raises device vulnerabilities and knowledge events. Damaged aggressors can caricature MAC owing to Piconet's age and design. Bluetooth Special Interest Group failed to stop this threat. Q.T. matches are popular. They offered unusual, long, and diversified PINs. [6]. Cabir Worms imitate Bluetooth devices. Planners may consider Bluetooth viral production after the Cabir worm revealed Bluetooth may coherently propagate to line lower infestations. [1]. Unrestricted Bluetooth transmissions are received during bluejacking. User-targeted attacks. Information is unavailable to opponents. Knowledge is needed for aggressive Blue Snarfing.

Blue bugging: attackers can remotely alter client data. Bluetooth blueprints include attack-planning device makers and models. Look for Bluetooth faults. Blue Over attacks on BlueBugged devices are dangerous. For stealing friend info, BlueBugging is great. Bluetooth phones with Blueover or Bluover II can sneak attack. Bluetooth radio answers reduce nonstandard data assaults. Slow device responsiveness may indicate display stack difficulties. Reflection assaults send data from objective devices to each other during exams, so attackers know nothing. Before system attacks, data may be split without owner or consumer consent. Calls, batteries, and electronics fail with aggressor neglect. Declutter Bluetooth. Helping individuals without keys, impersonation/Man in the Middle attacks transmit false testimony between devices. Completely aggregate data significance among linked devices to create a Piconet. [6]. Phreakers evaluate war profiteering with "War Nibbling". Test weak Bluetooth phones. They sniff open phones using PCs or red Fang-like equipment with fast receiving connections and sophisticated programming. Interception of all remote communications. Wi-Fi should be riskier than Bluetooth.

## 4. Dynamic Constituents and Models

Different Bluetooth Flavors secure data differently. Some of the four modes get alert signals from all Bluetooth types. Each Bluetooth device should have one. Every single one of the four modes:-

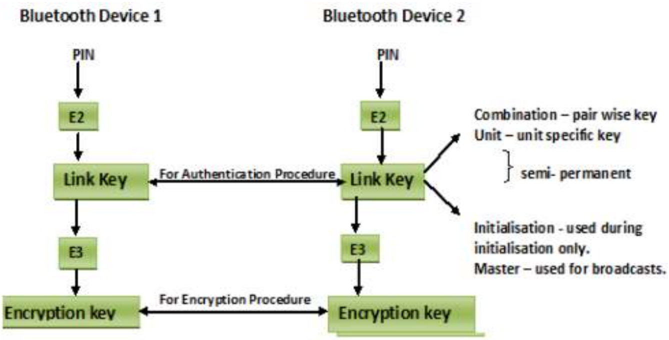


**Figure 1.**Bluetooth Generation Key From PIN

Security Mode 1:
Unsafe. The "beyond absurd" Bluetooth devices in this mode don't interfere with other Bluetooth associations.

Security Mode 2:
The combined pioneer informs exhibit and gadget users about access control. All Bluetooth devices support Security mode 2.

Security Mode 3:
Devices apply security before Bluetooth connections. Bluetooth Security Mode 3 needs authenticated, encrypted conversations. Device-based bonding. Sharing, monodirectional signaling, and encryption [7]. A difficult way is used to express this key when two devices are problematic. Working Bluetooth devices are "related." Initialization generates an association key. Bluetooth needs two linked devices to choose interface keys throughout the presentation after entering a questionable PIN. Figure 4 clearly illustrates PIN, device connection, and key verification. After initialization, devices connect securely. Bluetooth modules briefly import association keys from the upper layer key exchange. The Bluetooth PIN is 1-16 bytes. Application PINs might be four or five [7].

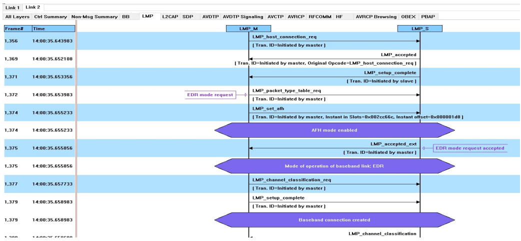
## 5. Result

This post analyses Smart Phone-Infotech BT Connection data with Sodera.
What's Sodera? OR for its purpose?
Analyzers like Sodera Bluetooth are small and versatile. In framework-powered time, Sodera detects Bluetooth LE/BR/EDR or both. Choose a method and collect data. These Sodera analyzers are simple

and useful. QA engineers and organizers collect data in labs, cars, and online. "Outing Mode" enables experts to initiate Bluetooth air traffic without a PC with one touch. Labs likely collect, decipher, and analyze data. Frontline Sodera's small size and disposable battery allow clandestine testing in vehicles and other power-limited environments.

## 5.1 Link Manager Protocol (LMP)

LMP maintains Bluetooth logical communication links. Other LMP features include device authentication, message encryption, and packet size negotiation.

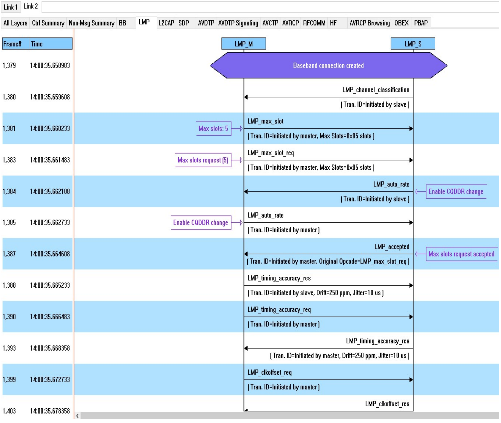


| Frame# | Time | LMP_M | LMP_S |
|---|---|---|---|
| 1,356 | 14:00:35.643983 | LMP_host_connection_req<br>( Tran. ID=Initiated by master ) | |
| 1,369 | 14:00:35.652108 | | LMP_accepted<br>( Tran. ID=Initiated by master, Original Opcode=LMP_host_connection_req ) |
| 1,371 | 14:00:35.653356 | | LMP_setup_complete<br>( Tran. ID=Initiated by slave ) |
| 1,372 | 14:00:35.653983 | EDR mode request<br>LMP_packet_type_table_req<br>( Tran. ID=Initiated by master ) | |
| 1,374 | 14:00:35.655233 | LMP_set_afh<br>( Tran. ID=Initiated by master, Instant in Slots=0x002cc66c, Instant offset=0x000001d8 ) | |
| 1,374 | 14:00:35.655233 | AFH mode enabled | |
| 1,375 | 14:00:35.655856 | | LMP_accepted_ext<br>( Tran. ID=Initiated by master )<br>EDR mode request accepted |
| 1,375 | 14:00:35.655856 | Mode of operation of baseband link: EDR | |
| 1,377 | 14:00:35.657733 | LMP_channel_classification_req<br>( Tran. ID=Initiated by master ) | |
| 1,379 | 14:00:35.658983 | LMP_setup_complete<br>( Tran. ID=Initiated by master ) | |
| 1,379 | 14:00:35.658983 | Baseband connection created | |
| | | | LMP_channel_classification |

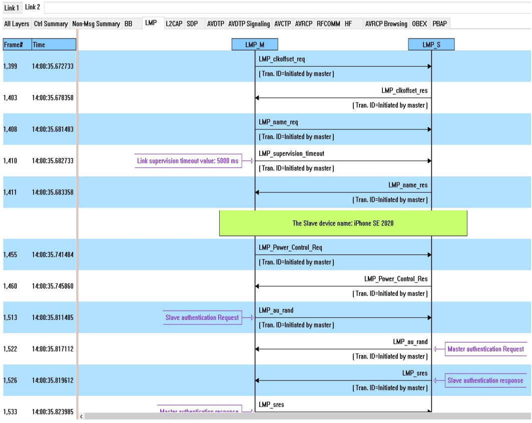
**Figure 2.**LMP (Detailed Fames of connection)

Figure 2. shows how the smart device and InfoTech system pair and connect when the user interacts with the BT on the screen.

LMP requests a connection in frame 1,356 after selecting InfoTech from the smartphone's Bluetooth list.
Frames 1,369 and 1,371 show LMP connecting and responding to the Smartphone.
The smartphone requests EDR mode at LMP frame 1,371.
InfoTech accepts 1,375-frame LMP EDR.



| Frame# | Time | LMP_M | LMP_S |
|---|---|---|---|
| 1,379 | 14:00:35.658983 | Baseband connection created | |
| 1,380 | 14:00:35.659608 | | LMP_channel_classification<br>( Tran. ID=Initiated by slave ) |
| 1,381 | 14:00:35.660233 | Max slots: 5<br>LMP_max_slot<br>( Tran. ID=Initiated by master, Max Slots=0x05 slots ) | |
| 1,383 | 14:00:35.661483 | Max slots request (5)<br>LMP_max_slot_req<br>( Tran. ID=Initiated by master, Max Slots=0x05 slots ) | |
| 1,384 | 14:00:35.662108 | | LMP_auto_rate<br>( Tran. ID=Initiated by slave )<br>Enable CQDDR change |
| 1,385 | 14:00:35.662733 | Enable CQDDR change<br>LMP_auto_rate<br>( Tran. ID=Initiated by master ) | |
| 1,387 | 14:00:35.664608 | | LMP_accepted<br>( Tran. ID=Initiated by master, Original Opcode=LMP_max_slot_req )<br>Max slots request accepted |
| 1,388 | 14:00:35.665233 | LMP_timing_accuracy_res<br>( Tran. ID=Initiated by slave, Drift=250 ppm, Jitter=10 us ) | |
| 1,390 | 14:00:35.666483 | LMP_timing_accuracy_req<br>( Tran. ID=Initiated by master ) | |
| 1,393 | 14:00:35.668358 | | LMP_timing_accuracy_res<br>( Tran. ID=Initiated by master, Drift=250 ppm, Jitter=10 us ) |
| 1,399 | 14:00:35.672733 | LMP_clkoffset_req<br>( Tran. ID=Initiated by master ) | |
| 1,403 | 14:00:35.678358 | | LMP_clkoffset_res |



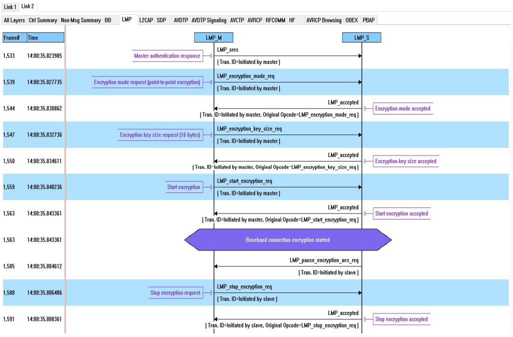
| Frame# | Time | LMP_M | LMP_S |
|---|---|---|---|
| 1,399 | 14:00:35.672733 | LMP_clkoffset_req<br>( Tran. ID=Initiated by master ) | |
| 1,403 | 14:00:35.678358 | | LMP_clkoffset_res<br>( Tran. ID=Initiated by master ) |
| 1,408 | 14:00:35.681483 | LMP_name_req<br>( Tran. ID=Initiated by master ) | |
| 1,410 | 14:00:35.682733 | Link supervision timeout value: 5000 ms<br>LMP_supervision_timeout<br>( Tran. ID=Initiated by master ) | |
| 1,411 | 14:00:35.683358 | | LMP_name_res<br>( Tran. ID=Initiated by master ) |
| | | The Slave device name: iPhone SE 2020 | |
| 1,455 | 14:00:35.741484 | LMP_Power_Control_Req<br>( Tran. ID=Initiated by master ) | |
| 1,460 | 14:00:35.745860 | | LMP_Power_Control_Res<br>( Tran. ID=Initiated by master ) |
| 1,513 | 14:00:35.811485 | Slave authentication Request<br>LMP_au_rand<br>( Tran. ID=Initiated by master ) | |
| 1,522 | 14:00:35.817112 | | LMP_au_rand<br>( Tran. ID=Initiated by master )<br>Master authentication Request |
| 1,526 | 14:00:35.819612 | | LMP_sres<br>( Tran. ID=Initiated by master )<br>Slave authentication response |
| 1,533 | 14:00:35.823985 | Master authentication response<br>LMP_sres | |

**Figure 3.**LMP (Baseband connection) **Figure 4.**LMP (Authentication setup)

The baseband connection with CQDDR changes and LMP channel slots is shown in Figure 3.

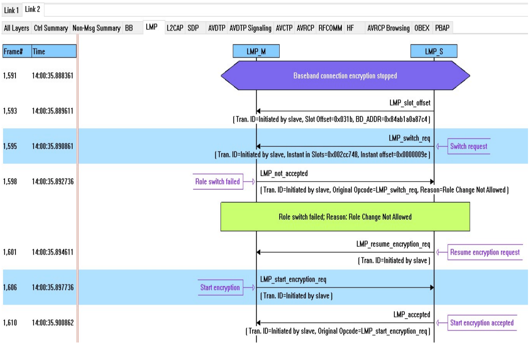
## 5.2 Bluetooth CQDDR

Bluetooth may reduce data transmission in poor reception conditions. Channel Quality Driven Data Rate controls frame length by noise. CQDDR is interesting for Bluetooth in cars. Internal clock setting, name verification, and authentication are shown in Figure 4.In frame 1,399 under the LMP, the clock offset is requested and in frame 1,403 under LMP, the response was sent to make sure the internal clock is set.



| Frame# | Time | |
|---|---|---|
| 1,533 | 14:00:35.823985 | Master authentication response<br>LMP_sres<br>[ Tran. ID=Initiated by master ] |
| 1,539 | 14:00:35.827735 | Encryption mode request (point-to-point encryption)<br>LMP_encryption_mode_req<br>[ Tran. ID=Initiated by master ] |
| 1,544 | 14:00:35.830862 | LMP_accepted<br>[ Tran. ID=Initiated by master, Original Opcode=LMP_encryption_mode_req ]<br>Encryption mode accepted |
| 1,547 | 14:00:35.832736 | Encryption key size request (16 bytes)<br>LMP_encryption_key_size_req<br>[ Tran. ID=Initiated by master ] |
| 1,550 | 14:00:35.834611 | LMP_accepted<br>[ Tran. ID=Initiated by master, Original Opcode=LMP_encryption_key_size_req ]<br>Encryption key size accepted |
| 1,559 | 14:00:35.840236 | Start encryption<br>LMP_start_encryption_req<br>[ Tran. ID=Initiated by master ] |
| 1,563 | 14:00:35.843361 | LMP_accepted<br>[ Tran. ID=Initiated by master, Original Opcode=LMP_start_encryption_req ]<br>Start encryption accepted |
| 1,563 | 14:00:35.843361 | Baseband connection encryption started |
| 1,585 | 14:00:35.884612 | LMP_pause_encryption_aes_req<br>[ Tran. ID=Initiated by slave ] |
| 1,588 | 14:00:35.886486 | Stop encryption request<br>LMP_stop_encryption_req<br>[ Tran. ID=Initiated by slave ] |
| 1,591 | 14:00:35.888361 | LMP_accepted<br>[ Tran. ID=Initiated by slave, Original Opcode=LMP_stop_encryption_req ]<br>Stop encryption accepted |

**Figure 5.** LMP (Encryption of Data setup)



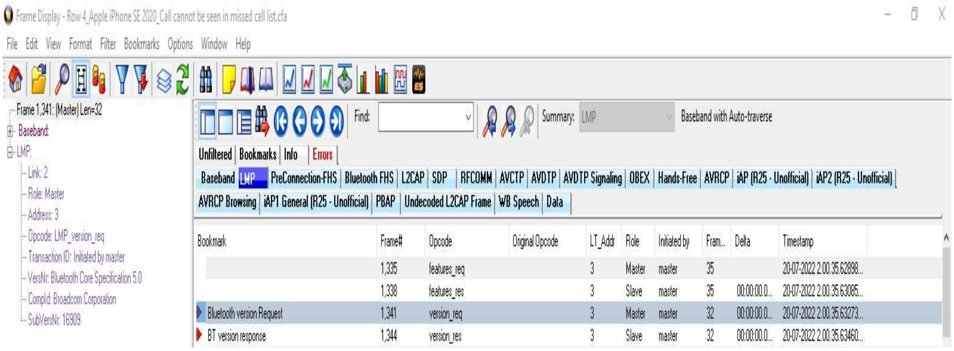
| Frame# | Time | |
|---|---|---|
| 1,591 | 14:00:35.888361 | Baseband connection encryption stopped |
| 1,593 | 14:00:35.889611 | LMP_slot_offset<br>[ Tran. ID=Initiated by slave, Slot Offset=0x031b, BD_ADDR=0x84ab1a0a87c4 ] |
| 1,595 | 14:00:35.890861 | LMP_switch_req<br>[ Tran. ID=Initiated by slave, Instant in Slots=0x002cc748, Instant offset=0x0000009e ]<br>Switch request |
| 1,598 | 14:00:35.892736 | Role switch failed<br>LMP_not_accepted<br>[ Tran. ID=Initiated by slave, Original Opcode=LMP_switch_req, Reason=Role Change Not Allowed ]<br>Role switch failed; Reason: Role Change Not Allowed |
| 1,601 | 14:00:35.894611 | LMP_resume_encryption_req<br>[ Tran. ID=Initiated by slave ]<br>Resume encryption request |
| 1,606 | 14:00:35.897736 | Start encryption<br>LMP_start_encryption_req<br>[ Tran. ID=Initiated by slave ] |
| 1,610 | 14:00:35.900862 | LMP_accepted<br>[ Tran. ID=Initiated by slave, Original Opcode=LMP_start_encryption_req ]<br>Start encryption accepted |

**Figure 6.** LMP (Role switch attempt)

In Figure 5. the Authentication process was completed, and the encryption of data was set for a more secure transition of data between the smartphone and InfoTech system.

In frame 1,533 under LMP, the authentication was completed.
Now in frame 1,539 under LMP, the master initiates by sending the encryption mode request (point to point).
In frame 1,544 under LMP, the encryption mode request (point to point) is accepted.
In frame 1,547 under LMP, the master request for the encryption key size (16 bytes).
In frame 1,550 under LMP, the master request for the encryption key size is accepted.
In frame 1,563 under LMP, the Encryption of data started.

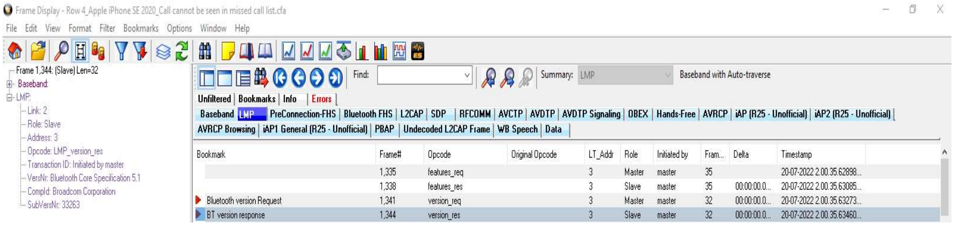
In Figure 6. the Slave requests for role switch but the master rejects and the role switch fails.



Frame 1,341: (Master) Len=32
Baseband:
LMP:
Link: 2
Role: Master
Address: 3
Opcode: LMP_version_req
Transaction ID: Initiated by master
VersNr: Bluetooth Core Specification 5.0
CompId: Broadcom Corporation
SubVersNr: 16909

| Bookmark | Frame# | Opcode | Original Opcode | LT_Addr | Role | Initiated by | Fram... | Delta | Timestamp |
|---|---|---|---|---|---|---|---|---|---|
| | 1,335 | features_req | | 3 | Master | master | 35 | | 20-07-2022 2.00.35.62898... |
| | 1,338 | features_res | | 3 | Slave | master | 35 | 00:00:00.0... | 20-07-2022 2.00.35.63085... |
| Bluetooth version Request | 1,341 | version_req | | 3 | Master | master | 32 | 00:00:00.0... | 20-07-2022 2.00.35.63273... |
| BT version response | 1,344 | version_res | | 3 | Slave | master | 32 | 00:00:00.0... | 20-07-2022 2.00.35.63460... |

**Figure 7.** LMP (Bluetooth Version request)


Frame Display - Row 4_Apple iPhone SE 2020_Call cannot be seen in missed call list.cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: LMP
Baseband with Auto-traverse
Unfiltered | Bookmarks | Info | Errors
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | SDP | RFCOMM | AVCTP | AVDTP | AVDTP Signaling | OBEX | Hands-Free | AVRCP | iAP (R25 - Unofficial) | iAP2 (R25 - Unofficial)
AVRCP Browsing | iAP1 General (R25 - Unofficial) | PBAP | Undecoded L2CAP Frame | WB Speech | Data

```
Frame 1,344: (Slave) Len=32
Baseband:
LMP:
    Link: 2
    Role: Slave
    Address: 3
    Opcode: LMP_version_res
    Transaction ID: Initiated by master
    VersNr: Bluetooth Core Specification 5.1
    CompId: Broadcom Corporation
    SubVersNr: 33263
```

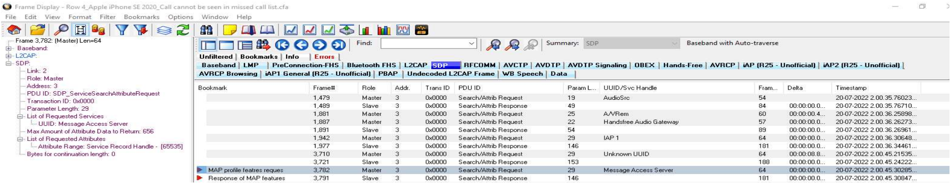
| Bookmark | Frame# | Opcode | Original Opcode | LT_Addr | Role | Initiated by | Fram... | Delta | Timestamp |
|---|---|---|---|---|---|---|---|---|---|
| | 1,335 | features_req | | 3 | Master | master | 35 | | 20-07-2022 2.00.35.62898... |
| | 1,338 | features_res | | 3 | Slave | master | 35 | 00:00:00.0... | 20-07-2022 2.00.35.63085... |
| Bluetooth version Request | 1,341 | version_req | | 3 | Master | master | 32 | 00:00:00.0... | 20-07-2022 2.00.35.63273... |
| BT version response | 1,344 | version_res | | 3 | Slave | master | 32 | 00:00:00.0... | 20-07-2022 2.00.35.63460... |

**Figure 8.** LMP (Bluetooth version response)

In figures 7. and 8. the Devices Bluetooth version is requested under LMP in frame 1,341 and frame 1,344 the BT version is sent in response to Bluetooth core specification 5.1.

## 5.3 Service Discovery Protocol (SDP)

Bluetooth ad-hoc networking requires service discovery. Bluetooth devices can discover and connect via Bluetooth SDP. It shows devices what services other Bluetooth devices support and lists everything the device supports.

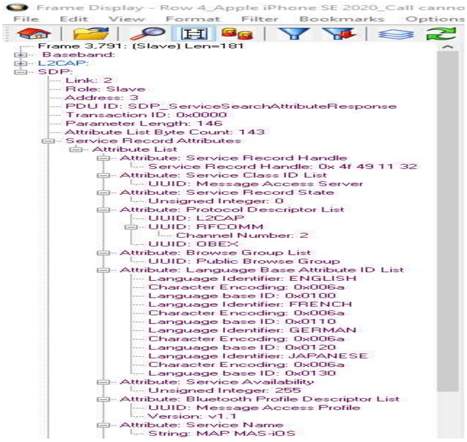

Frame Display - Row 4_Apple iPhone SE 2020_Call cannot be seen in missed call list.cfa
File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: SDP
Baseband with Auto-traverse
Unfiltered | Bookmarks | Info | Errors
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | SDP | RFCOMM | AVCTP | AVDTP | AVDTP Signaling | OBEX | Hands-Free | AVRCP | iAP (R25 - Unofficial) | iAP2 (R25 - Unofficial)
AVRCP Browsing | iAP1 General (R25 - Unofficial) | PBAP | Undecoded L2CAP Frame | WB Speech | Data

```
Frame 3,782: (Master) Len=64
Baseband:
L2CAP:
SDP:
    Link: 2
    Role: Master
    Address: 3
    PDU ID: SDP_ServiceSearchAttributeRequest
    Transaction ID: 0x0000
    Parameter Length: 29
    List of Requested Services
        UUID: Message Access Server
    Max Amount of Attribute Data to Return: 656
    List of Requested Attributes
        Attribute Range: Service Record Handle -  [65535]
    Bytes for continuation length: 0
```

| Bookmark | Frame# | Role | Addr. | Trans ID | PDU ID | Param L... | UUID/Svc Handle | Fram... | Delta | Timestamp |
|---|---|---|---|---|---|---|---|---|---|---|
| | 1,479 | Master | 3 | 0x0000 | Search/Attrib Request | 19 | AudioSrc | 54 | | 20-07-2022 2.00.35.76023... |
| | 1,489 | Slave | 3 | 0x0000 | Search/Attrib Response | 49 | | 84 | 00:00:00.0... | 20-07-2022 2.00.35.76710... |
| | 1,881 | Master | 3 | 0x0000 | Search/Attrib Request | 25 | A/VRem | 60 | 00:00:00.4... | 20-07-2022 2.00.36.25898... |
| | 1,887 | Master | 3 | 0x0000 | Search/Attrib Request | 22 | Handsfree Audio Gateway | 57 | 00:00:00.0... | 20-07-2022 2.00.36.26273... |
| | 1,891 | Slave | 3 | 0x0000 | Search/Attrib Response | 54 | | 89 | 00:00:00.0... | 20-07-2022 2.00.36.26961... |
| | 1,942 | Master | 3 | 0x0000 | Search/Attrib Request | 29 | IAP 1 | 64 | 00:00:00.0... | 20-07-2022 2.00.36.30648... |
| | 1,977 | Slave | 3 | 0x0000 | Search/Attrib Response | 146 | | 181 | 00:00:00.0... | 20-07-2022 2.00.36.34461... |
| | 3,710 | Master | 3 | 0x0000 | Search/Attrib Request | 29 | Unknown UUID | 64 | 00:00:08.8... | 20-07-2022 2.00.45.21535... |
| | 3,721 | Slave | 3 | 0x0000 | Search/Attrib Response | 153 | | 188 | 00:00:00.0... | 20-07-2022 2.00.45.24222... |
| MAP profile featres reques | 3,782 | Master | 3 | 0x0000 | Search/Attrib Request | 29 | Message Access Server | 64 | 00:00:00.0... | 20-07-2022 2.00.45.30285... |
| Response of MAP features | 3,791 | Slave | 3 | 0x0000 | Search/Attrib Response | 146 | | 181 | 00:00:00.0... | 20-07-2022 2.00.45.30847... |

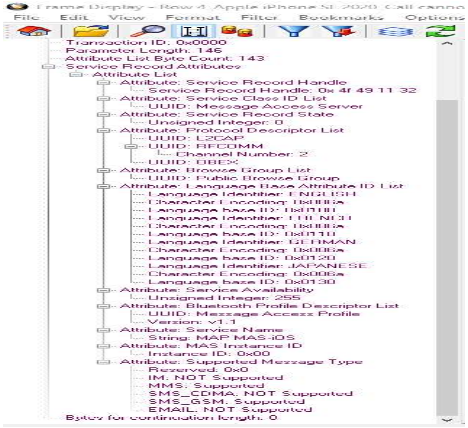
**Figure 9:** SDP (Massage access profile frames)

In figure 9. the frame was captured of the MAP profile attributes and features that are supported.


Frame Display - Row 4_Apple iPhone SE 2020_Call canno
File Edit View Format Filter Bookmarks Options

```
Frame 3,791: (Slave) Len=181
Baseband:
L2CAP:
SDP:
    Link: 2
    Role: Slave
    Address: 3
    PDU ID: SDP_ServiceSearchAttributeResponse
    Transaction ID: 0x0000
    Parameter Length: 146
    Attribute List Byte Count: 143
    Service Record Attributes
        Attribute List
            Attribute: Service Record Handle
                Service Record Handle: 0x 4f 49 11 32
            Attribute: Service Class ID List
                UUID: Message Access Server
            Attribute: Service Record State
                Unsigned Integer: 0
            Attribute: Protocol Descriptor List
                UUID: L2CAP
                UUID: RFCOMM
                    Channel Number: 2
                UUID: OBEX
            Attribute: Browse Group List
                UUID: Public Browse Group
            Attribute: Language Base Attribute ID List
                Language Identifier: ENGLISH
                Character Encoding: 0x006a
                Language base ID: 0x0100
                Language Identifier: FRENCH
                Character Encoding: 0x006a
                Language base ID: 0x0110
                Language Identifier: GERMAN
                Character Encoding: 0x006a
                Language base ID: 0x0120
                Language Identifier: JAPANESE
                Character Encoding: 0x006a
                Language base ID: 0x0130
            Attribute: Service Availability
                Unsigned Integer: 255
            Attribute: Bluetooth Profile Descriptor List
                UUID: Message Access Profile
                Version: v1.1
            Attribute: Service Name
                String: MAP MAS-iOS
```

**Figure 10.** SDP (MAP attributes request)


Frame Display - Row 4_Apple iPhone SE 2020_Call canno
File Edit View Format Filter Bookmarks Options

```
    Transaction ID: 0x0000
    Parameter Length: 146
    Attribute List Byte Count: 143
    Service Record Attributes
        Attribute List
            Attribute: Service Record Handle
                Service Record Handle: 0x 4f 49 11 32
            Attribute: Service Class ID List
                UUID: Message Access Server
            Attribute: Service Record State
                Unsigned Integer: 0
            Attribute: Protocol Descriptor List
                UUID: L2CAP
                UUID: RFCOMM
                    Channel Number: 2
                UUID: OBEX
            Attribute: Browse Group List
                UUID: Public Browse Group
            Attribute: Language Base Attribute ID List
                Language Identifier: ENGLISH
                Character Encoding: 0x006a
                Language base ID: 0x0100
                Language Identifier: FRENCH
                Character Encoding: 0x006a
                Language base ID: 0x0110
                Language Identifier: GERMAN
                Character Encoding: 0x006a
                Language base ID: 0x0120
                Language Identifier: JAPANESE
                Character Encoding: 0x006a
                Language base ID: 0x0130
            Attribute: Service Availability
                Unsigned Integer: 255
            Attribute: Bluetooth Profile Descriptor List
                UUID: Message Access Profile
                Version: v1.1
            Attribute: Service Name
                String: MAP MAS-iOS
            Attribute: MAS Instance ID
                Instance ID: 0x00
            Attribute: Supported Message Type
                Reserved: 0x0
                IM: NOT Supported
                MMS: Supported
                SMS_CDMA: NOT Supported
                SMS_GSM: Supported
                EMAIL: NOT Supported
    Bytes for continuation length: 0
```

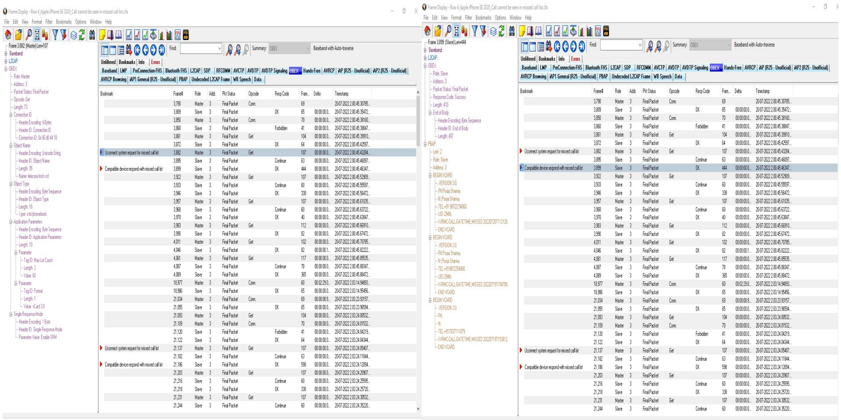
**Figure 11.** SDP (MAP attributes response)

In Figure10. the list is under SDP with the request for MAP profile attributes.
In Figure11. the list is under SDP with all the MAP profile features that are supported or not supported.

### 5.4 Object Exchange (OBEX):

OBEX works with Bluetooth and other wireless devices. Binary data is sent by OBEX. It has stronger transaction restrictions than HTTP, a prominent Internet data transfer protocol.

The Bluetooth Developer Portal says object transmission allows devices to communicate more data "in a resource-sensitive, standardized fashion." In the classic client/server model, OBEX considers the requesting device the client. Sharing digital business cards and other materials between devices is easy.



Frame Display - Row 4_Apple iPhone SE 2020_Call cannot be seen in missed call list.cfa

File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: OBEX
Baseband with Auto-traverse
Unfiltered | Bookmarks | Info | Errors
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | SDP | RFCOMM | AVCTP | AVDTP | AVDTP Signaling | OBEX | Hands-Free | AVRCP | iAP (R25 - Unofficial) | iAP2 (R25 - Unofficial)
AVRCP Browsing | iAP1 General (R25 - Unofficial) | PBAP | Undecoded L2CAP Frame | WB Speech | Data

```
Frame 3,882: (Master) Len=107
⊞ Baseband:
⊞ L2CAP:
⊟ OBEX:
   Role: Master
   Address: 3
   Packet Status: Final Packet
   Opcode: Get
   Length: 73
   ⊟ Connection ID
      Header Encoding: 4 Bytes
      Header ID: Connection ID
      Connection ID: 0x 06 d0 44 10
   ⊟ Object Name
      Header Encoding: Unicode String
      Header ID: Object Name
      Length: 35
      Name: telecom/mch.vcf
   ⊟ Object Type
      Header Encoding: Byte Sequence
      Header ID: Object Type
      Length: 18
      Type: x-bt/phonebook
   ⊟ Application Parameters
      Header Encoding: Byte Sequence
      Header ID: Application Parameters
      Length: 10
      ⊟ Parameter
         Tag ID: Max List Count
         Length: 2
         Value: 60
      ⊟ Parameter
         Tag ID: Format
         Length: 1
         Value: vCard 3.0
   ⊟ Single Response Mode
      Header Encoding: 1 Byte
      Header ID: Single Response Mode
      Parameter Value: Enable SRM
```

| Bookmark | Frame# | Role | Addr. | Pkt Status | Opcode | Resp Code | Fram... | Delta | Timestamp |
|---|---|---|---|---|---|---|---|---|---|
| | 3,790 | Master | 3 | Final Packet | Conn. | | 69 | | 20-07-2022 2:00:45.30785... |
| | 3,809 | Slave | 3 | Final Packet | | OK | 65 | 00:00:00.0... | 20-07-2022 2:00:45.35472... |
| | 3,850 | Master | 3 | Final Packet | Conn. | | 70 | 00:00:00.0... | 20-07-2022 2:00:45.38160... |
| | 3,860 | Slave | 3 | Final Packet | | Forbidden | 41 | 00:00:00.0... | 20-07-2022 2:00:45.38847... |
| | 3,861 | Master | 3 | Final Packet | Get | | 104 | 00:00:00.0... | 20-07-2022 2:00:45.39910... |
| | 3,872 | Slave | 3 | Final Packet | | OK | 64 | 00:00:00.0... | 20-07-2022 2:00:45.42597... |
| ▶ Uconnect system request for missed call list | 3,882 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:00:45.43284... |
| | 3,895 | Slave | 3 | Final Packet | | Continue | 63 | 00:00:00.0... | 20-07-2022 2:00:45.46097... |
| ▶ Compatible device respond with missed call list | 3,899 | Slave | 3 | Final Packet | | OK | 444 | 00:00:00.0... | 20-07-2022 2:00:45.46347... |
| | 3,922 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:00:45.52909... |
| | 3,933 | Slave | 3 | Final Packet | | Continue | 60 | 00:00:00.0... | 20-07-2022 2:00:45.55597... |
| | 3,946 | Slave | 3 | Final Packet | | OK | 338 | 00:00:00.0... | 20-07-2022 2:00:45.56472... |
| | 3,957 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:00:45.61035... |
| | 3,968 | Slave | 3 | Final Packet | | Continue | 60 | 00:00:00.0... | 20-07-2022 2:00:45.63722... |
| | 3,970 | Slave | 3 | Final Packet | | OK | 40 | 00:00:00.0... | 20-07-2022 2:00:45.63847... |
| | 3,983 | Master | 3 | Final Packet | Get | | 112 | 00:00:00.0... | 20-07-2022 2:00:45.66910... |
| | 3,990 | Slave | 3 | Final Packet | | OK | 82 | 00:00:00.0... | 20-07-2022 2:00:45.67472... |
| | 4,011 | Master | 3 | Final Packet | Get | | 102 | 00:00:00.0... | 20-07-2022 2:00:45.70785... |
| | 4,046 | Slave | 3 | Final Packet | | OK | 82 | 00:00:00.1... | 20-07-2022 2:00:45.82222... |
| | 4,061 | Master | 3 | Final Packet | Get | | 117 | 00:00:00.0... | 20-07-2022 2:00:45.85535... |
| | 4,087 | Slave | 3 | Final Packet | | Continue | 78 | 00:00:00.0... | 20-07-2022 2:00:45.88347... |
| | 4,089 | Slave | 3 | Final Packet | | OK | 365 | 00:00:00.0... | 20-07-2022 2:00:45.88472... |
| | 18,977 | Master | 3 | Final Packet | Conn. | | 60 | 00:02:29.0... | 20-07-2022 2:03:14.94893... |
| | 18,986 | Slave | 3 | Final Packet | | OK | 65 | 00:00:00.0... | 20-07-2022 2:03:14.95456... |
| | 21,034 | Master | 3 | Final Packet | Conn. | | 69 | 00:00:08.9... | 20-07-2022 2:03:23.93157... |
| | 21,055 | Slave | 3 | Final Packet | | OK | 65 | 00:00:00.0... | 20-07-2022 2:03:23.96594... |
| | 21,093 | Master | 3 | Final Packet | Get | | 104 | 00:00:00.0... | 20-07-2022 2:03:24.00532... |
| | 21,109 | Master | 3 | Final Packet | Conn. | | 70 | 00:00:00.0... | 20-07-2022 2:03:24.01532... |
| | 21,120 | Slave | 3 | Final Packet | | Forbidden | 41 | 00:00:00.0... | 20-07-2022 2:03:24.04219... |
| | 21,122 | Slave | 3 | Final Packet | | OK | 64 | 00:00:00.0... | 20-07-2022 2:03:24.04344... |
| ▶ Uconnect system request for missed call list | 21,137 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:03:24.05407... |
| | 21,182 | Slave | 3 | Final Packet | | Continue | 63 | 00:00:00.0... | 20-07-2022 2:03:24.11844... |
| ▶ Compatible device respond with missed call list | 21,186 | Slave | 3 | Final Packet | | OK | 598 | 00:00:00.0... | 20-07-2022 2:03:24.12094... |
| | 21,203 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:03:24.20907... |
| | 21,216 | Slave | 3 | Final Packet | | Continue | 60 | 00:00:00.0... | 20-07-2022 2:03:24.25595... |
| | 21,218 | Slave | 3 | Final Packet | | OK | 338 | 00:00:00.0... | 20-07-2022 2:03:24.25720... |
| | 21,231 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:03:24.30532... |
| | 21,244 | Slave | 3 | Final Packet | | Continue | 60 | 00:00:00.0... | 20-07-2022 2:03:24.35220... |

Frame Display - Row 4_Apple iPhone SE 2020_Call cannot be seen in missed call list.cfa

File Edit View Format Filter Bookmarks Options Window Help
Find:
Summary: OBEX
Baseband with Auto-traverse
Unfiltered | Bookmarks | Info | Errors
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | SDP | RFCOMM | AVCTP | AVDTP | AVDTP Signaling | OBEX | Hands-Free | AVRCP | iAP (R25 - Unofficial) | iAP2 (R25 - Unofficial)
AVRCP Browsing | iAP1 General (R25 - Unofficial) | PBAP | Undecoded L2CAP Frame | WB Speech | Data

```
Frame 3,899: (Slave) Len=444
⊞ Baseband:
⊞ L2CAP:
⊟ OBEX:
   Role: Slave
   Address: 3
   Packet Status: Final Packet
   Response Code: Success
   Length: 410
   ⊟ End of Body
      Header Encoding: Byte Sequence
      Header ID: End of Body
      Length: 407
⊟ PBAP:
   Link: 2
   Role: Slave
   Address: 3
   ⊟ BEGIN:VCARD
      .VERSION:3.0.
      FN:Pooja Sharma.
      N:;Pooja Sharma.
      TEL:+91 98722 54060.
      UID:294fb.
      X-IRMC-CALL-DATETIME;MISSED:20220720T112120.
      END:VCARD.
   ⊟ BEGIN:VCARD
      .VERSION:3.0.
      FN:Pooja Sharma.
      N:;Pooja Sharma.
      TEL:+919872254060.
      UID:294fb.
      X-IRMC-CALL-DATETIME;MISSED:20220719T154700.
      END:VCARD.
   ⊟ BEGIN:VCARD
      .VERSION:3.0.
      FN:.
      N:.
      TEL:+917837111079.
      X-IRMC-CALL-DATETIME;MISSED:20220719T153612.
      END:VCARD.
```

| Bookmark | Frame# | Role | Addr. | Pkt Status | Opcode | Resp Code | Fram... | Delta | Timestamp |
|---|---|---|---|---|---|---|---|---|---|
| | 3,790 | Master | 3 | Final Packet | Conn. | | 69 | | 20-07-2022 2:00:45.30785... |
| | 3,809 | Slave | 3 | Final Packet | | OK | 65 | 00:00:00.0... | 20-07-2022 2:00:45.35472... |
| | 3,850 | Master | 3 | Final Packet | Conn. | | 70 | 00:00:00.0... | 20-07-2022 2:00:45.38160... |
| | 3,860 | Slave | 3 | Final Packet | | Forbidden | 41 | 00:00:00.0... | 20-07-2022 2:00:45.38847... |
| | 3,861 | Master | 3 | Final Packet | Get | | 104 | 00:00:00.0... | 20-07-2022 2:00:45.39910... |
| | 3,872 | Slave | 3 | Final Packet | | OK | 64 | 00:00:00.0... | 20-07-2022 2:00:45.42597... |
| ▶ Uconnect system request for missed call list | 3,882 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:00:45.43284... |
| | 3,895 | Slave | 3 | Final Packet | | Continue | 63 | 00:00:00.0... | 20-07-2022 2:00:45.46097... |
| ▶ Compatible device respond with missed call list | 3,899 | Slave | 3 | Final Packet | | OK | 444 | 00:00:00.0... | 20-07-2022 2:00:45.46347... |
| | 3,922 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:00:45.52909... |
| | 3,933 | Slave | 3 | Final Packet | | Continue | 60 | 00:00:00.0... | 20-07-2022 2:00:45.55597... |
| | 3,946 | Slave | 3 | Final Packet | | OK | 338 | 00:00:00.0... | 20-07-2022 2:00:45.56472... |
| | 3,957 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:00:45.61035... |
| | 3,968 | Slave | 3 | Final Packet | | Continue | 60 | 00:00:00.0... | 20-07-2022 2:00:45.63722... |
| | 3,970 | Slave | 3 | Final Packet | | OK | 40 | 00:00:00.0... | 20-07-2022 2:00:45.63847... |
| | 3,983 | Master | 3 | Final Packet | Get | | 112 | 00:00:00.0... | 20-07-2022 2:00:45.66910... |
| | 3,990 | Slave | 3 | Final Packet | | OK | 82 | 00:00:00.0... | 20-07-2022 2:00:45.67472... |
| | 4,011 | Master | 3 | Final Packet | Get | | 102 | 00:00:00.0... | 20-07-2022 2:00:45.70785... |
| | 4,046 | Slave | 3 | Final Packet | | OK | 82 | 00:00:00.1... | 20-07-2022 2:00:45.82222... |
| | 4,061 | Master | 3 | Final Packet | Get | | 117 | 00:00:00.0... | 20-07-2022 2:00:45.85535... |
| | 4,087 | Slave | 3 | Final Packet | | Continue | 78 | 00:00:00.0... | 20-07-2022 2:00:45.88347... |
| | 4,089 | Slave | 3 | Final Packet | | OK | 365 | 00:00:00.0... | 20-07-2022 2:00:45.88472... |
| | 18,977 | Master | 3 | Final Packet | Conn. | | 60 | 00:02:29.0... | 20-07-2022 2:03:14.94893... |
| | 18,986 | Slave | 3 | Final Packet | | OK | 65 | 00:00:00.0... | 20-07-2022 2:03:14.95456... |
| | 21,034 | Master | 3 | Final Packet | Conn. | | 69 | 00:00:08.9... | 20-07-2022 2:03:23.93157... |
| | 21,055 | Slave | 3 | Final Packet | | OK | 65 | 00:00:00.0... | 20-07-2022 2:03:23.96594... |
| | 21,093 | Master | 3 | Final Packet | Get | | 104 | 00:00:00.0... | 20-07-2022 2:03:24.00532... |
| | 21,109 | Master | 3 | Final Packet | Conn. | | 70 | 00:00:00.0... | 20-07-2022 2:03:24.01532... |
| | 21,120 | Slave | 3 | Final Packet | | Forbidden | 41 | 00:00:00.0... | 20-07-2022 2:03:24.04219... |
| | 21,122 | Slave | 3 | Final Packet | | OK | 64 | 00:00:00.0... | 20-07-2022 2:03:24.04344... |
| ▶ Uconnect system request for missed call list | 21,137 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:03:24.05407... |
| | 21,182 | Slave | 3 | Final Packet | | Continue | 63 | 00:00:00.0... | 20-07-2022 2:03:24.11844... |
| ▶ Compatible device respond with missed call list | 21,186 | Slave | 3 | Final Packet | | OK | 598 | 00:00:00.0... | 20-07-2022 2:03:24.12094... |
| | 21,203 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:03:24.20907... |
| | 21,216 | Slave | 3 | Final Packet | | Continue | 60 | 00:00:00.0... | 20-07-2022 2:03:24.25595... |
| | 21,218 | Slave | 3 | Final Packet | | OK | 338 | 00:00:00.0... | 20-07-2022 2:03:24.25720... |
| | 21,231 | Master | 3 | Final Packet | Get | | 107 | 00:00:00.0... | 20-07-2022 2:03:24.30532... |
| | 21,244 | Slave | 3 | Final Packet | | Continue | 60 | 00:00:00.0... | 20-07-2022 2:03:24.35220... |

**Figure 12.**OBEX (Missed Call history request Frames)

## 6. Discussion

We examine the stunning process of using this Bluetooth innovation to recall competent communication systems in this paper. It also covers other fundamental centers, such as Bluetooth structure data, applications, and security challenges. Needs Bluetooth drives and bets against them are eliminated.

Bluetooth security specialists should update security displays and client certificate structures for each new security breach when protecting device users' data becomes the standard. Bluetooth security specialists should offer these upgrades at an unspecified time. We shall investigate the height of endless redesigns and Bluetooth progress overhauls in the future.

## References

[1] Nateq Be-Nazir Ibn Minar and Mohammed Tarique, “Bluetooth Security Threats and Solution” A Survey. In International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[2] Dieter Gollmann., “Computer security”, 2nd Edition, paperback January 1,2007.

[3] Satwant Kaur First Lady of Emerging Technologies Silicon Valley, USA,2014.

[4] Tarun Kumar, ”Improving pairing mechanism in Bluetooth security” International Journal of Recent Trends in Engineering, Vol 2, No. 2, November 2009.

[5] Karen Scarfone and john Padgette, “Guide to Bluetooth Security”, paperback June 30,2012.
[6] Trishna Panse and Prashant Panse, “A Survey on Security Threats and Vulnerability attacks on Bluetooth Communication” ISSN: 0975-9646.
[7] Praveen kumar mishra, “Bluetooth Security Threats.” International Journal of Computer Science & Engineering Technology (IJCSET)
[8] Tzu-Chang Yeh, Jian-Ren Peng, Sheng-Shih Wang, and Jun-Ping Hsu, “Securing Bluetooth communication” International Journal of Network Security, Vol.14, No.4, PP.229-235, July 2012.