
Frontline Soderaを使った Bluetoothペアリング時間の 測定方法について

2018年11月27日

コーンズテクノロジー株式会社

目次

- はじめに
- Pageについて
- Connectionについて
- Pairingについて
- Bluetoothペアリング時間計測例

はじめに

- 本資料では、BTペアリング時間の測定方法として、キャプチャーデータのどこからどこまでを確認すればよいかという観点で、キャプチャーデータ上で「Page」「Connection」「Pairing」の各処理をBluetoothコア仕様を元に確認する方法の例を記載している。
- また、ペアリング時間計測の例として、PageからPairing完了までと、Pairing処理のみの場合の見方を記載している。

PAGEについて

Pageについて

- Page(Bluetooth機器の呼び出し)については、Bluetooth SIG発行のコア仕様に処理ステップが記載されており、キャプチャーデータ上で該当箇所を見つけることで処理を確認できる。

記載箇所: Table 8.3: Initial messaging during start-up (BLUETOOTH SPECIFICATION Version 5.0 | Vol 2, Part B).

Step	Message	Packet Type	Direction	Hopping Sequence	Access Code and Clock
1	Page	ID	Master to slave	Page	Slave
2	First slave page response	ID	Slave to master	Page response	Slave
3	Master page response	FHS	Master to slave	Page	Slave
4	Second slave page response	ID	Slave to master	Page response	Slave
5	1st packet master	POLL	Master to slave	Channel	
6	1st packet slave	Any type	Slave to master	Channel	

FHS packets are used to confirm the location in the capture data.

Table 8.3: Initial messaging during start-up

Frame DisplayでFHSパケットを確認

The screenshot shows the Frame Display application interface. The title bar reads "Frame Display". The menu bar includes "File", "Edit", "View", "Format", "Live", "Filter", "Bookmarks", "Options", "Window", and "Help". The toolbar contains various icons for file operations and analysis. The main window is divided into several panes:

- Left Pane:** Shows details for "Frame 10,321: (Master) Len=44". Under "Baseband:", it lists "RSSI: -30.500 dBm (strong)", "Link: 2", "Role: Master (0x14-ab-c5-d8-01-34)", "Channel: 43 - 2445 MHz", "Packet Status: OK", and "Clock: 0x02cb9980". Under "Bluetooth FHS:", it lists "TYPE: FHS" (highlighted with a red box), "Payload Data", "LT_ADDR", "SEQN:", "ARQN:", "L2CAP", "Logical", "Decrypt", "Payload", "PreConnect", "Packet", "Bluetooth FHS", "Link: 2", "Parity: 0x34ce744ef", "LAP: 0x00d80134", "EIR: 0x1", and "Undefined: 0x0". A callout bubble points to "TYPE: FHS" with the text "パケットタイプは FHS".
- Top Right Pane:** Shows a tabbed interface with "Bluetooth FHS" selected (highlighted with a red box). Other tabs include "Baseband", "Extended Inquiry Response", "LMP", "PreConnection-FHS", "SDP", "RFCOMM", "OBEX", and "OPP". A callout bubble points to this tab with the text "このタブにあるパケットは FHSパケット".
- Bottom Pane:** A table listing frames with columns: "B...", "Frame#", "EIR", "LAP", "SP", "SM", "NAP", "Address", "Clock", and "SR". The selected frame 10,321 is highlighted in blue. Below the table is a hex dump of the packet data.

At the bottom of the window, it displays "Total Frames: 41,869", "Frames Filtered In: 12", and "Frame #s Selected: 10,321; (1 total)". The status bar shows "For Help Press F1" and "Filtering... 100%".

COBNER

Message Sequence ChartでPage処理に該当するか確認

Message Sequence Chart

The screenshot shows a Message Sequence Chart (MSC) tool interface. The main window displays a sequence of messages between two lifelines: BB M and BB S. The messages are numbered 1 through 6, corresponding to the table on the left. A red dashed box highlights the sequence of messages in the chart. The 'BB' layer is selected in the top menu.

Step	Message	Packet Type
1	Page	ID
2	First slave page response	ID
3	Master page response	FHS
4	Second slave page response	ID
5	1st packet master	POLL
6	1st packet slave	Any type

The MSC diagram shows the following sequence of messages:

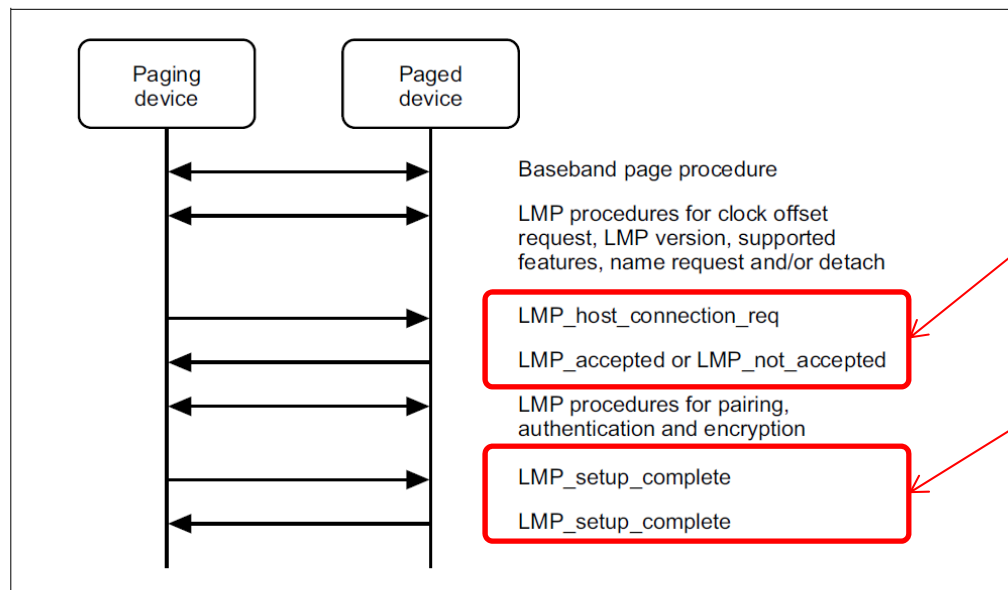
- Step 1: BB M sends ID to BB S.
- Step 2: BB S sends ID to BB M.
- Step 3: BB M sends FHS (LT_ADDR=0, SEQN=0, ARQN=0) to BB S.
- Step 4: BB S sends ID to BB M.
- Step 5: BB M sends POLL (LT_ADDR=1, SEQN=1, ARQN=0) to BB S.
- Step 6: BB S sends NULL (LT_ADDR=1, SEQN=1, ARQN=0) to BB M.

CONNECTIONについて

- Connection(ページ処理後に行われる無線接続)は、Bluetooth SIG発行のコア仕様に処理ステップが記載されており、キャプチャーデータ上で該当箇所を見つけることで処理を確認できる。
 - 記載箇所:4.1.1 Connection Establishment (BLUETOOTH SPECIFICATION Version 5.0 | Vol 2, Part C)

4.1.1 Connection Establishment

After the paging procedure, LMP procedures for clock offset request, LMP version, supported features, name request and detach may then be initiated.

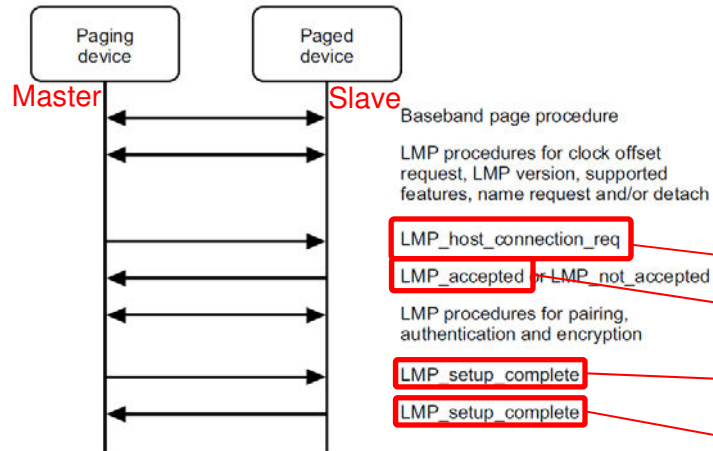


Connectionのうち、左記パケットを確認する

Figure 4.1: Connection establishment

Frame Displayで該当部分の確認

コア仕様



Frame Display

The screenshot shows the Frame Display tool interface for a Bluetooth LMP transfer. The protocol tree on the left shows the following structure:

- Frame 10,443: (Master) Len=27
 - Baseband:
 - Role: Master [0x14-ab-c5-d8-01-34]
 - Channel: 44 - 2446 MHz
 - Packet Status: OK
 - TYPE: DM1
 - Payload Data Rate: 1 Mbps
 - LT_ADDR: 1
 - SEQN: 1
 - ARQN: 0
 - L2CAP Flow: N/A [1]
 - Logical Link ID: LMP
 - Decrypted by Bluetooth ComProbe: No
 - Payload Length: 1
 - LMP:
 - Link: 2
 - Role: Master
 - Address: 1
 - Opcode: LMP_setup_complete
 - Transaction ID: Initiated by master

The frame list on the right shows the following frames:

B	Frame#	Initiated by	Opcode	Original Opcode	L1
	10,355	master	features_req_ext		1
	10,358	master	features_res_ext		1
	10,360	master	host_connection_req		1
	10,363	slave	version_req		1
	10,365	slave	version_res		1
	10,376	master	accepted	host_connection_req	1
	10,378	slave	setup_complete		1
	10,381	master	SET_AFH		1
	10,433	master	channel_classification_req		1
	10,436	slave	channel_classification		1
	10,438	master	packet_type_table_req		1
	10,441	master	accepted_ext	packet_type_table_req	1
	10,443	master	setup_complete		1
	10,446	slave	timing_accuracy_req		1
	10,447	master	timing_accuracy_req		1
	10,448	slave	max_slot		1
	10,457	master	max_slot_req		1

Red boxes in the image highlight the following frames and fields:

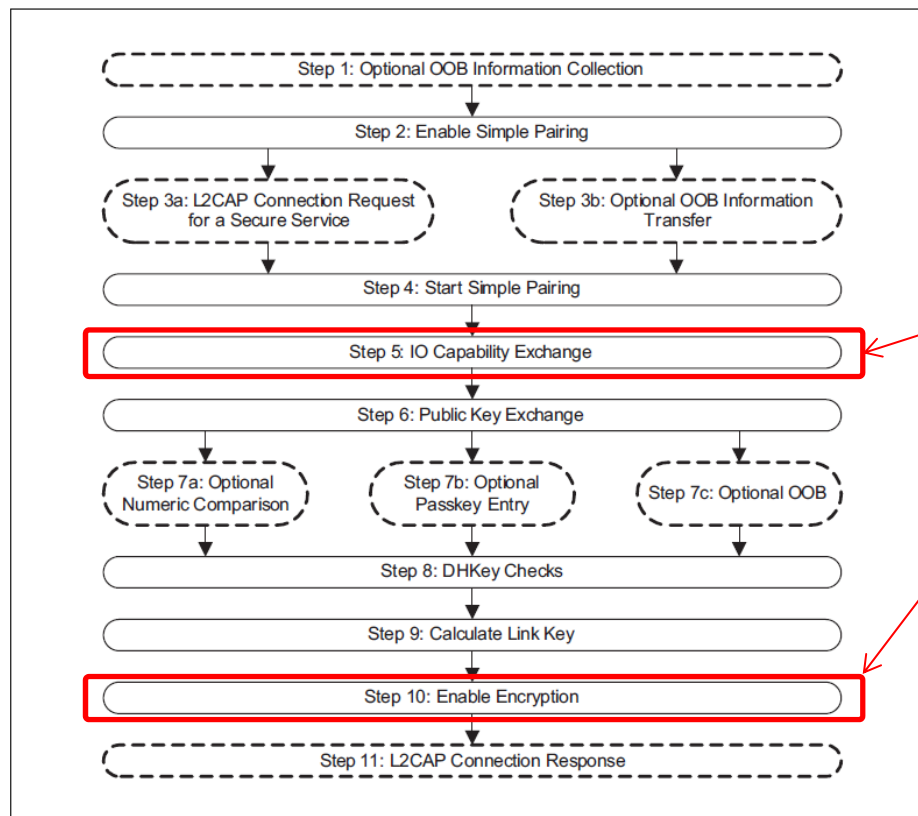
- Frame 10,360: master, host_connection_req
- Frame 10,376: master, accepted, host_connection_req
- Frame 10,378: slave, setup_complete
- Frame 10,443: master, setup_complete

The bottom status bar shows: Total Frames: 41,869 | Frames Filtered In: 183 | Frame #s Selected: (2 total) 10,360;10,443; Delta: 00:00:00.215002

PAIRINGについて

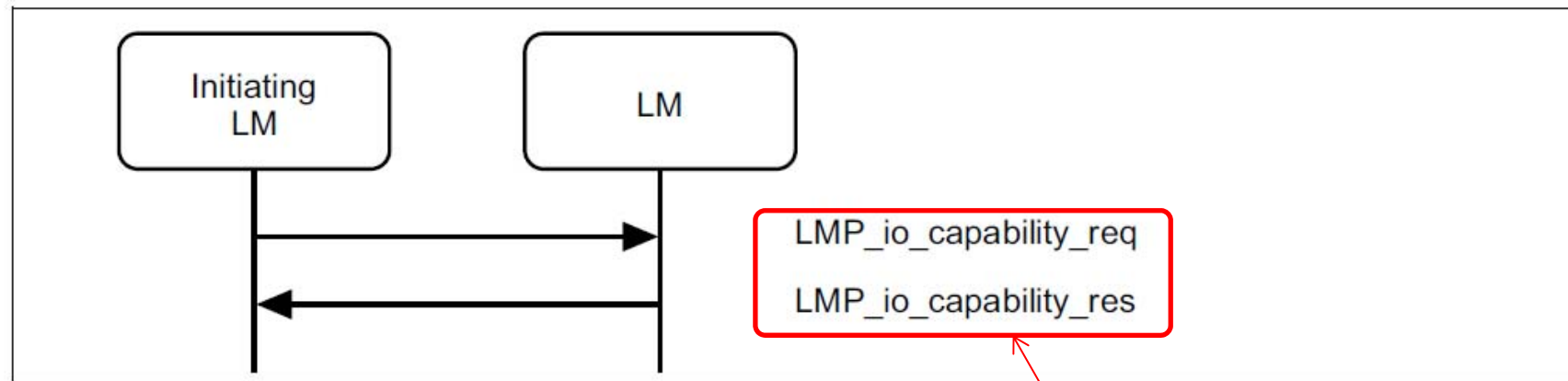
Pairingについて

- Pairingについては、Bluetooth SIG発行のコア仕様に処理ステップが記載されており、キャプチャーデータ上で該当箇所を見つけることで処理を確認できる。
 - 記載箇所: 4.2 SIMPLE PAIRING MESSAGE SEQUENCE CHARTS (BLUETOOTH SPECIFICATION Version 5.0 | Vol 2, Part F)



Step 5: IO Capability Exchange
Step 10: Enable Encryption
に着目する

Pairing - IO Capability Exchange (コア仕様より抜粋)



Sequence 56: IO Capability Exchange

IO Capability Exchange
の上記2つのパケットを確認

Frame Displayから該当部分の確認

Frame Display

Message Sequence Chart

Frame#	Initiated by	Opcode	Original Opcode
11,453	slave	power_control_res	
11,826	master	power_control_req	
11,869	master	power_control_res	
11,949	master	IO_Capability_req	
12,063	master	IO_Capability_res	
12,335	master	encapsulated_header	
12,336	master	accepted	encapsulated_header
12,371	master	encapsulated_payload	

Frame#	Time	Message	Direction	Notes
11,826	19:55:16.676491	LMP_Power_Control_Req	M → S	(Tran. ID=Initiated by master)
11,869	19:55:16.707119	LMP_Power_Control_Res	S → M	(Tran. ID=Initiated by master)
11,949	19:55:16.795242	LMP_IO_Capability_req	M → S	IO capability request (Tran. ID=Initiated by master)
12,063	19:55:16.908370	LMP_IO_Capability_res	S → M	IO capability response (Tran. ID=Initiated by master)
12,335	19:55:17.145245	LMP_encapsulated_header	M → S	Request to send encapsulated (Tran. ID=Initiated by master)
12,371	19:55:17.152455	LMP_accepted	S → M	Request to send encapsulated
12,372	19:55:17.152455	LMP_encapsulated_payload	M → S	Public key (Tran. ID=Initiated by master)
12,373	19:55:17.152455	LMP_accepted	S → M	Public key accepted (Tran. ID=Initiated by master, Original Opcode=...)
12,374	19:55:17.152455	LMP_encapsulated_payload	M → S	Public key (Tran. ID=Initiated by master)
12,375	19:55:17.152455	LMP_accepted	S → M	Public key accepted (Tran. ID=Initiated by master, Original Opcode=...)

11,949	master	IO_Capability_req
12,063	master	IO_Capability_res

Pairing - Enable Encryption (コア仕様より抜粋)



Step 8: Once the pairing or authentication procedure is successful, the encryption procedure may be started. This MSC only shows the set up of an encrypted point-to-point connection. (See [Figure 3.12.](#))

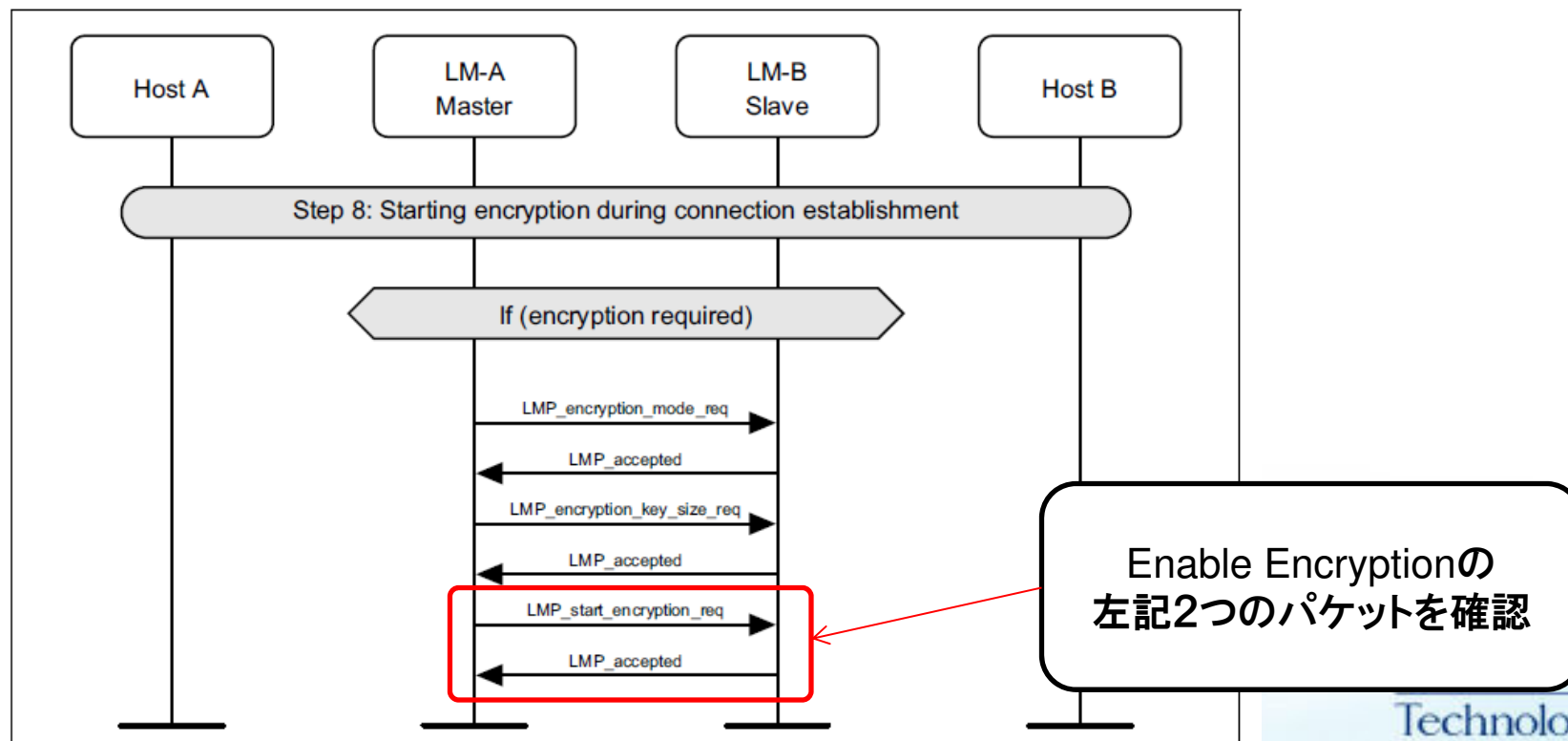


Figure 3.12: Starting encryption during connection setup

Frame Displayから該当部分の確認

Frame Display

Message Sequence Chart

Frame 17,776: (Slave) Len=28

Baseband:

- RSSI: -57.125 dBm (weak)
- Link: 2
- Role: Slave (0x64-bc-0c-fe-ac-a7)
- Channel: 53 - 2455 MHz
- Clock: 0x02cc17ea
- Packet Status: OK
- FLOW: Go
- TYPE: DM1
- Payload Data Rate: 1 Mbps
- LT_ADDR: 1
- SEQN: 0
- ARQN: 0
- L2CAP Flow: N/A [1]
- Logical Link ID: LMP
- Decrypted by Bluetooth ComProbe: Yes
- Payload Length: 2

LMP:

- Link: 2
- Role: Slave
- Address: 1
- Opcode: LMP_accepted
- Transaction ID: Initiated by master
- Original Opcode: LMP_start_encryption_req

B	Frame#	Initiated by	Opcode	Original Opcode	LT
	17,631	slave	preferred_rate		1
	17,677	master	sres		1
	17,692	master	encrypt_mode_req		1
	17,693	slave	name_req		1
	17,695	master	accepted	encrypt_mode_req	1
	17,696	slave	name_res		1
	17,698	master	encrypt_key_size_req		1
	17,717	master	accepted	encrypt_key_size_req	1
	17,755	master	start_encrypt_req		1
	17,776	master	accepted	start_encrypt_req	1
	19,123	slave	preferred_rate		1
	19,581	master	SET_AFH		1
	21,305	master	SET_AFH		1
	22,154	slave	channel_classification		1
	22,171	master	SET_AFH		1
	23,143	slave	channel_classification		1
	23,147	master	SET_AFH		1

```

BINARY
00011010 00000011 00110101 11001111 11001100
00000010 10011001 00011100 00001111 10101100
11111110 00001100 10111100 00001111 00110111
11111110 11111111 11111111 11111111 11111111
00000010 00000000 00000110 00000000 00000000
    
```

Frame#	Time	Message	Direction
17,692	19:55:25.057818	LMP_encryption_mode_req (Tran. ID=Initiated by master)	→
17,693	19:55:25.058444	LMP_name_req (Tran. ID=Initiated by slave)	→
17,695	19:55:25.059696	LMP_accepted (Tran. ID=Initiated by master, Original Opcode=LMP_...)	←
17,696	19:55:25.060318	LMP_name_res (Tran. ID=Initiated by slave)	→
17,698	19:55:25.061568	LMP_encryption_key_size_req (Tran. ID=Initiated by master)	→
17,717	19:55:25.107196	LMP_accepted (Tran. ID=Initiated by master, Original Opcode=LMP_...)	←
17,755	19:55:25.157819	LMP_start_encryption_req (Tran. ID=Initiated by master)	→
17,776	19:55:25.207197	LMP_accepted (Tran. ID=Initiated by master, Original Opcode=LMP_s...)	←
17,776	19:55:25.207197	LMP_preferred_rate	←

Encryption mode request → LMP_M → LMP_S
Encryption key size request → LMP_M → LMP_S
Start → LMP_M → LMP_S
Baseband connection encryption started

17,755	master	start_encrypt_req
17,776	master	accepted

BLUETOOTHペアリング時間計測例

Bluetoothペアリング時間計測例1：PageからPairing完了 (1/3)

- FHS packets are used as capture data for Page processing. Select the first ID packet and set a bookmark.

The screenshot shows the Wireshark interface with a packet capture of Bluetooth FHS (Frequency Hopping Spread) packets. The main window displays a list of packets with columns for Frame#, CLK, Chan, Role, LT, Pac, DS, TYPE, LLID, and P. Packet 10,319 is highlighted in blue. A red box highlights the 'Bookmark' icon in the toolbar. A dialog box titled 'Add Bookmark' is open, showing 'Bookmark for frame #10319' and an 'OK' button. Three callout boxes provide instructions: ① Select the corresponding packet, ② Click the bookmark, and ③ Record the bookmark name and click OK.

① 該当パケットを選択

② Bookmarkをクリック

③ Bookmark名など記載してOKをクリック

B...	Frame#	CLK	Chan	Role	LT...	Pac...	DS	TYPE	LLID	P...
	10,316		62					ID		
	10,317		68					ID		
	10,318		60					ID		
	10,319		43					ID		
	10,320		45					ID		
	10,321	0x02cb9980	43	M...	0	OK	N	FHS	N/...	S
	10,322		28					ID		
	10,323	0x02cb9984	46	M...	1	OK	N	POLL	N/...	C

Bluetoothペアリング時間計測例1：PageからPairing完了 (2/3)

- LMP_start_encryptionに対する応答のLMP_acceptedをキャプチャーデータで選択してBookmarkをつける

The screenshot shows the Wireshark interface with a Bluetooth L2CAP capture. The main pane displays a list of packets. Packet 17,776 is highlighted in blue and has a red box around it. A red box also highlights the 'Bookmarks' icon in the toolbar. A dialog box titled 'Add Bookmark' is open, showing 'Bookmark for frame #17776' and an 'OK' button highlighted with a red box. Three callout boxes provide instructions: ① 該当パケットを選択 (Select the corresponding packet), ② Bookmarkをクリック (Click Bookmark), and ③ Bookmark名など記載してOKをクリック (Enter bookmark name etc. and click OK).

Bookmark	Frame#	Initiated by	Opcode	Timestamp
	17,627	master	sres	
	17,629	master	au_rand	
	17,631	slave	preferred_rate	17,696 19:55:25.060318
	17,677	master	sres	
	17,692	master	encrypt_mode_req	
	17,693	slave	name_req	
	17,695	master	accepted	17,698 19:55:25.061568
	17,696	slave	name_res	
	17,698	master	encrypt_key_size_req	
	17,717	master	accepted	17,717 19:55:25.107196
	17,755	master	start_encrypt_req	
	17,776	master	accepted	17,755 19:55:25.157819
	19,123	slave	preferred_rate	

Add Bookmark dialog box content:

Bookmark for frame #17776

EndPoint

OK

Bluetoothペアリング時間計測例1：PageからPairing完了 (3/3)

- Bookmarkタブを開き、先ほどBookmarkした2つのパケットを選択すると選択パケット間の処理時間が表示される。

該当パケットを選択する

Bookmark	Frame#	Initiated by	Opcode	Original Opcode
Start-Point	10,319			
End-Point	17,776	master	accepted	start_encrypt_req

選択パケット間の処理時間が表示される
(PageからPairing完了までの処理時間)

Delta: 00:00:10.114158

Bluetoothペアリング時間計測例2: Pairingのみ (1/3)

- LMP_IO_Capability_reqをキャプチャーデータで選択してBookmarkをつける

The screenshot shows the Wireshark interface with a Bluetooth capture. The main pane displays a list of packets, with frame 11,949 (LMP_IO_Capability_req) highlighted in red. A callout box labeled '①該当パケットを選択' points to this frame. The toolbar has a 'Bookmark' icon highlighted with a red box, and a callout box labeled '②Bookmarkをクリック' points to it. An 'Add Bookmark' dialog box is open, showing 'Bookmark for frame #11949' and a 'Start-Point' field. The 'OK' button in the dialog is highlighted with a red box, and a callout box labeled '③Bookmark名など記載してOKをクリック' points to it.

①該当パケットを選択

②Bookmarkをクリック

③Bookmark名など記載してOKをクリック

Bookmark	Frame#	Initiated by	Opcode	Original Opcode
	11,453	slave	power_control_res	
	11,826	master	power_control_req	
	11,869	master	power_control_req	
	11,949	master	IO_Capability_req	
	12,063	master	IO_Capability_res	
	12,335	master	encapsulated_header	
	12,336	master	accepted	encapsulated
	12,371	master	encapsulated_payload	

Bluetoothペアリング時間計測例2: Pairingのみ (2/3)

- LMP_start_encryptionに対する応答のLMP_acceptedをキャプチャーデータで選択してBookmarkをつける

The screenshot shows the Wireshark interface with a Bluetooth L2CAP capture. The main pane displays a list of packets. Packet 17,776 is highlighted in blue and has a red box around it. A callout bubble labeled '①該当パケットを選択' points to this packet. The packet details pane shows the LMP_accepted structure. A toolbar icon for adding a bookmark is highlighted with a red box and a callout bubble labeled '②Bookmarkをクリック'. An 'Add Bookmark' dialog box is open, showing 'Bookmark for frame #17776' and an 'EndPoint' field. The 'OK' button in the dialog is highlighted with a red box and a callout bubble labeled '③Bookmark名など記載してOKをクリック'.

Bookmark	Frame#	Initiated by	Opcode	Timestamp
	17,627	master	sres	
	17,629	master	au_rand	
	17,631	slave	preferred_rate	17,696 19:55:25.060318
	17,677	master	sres	
	17,692	master	encrypt_mode_req	
	17,693	slave	name_req	
	17,695	master	accepted	17,698 19:55:25.061568
	17,696	slave	name_res	
	17,698	master	encrypt_key_size_req	
	17,717	master	accepted	17,717 19:55:25.107196
	17,755	master	start_encrypt_req	
	17,776	master	accepted	17,755 19:55:25.157819
	19,123	slave	preferred_rate	

Add Bookmark dialog box content:

Bookmark for frame #17776

EndPoint

OK

Cancel

Bluetoothペアリング時間計測例2: Pairingのみ (3/3)

- Bookmarkタブを開き、先ほどBookmarkした2つのパケットを選択すると選択パケット間の処理時間が表示される。

該当パケットを選択する

Bookmark	Frame#	Initiated by	Opcode	Original Opcode
Start-Point	11,949	master	IO_Capability_req	
End-Point	17,776	master	accepted	start_encrypt_re

選択パケット間の処理時間が表示される (Pairingのみの処理時間)

Delta: 00:00:08.411955