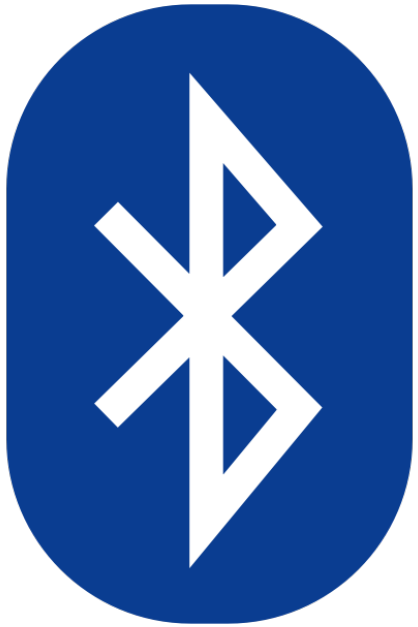
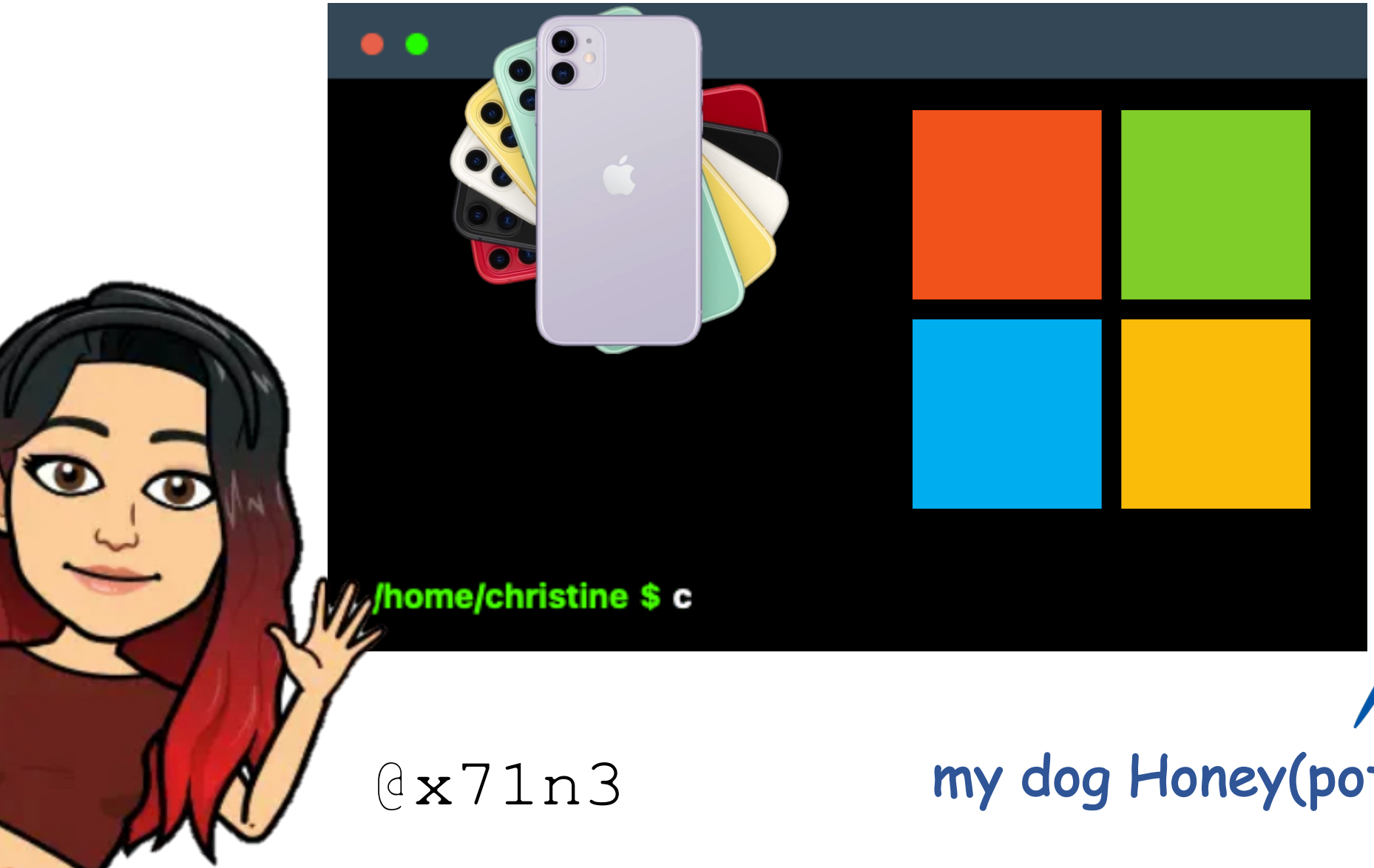
Handoff All Your Privacy(Again)

By Christine Fossaceca

PLEASE TURN OFF
YOUR BLUETOOTH



$whoami

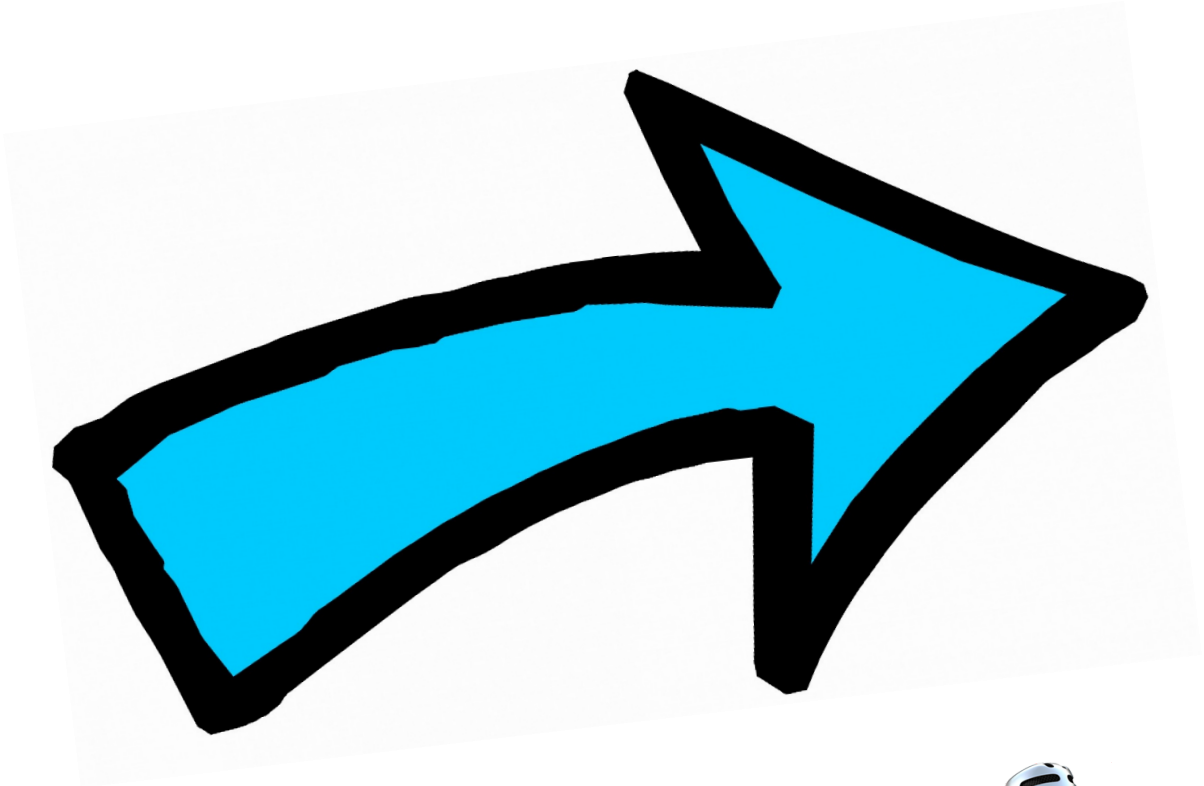


her hax
PODCAST

@x71n3

my dog Honey(pot)

STREAM SEASON 2 NOW!



@herhaxpodcast

her hax
PODCAST

Agenda

- What is the Continuity Protocol?
- How to Capture Continuity Data
- Packet Breakdown
- ✨Live DEMO!✨
- FindMy Protocol + Airtag Packets
- Airtag Encryption

Continuity Protocol Explained

It's not a bug, it's a feature!

- "Continuity" allows for information sharing and "seamless" experience" across Apple products and peripherals
    - Examples: Resume browsing from iPhone to MacBook, Universal Clipboard, Instant Hotspot, WiFi Password

- Powered via a combination of Wi-Fi and Bluetooth LE

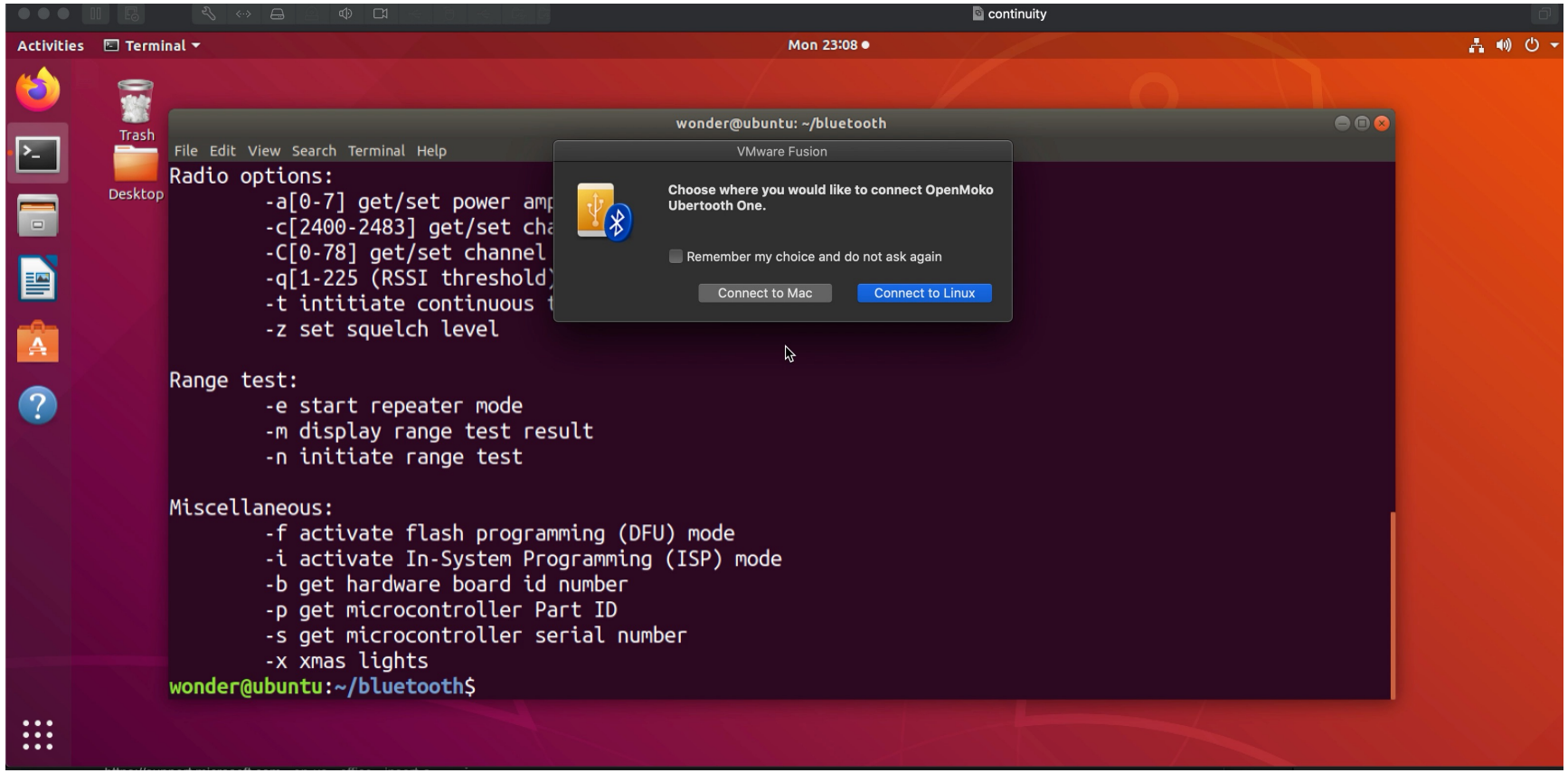
furiousMAC

- Proprietary! But we have reverse engineered this protocol and disclosed to Apple where Continuity exposes sensitive information or is poorly implemented**. Shmoocon 2020. Objective By the Sea 2022. Jailbreak Security Summit 2022.**

- Past @furiousmac Papers: **Handoff All Your Privacy – A Review of Apple's Bluetooth Low Energy Continuity Protocol**; **Who Tracks the Trackers? Circumventing Apple's Anti-Tracking Alerts in the Find My Network**;
- Other research: Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols; TU Darmstadt (multiple works) such as Open Haystack and AirGuard

So you might be wondering…

- What types of information are being sent in the clear?

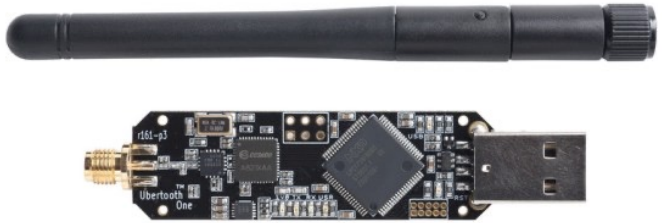


- And how are you capturing this?

How to Capture Continuity Data

- Bluetooth Hardware Dongle
  - Ubertooth or NRF Dongle

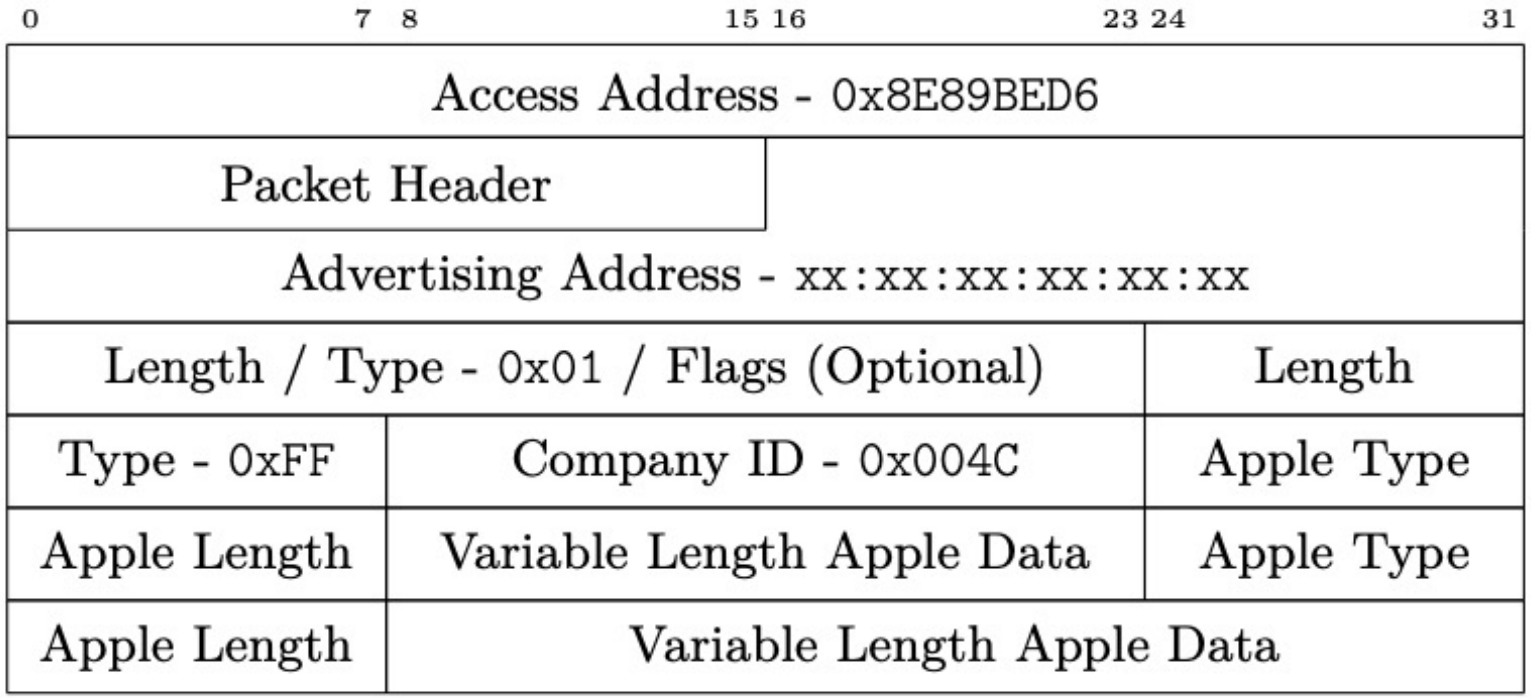
- Wireshark (compiled from source)
- furiousMAC custom dissector!
  - https://github.com/furiousMAC/continuity



- Check out our repository with build instructions!

Continuity Protocol Explained

It's not a bug, it's a feature!



Apple BLE Frame Format

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

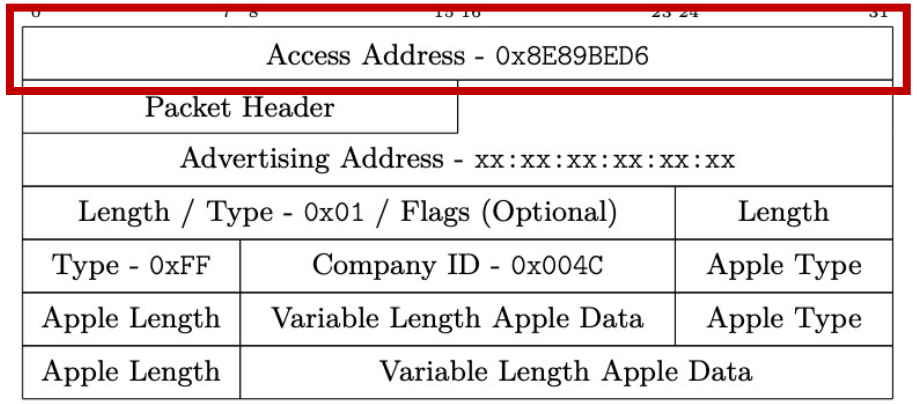
```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  22 68 06 08 e4 de 42 00  d6 be 89 8e 42 0e 17 df   "h....B. ....B...
0020  c8 98 b6 c2 07 ff 4c 00  12 02 00 00 90 88 04      ......L. .......
```

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  f5 09 17 08 f2 e0 95 00  d6 be 89 8e 00 14 bc 7b   ........ .......{
0020  75 da 7d 14 02 01 06 0a  ff 4c 00 10 05 06 1c e7   u.}..... .L......
0030  52 b4 a7 aa de                                     R....
```

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  aa 94 bd 07 f1 de 77 00  d6 be 89 8e 40 1d 8b 6f   ......w. ....@..o
0020  e4 9d 7e 60 02 01 06 13  ff 4c 00 0c 0e 00 e3 0e   ..~`.... .L......
0030  96 85 71 c6 dd aa 08 5c  b3 1e d7 d6 93 0d         ..q....\ ......
```

Continuity Protocol Explained

It's not a bug, it's a feature!



Access Address - 0x8E89BED6		
Packet Header		
Advertising Address - xx:xx:xx:xx:xx:xx		
Length / Type - 0x01 / Flags (Optional)		Length
Type - 0xFF	Company ID - 0x004C	Apple Type
Apple Length	Variable Length Apple Data	Apple Type
Apple Length	Variable Length Apple Data	

Apple BLE Frame Format

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  22 68 06 08 e4 de 42 00  d6 be 89 8e 42 0e 17 df   "h....B. ....B...
0020  c8 98 b6 c2 07 ff 4c 00  12 02 00 00 90 88 04      ......L. .......
```

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  f5 09 17 08 f2 e0 95 00  d6 be 89 8e 00 14 bc 7b   ........ .......{
0020  75 da 7d 14 02 01 06 0a  ff 4c 00 10 05 06 1c e7   u.}..... .L......
0030  52 b4 a7 aa de                                     R....
```

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  aa 94 bd 07 f1 de 77 00  d6 be 89 8e 40 1d 8b 6f   ......w. ....@..o
0020  e4 9d 7e 60 02 01 06 13  ff 4c 00 0c 0e 00 e3 0e   ..~`.... .L......
0030  96 85 71 c6 dd aa 08 5c  b3 1e d7 d6 93 0d         ..q....\ ......
```

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

The access address is at a 24 byte offset

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  22 68 06 08 e4 de 42 00  d6 be 89 8e 42 0e 17 df   "h....B. ....B...
0020  c8 98 b6 c2 07 ff 4c 00  12 02 00 00 90 88 04      ......L. .......
```

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  f5 09 17 08 f2 e0 95 00  d6 be 89 8e 00 14 bc 7b   ........ .......{
0020  75 da 7d 14 02 01 06 0a  ff 4c 00 10 05 06 1c e7   u.}..... .L......
0030  52 b4 a7 aa de                                     R....
```

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  aa 94 bd 07 f1 de 77 00  d6 be 89 8e 40 1d 8b 6f   ......w. ....@..o
0020  e4 9d 7e 60 02 01 06 13  ff 4c 00 0c 0e 00 e3 0e   ..~`.... .L......
0030  96 85 71 c6 dd aa 08 5c  b3 1e d7 d6 93 0d         ..q....\ ......
```

Continuity Protocol Explained

It's not a bug, it's a feature!

Access Address - 0x8E89BED6		
Packet Header		
Advertising Address - xx:xx:xx:xx:xx:xx		
Length / Type - 0x01 / Flags (Optional)		Length
Type - 0xFF	Company ID - 0x004C	Apple Type
Apple Length	Variable Length Apple Data	Apple Type
Apple Length	Variable Length Apple Data	

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted] d6 be 89 8e 42 0e 17 df          "h····B· ····B···
0020 c8 98 b6 c2 07 ff 4c 00  12 02 00 00 90 88 04   ·····L· ·······
```

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted] d6 be 89 8e 00 14 bc 7b          ........ .......{
0020 75 da 7d 14 02 01 06 0a  ff 4c 00 10 05 06 1c e7   u·}····· ·L·····
0030 52 b4 a7 aa de                              R····
```

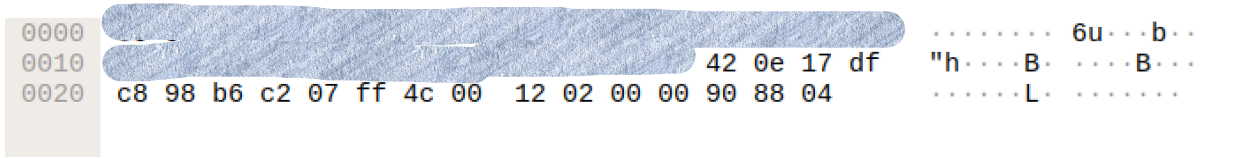
```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted] d6 be 89 8e 40 1d 8b 6f          ·····w·· ····@··o
0020 e4 9d 7e 60 02 01 06 13  ff 4c 00 0c 0e 00 e3 0e   ··~`···· ·L·····
0030 96 85 71 c6 dd aa 08 5c  b3 1e d7 d6 93 0d         ··q····\ ·····
```

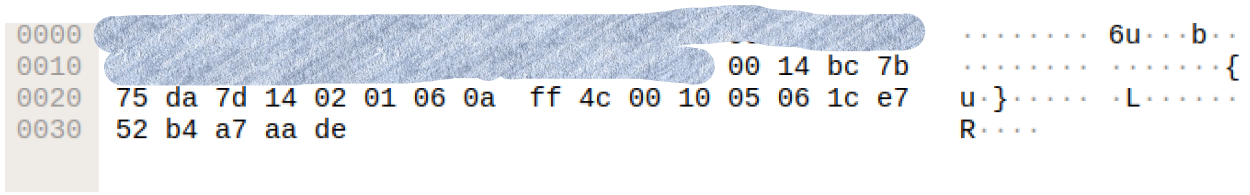
Continuity Protocol Explained

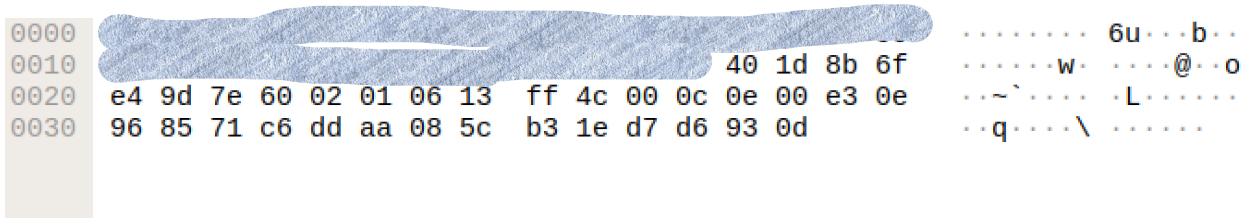
It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format





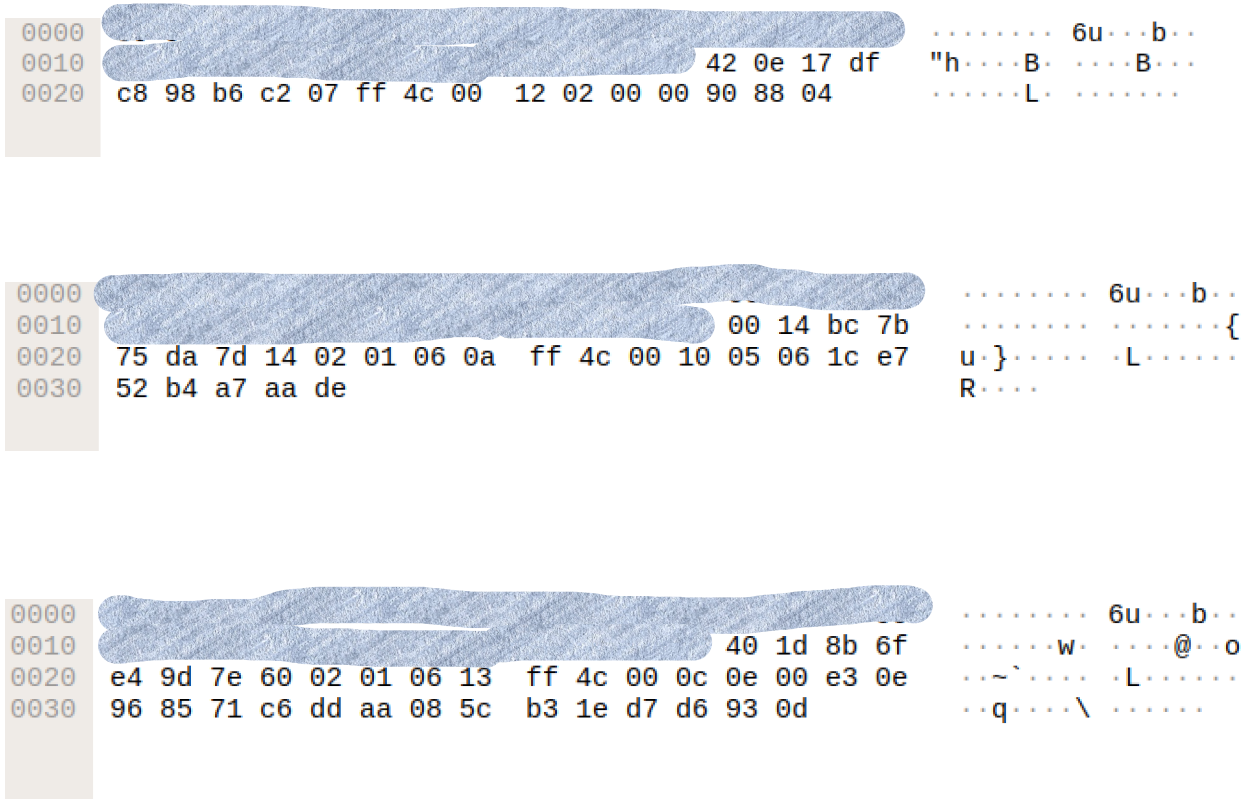


Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format



Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted]                 42 0e 17 df      "h····B· ····B···
0020 c8 98 b6 c2 07 ff 4c 00  12 02 00 00 90 88 04      ·····L· ·······
```

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted]                 00 14 bc 7b      ........ .......{
0020 75 da 7d 14 02 01 06 0a  ff 4c 00 10 05 06 1c e7   u·}····· ·L·····
0030 52 b4 a7 aa de                              R····
```

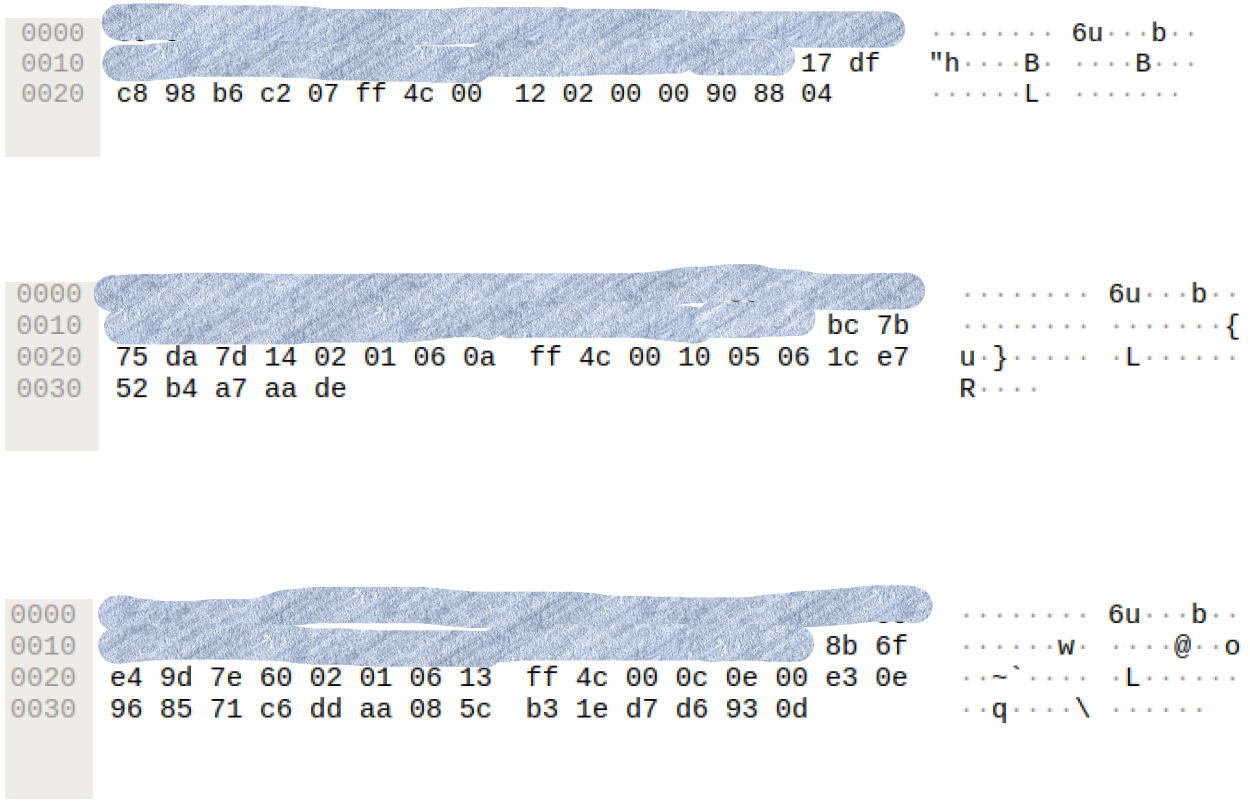
```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted]                 40 1d 8b 6f      ·····w·· ····@··o
0020 e4 9d 7e 60 02 01 06 13  ff 4c 00 0c 0e 00 e3 0e   ··~`···· ·L·····
0030 96 85 71 c6 dd aa 08 5c  b3 1e d7 d6 93 0d         ··q····\ ·····
```

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format

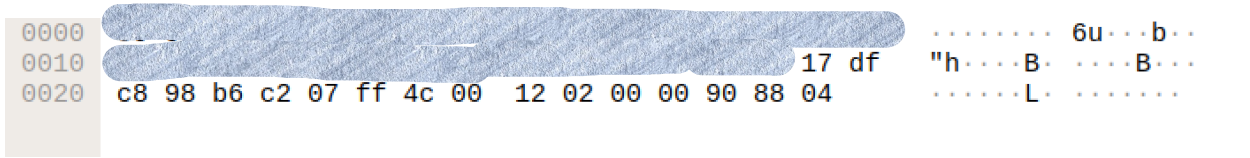


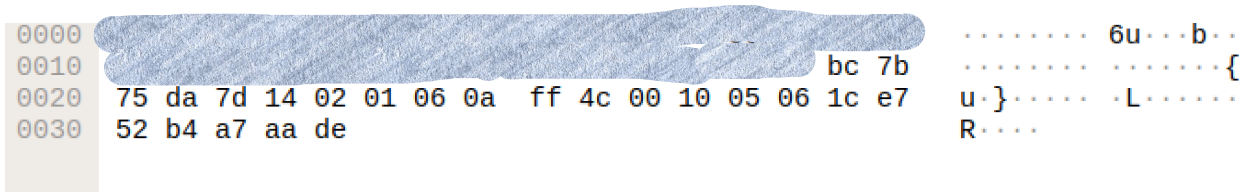
Continuity Protocol Explained

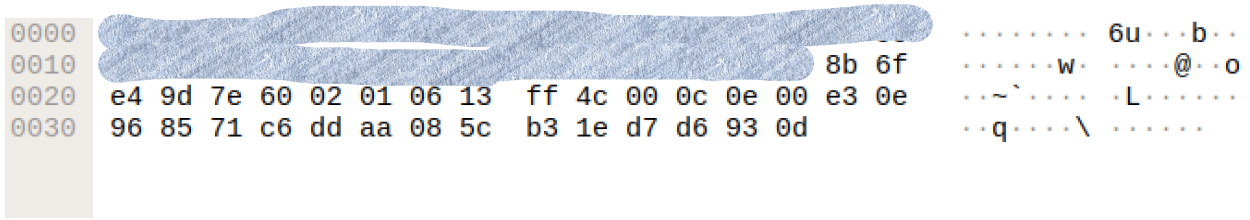
It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format





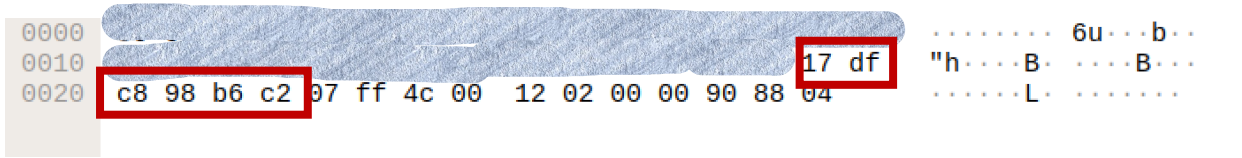


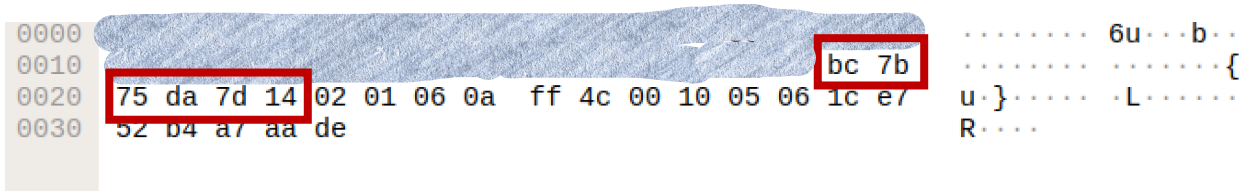
Continuity Protocol Explained

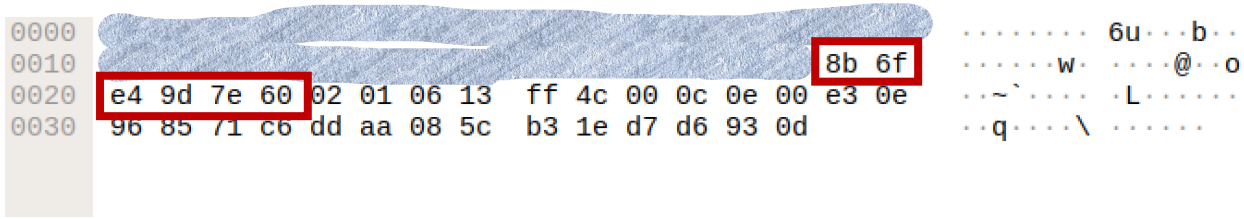
It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format





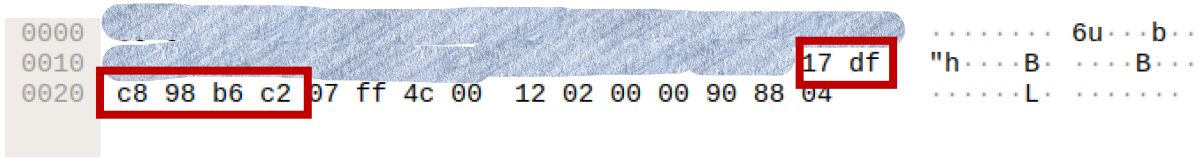


Continuity Protocol Explained

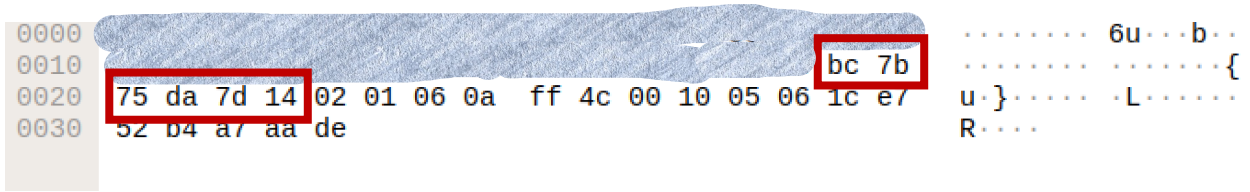
It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

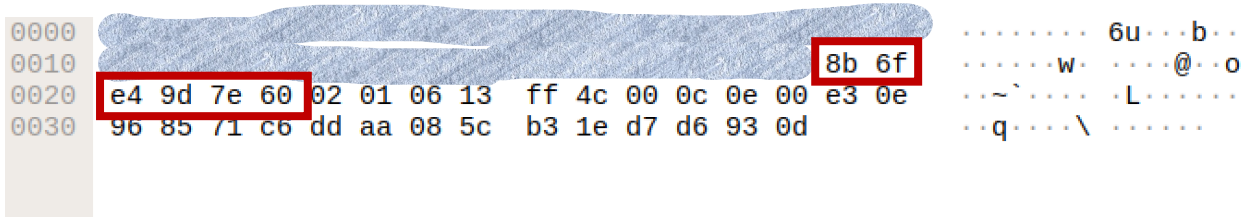
Apple BLE Frame Format



c2:b6:98:c8:df:17



14:7d:da:75:7b:bc



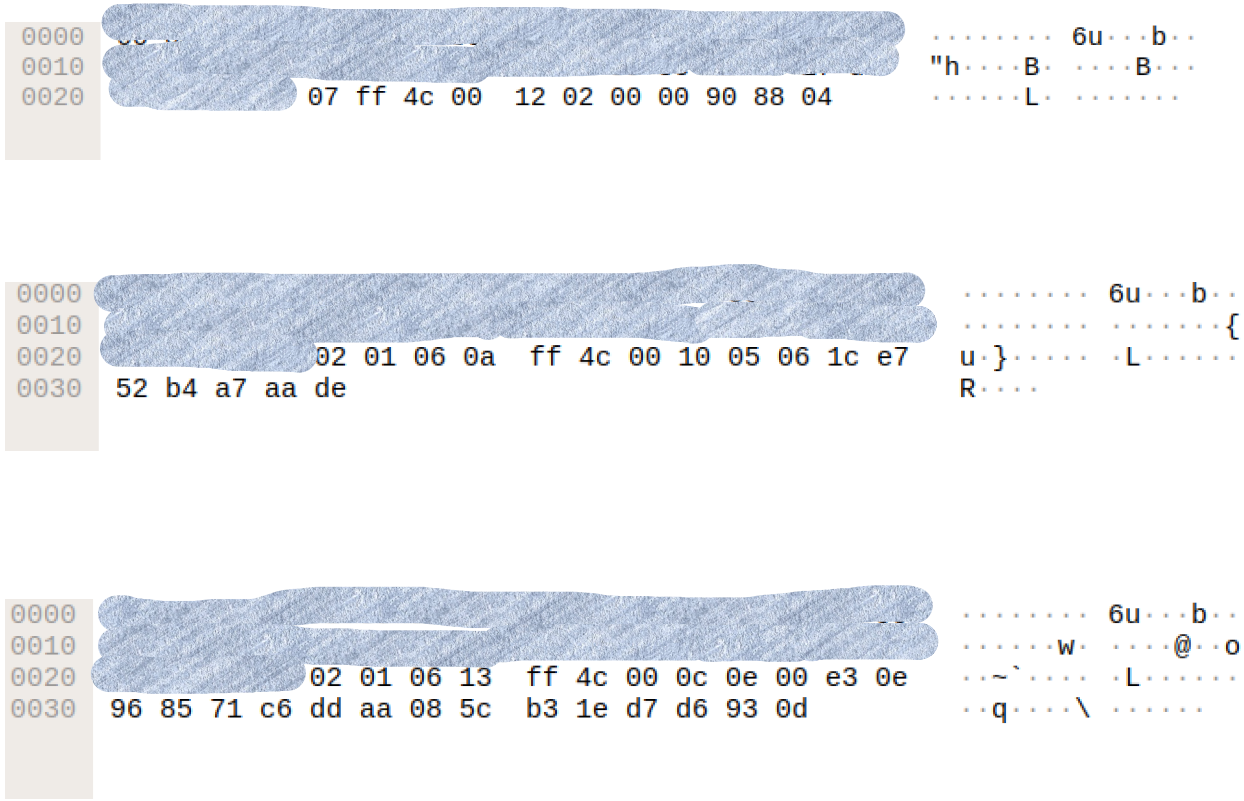
60:7e:9d:e4:6f:8b

Continuity Protocol Explained

It's not a bug, it's a feature!

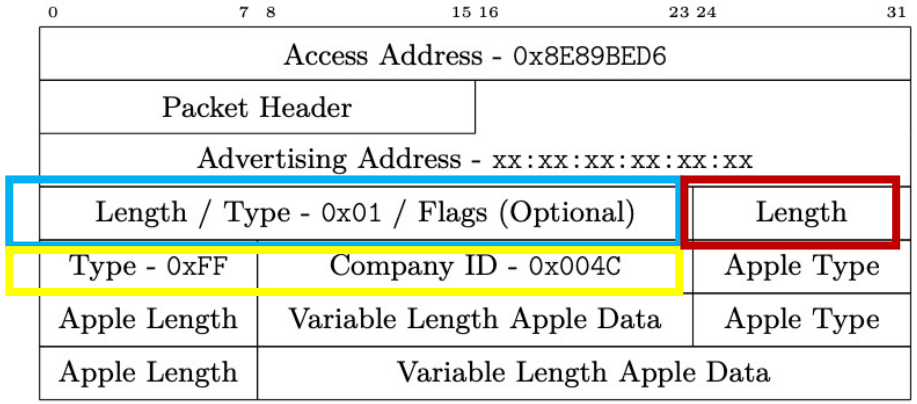
0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

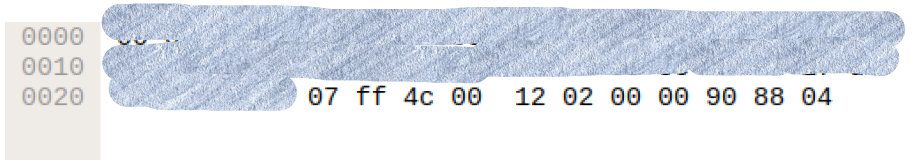


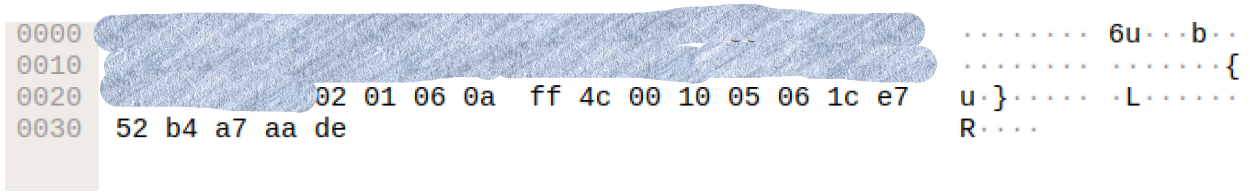
Continuity Protocol Explained

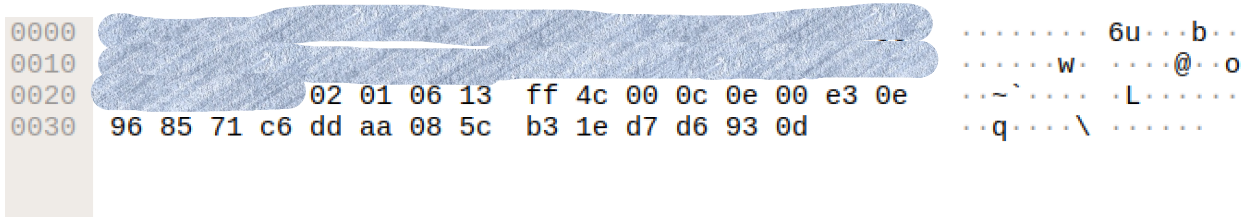
It's not a bug, it's a feature!



Apple BLE Frame Format

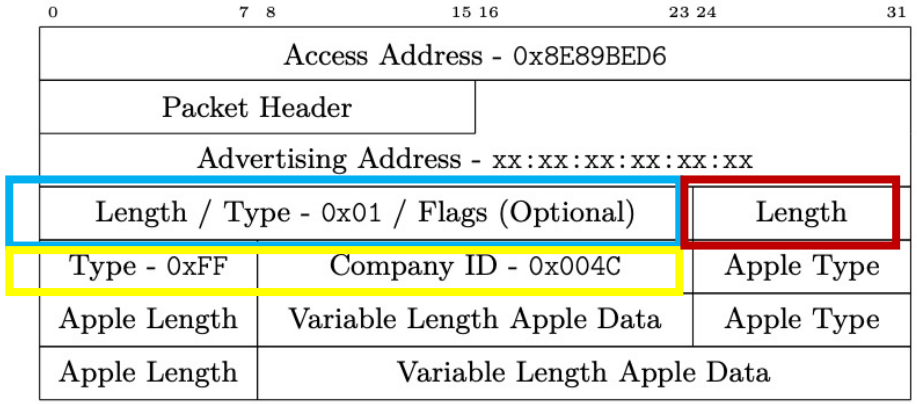




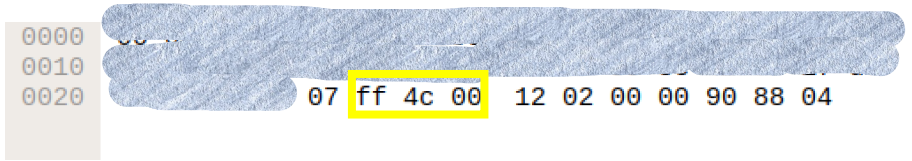


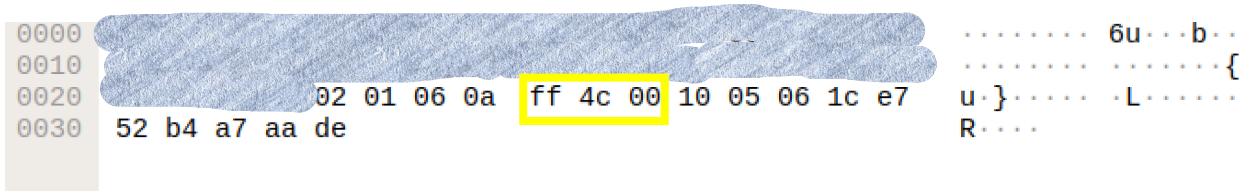
Continuity Protocol Explained

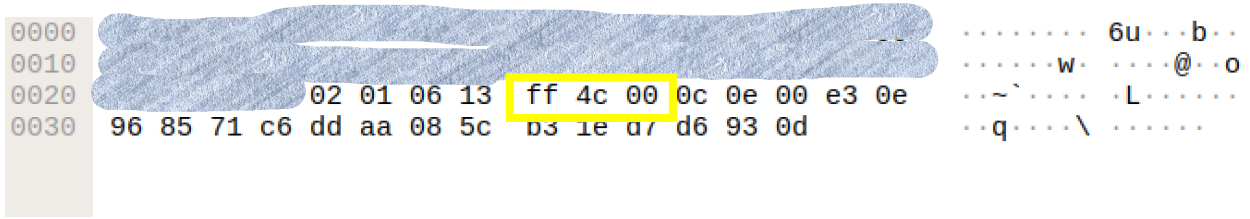
It's not a bug, it's a feature!



Apple BLE Frame Format





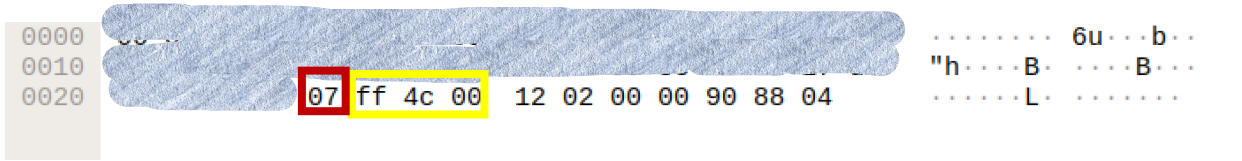


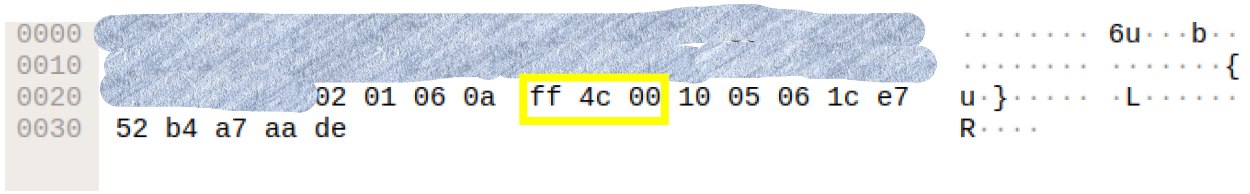
Continuity Protocol Explained

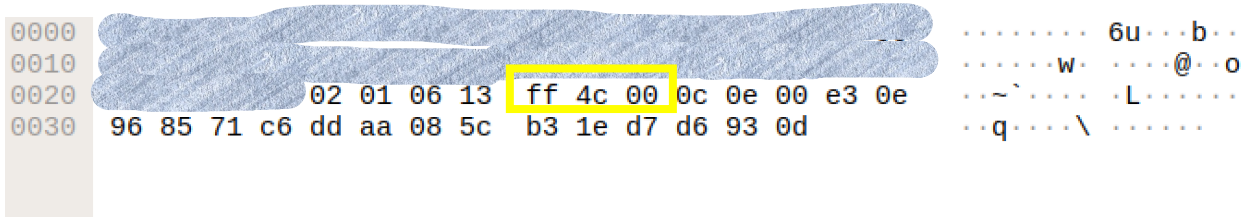
It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format





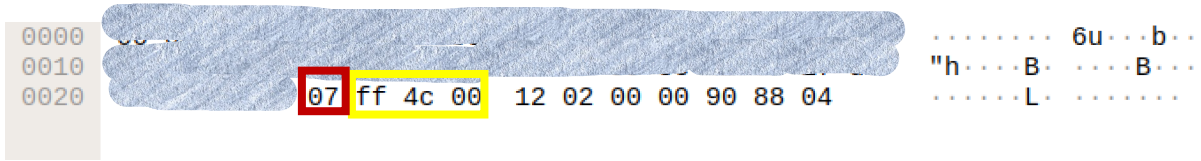


Continuity Protocol Explained

It's not a bug, it's a feature!

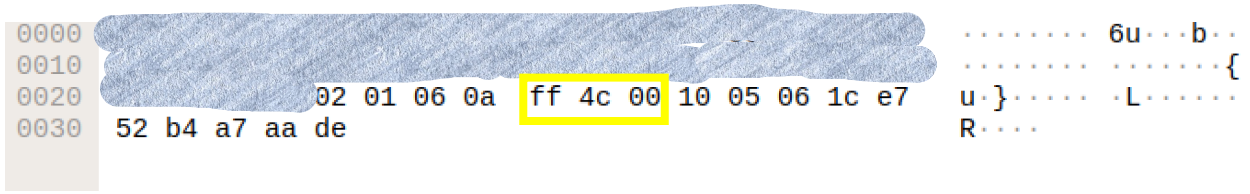
0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

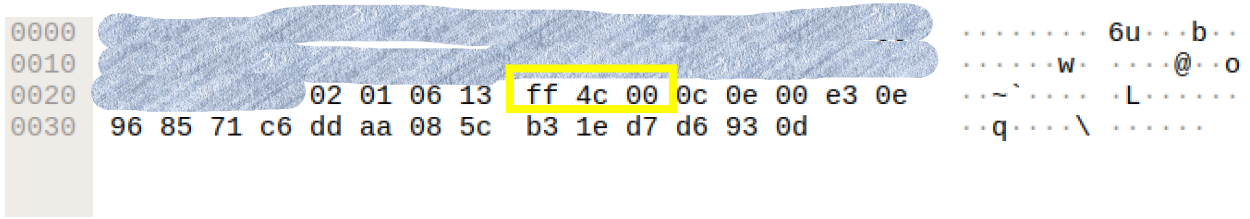
Apple BLE Frame Format



Length only

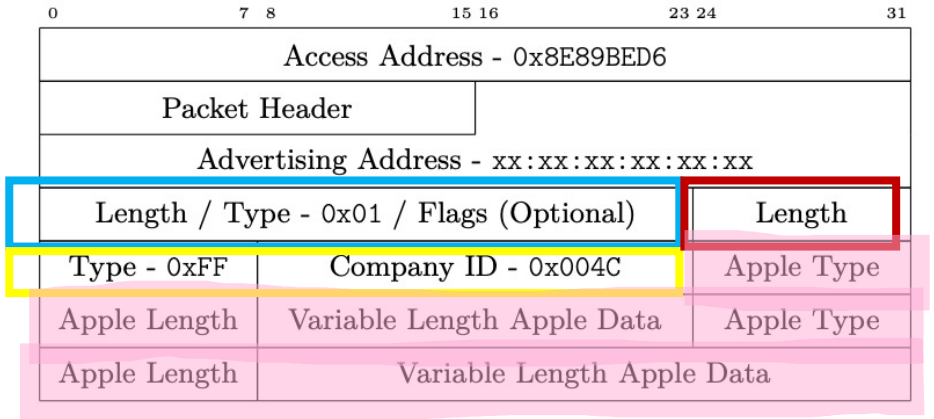
7 Bytes



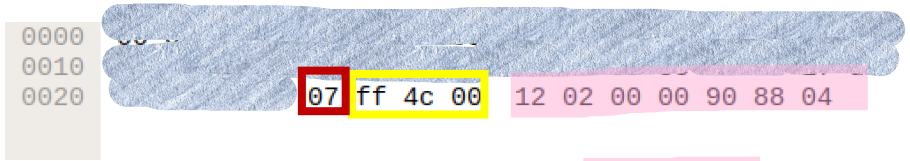


Continuity Protocol Explained

It's not a bug, it's a feature!

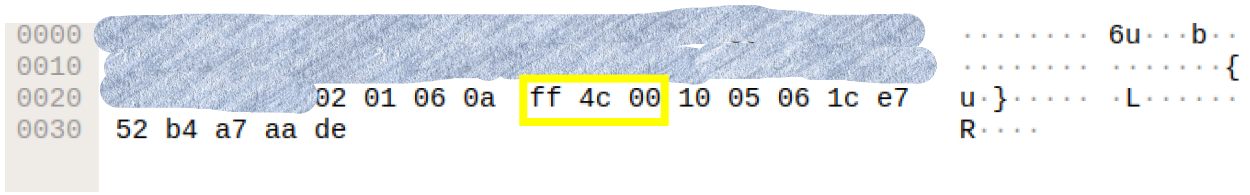


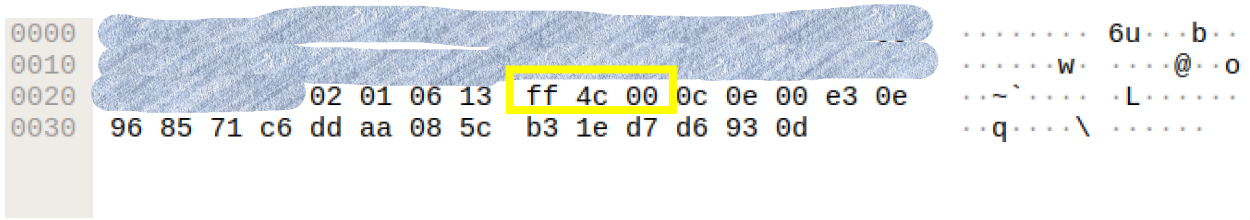
Apple BLE Frame Format



Length only

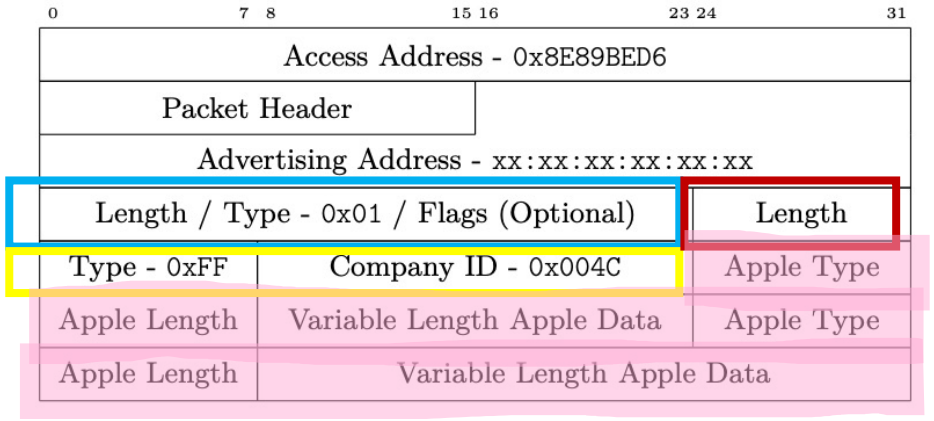
7 Bytes



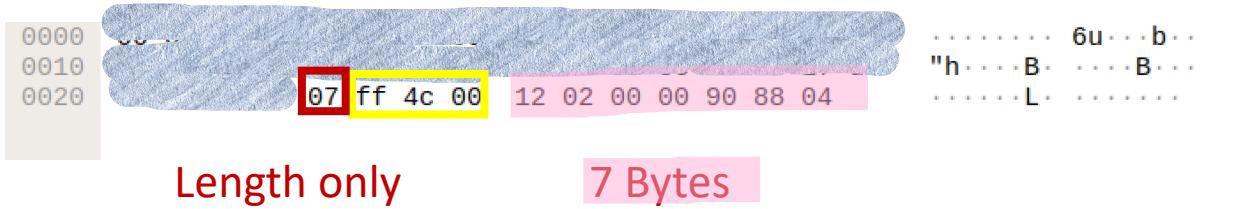


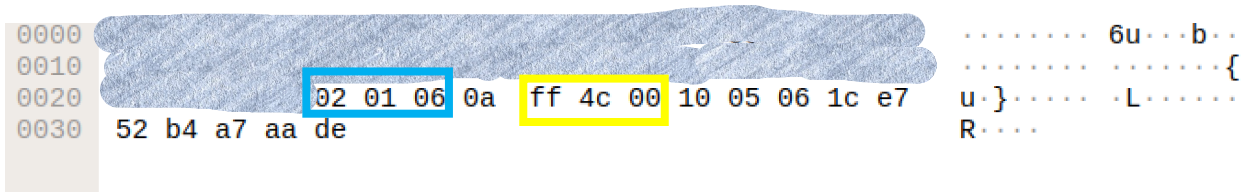
Continuity Protocol Explained

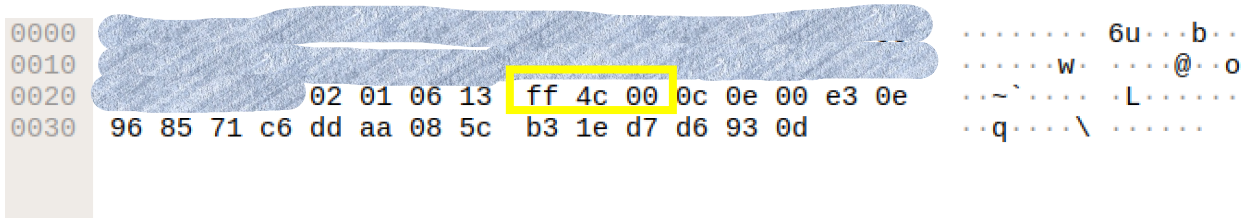
It's not a bug, it's a feature!



Apple BLE Frame Format



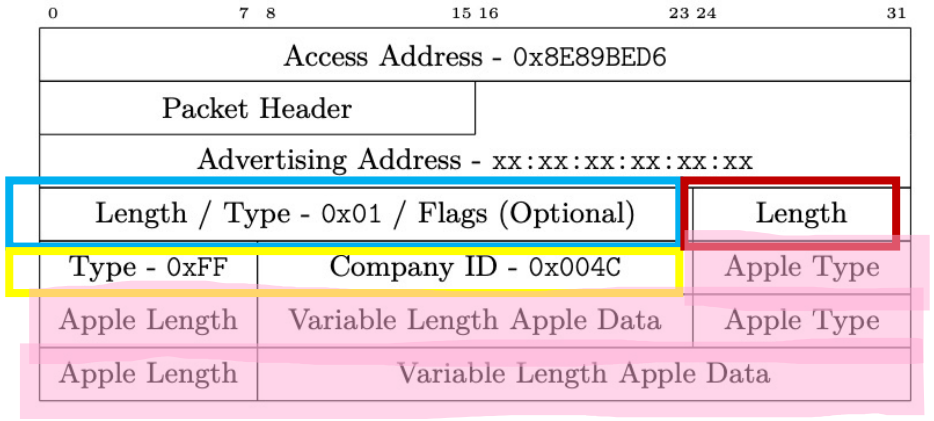




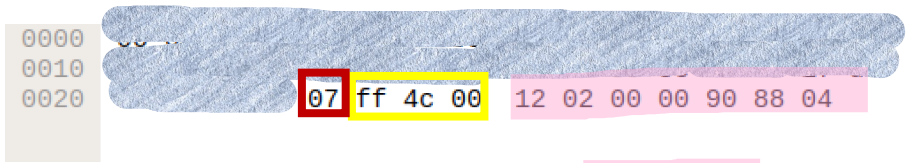
BLE flags related to discoverability and transmission power (not Apple Specific)

Continuity Protocol Explained

It's not a bug, it's a feature!

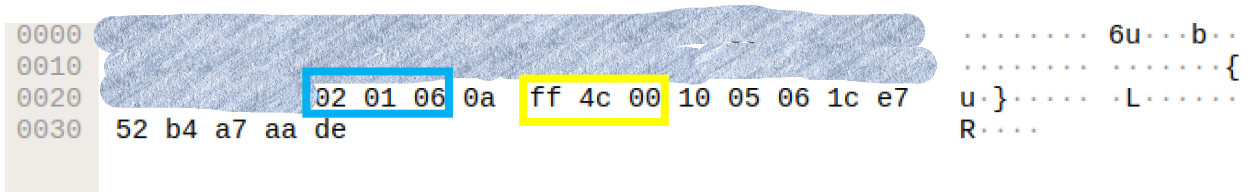


Apple BLE Frame Format

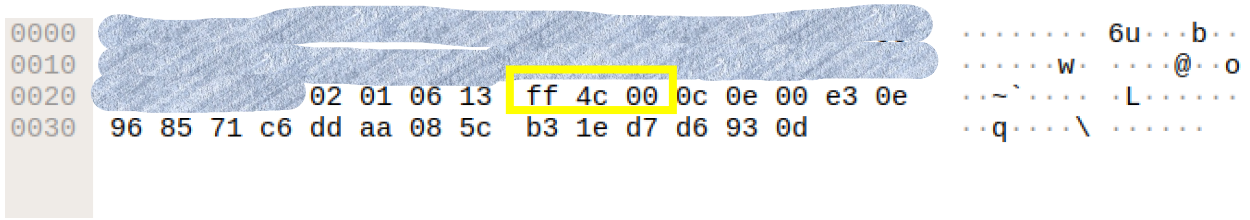


Length only

7 Bytes

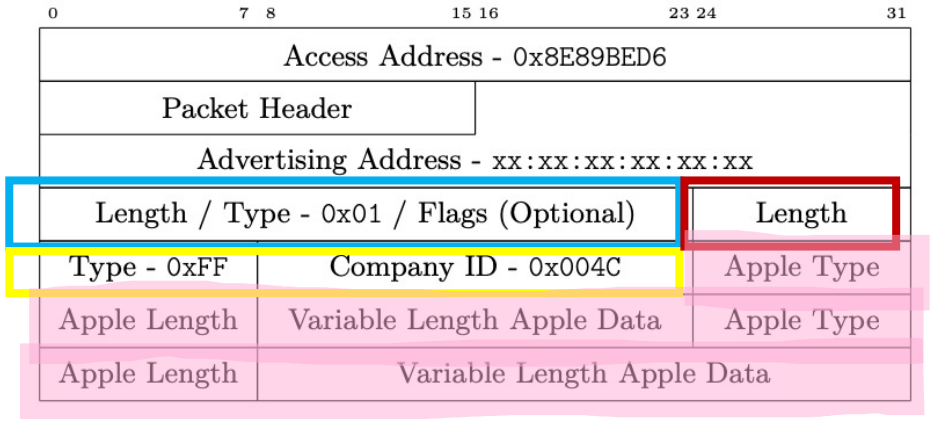


Length 0x2, 2 bytes of flag info

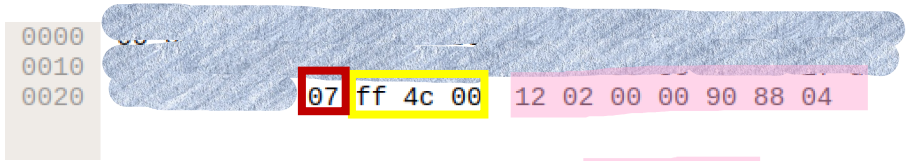


Continuity Protocol Explained

It's not a bug, it's a feature!

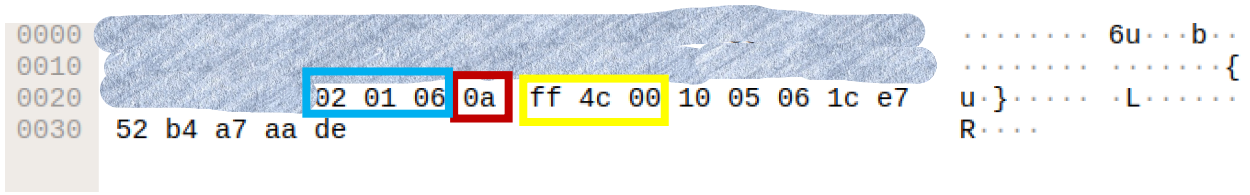


Apple BLE Frame Format

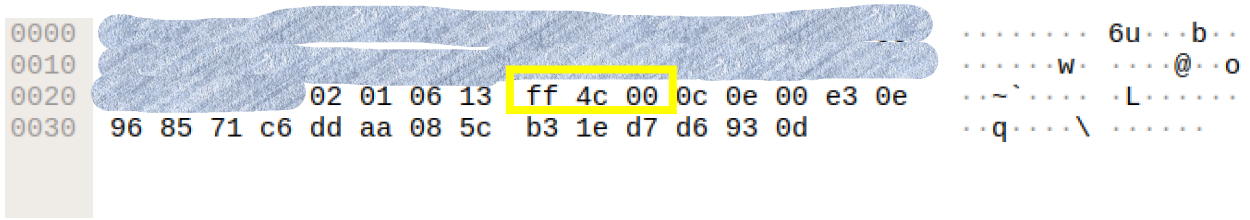


Length only

7 Bytes

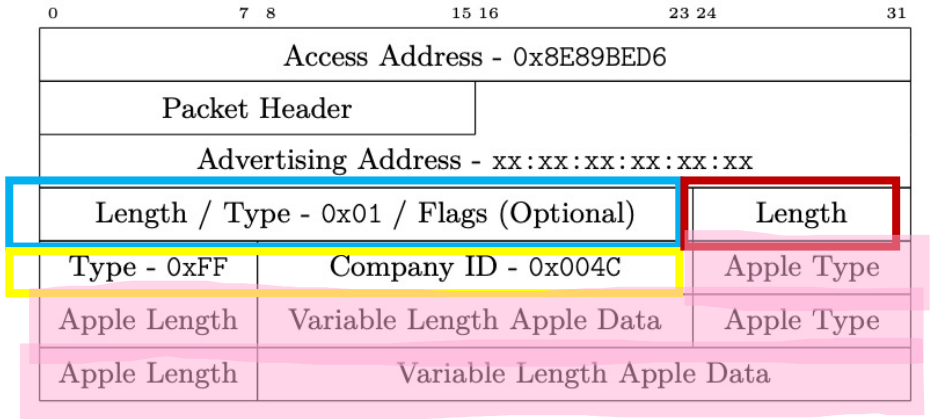


Length 0x2, 2 bytes of flag info

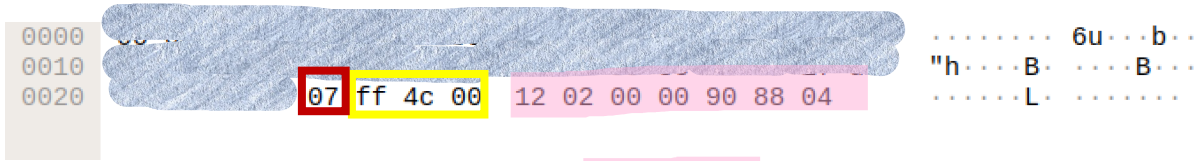


Continuity Protocol Explained

It's not a bug, it's a feature!

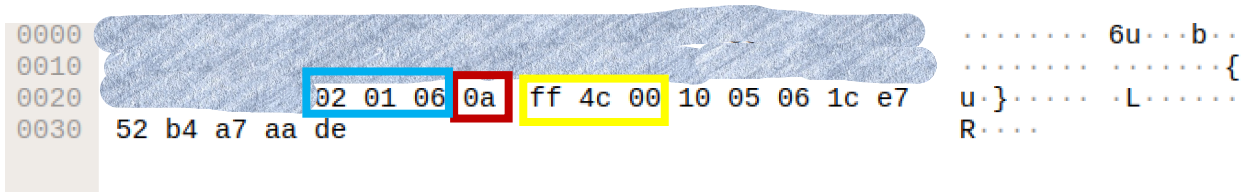


Apple BLE Frame Format

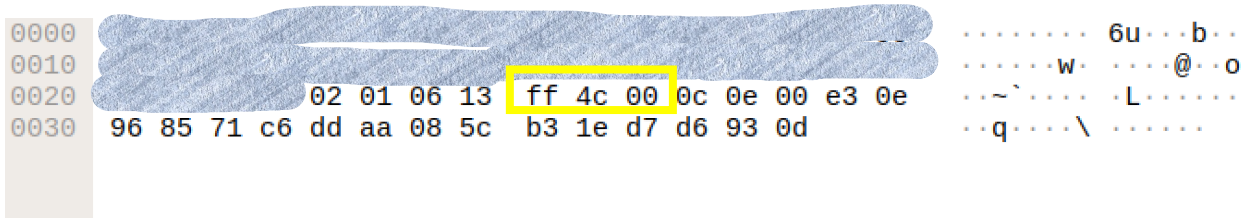


Length only

7 Bytes

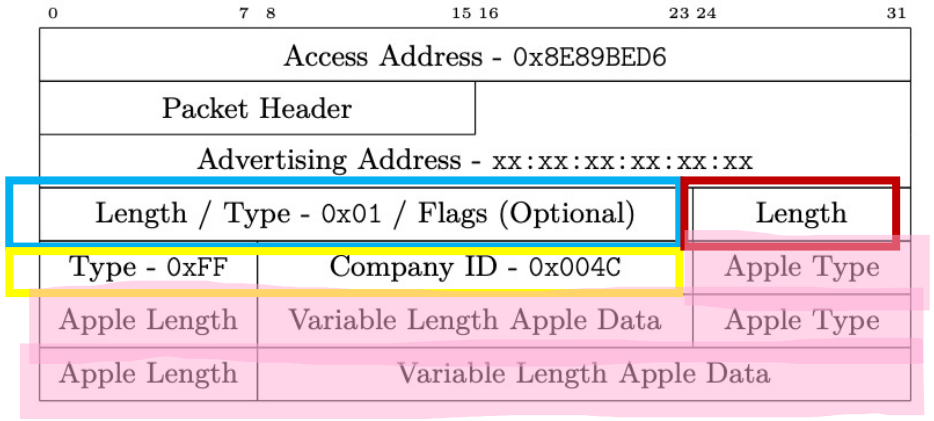


Length 0x2, 2 bytes of flag info Length 0xa, 10 bytes succeeding

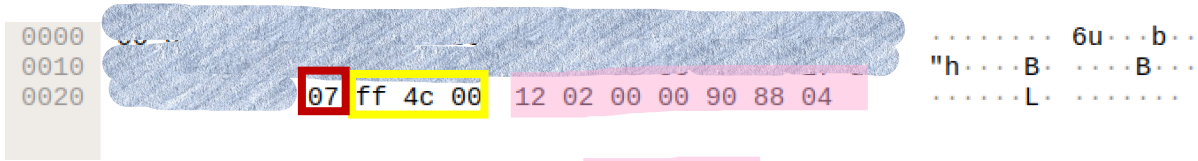


Continuity Protocol Explained

It's not a bug, it's a feature!

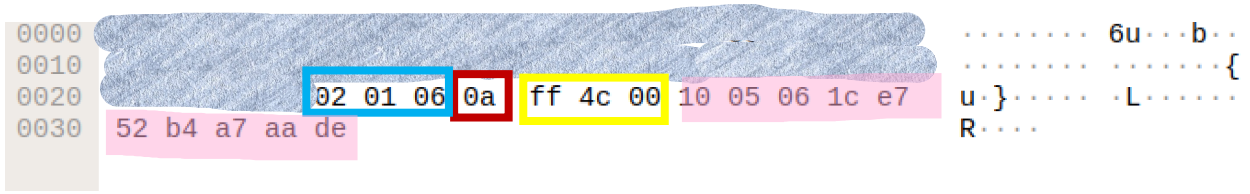


Apple BLE Frame Format

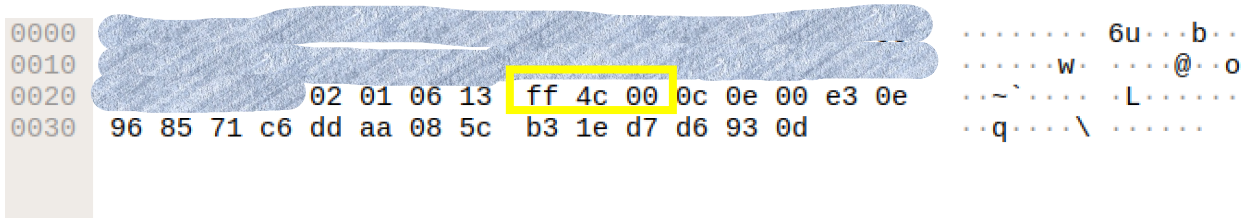


Length only

7 Bytes

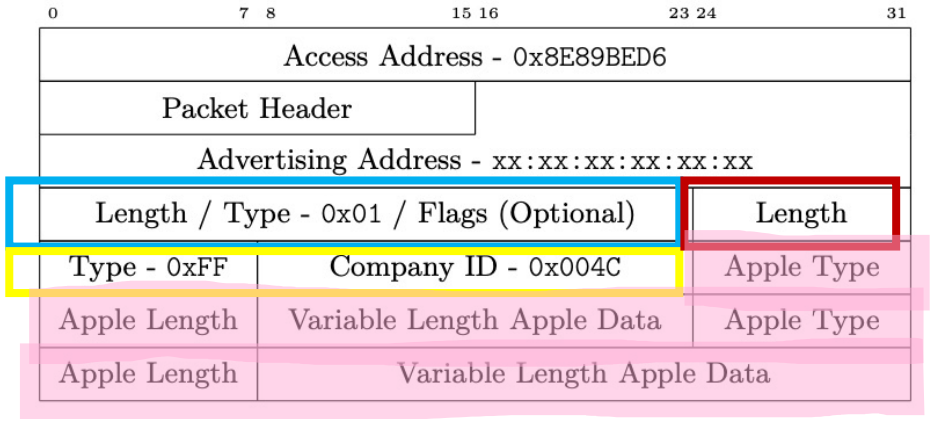


Length 0x2, 2 bytes of flag info Length 0xa, 10 bytes succeeding

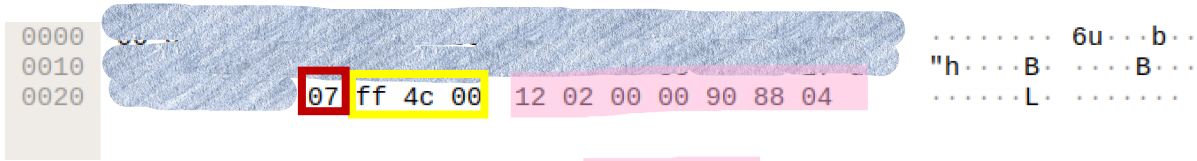


Continuity Protocol Explained

It's not a bug, it's a feature!

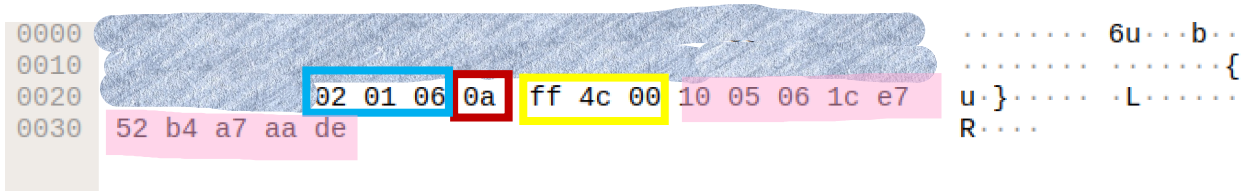


Apple BLE Frame Format

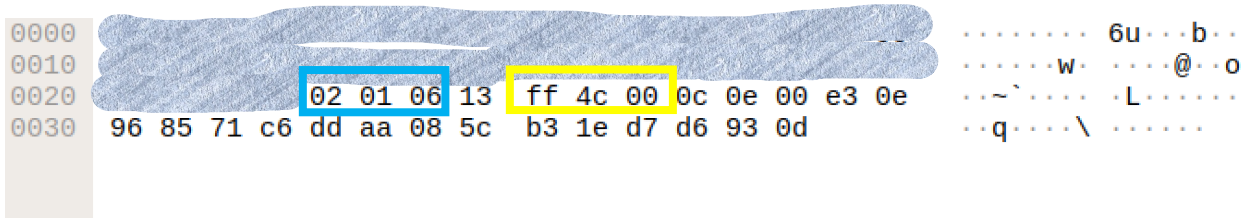


Length only

7 Bytes

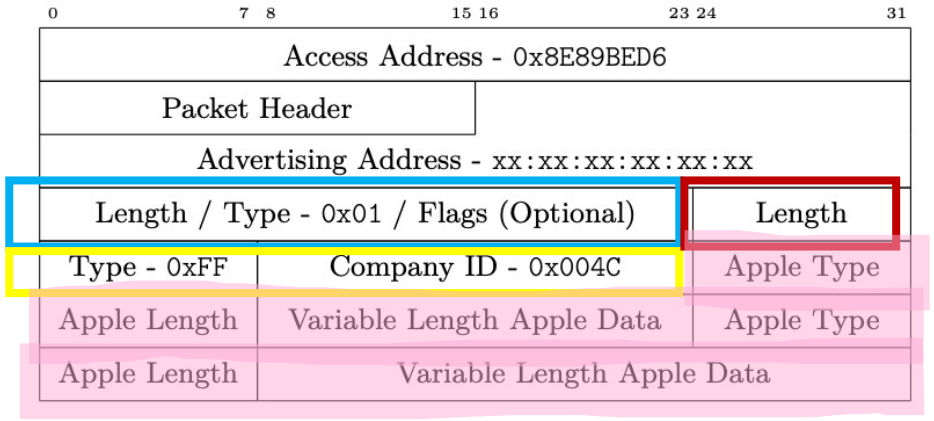


Length 0x2, 2 bytes of flag info Length 0xa, 10 bytes succeeding

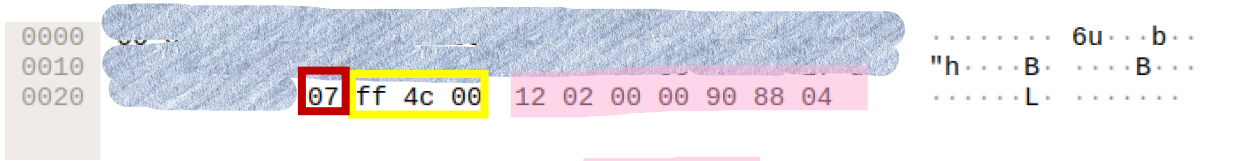


Continuity Protocol Explained

It's not a bug, it's a feature!

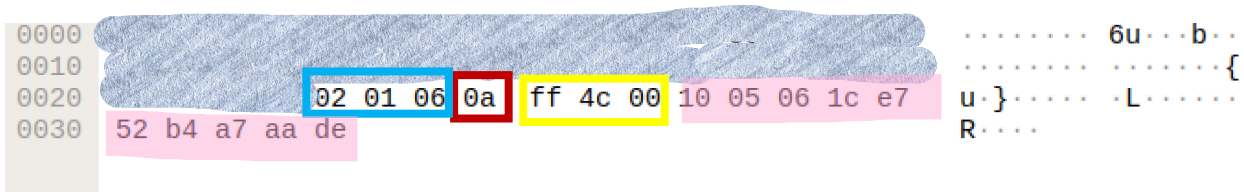


Apple BLE Frame Format

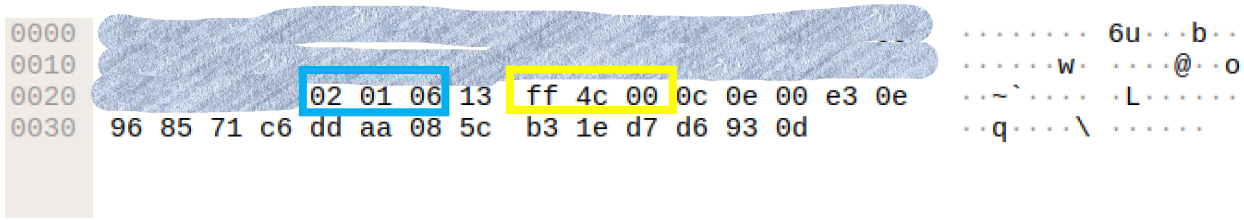


Length only

7 Bytes



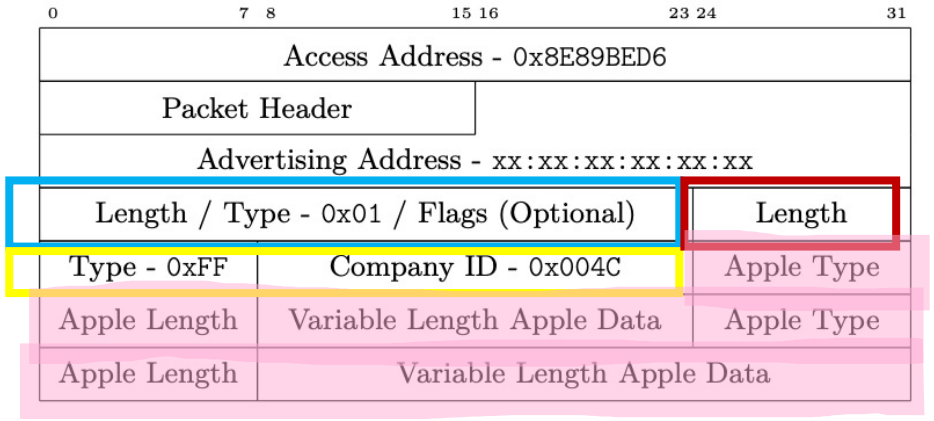
Length 0x2, 2 bytes of flag info Length 0xa, 10 bytes succeeding



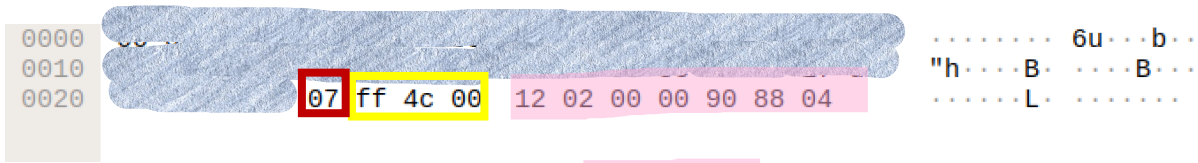
Length 0x2, 2 bytes of flag info

Continuity Protocol Explained

It's not a bug, it's a feature!

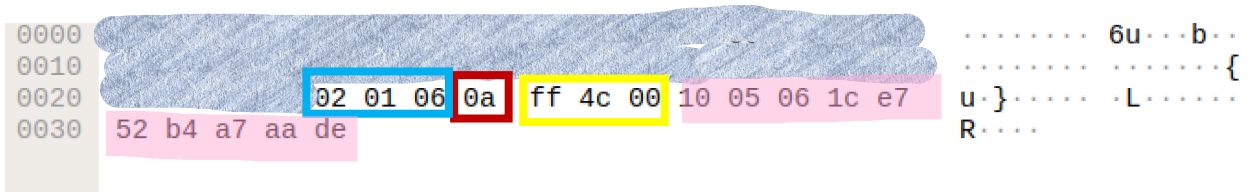


Apple BLE Frame Format

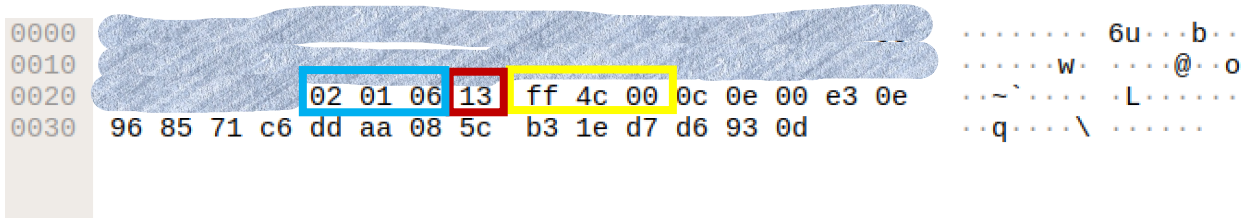


Length only

7 Bytes



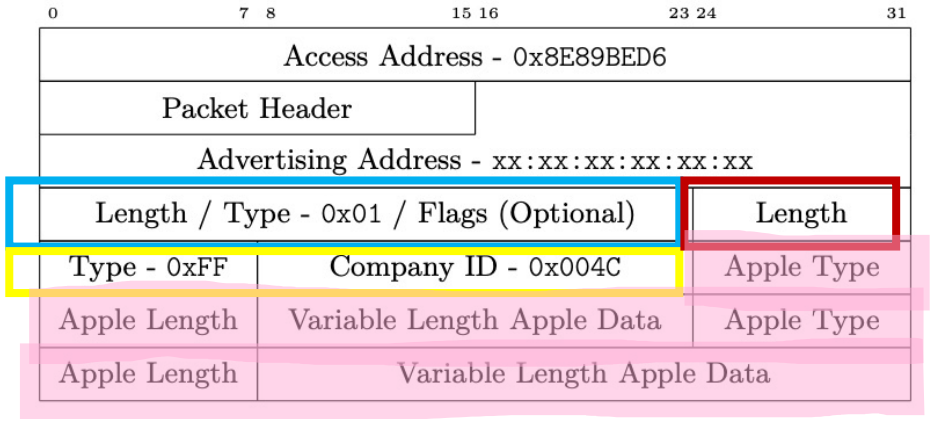
Length 0x2, 2 bytes of flag info Length 0xa, 10 bytes succeeding



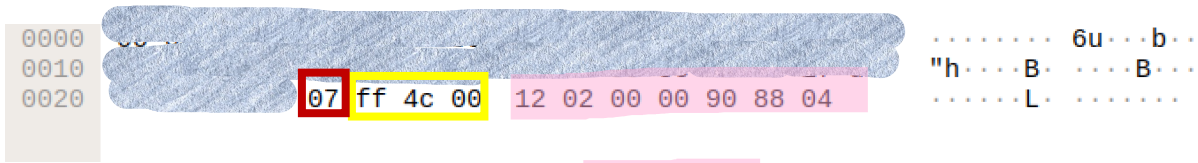
Length 0x2, 2 bytes of flag info

Continuity Protocol Explained

It's not a bug, it's a feature!

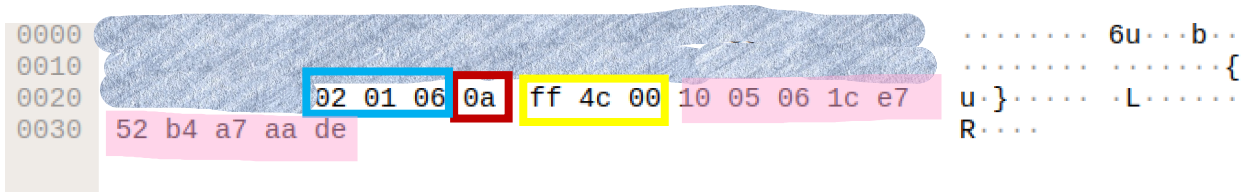


Apple BLE Frame Format

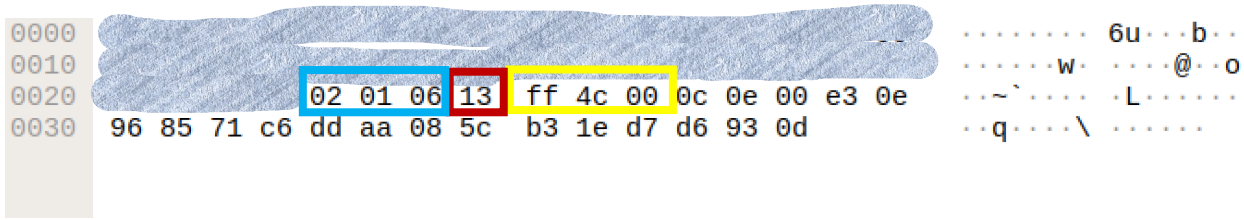


Length only

7 Bytes



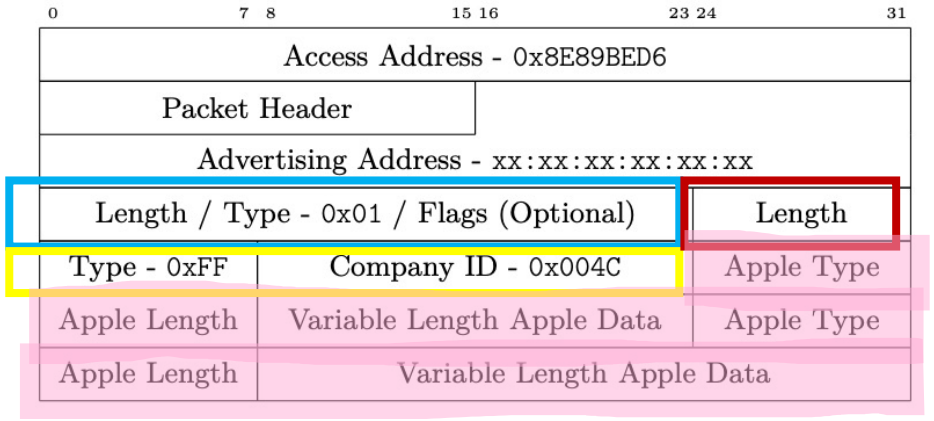
Length 0x2, 2 bytes of flag info Length 0xa, 10 bytes succeeding



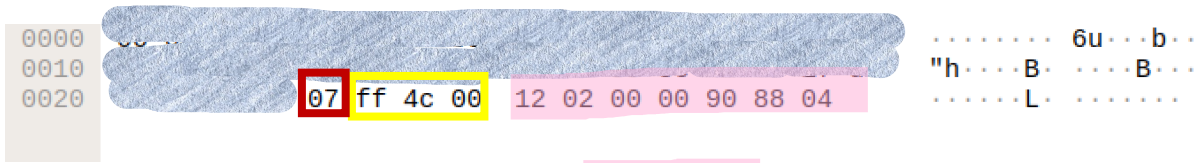
Length 0x2, 2 bytes of flag info Length 0x13, 19 bytes succeeding

Continuity Protocol Explained

It's not a bug, it's a feature!

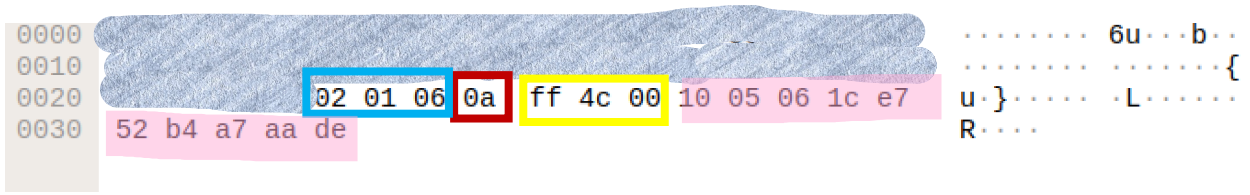


Apple BLE Frame Format

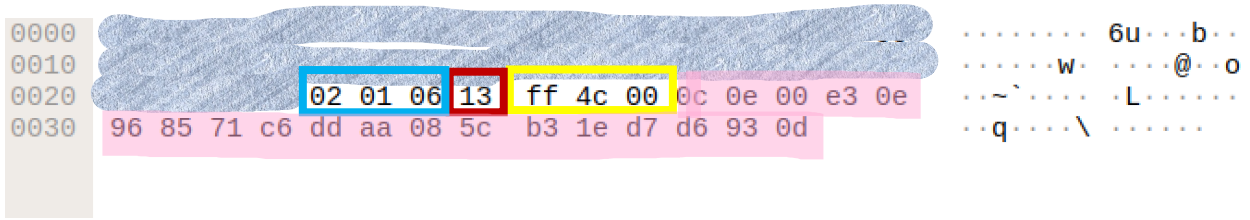


Length only

7 Bytes



Length 0x2, 2 bytes of flag info Length 0xa, 10 bytes succeeding



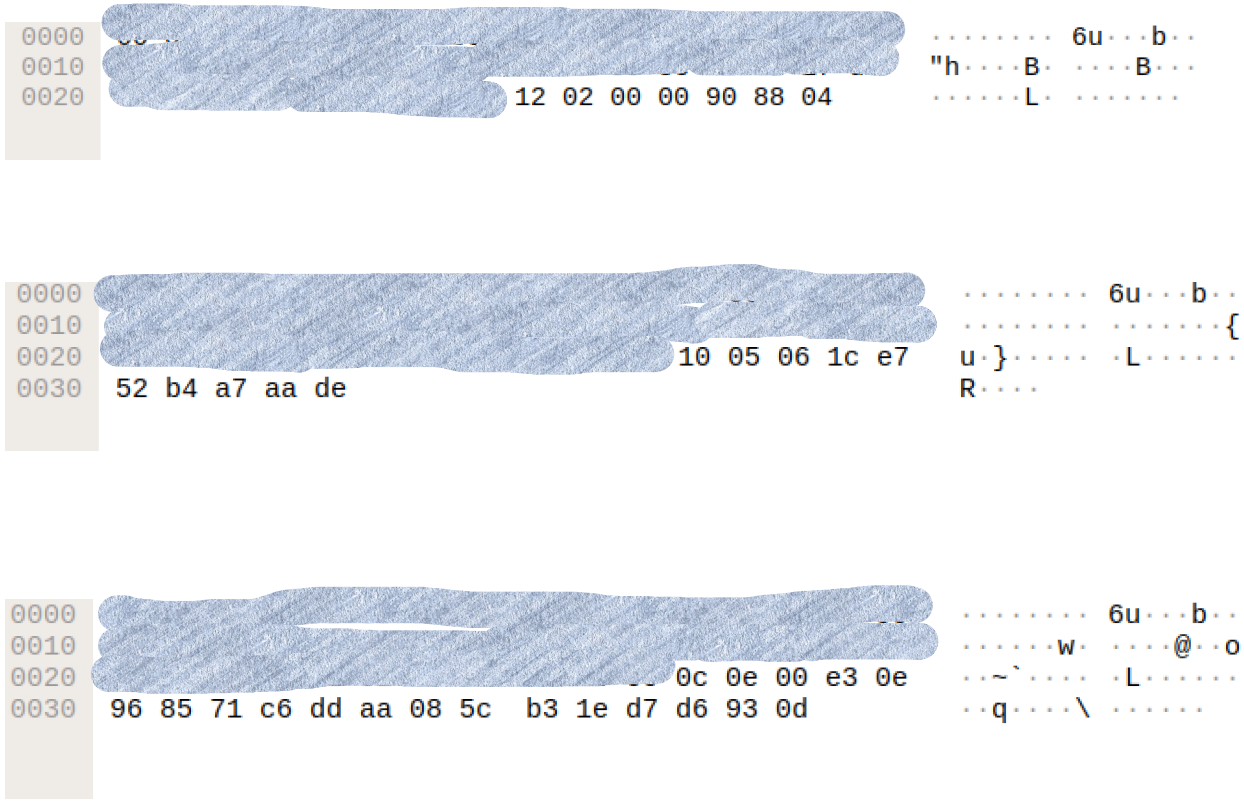
Length 0x2, 2 bytes of flag info Length 0x13, 19 bytes succeeding

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

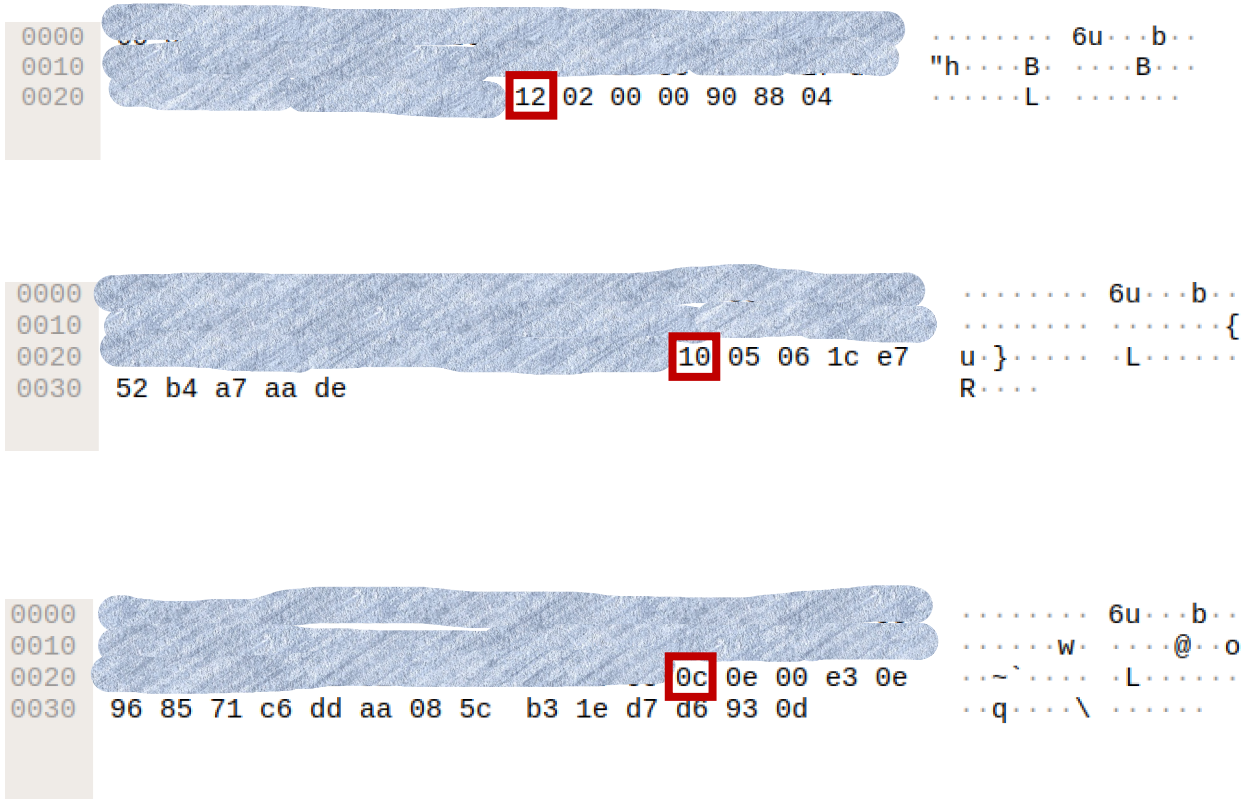


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

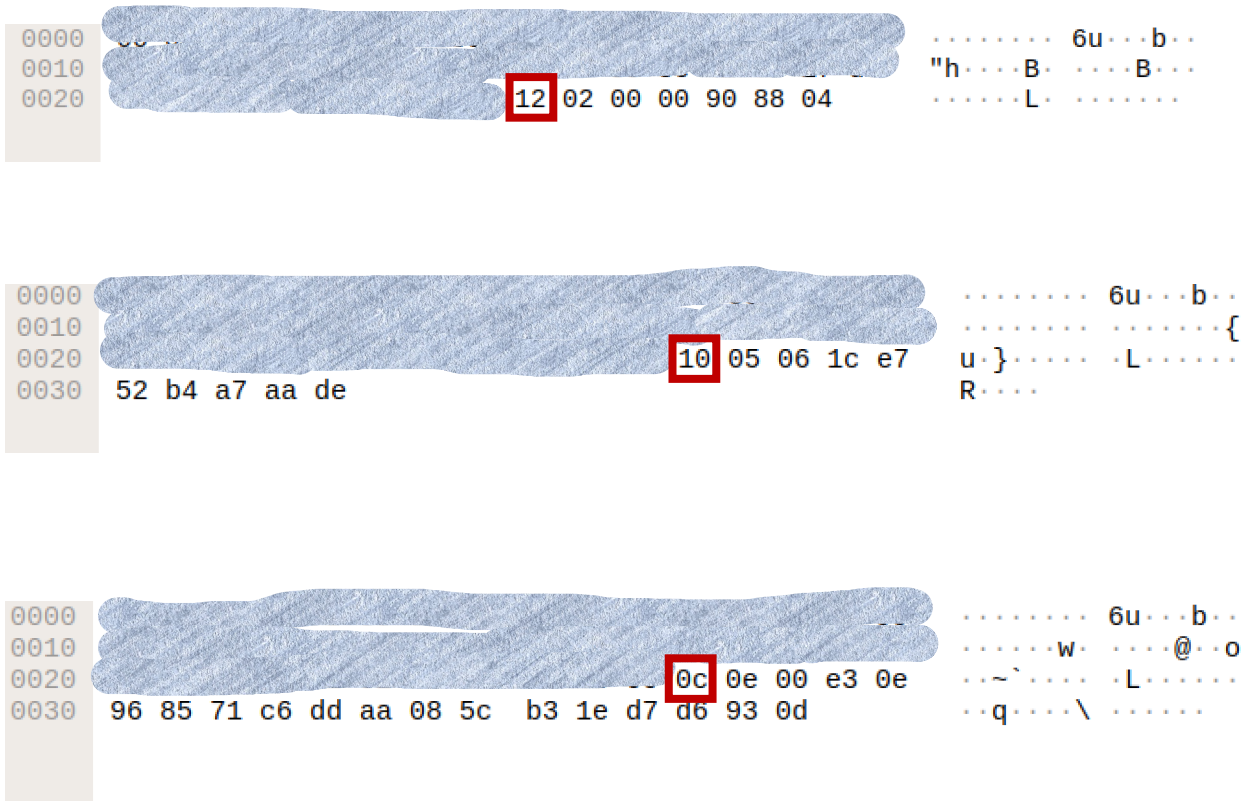
Apple BLE Frame Format



Continuity Protocol Explained

It's not a bug, it's a feature!

Message Type	Dec Value	Hex Value
AirDrop	5	0x05
Proximity Pairing	7	0x07
Hey Siri	8	0x08
Magic Switch	11	0xb
Handoff	12	0xc
Instant Hotpot	14	0xfe
Nearby Action	15	0xff
Nearby Info	16	0x10
FindMy	18	0x12

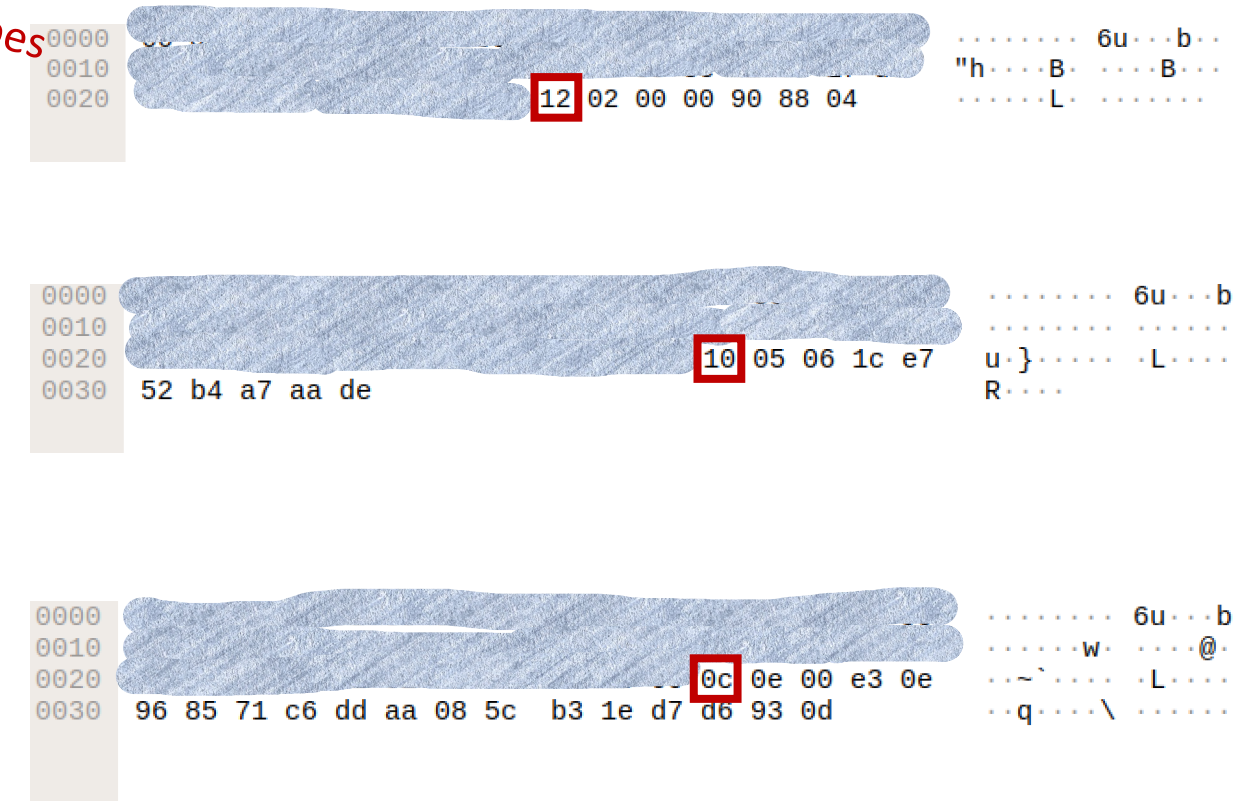


Continuity Protocol Explained

It's not a bug, it's a feature!

Message Type	Dec Value	Hex Value
AirDrop	5	0x05
Proximity Pairing	7	0x07
Hey Siri	8	0x08
Magic Switch	11	0xb
Handoff	12	0xc
Instant Hotpot	14	0xfe
Nearby Action	15	0xff
Nearby Info	16	0x10
FindMy	18	0x12

Apple Message Types

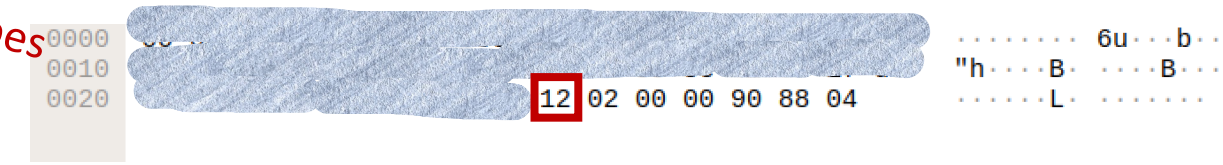


Continuity Protocol Explained

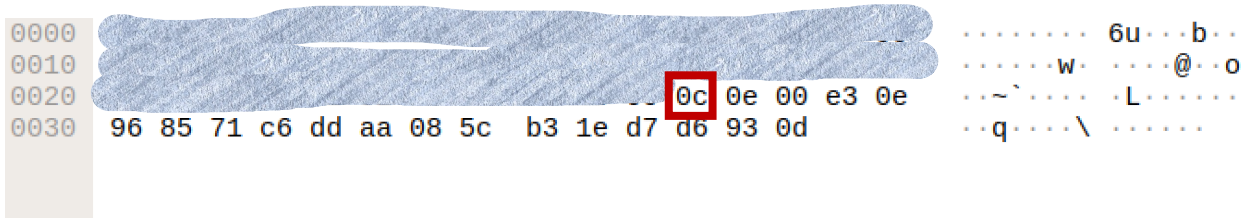
It's not a bug, it's a feature!

Message Type	Dec Value	Hex Value
AirDrop	5	0x05
Proximity Pairing	7	0x07
Hey Siri	8	0x08
Magic Switch	11	0xb
Handoff	12	0xc
Instant Hotpot	14	0xfe
Nearby Action	15	0xff
Nearby Info	16	0x10
FindMy	18	0x12

Apple Message Types



Type 18: Find My

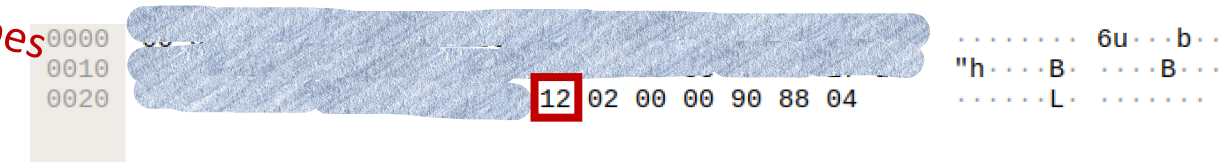


Continuity Protocol Explained

It's not a bug, it's a feature!

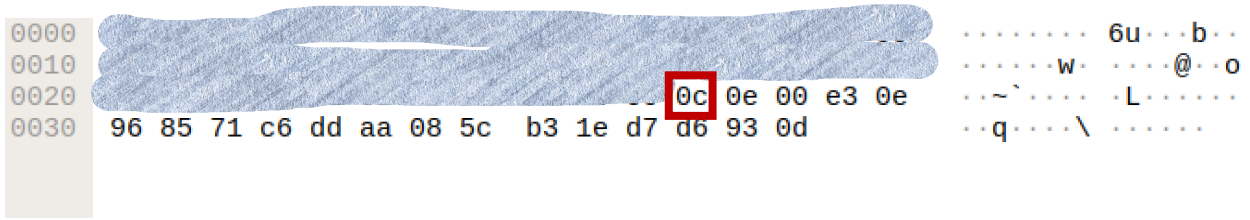
Message Type	Dec Value	Hex Value
AirDrop	5	0x05
Proximity Pairing	7	0x07
Hey Siri	8	0x08
Magic Switch	11	0xb
Handoff	12	0xc
Instant Hotpot	14	0xfe
Nearby Action	15	0xff
Nearby Info	16	0x10
FindMy	18	0x12

Apple Message Types



Type 18: Find My

✨samteplov.com✨

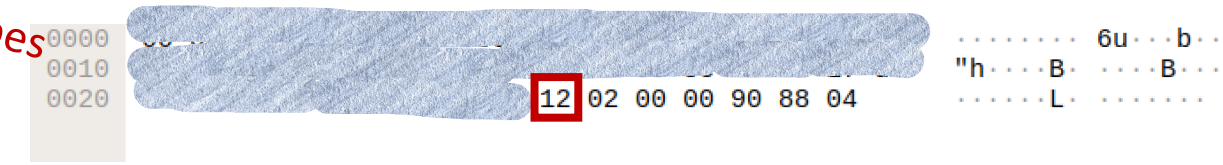


Continuity Protocol Explained

It's not a bug, it's a feature!

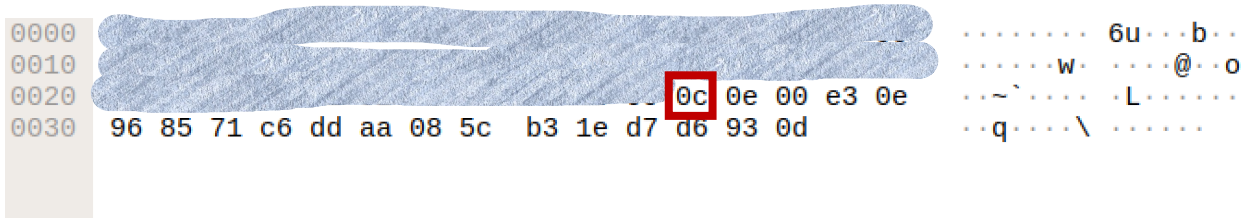
Message Type	Dec Value	Hex Value
AirDrop	5	0x05
Proximity Pairing	7	0x07
Hey Siri	8	0x08
Magic Switch	11	0xb
Handoff	12	0xc
Instant Hotpot	14	0xfe
Nearby Action	15	0xff
Nearby Info	16	0x10
FindMy	18	0x12

Apple Message Types



Type 18: Find My

Type 16: Nearby

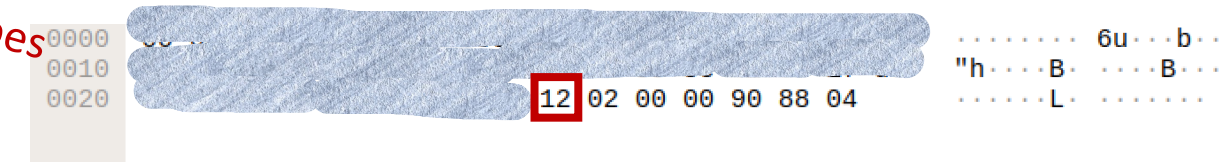


Continuity Protocol Explained

It's not a bug, it's a feature!

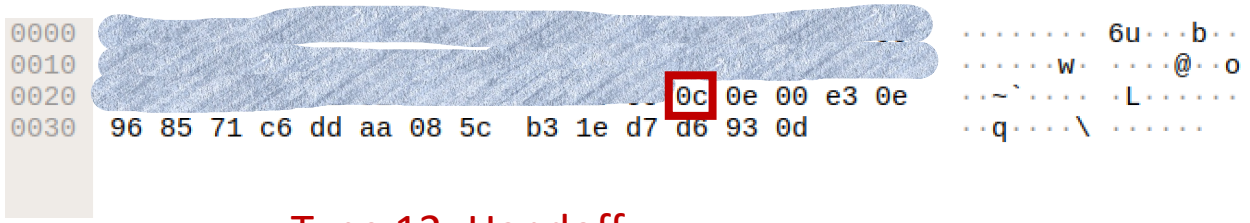
Message Type	Dec Value	Hex Value
AirDrop	5	0x05
Proximity Pairing	7	0x07
Hey Siri	8	0x08
Magic Switch	11	0xb
Handoff	12	0xc
Instant Hotpot	14	0xfe
Nearby Action	15	0xff
Nearby Info	16	0x10
FindMy	18	0x12

Apple Message Types



Type 18: Find My

Type 16: Nearby



Type 12: Handoff

Continuity Protocol Explained

It's not a bug, it's a feature!

Apple Message Types

Message Type	Dec Value	Hex Value
AirDrop	5	0x05
Proximity Pairing	7	0x07
Hey Siri	8	0x08
Magic Switch	11	0xb
Handoff	12	0xc
Instant Hotpot	14	0xfe
Nearby Action	15	0xff
Nearby Info	16	0x10
FindMy	18	0x12

Type 16: Nearby

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

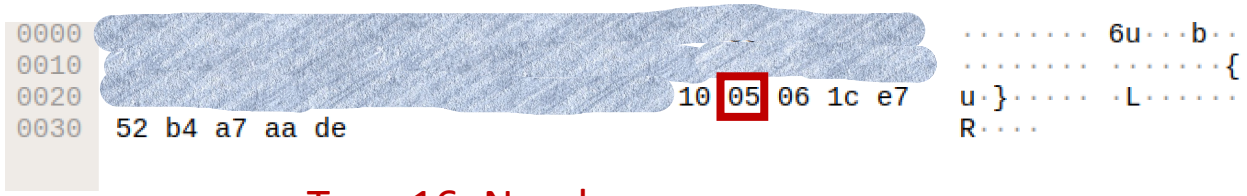
Type 16: Nearby

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7	8	15	16	23	24	31
Access Address - 0x8E89BED6							
Packet Header							
Advertising Address - xx:xx:xx:xx:xx:xx							
Length / Type - 0x01 / Flags (Optional)							Length
Type - 0xFF			Company ID - 0x004C				Apple Type
Apple Length			Variable Length Apple Data				Apple Type
Apple Length			Variable Length Apple Data				

Apple BLE Frame Format



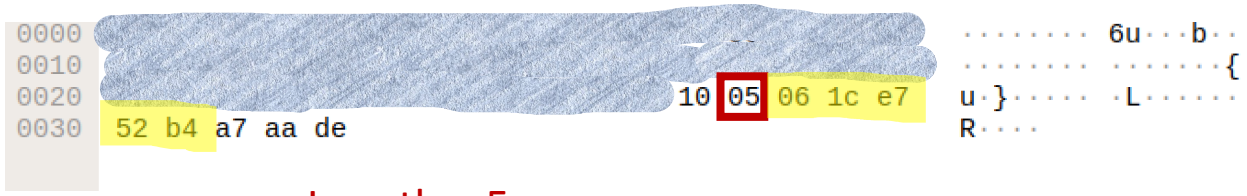
Type 16: Nearby

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format



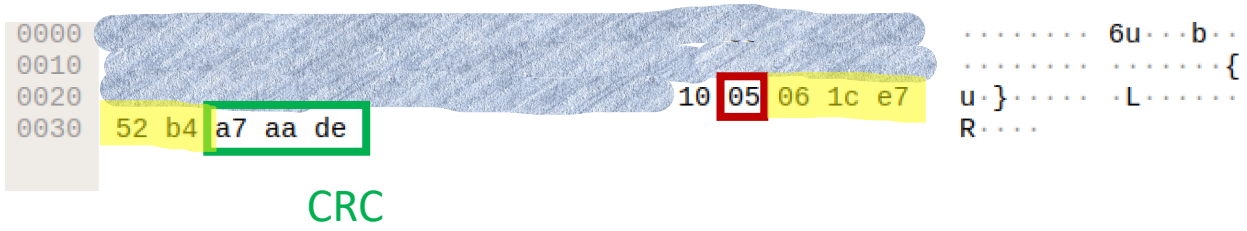
Length = 5

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format

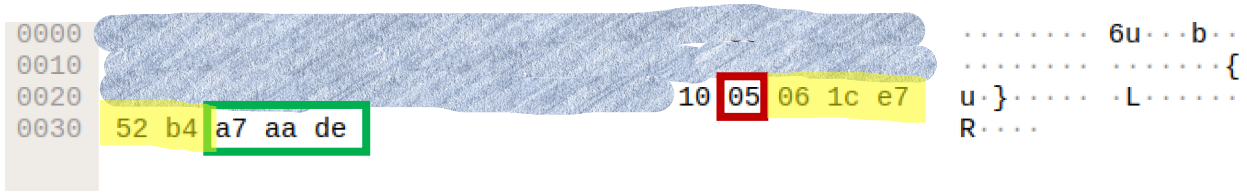


Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format



Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

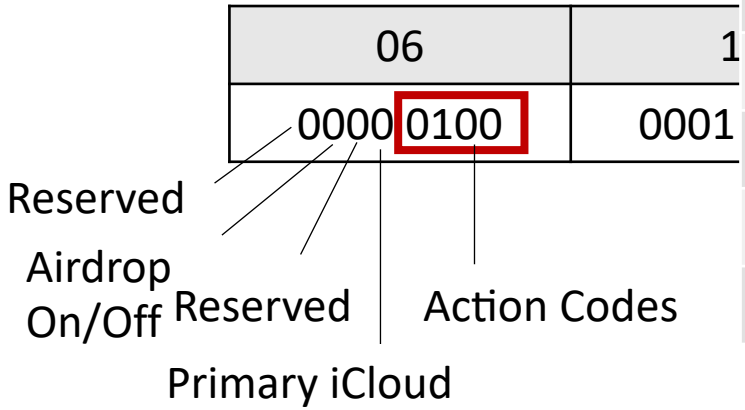
06	1c
0000 0100	0001 1100

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



Action Code	Meaning
1	Activity Unknown
2	Activity Reporting Disabled
3	Idle
4	Locked Phone
5	Audio is playing with screen off
7	Transition Idle from Locked Screen
9	Screen is on and video is playing
10	Phone locked; push notifications to watch
11	Active user
13	User is driving in a vehicle
14	Phone in phone call or face time

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Auth Tag is 0xe752b4

Apple BLE Frame Format

06	1c
0000 0100	0001 1100

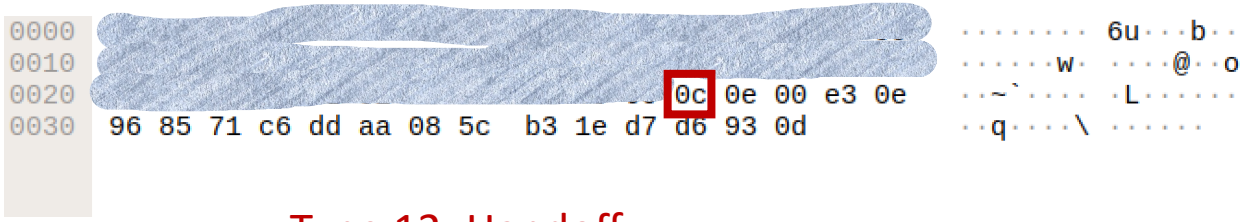
- Auto Unlock
- Auto Unlock Watch
- Watch Locked
- AuthTag Present
- Reserved
- WiFi On/Off
- 4 Byte Auth Tag
- Airpods Connected

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



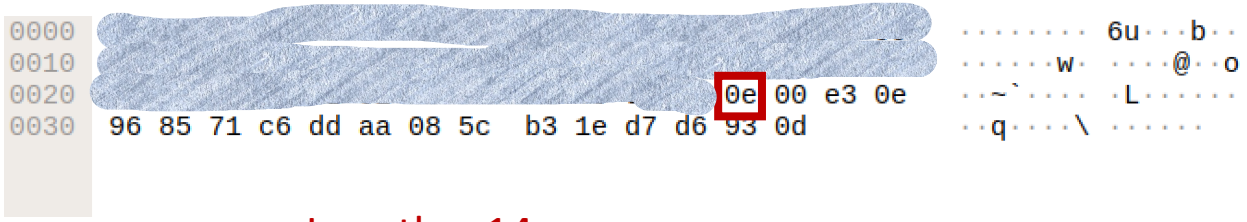
Type 12: Handoff

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



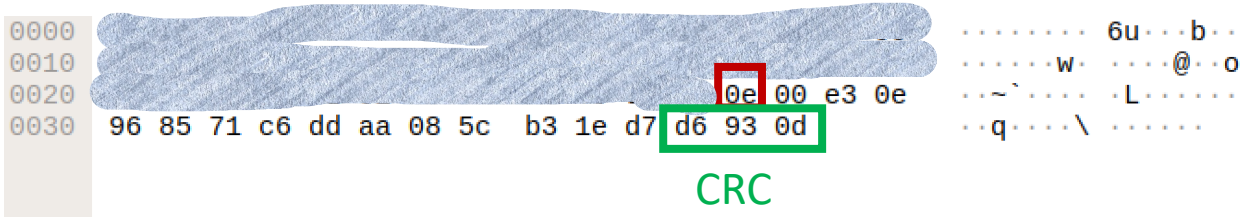
Length = 14

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

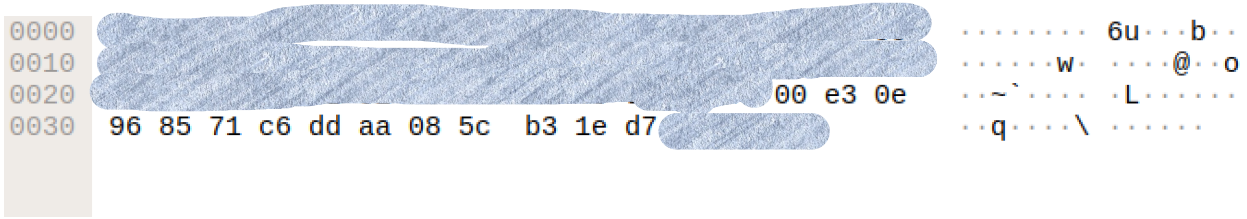


Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format

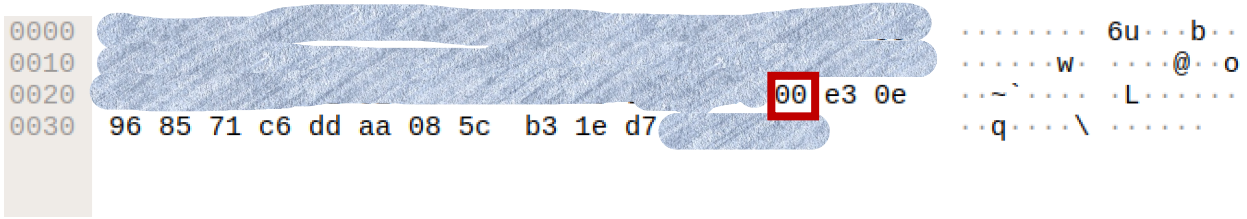


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



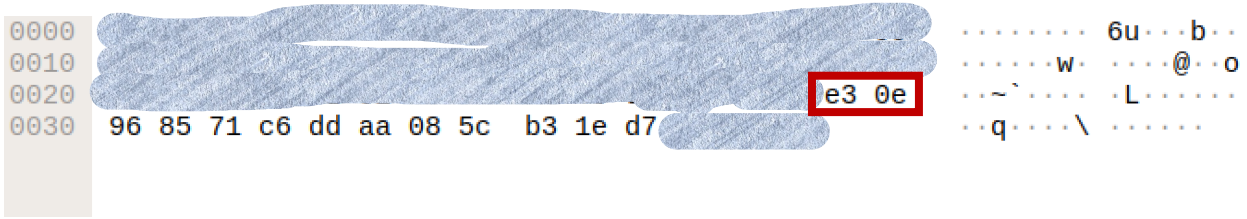
Cut/Copy performed

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format



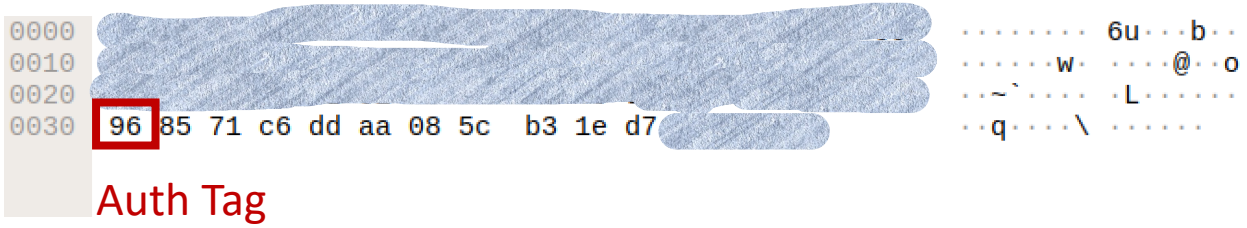
IV Seq Num

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

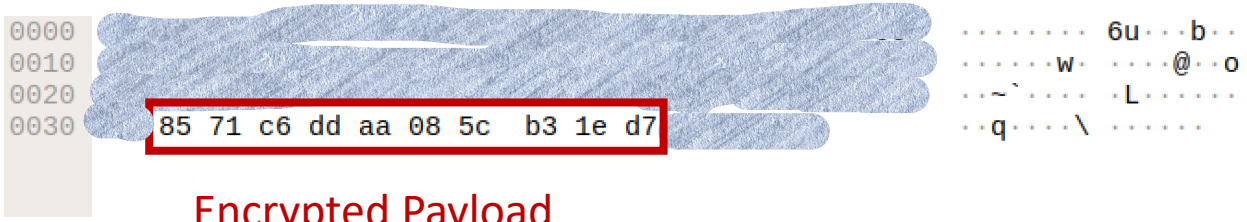


Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format



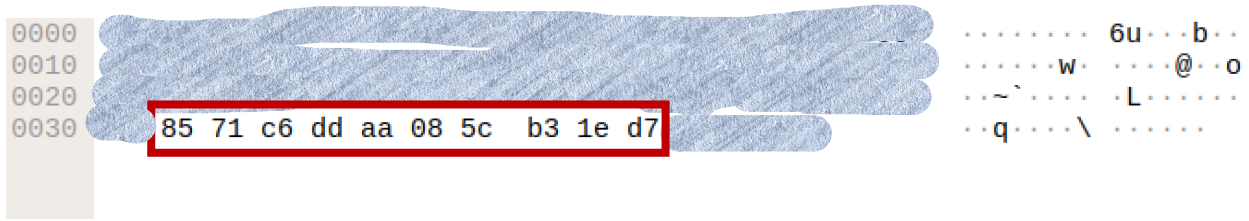
Encrypted Payload

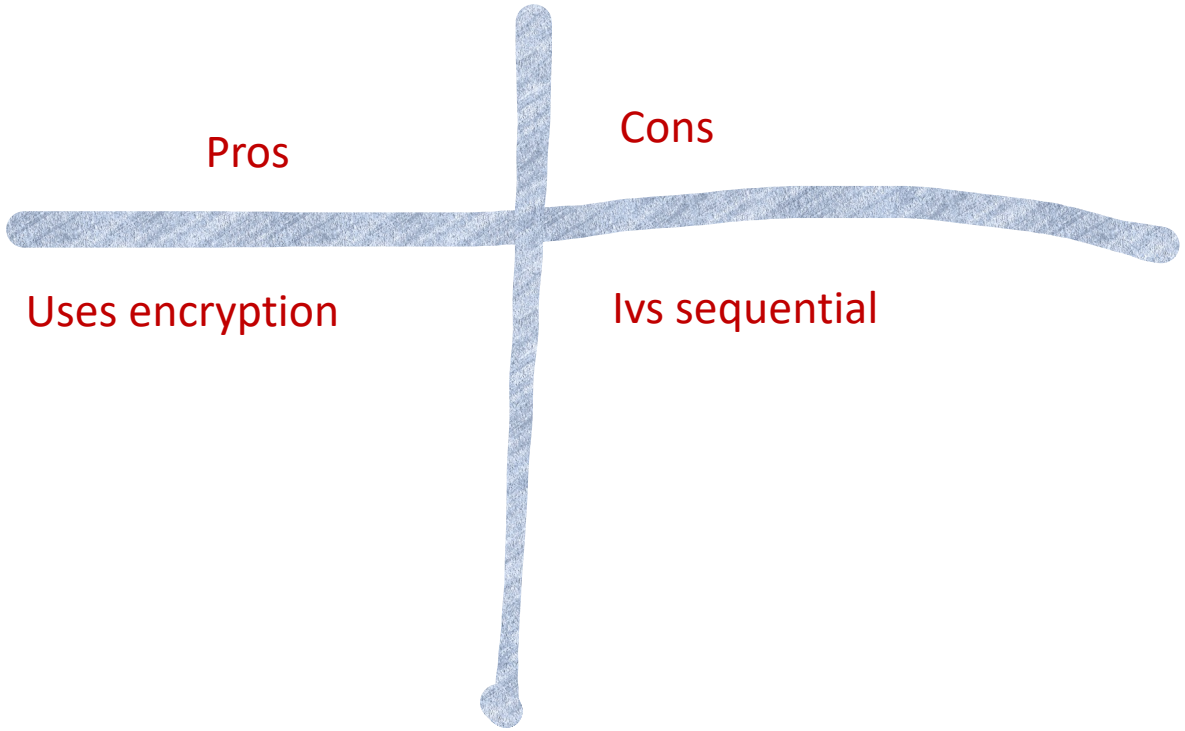
Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format





Continuity Protocol Explained

It's not a bug, it's a feature!

Message Type	Dec Value	Hex Value
AirDrop	5	0x05
Proximity Pairing	7	0x07
Hey Siri	8	0x08
Magic Switch	11	0xb
Handoff	12	0xc
Instant Hotpot	14	0xfe
Nearby Action	15	0xff
Nearby Info	16	0x10
FindMy	18	0x12

Apple Message Types

```
0000  00 e3 80 00 d6 be 89 8e  37 00 d6 be 89 8e 46 25   ........ 7.....F%
0010  76 b6 5b 26 f8 4f 1e ff  4c 00 07 19 01 0f 20 23   v.[&.O.. L..... #
0020  99 8f 01 00 04 cc 89 33  65 18 72 33 c9 3e 1e 39   .......3 e.r3.>.9
0030  28 f5 a1 79 ef b1 83 52                           (..y...R
```

Type 7: Proximity Pairing

Continuity Protocol Explained

It's not a bug, it's a feature!

0 – 7	8 – 15	16 – 23	24 – 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format

```
0000  [redacted]                                        ........ 7.....F%
0010  [redacted]                 07 19 01 0f 20 23      v.[&.O.. L.....  #
0020  99 8f 01 00 04 cc 89 33  65 18 72 33 c9 3e 1e 39  .......3 e.r3.>.9
0030  28 f5 a1 79 ef b1 83 52                           (..y...R
```

Type 7: Proximity Pairing

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000                                                ·····7·····F%
0010                                  19 01 0f 20 23 v·[&·O·· L····· #
0020  99 8f 01 00 04 cc 89 33  65 18 72 33 c9 3e 1e 39 ·······3 e·r3·>·9
0030  28 f5 a1 79 ef b1 83 52                         (··y···R
```

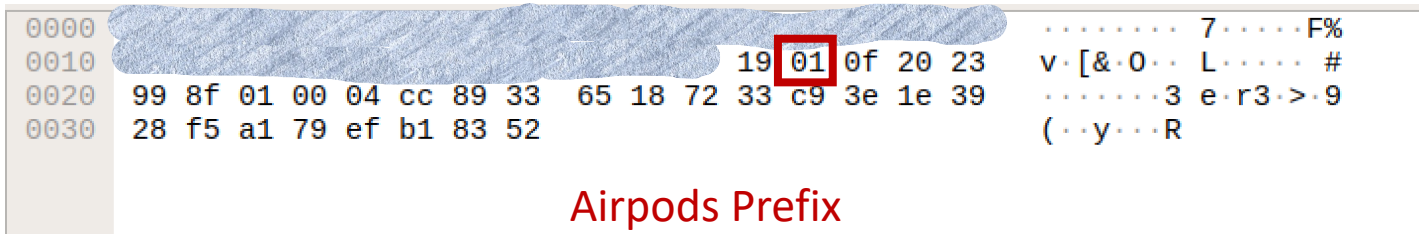
Length =25

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format



Airpods Prefix

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000  [redacted]                                        ·····7·····F%
0010  [redacted]                19 01 0f 20 23   v·[&·O··L·····#
0020  99 8f 01 00 04 cc 89 33  65 18 72 33 c9 3e 1e 39   ·····3e·r3·>·9
0030  28 f5 a1 79 ef b1 83 52                           (··y···R
```

Device Model

```
static const value_string airpods_device_vals[] = {
    { 0x0220, "AirPods 1" },
    { 0x0f20, "AirPods 2" },
    { 0x0e20, "AirPods Pro" },
    { 0x0320, "Powerbeats3" },
    { 0x0520, "BeatsX" },
    { 0x0620, "Beats Solo 3" },
    { 0, NULL}
};
```

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000  [redacted]                                        ·····7·····F%
0010  [redacted]                19 01 0f 20 23   v·[&·O··L·····#
0020  99 8f 01 00 04 cc 89 33  65 18 72 33 c9 3e 1e 39   ·····3e·r3·>·9
0030  28 f5 a1 79 ef b1 83 52                           (··y···R
```

Device Model

```
static const value_string airpods_device_vals[] = {
    { 0x0220, "AirPods 1" },
    { 0x0f20, "AirPods 2" },
    { 0x0e20, "AirPods Pro" },
    { 0x0320, "Powerbeats3" },
    { 0x0520, "BeatsX" },
    { 0x0620, "Beats Solo 3" },
    { 0, NULL}
};
```

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 7.....F%
0010 [redacted]                 19 01 0f 20 23   v.[&.O.. L..... #
0020 99 8f 01 00 04 cc 89 33  65 18 72 33 c9 3e 1e 39   .......3 e.r3.>.9
0030 28 f5 a1 79 ef b1 83 52                     (..y...R
```

Status Codes

Functional🤓 or spooky?👻

```
{ 0x2b, "Both AirPods in ear" },
{ 0x0b, "Both AirPods in ear" },
{ 0x01, "AirPods: Both out of case, not in ear" },
{ 0x21, "Both taken out of ears, Pause Audio" },
{ 0x02, "Right in ear, Left in case" },
{ 0x22, "Left in ear, Right in case" },
{ 0x75, "Case: Both AirPods in case" },
{ 0x55, "Case: Both AirPods in case" },
{ 0x03, "AirPods: Right in ear, Left out of case" },
{ 0x23, "AirPods: Left in ear, Right out of case" },
{ 0x33, "AirPods: Left in ear, Right in case" },
{ 0x53, "Case: Left in ear, Right in case" },
{ 0x13, "AirPods: Right in ear, Left in case" },
{ 0x73, "Case: Right in ear, Left in case" },
{ 0x11, "AirPods: Right out of case, Left in case" },
{ 0x71, "Case: Right out of case, Left in case" },
{ 0x31, "AirPods: Left out of case, Right in case" },
{ 0x51, "Case: Left out of case, Right in case" },
{ 0, NULL}
```

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 7.....F%
0010 [redacted]                 19 01 0f 20 23   v.[&.O.. L..... #
0020 99 8f 01 00 04 cc 89 33  65 18 72 33 c9 3e 1e 39   .......3 e.r3.>.9
0030 28 f5 a1 79 ef b1 83 52                            (..y...R
```

Battery Levels 🔋

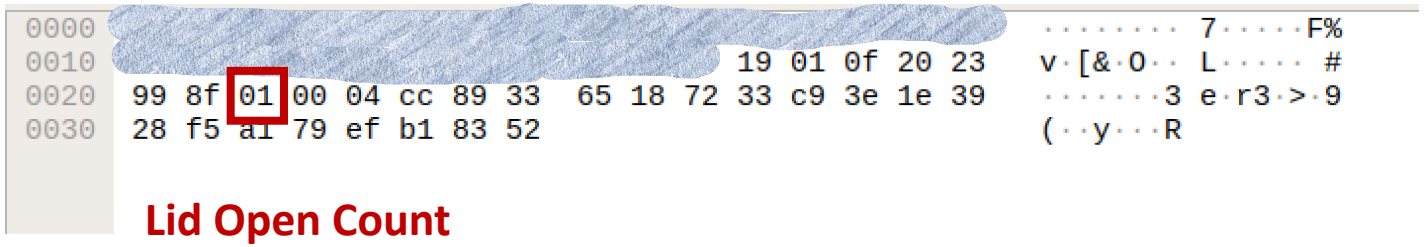
9	9	8	f
Left Airpod	Right Airpod	Is charging? (3bits)	Case

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format



Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000                                                  ........ 7.....F%
0010                                    19 01 0f 20 23  v.[&.O.. L..... #
0020  99 8f 01 00 04 cc 89 33  65 18 72 33 c9 3e 1e 39  .......3 e.r3.>.9
0030  28 f5 a1 79 ef b1 83 52                          (..y...R
```

Device Color

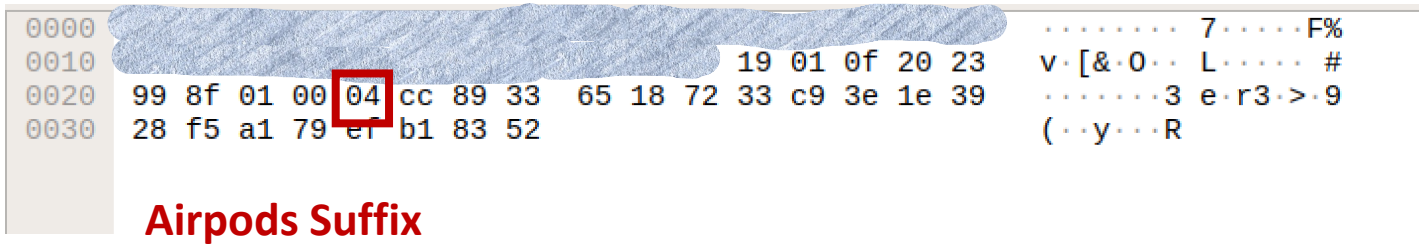
```
{ 0x00, "White" },
{ 0x01, "Black" },
{ 0x02, "Red" },
{ 0x03, "Blue" },
{ 0x04, "Pink" },
{ 0x05, "Gray" },
{ 0x06, "Silver" },
{ 0x07, "Gold" },
{ 0x08, "Rose Gold" },
{ 0x09, "Space Gray" },
{ 0x0A, "Dark Blue" },
{ 0x0B, "Light Blue" },
{ 0x0C, "Yellow" },
```

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format

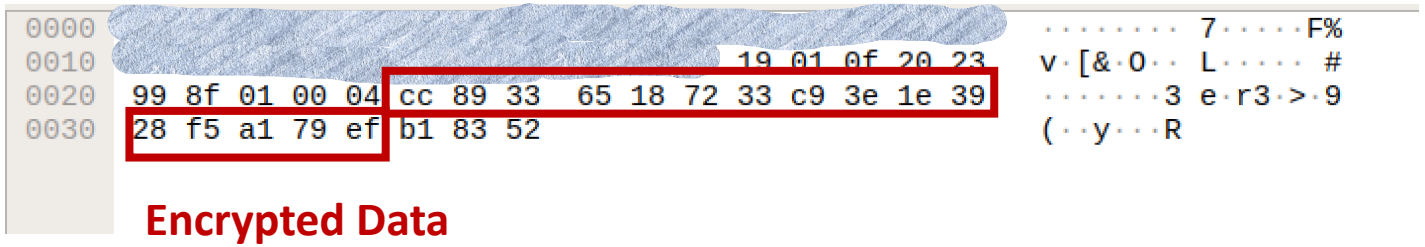


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

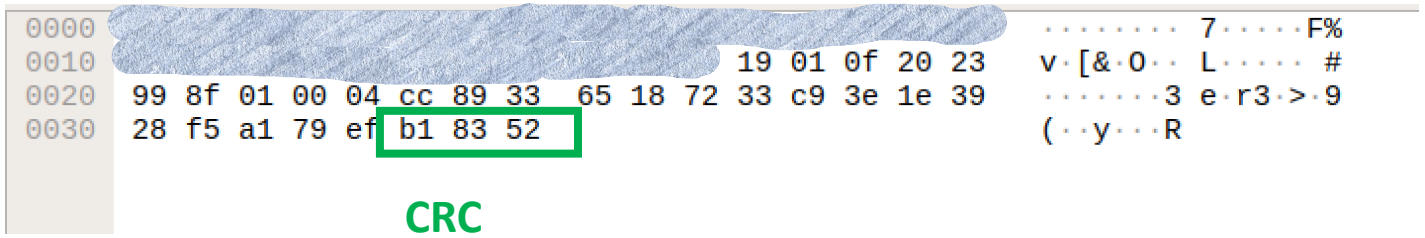


Continuity Protocol Explained

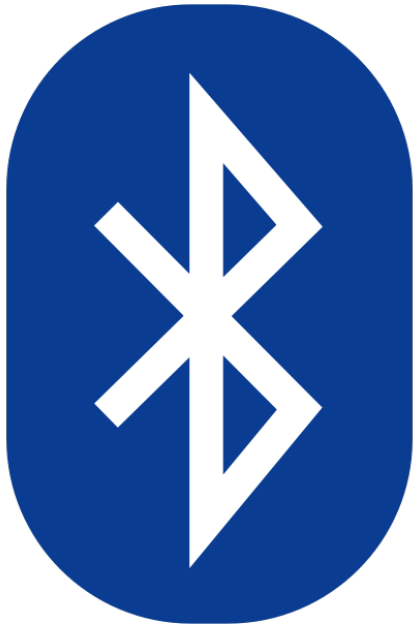
It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

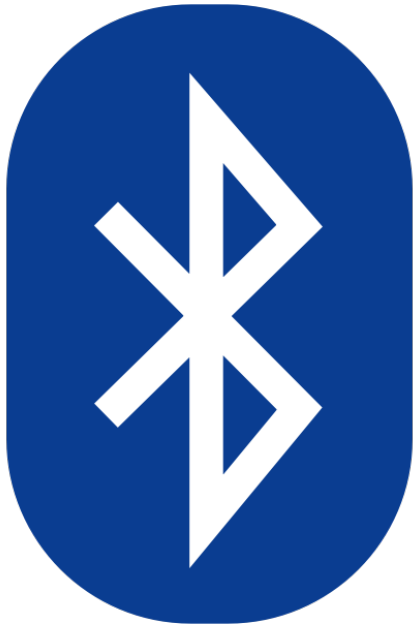


PLEASE TURN OFF
YOUR BLUETOOTH



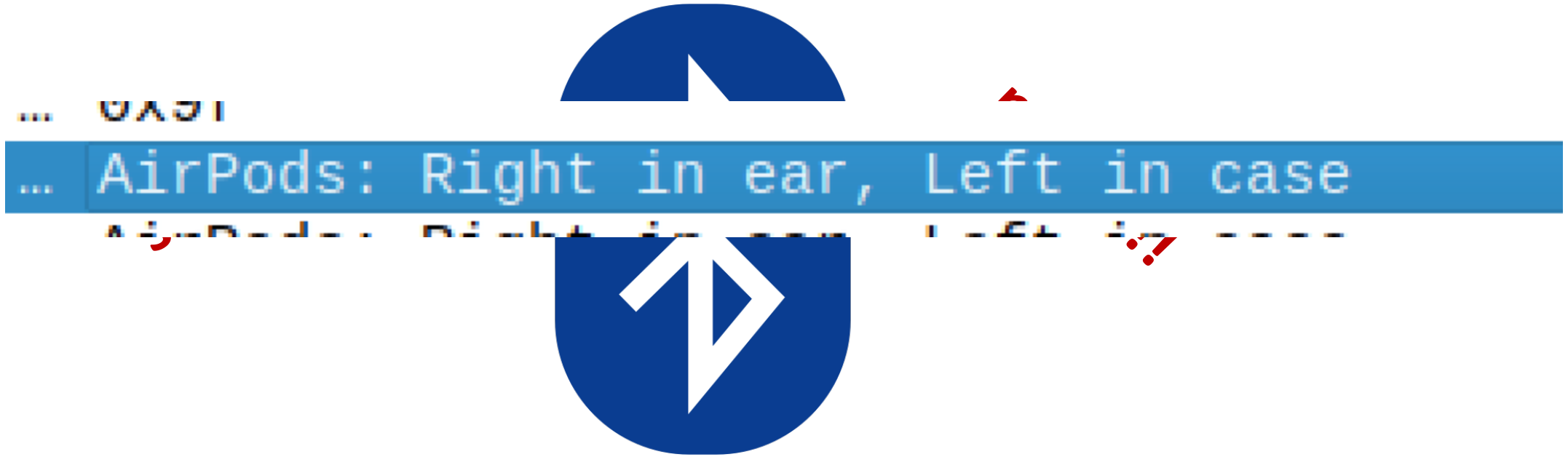
PLEASE TURN OFF YOUR BLUETOOTH

seriously



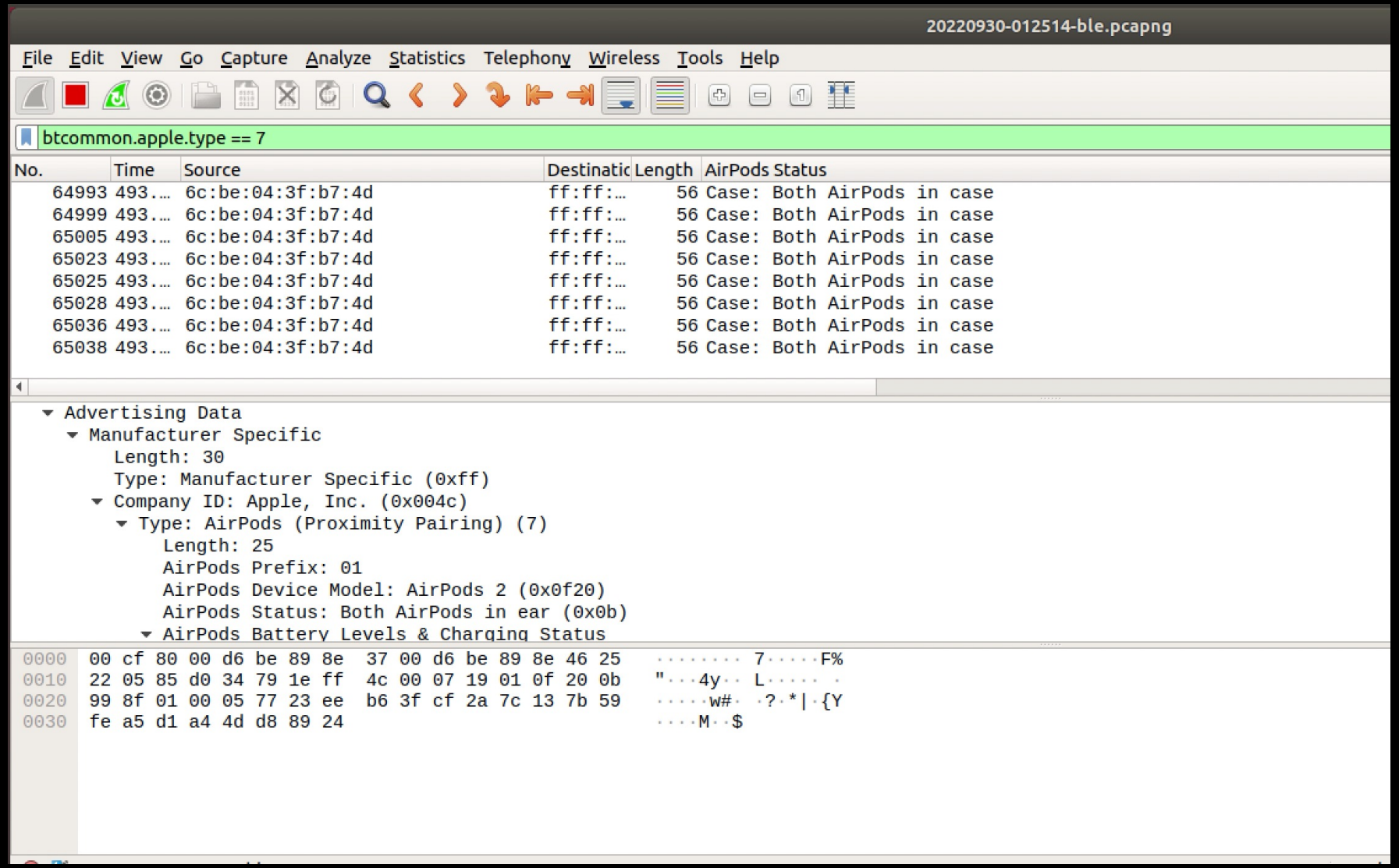
please!!

PLEASE TURN OFF YOUR BLUETOOTH



Demo 🔥

Demo Backup🔥


20220930-012514-ble.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
btcommon.apple.type == 7
No. Time Source Destinatic Length AirPods Status
64993 493.… 6c:be:04:3f:b7:4d ff:ff:… 56 Case: Both AirPods in case
64999 493.… 6c:be:04:3f:b7:4d ff:ff:… 56 Case: Both AirPods in case
65005 493.… 6c:be:04:3f:b7:4d ff:ff:… 56 Case: Both AirPods in case
65023 493.… 6c:be:04:3f:b7:4d ff:ff:… 56 Case: Both AirPods in case
65025 493.… 6c:be:04:3f:b7:4d ff:ff:… 56 Case: Both AirPods in case
65028 493.… 6c:be:04:3f:b7:4d ff:ff:… 56 Case: Both AirPods in case
65036 493.… 6c:be:04:3f:b7:4d ff:ff:… 56 Case: Both AirPods in case
65038 493.… 6c:be:04:3f:b7:4d ff:ff:… 56 Case: Both AirPods in case
Advertising Data
Manufacturer Specific
Length: 30
Type: Manufacturer Specific (0xff)
Company ID: Apple, Inc. (0x004c)
Type: AirPods (Proximity Pairing) (7)
Length: 25
AirPods Prefix: 01
AirPods Device Model: AirPods 2 (0x0f20)
AirPods Status: Both AirPods in ear (0x0b)
AirPods Battery Levels & Charging Status
0000 00 cf 80 00 d6 be 89 8e 37 00 d6 be 89 8e 46 25
0010 22 05 85 d0 34 79 1e ff 4c 00 07 19 01 0f 20 0b
0020 99 8f 01 00 05 77 23 ee b6 3f cf 2a 7c 13 7b 59
0030 fe a5 d1 a4 4d d8 89 24

Continuity Protocol Explained

It's not a bug, it's a feature!

AirTag

npr

WAMU 88.5
AMERICAN UNIVERSITY RADIO

TECHNOLOGY

AirTags are being used
and cars. Here's what

AirTag stalking: What is it, and how can I avoid it?

people
ne about

'I didn't want it anywhere n
how the Apple AirTag b
stalkers

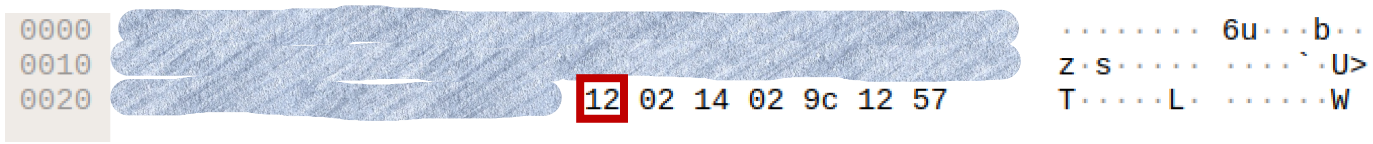
theguardian

me':
ift to

Continuity Protocol Explained

It's not a bug, it's a feature!

Message Type	Dec Value	Hex Value
AirDrop	5	0x05
Proximity Pairing	7	0x07
Hey Siri	8	0x08
Magic Switch	11	0xb
Handoff	12	0xc
Instant Hotpot	14	0xfe
Nearby Action	15	0xff
Nearby Info	16	0x10
FindMy	18	0x12



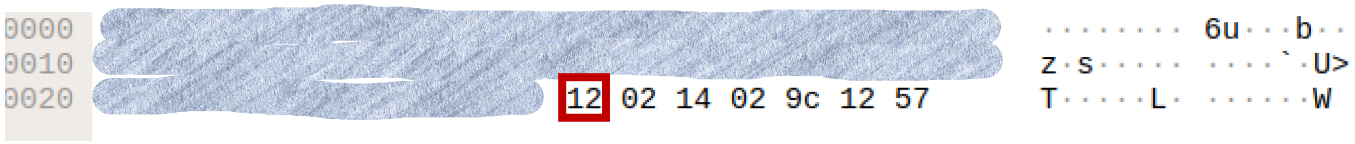
Type 18: Find My

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



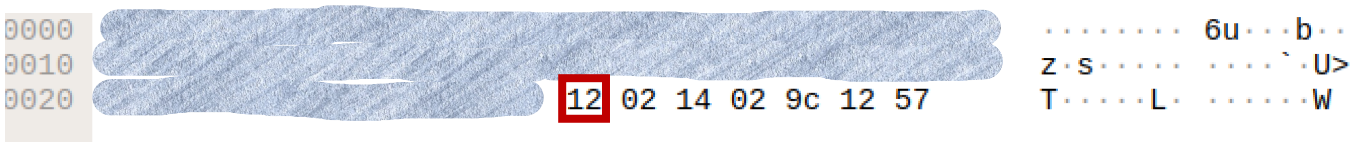
Type 18: Find My

Continuity Protocol Explained

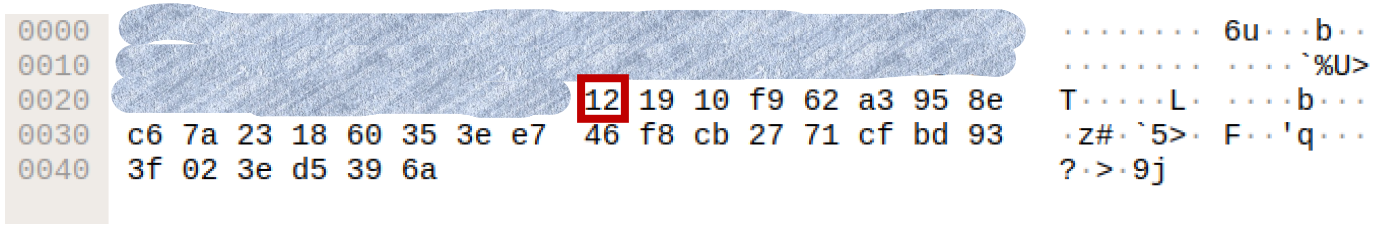
It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



Type 18: Find My



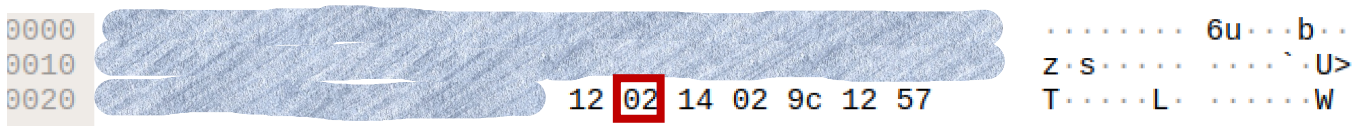
Type 18: Find My

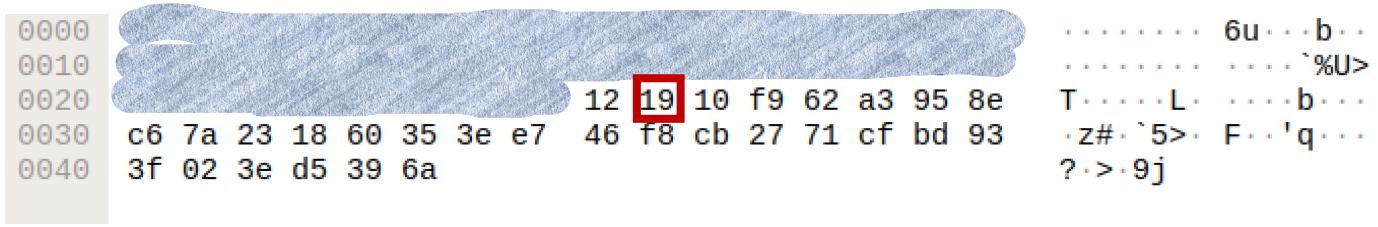
Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format





Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted]                                  z·s····· ····`·U>
0020 [redacted] 12 02 14 02 9c 12 57             T·····L· ·····W
```

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted]                                  ........ ····`%U>
0020 [redacted] 12 19 10 f9 62 a3 95 8e          T·····L· ····b···
0030 c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   ·z#·`5>· F··'q···
0040 3f 02 3e d5 39 6a                           ?·>·9j
```

PAUSE: WHY ARE THESE DIFFERENT?!

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 6u...b..
0010 [redacted]                                  z.s..... ....`.U>
0020 [redacted] 12 02 14 02 9c 12 57             T.....L. ......W
```

Nearby

```
0000 [redacted]                                  ........ 6u...b..
0010 [redacted]                                  ........ ....`%U>
0020 [redacted] 12 19 10 f9 62 a3 95 8e          T.....L. ....b...
0030 c6 7a 23 18 60 35 3e e7 46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040 3f 02 3e d5 39 6a                           ?.>.9j
```

PAUSE: WHY ARE THESE DIFFERENT?!

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted]                                  z·s····· ····`·U>
0020 [redacted] 12 02 14 02 9c 12 57             T·····L· ·····W
```

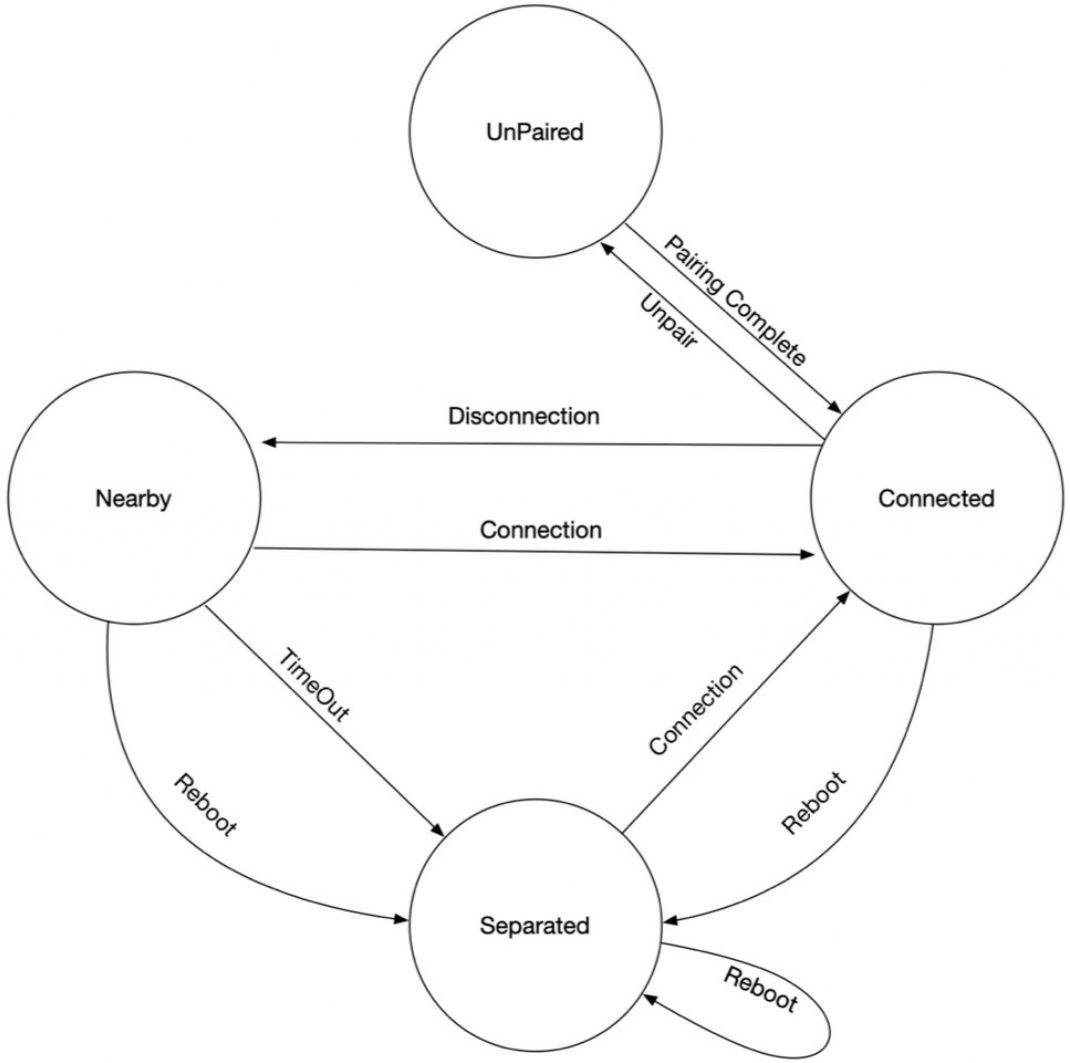
Nearby

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted]                                  ........ ····`%U>
0020 [redacted] 12 19 10 f9 62 a3 95 8e          T·····L· ····b···
0030 c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   ·z#·`5>· F··'q···
0040 3f 02 3e d5 39 6a                           ?·>·9j
```

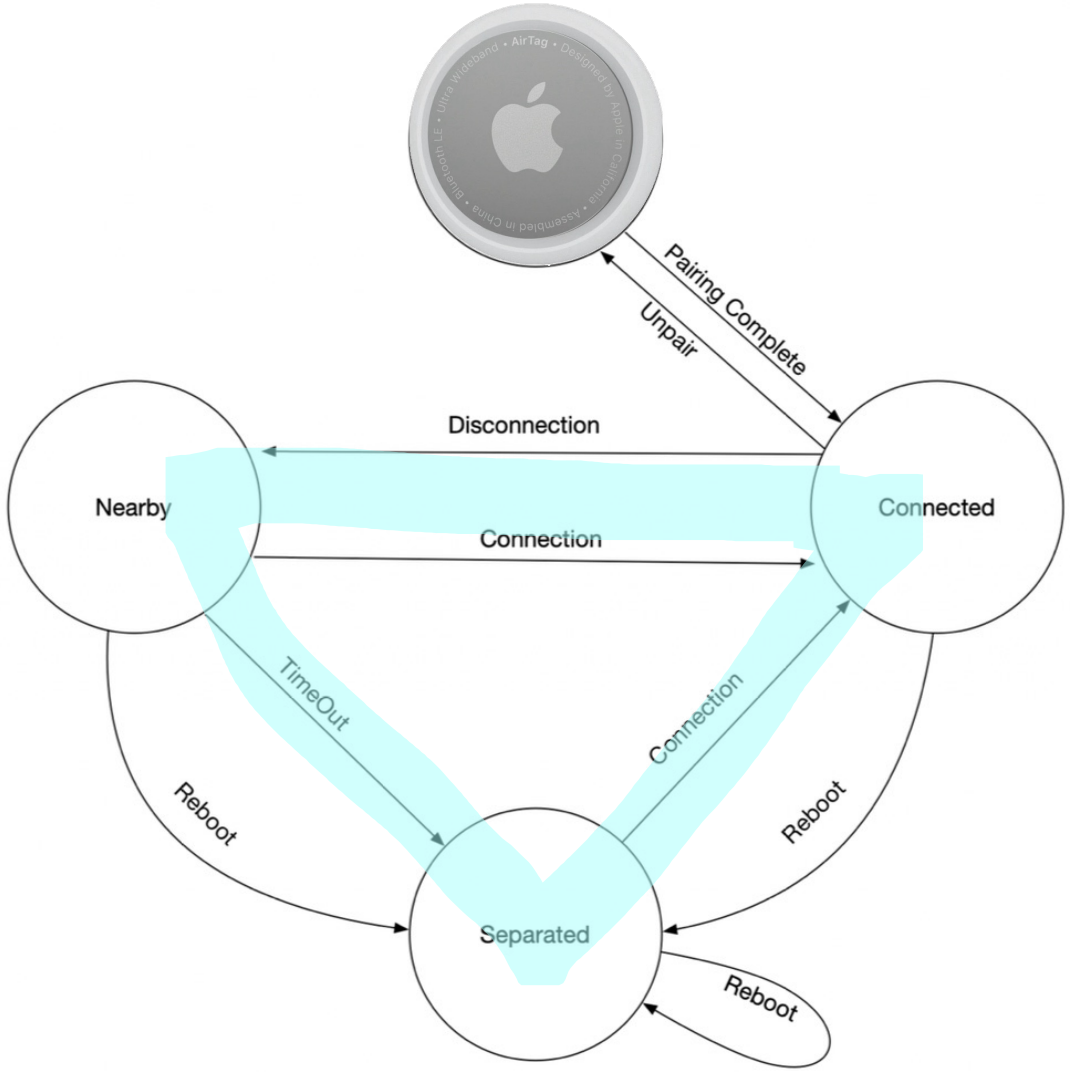
Separated

PAUSE: WHY ARE THESE DIFFERENT?!

The State Machine of the AirTag



The State Machine of the AirTag



Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted]                                  z·s····· ····`·U>
0020 [redacted] 12 02 14 02 9c 12 57             T·····L· ·····W
```

Nearby

```
0000 [redacted]                                  ........ 6u···b··
0010 [redacted]                                  ........ ····`%U>
0020 [redacted] 12 19 10 f9 62 a3 95 8e          T·····L· ····b···
0030 c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   ·z#·`5>· F··'q···
0040 3f 02 3e d5 39 6a                           ?·>·9j
```

Separated

PAUSE: WHY ARE THESE DIFFERENT?!

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 6u...b..
0010 [redacted]                                  z.s..... ....`.U>
0020 [redacted] 12 02 14 02 9c 12 57             T.....L. ......W
```

Length = 2

Nearby

```
0000 [redacted]                                  ........ 6u...b..
0010 [redacted]                                  ........ ....`%U>
0020 [redacted] 12 19 10 f9 62 a3 95 8e          T.....L. ....b...
0030 c6 7a 23 18 60 35 3e e7 46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040 3f 02 3e d5 39 6a                           ?.>.9j
```

Separated

PAUSE: WHY ARE THESE DIFFERENT?!

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000 [redacted]                                  ........ 6u...b..
0010 [redacted]                                  z.s..... ....`.U>
0020 [redacted] 12 02 14 02 9c 12 57             T.....L. ......W
```

Length = 2

2 bytes

Nearby

```
0000 [redacted]                                  ........ 6u...b..
0010 [redacted]                                  ........ ....`%U>
0020 [redacted] 12 19 10 f9 62 a3 95 8e          T.....L. ....b...
0030 c6 7a 23 18 60 35 3e e7 46 f8 cb 27 71 cf bd 93  .z#.`5>. F..'q...
0040 3f 02 3e d5 39 6a                           ?.>.9j
```

Separated

PAUSE: WHY ARE THESE DIFFERENT?!

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

```
0000  [redacted]                                  ........ 6u···b··
0010  [redacted]                                  z·s····· ····`·U>
0020  [redacted] 12 02 14 02 9c 12 57             T·····L· ·····W
```

Length = 2

2 bytes

Nearby

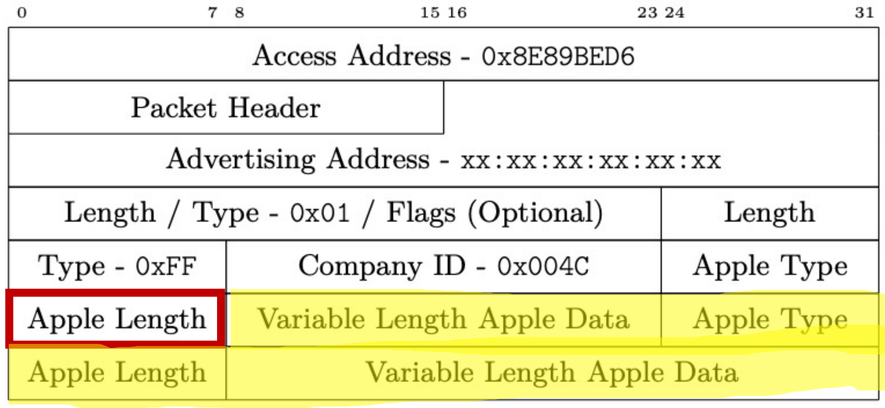
```
0000  [redacted]                                  ........ 6u···b··
0010  [redacted]                                  ........ ····`%U>
0020  [redacted] 12 19 10 f9 62 a3 95 8e          T·····L· ····b···
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   ·z#·`5>· F··'q···
0040  3f 02 3e d5 39 6a                          ?·>·9j
```

Separated

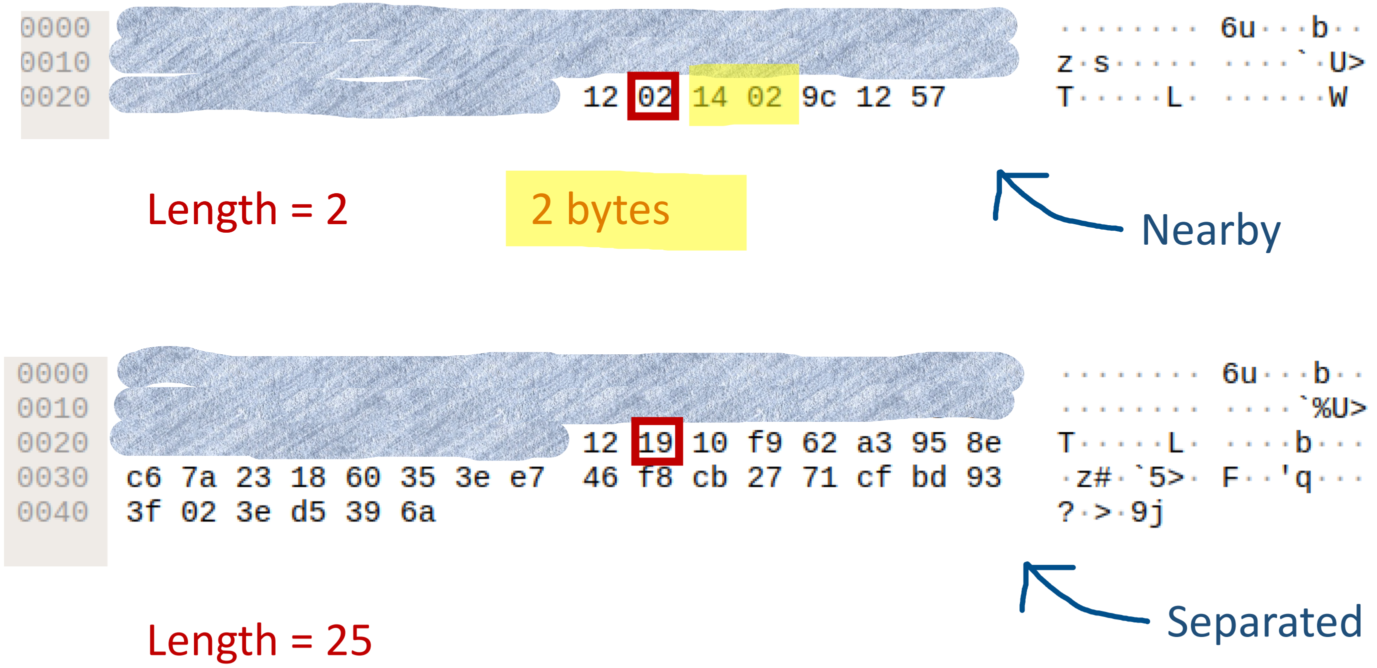
PAUSE: WHY ARE THESE DIFFERENT?!

Continuity Protocol Explained

It's not a bug, it's a feature!



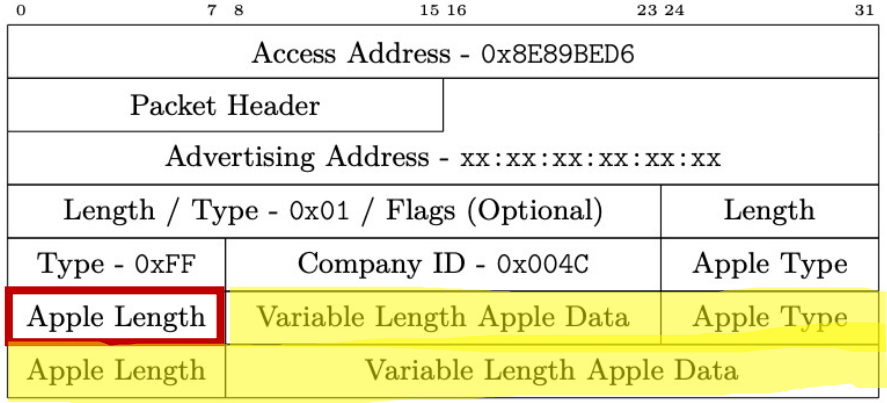
Apple BLE Frame Format



PAUSE: WHY ARE THESE DIFFERENT?!

Continuity Protocol Explained

It's not a bug, it's a feature!



Apple BLE Frame Format

```
0000 ·····  6u···b··
0010 ·····  ····`·U>
0020 12 02 14 02 9c 12 57  T·····L·  ·····W
```

Length = 2

2 bytes

Nearby

```
0000 ·····  6u···b··
0010 ·····  ····`%U>
0020 12 19 10 f9 62 a3 95 8e  T·····L·  ····b···
0030 c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93  ·z#·`5>·  F··'q···
0040 3f 02 3e d5 39 6a  ?·>·9j
```

Length = 25

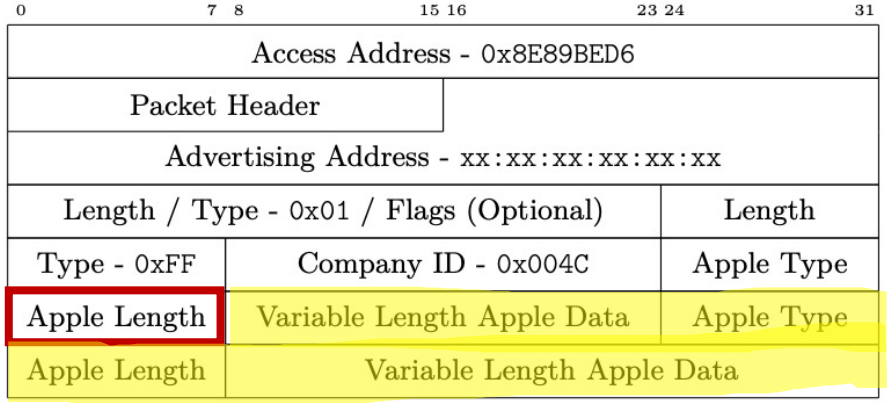
25 bytes

Separated

PAUSE: WHY ARE THESE DIFFERENT?!

Continuity Protocol Explained

It's not a bug, it's a feature!



Apple BLE Frame Format

```
0000  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· 6u ·· ·b ··
0010  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0020  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0030  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0040  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0050  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0060  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0070  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0080  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0090  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00a0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00b0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00c0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00d0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00e0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00f0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0100  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0110  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0120  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0130  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0140  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0150  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0160  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0170  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0180  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0190  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01a0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01b0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01c0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01d0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01e0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01f0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
```

Length = 2

2 bytes

Nearby

```
0000  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· 6u ·· ·b ··
0010  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0020  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0030  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0040  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0050  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0060  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0070  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0080  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0090  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00a0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00b0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00c0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00d0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00e0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
00f0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0100  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0110  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0120  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0130  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0140  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0150  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0160  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0170  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0180  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
0190  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01a0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01b0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01c0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01d0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01e0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
01f0  ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··
```

Length = 25

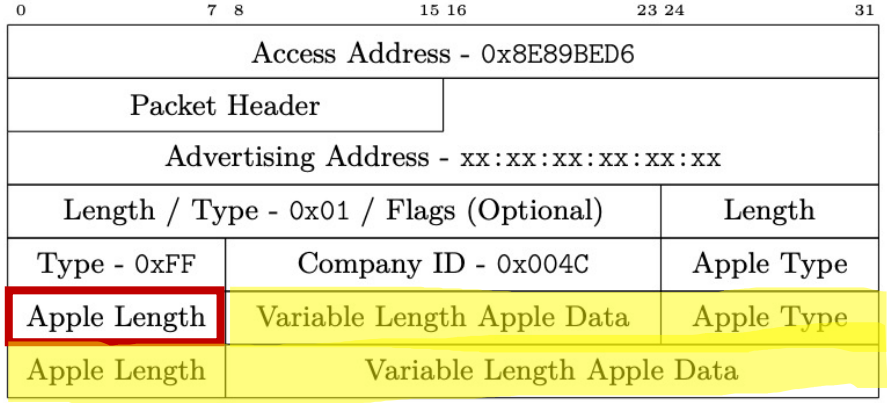
25 bytes

Separated

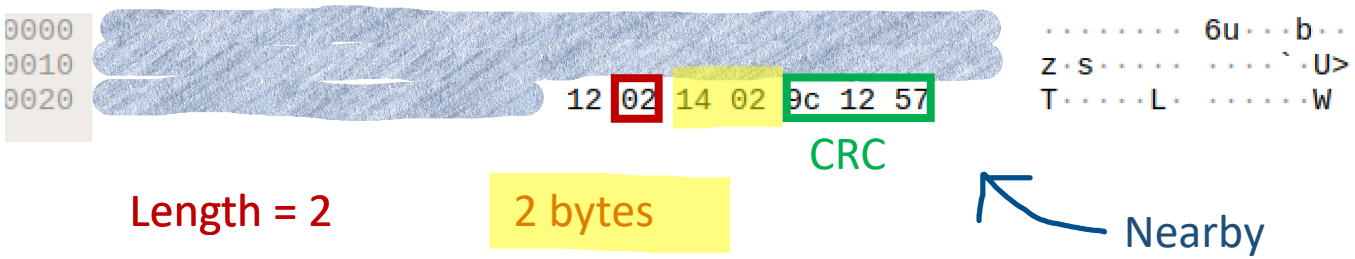
PAUSE: WHY ARE THESE DIFFERENT?!

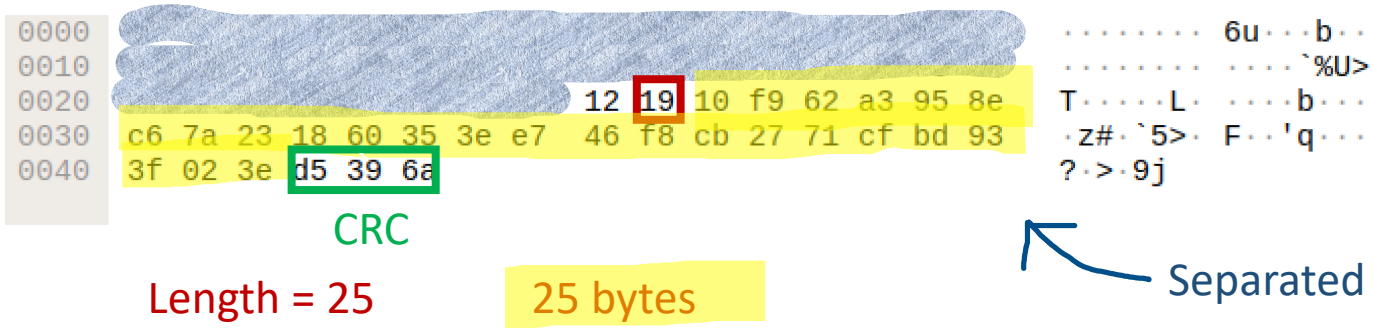
Continuity Protocol Explained

It's not a bug, it's a feature!



Apple BLE Frame Format

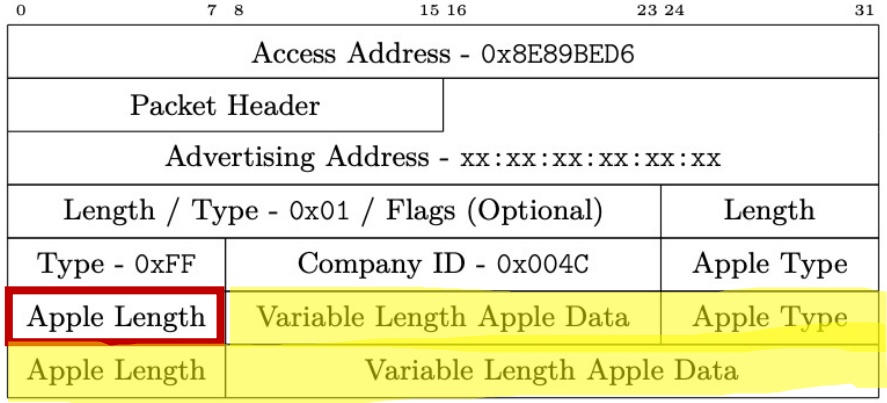




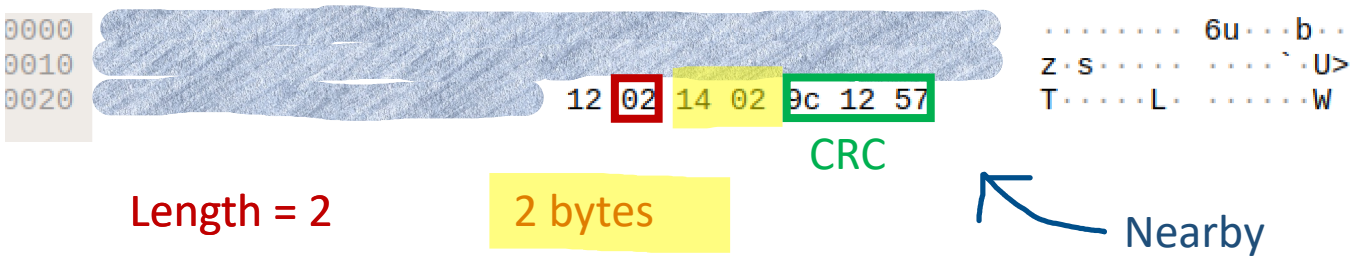
PAUSE: WHY ARE THESE DIFFERENT?!

Continuity Protocol Explained

It's not a bug, it's a feature!



Apple BLE Frame Format

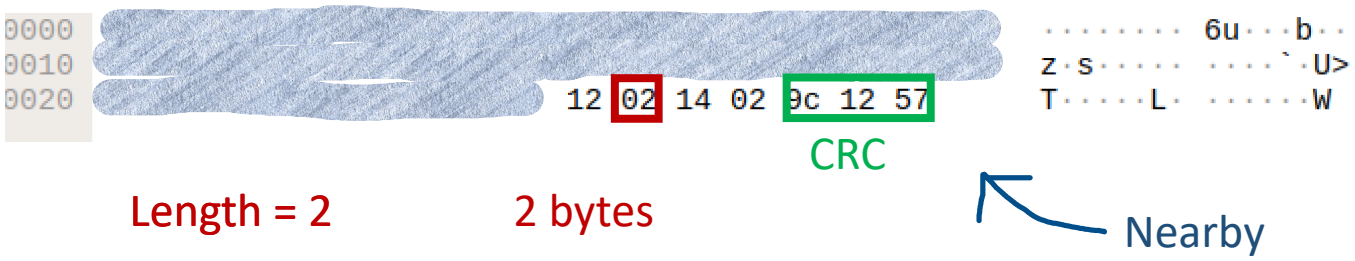


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

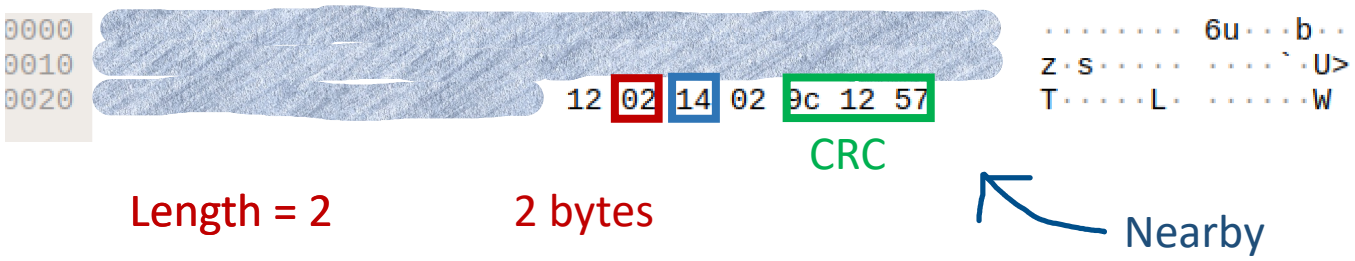


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

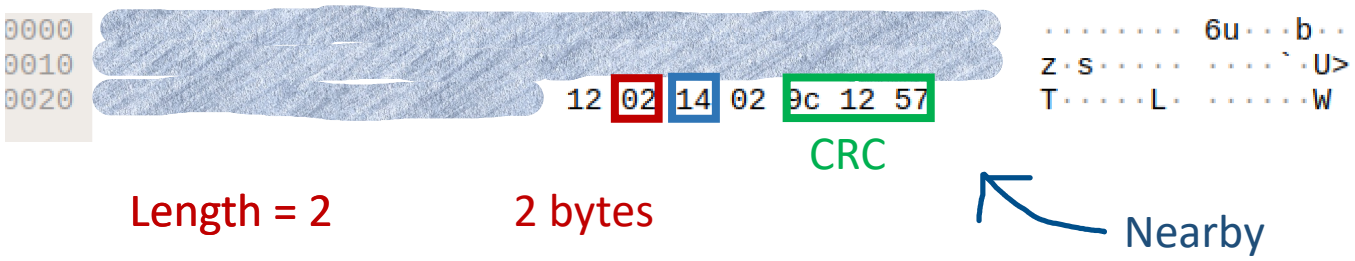


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



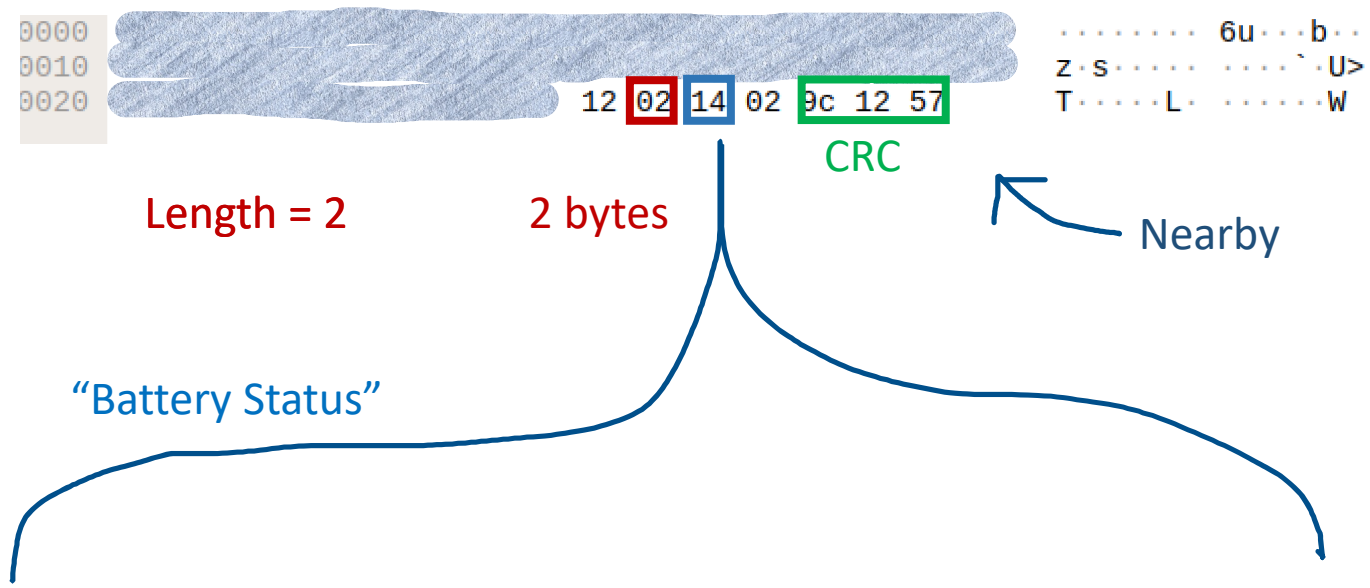
"Battery Status"

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



Continuity Protocol Explained

It's not a bug, it's a feature!

0	7	8	15	16	23	24	31
Access Address - 0x8E89BED6							
Packet Header							
Advertising Address - xx:xx:xx:xx:xx:xx							
Length / Type - 0x01 / Flags (Optional)							Length
Type - 0xFF		Company ID - 0x004C					Apple Type
Apple Length		Variable Length Apple Data					Apple Type
Apple Length		Variable Length Apple Data					

Apple BLE Frame Format

CRC

Length = 2

2 bytes

Nearby

"Battery Status"

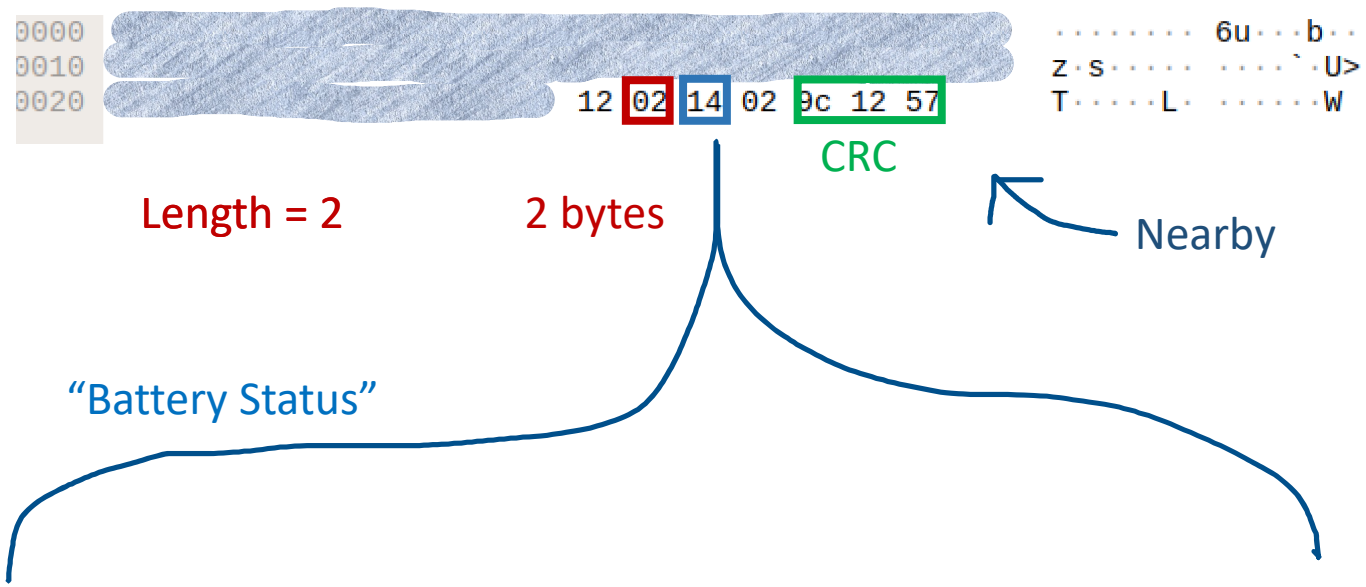
7	6	5	4	3	2	1	0

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



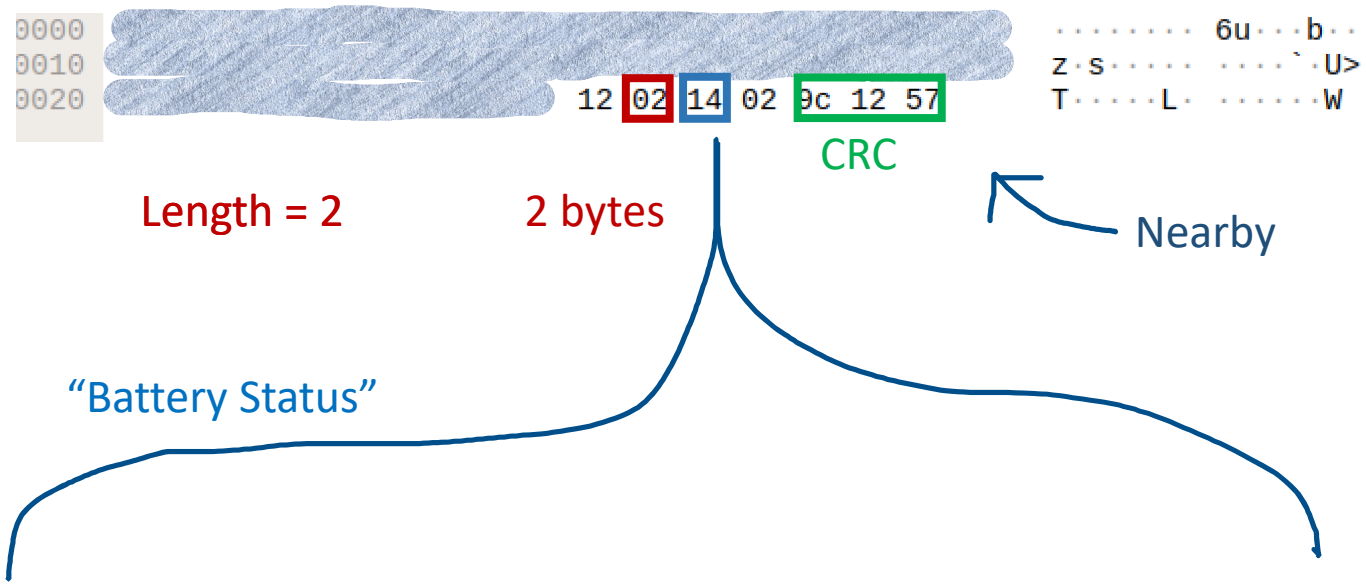
7	6	5	4	3	2	1	0
0	0	0	1	0	1	0	0

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7	8	15	16	23	24	31
Access Address - 0x8E89BED6							
Packet Header							
Advertising Address - xx:xx:xx:xx:xx:xx							
Length / Type - 0x01 / Flags (Optional)							Length
Type - 0xFF		Company ID - 0x004C					Apple Type
Apple Length		Variable Length Apple Data					Apple Type
Apple Length		Variable Length Apple Data					

Apple BLE Frame Format



4.5.3.4.13. Battery status

Description

0 = Full
1 = Medium
2 = Low
3 = Critically low

7	6	5	4	3	2	1	0
0	0	0	1	0	1	0	0
Battery	Battery	Reserved	Tracking	Reserved	Maintained	Reserved	Reserved

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

CRC

Length = 2

2 bytes

Nearby

"Battery Status"

4.5.3.4.13. Battery status

Description

0 = Full
1 = Medium
2 = Low
3 = Critically low

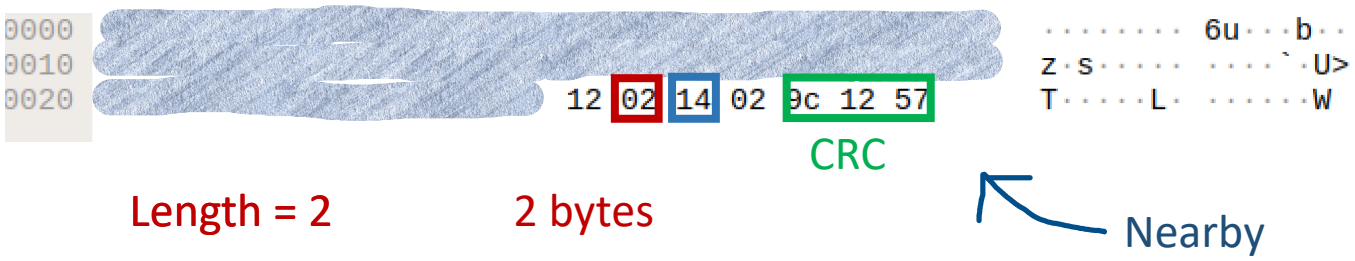
7	6	5	4	3	2	1	0
0	0	0	1	0	1	0	0
Battery	Battery	Reserved	Tracking	Reserved	Maintained	Reserved	Reserved

OLD tracking bit!

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			



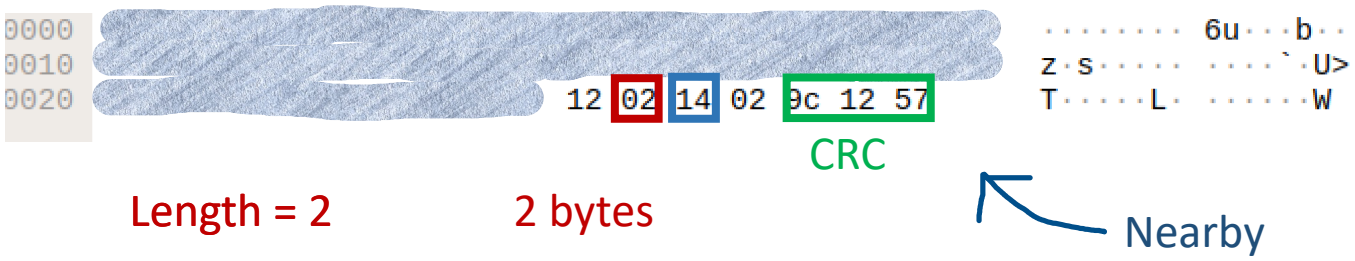

```
static const value_string findmy_status_vals[] = {
    { 0x00, "Owner did not connect within key rotation period (15 min.)" },
    { 0xe4, "Owner connected within key roation period, Battery Critically Low" },
    { 0xa4, "Owner connected within key roation period, Battery Low" },
    { 0x64, "Owner connected within key roation period, Battery Medium" },
    { 0x24, "Owner connected with key roation period, Battery Full" },
};
```

DISSECTOR CODE

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			



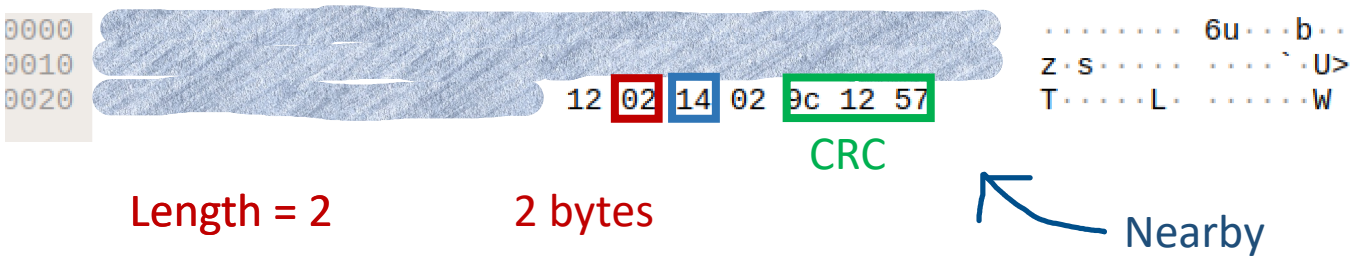

```
static const
    { 0x00,
    { 0xe4,
    { 0xa4,
    { 0x64,
    { 0x24,
};
```

Old Left nibble	Bit 5 tracking	Bit 4 tracking	New Left nibble
0	0000	0000	0
e	1110	1101	d
a	1010	1001	9
6	0110	0101	5
2	0010	0001	1

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		




```
static const value_string findmy_status_vals[] = {
    { 0x00,  -> 0x00                    in key rotation period (15 min.)" },
    { 0xe4,  -> 0xd4                    roation period, Battery Critically Low" },
    { 0xa4,  -> 0x94                    roation period, Battery Low" },
    { 0x64,  -> 0x54                    roation period, Battery Medium" },
    { 0x24,  -> 0x14                    oation period, Battery Full" },
};
```

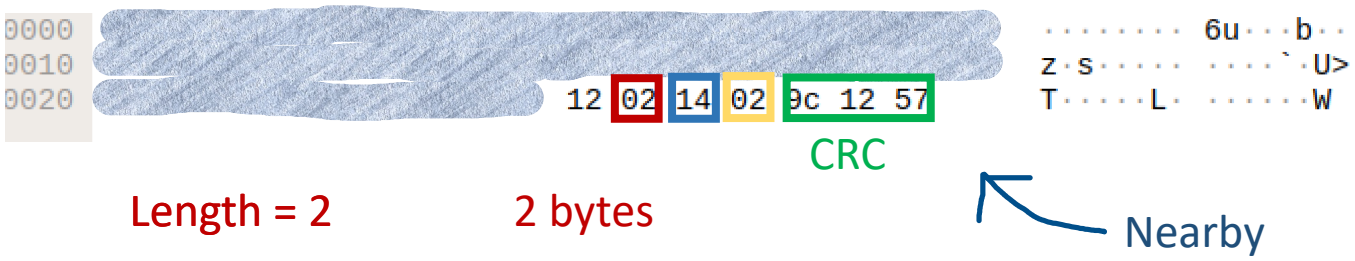
DISSECTOR CODE

Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format

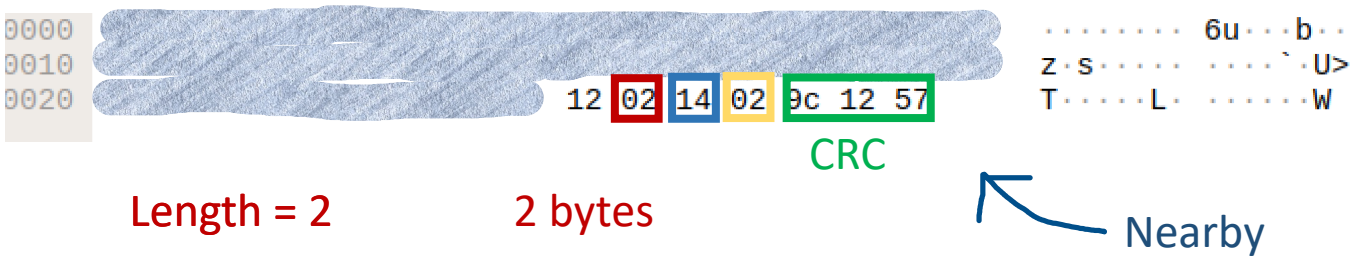


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

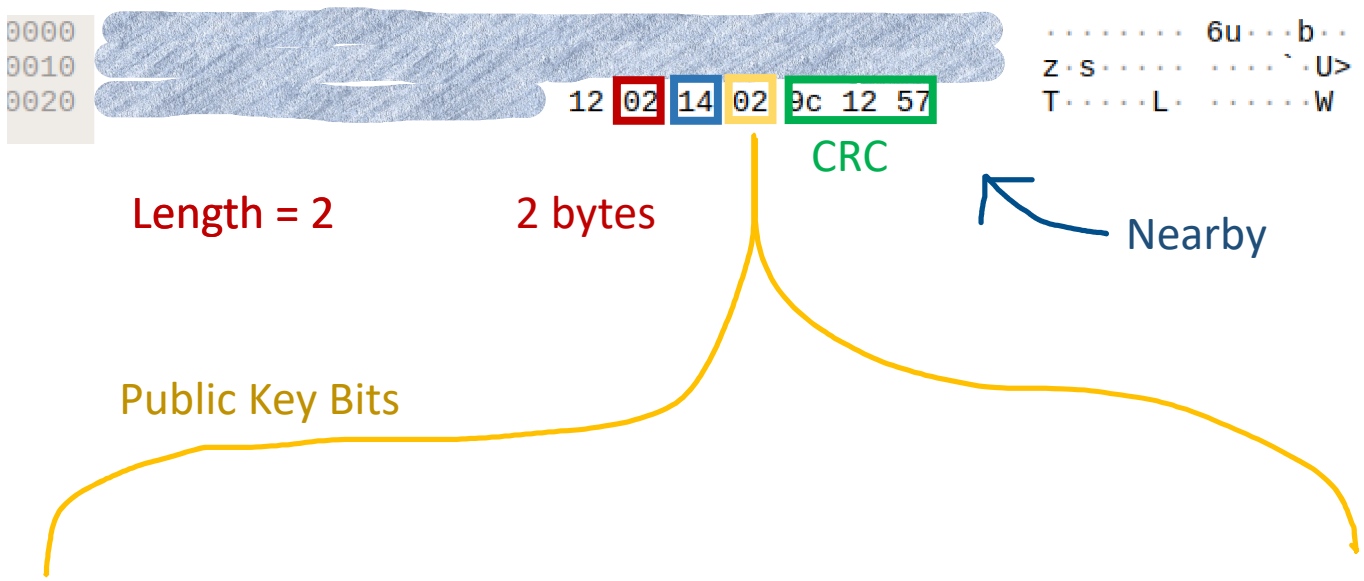


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

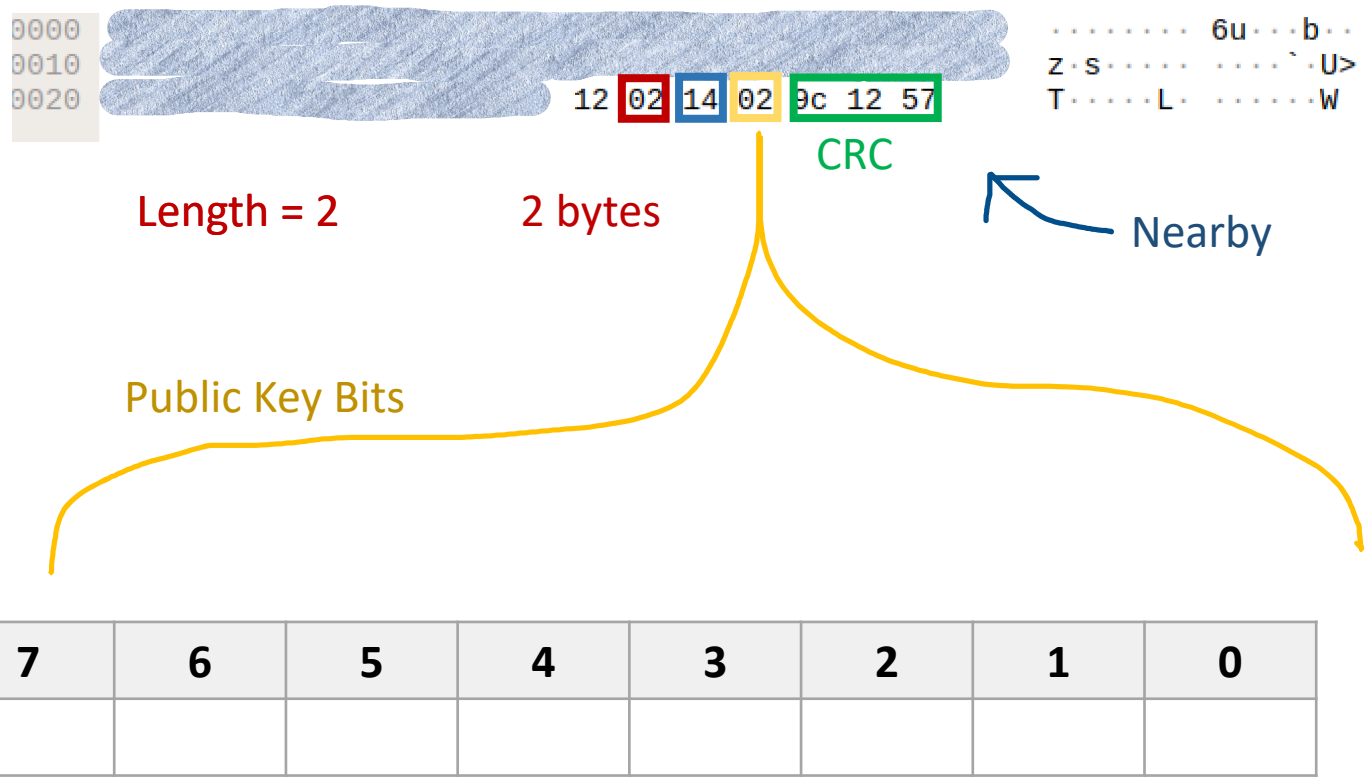


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



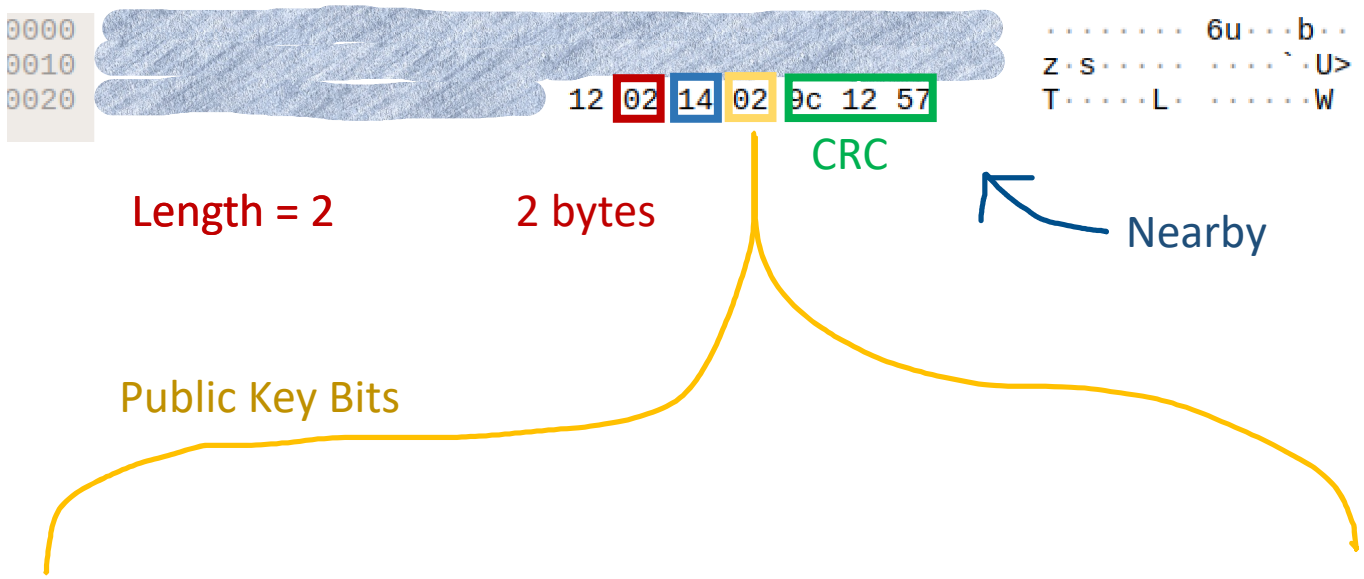
7	6	5	4	3	2	1	0

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7	8	15	16	23	24	31
Access Address - 0x8E89BED6							
Packet Header							
Advertising Address - xx:xx:xx:xx:xx:xx							
Length / Type - 0x01 / Flags (Optional)							Length
Type - 0xFF		Company ID - 0x004C					Apple Type
Apple Length		Variable Length Apple Data					Apple Type
Apple Length		Variable Length Apple Data					

Apple BLE Frame Format



7	6	5	4	3	2	1	0
0	0	0	0	0	0	1	0

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7	8	15	16	23	24	31
Access Address - 0x8E89BED6							
Packet Header							
Advertising Address - xx:xx:xx:xx:xx:xx							
Length / Type - 0x01 / Flags (Optional)							Length
Type - 0xFF		Company ID - 0x004C					Apple Type
Apple Length		Variable Length Apple Data					Apple Type
Apple Length		Variable Length Apple Data					

Apple BLE Frame Format

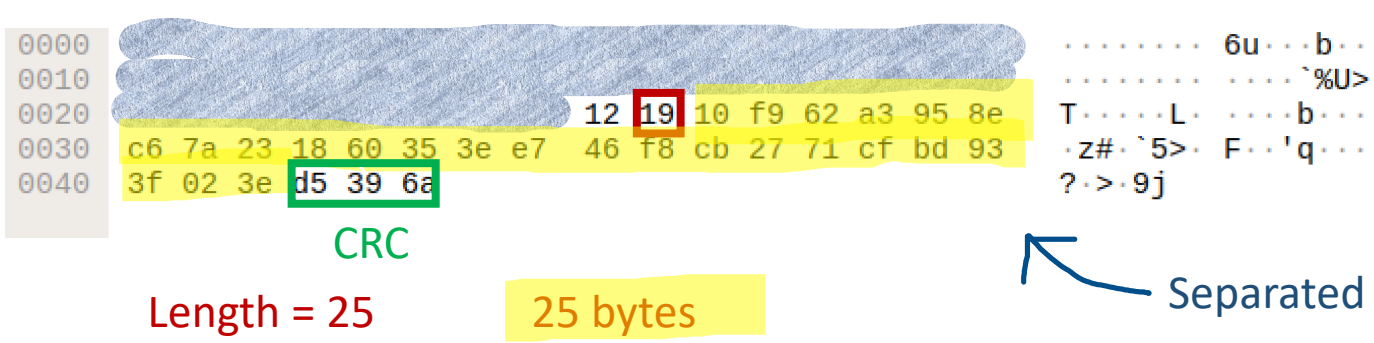
7	6	5	4	3	2	1	0
0	0	0	0	0	0	1	0
Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Pub Key	Pub Key

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

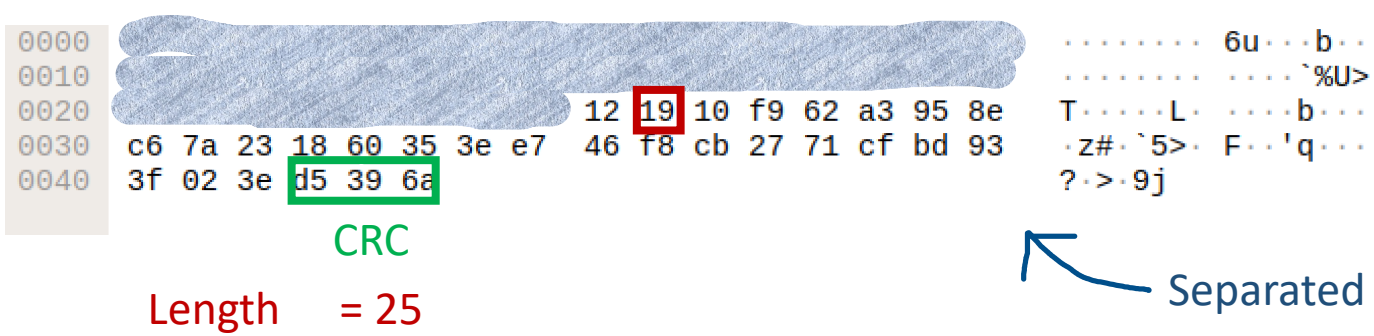


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

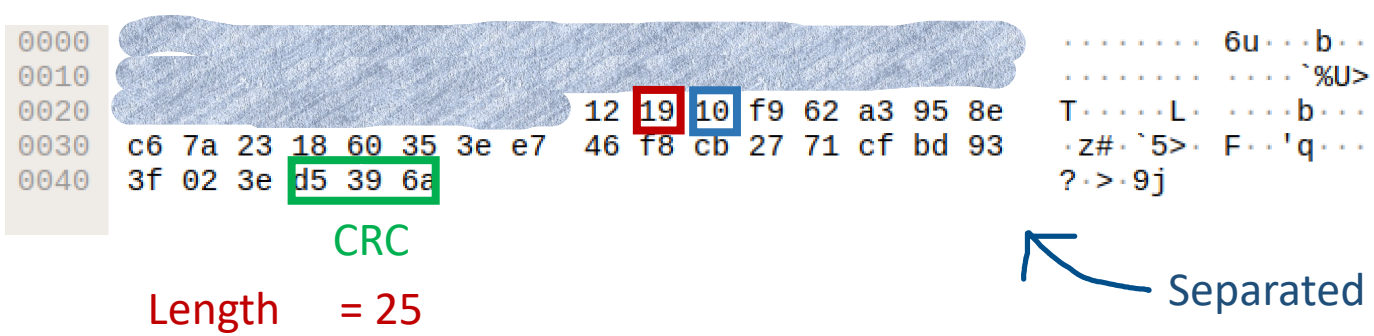


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

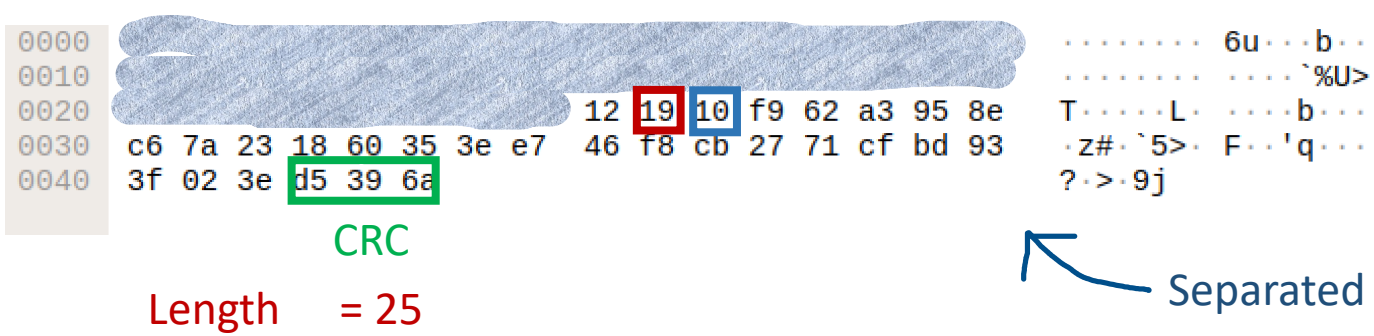


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

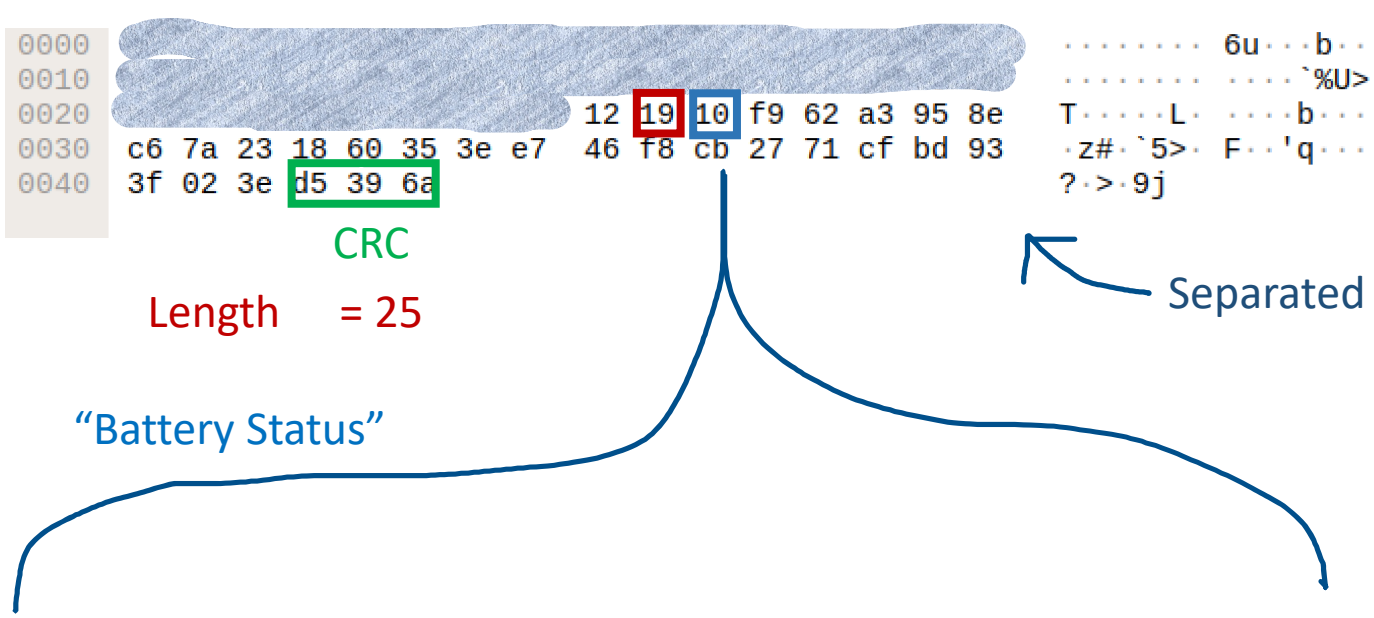


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

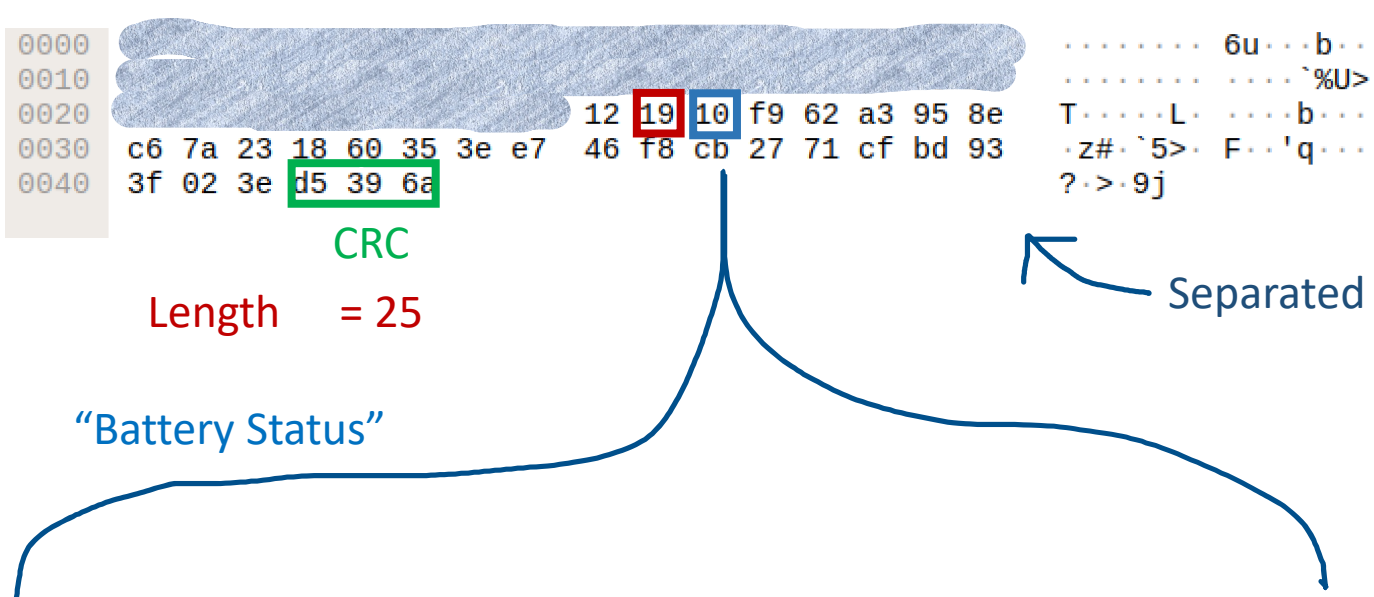


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



4.5.3.4.13. Battery status

Description

0 = Full
1 = Medium
2 = Low
3 = Critically low

7	6	5	4	3	2	1	0
0	0	0	1	0	0	0	0
Battery	Battery	Reserved	Tracking	Reserved	Maintained	Reserved	Reserved

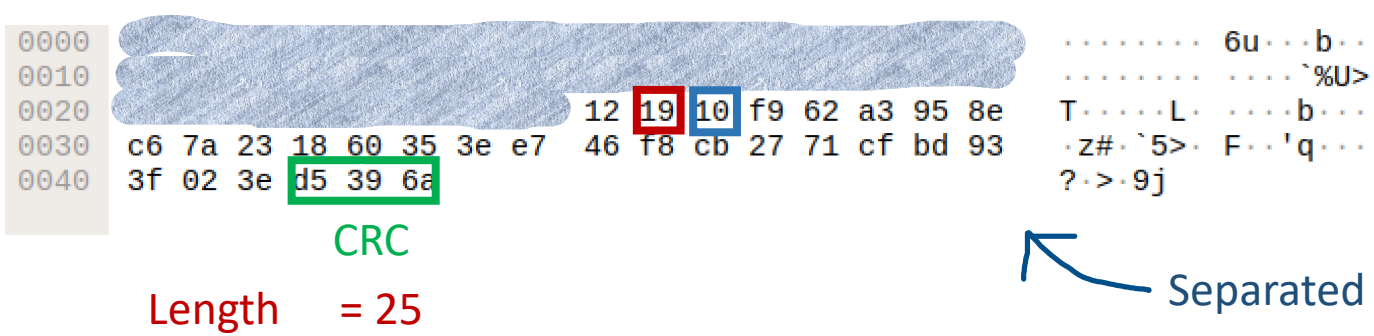
Disconnected

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

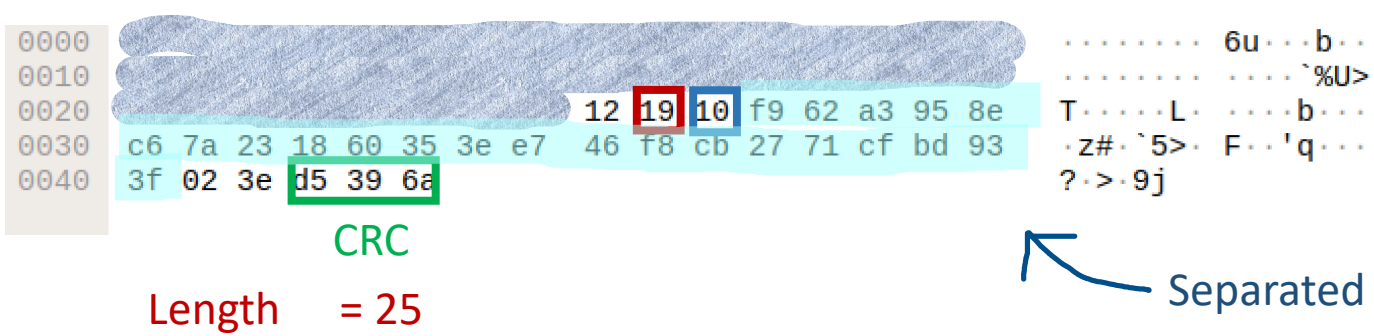


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

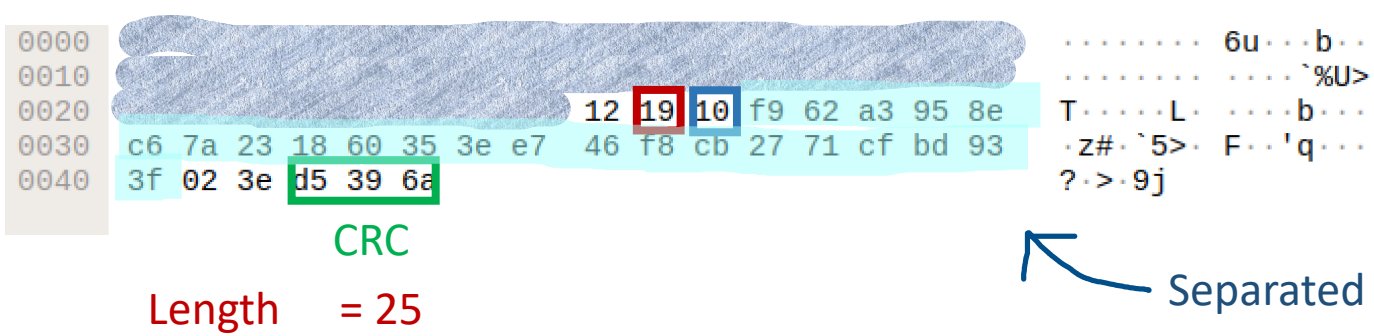


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

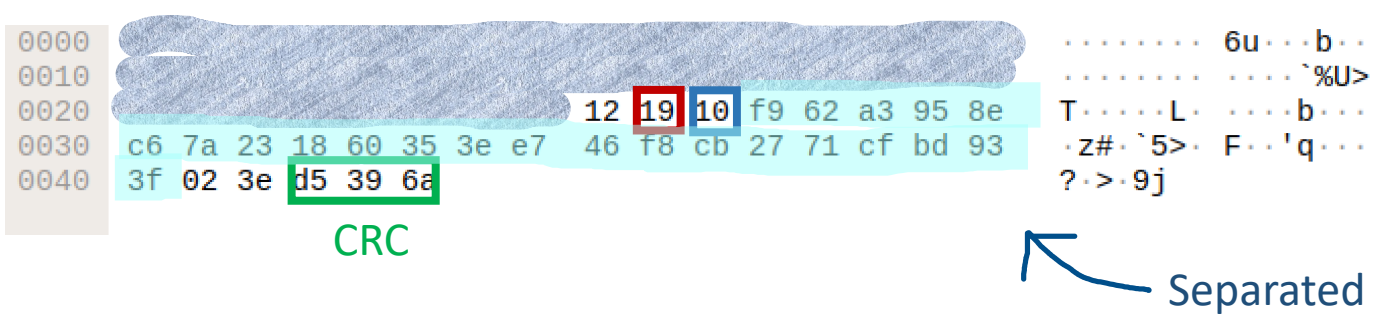


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

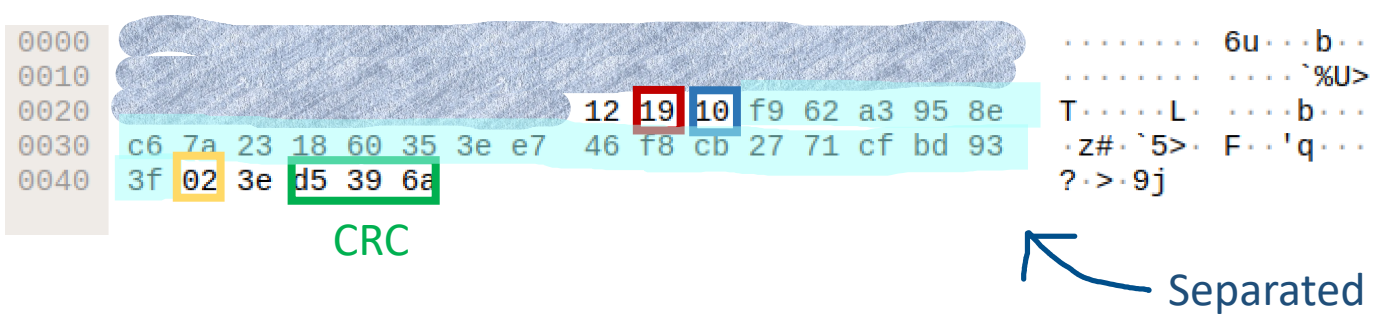


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

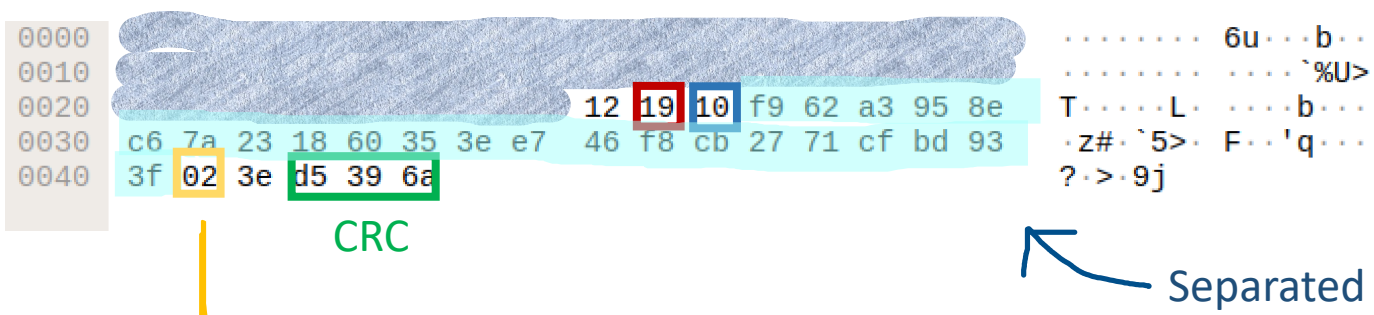


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



Continuity Protocol Explained

It's not a bug, it's a feature!

0	7	8	15	16	23	24	31
Access Address - 0x8E89BED6							
Packet Header							
Advertising Address - xx:xx:xx:xx:xx:xx							
Length / Type - 0x01 / Flags (Optional)							Length
Type - 0xFF		Company ID - 0x004C					Apple Type
Apple Length		Variable Length Apple Data					Apple Type
Apple Length		Variable Length Apple Data					

```
0000  ·····  6u···b··
0010  ·····  ····`%U>
0020  12 19 10 f9 62 a3 95 8e  T·····L·  ····b···
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93  ·z#·`5>·  F··'q···
0040  3f 02 3e d5 39 6a  ?·>·9j
```

CRC

Separated

"Public Key Bits"

Apple BLE Frame Format

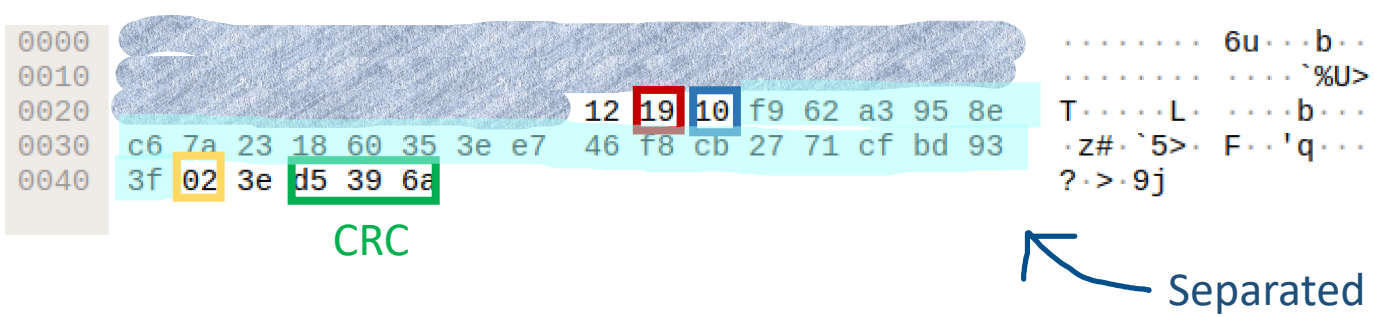
7	6	5	4	3	2	1	0
0	0	0	0	0	0	1	0
Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Pub Key	Pub Key

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

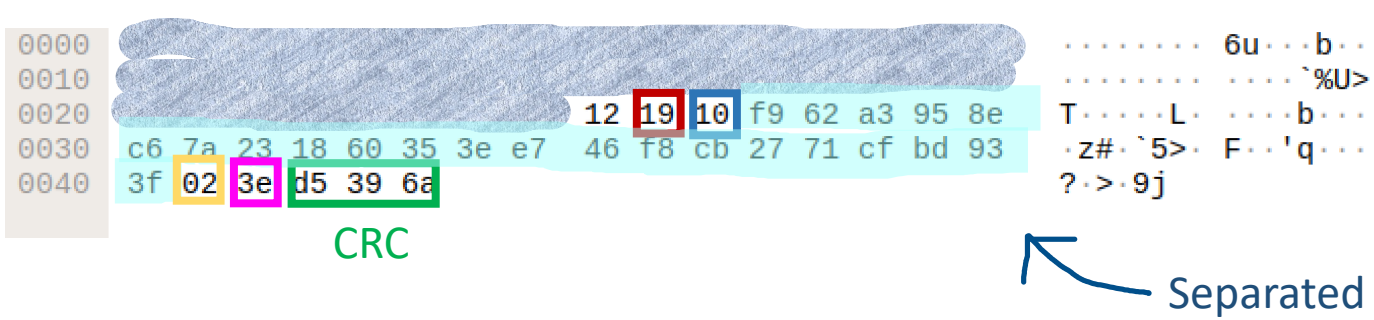


Continuity Protocol Explained

It's not a bug, it's a feature!

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format

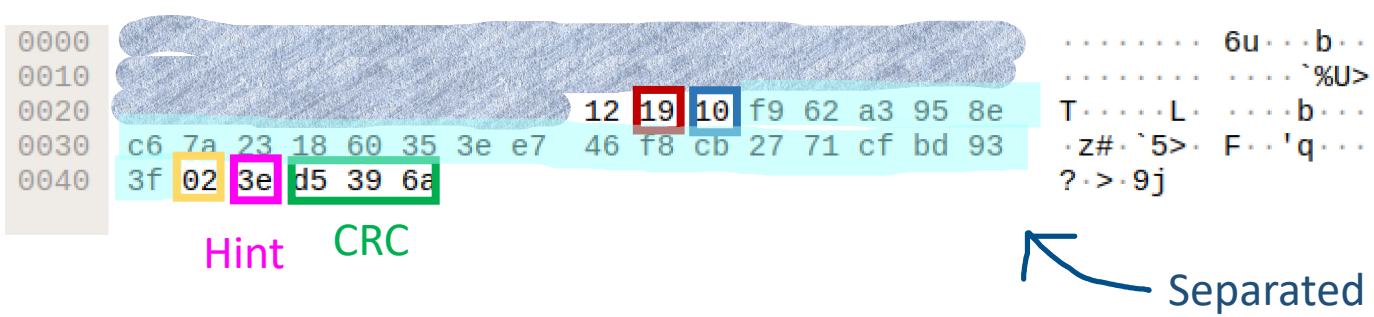


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

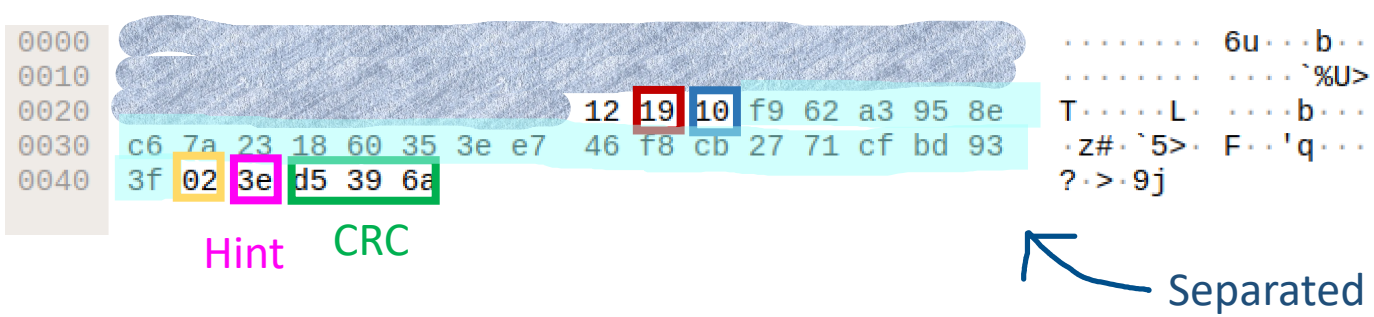


Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)			Length	
Type - 0xFF	Company ID - 0x004C		Apple Type	
Apple Length	Variable Length Apple Data		Apple Type	
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format



(also related to public key)

Continuity Protocol Explained

It’s not a bug, it’s a feature!

Continuity Protocol Explained

It’s not a bug, it’s a feature!

In 5 Minutes

Continuity Protocol Explained

It’s not a bug, it’s a feature!

No GPS!

Continuity Protocol Explained

It’s not a bug, it’s a feature!

No GPS!

..so how does it work?

Continuity Protocol Explained

It’s not a bug, it’s a feature!

Encryption 101

PUBLIC KEY = encrypt

PRIVATE KEY = decrypt

Continuity Protocol Explained

It’s not a bug, it’s a feature!

Continuity Protocol Explained

It’s not a bug, it’s a feature!

airtag

Continuity Protocol Explained

It’s not a bug, it’s a feature!

No GPS but… BLUETOOTH!

airtag

Continuity Protocol Explained

It’s not a bug, it’s a feature!

No GPS but… BLUETOOTH!

airtag

Continuity Protocol Explained

It’s not a bug, it’s a feature!

No GPS but… BLUETOOTH!

airtag

Continuity Protocol Explained

It’s not a bug, it’s a feature!

No GPS but… BLUETOOTH!

0x12345678910ABCDEFABCDEF

airtag

Continuity Protocol Explained

It’s not a bug, it’s a feature!

No GPS but… BLUETOOTH!

airtag

0x12345678910ABCDEFABCDEF

Notional key PubKey

Continuity Protocol Explained

It's not a bug, it's a feature!

No GPS but… BLUETOOTH!

airtag

0x12345678910ABCDEFABCDEF

Notional key PubKey

P224 ELLIPTIC CURVE PUBLIC KEY
224 bits in PubKey = 28 byte key

Continuity Protocol Explained

It’s not a bug, it’s a feature!

No GPS but… BLUETOOTH!

PubKey

airtag

Continuity Protocol Explained

It’s not a bug, it’s a feature!

No GPS but… BLUETOOTH!

PubKey

airtag

Continuity Protocol Explained

It’s not a bug, it’s a feature!

Apple Server

No GPS but… BLUETOOTH!

PubKey

airtag

Continuity Protocol Explained

It’s not a bug, it’s a feature!

Apple Server

No GPS but… BLUETOOTH!

PubKey

airtag

Continuity Protocol Explained

It’s not a bug, it’s a feature!

Apple Server

No GPS but… BLUETOOTH!

PubKey

airtag

Continuity Protocol Explained

It's not a bug, it's a feature!

No GPS but… BLUETOOTH!

PubKey

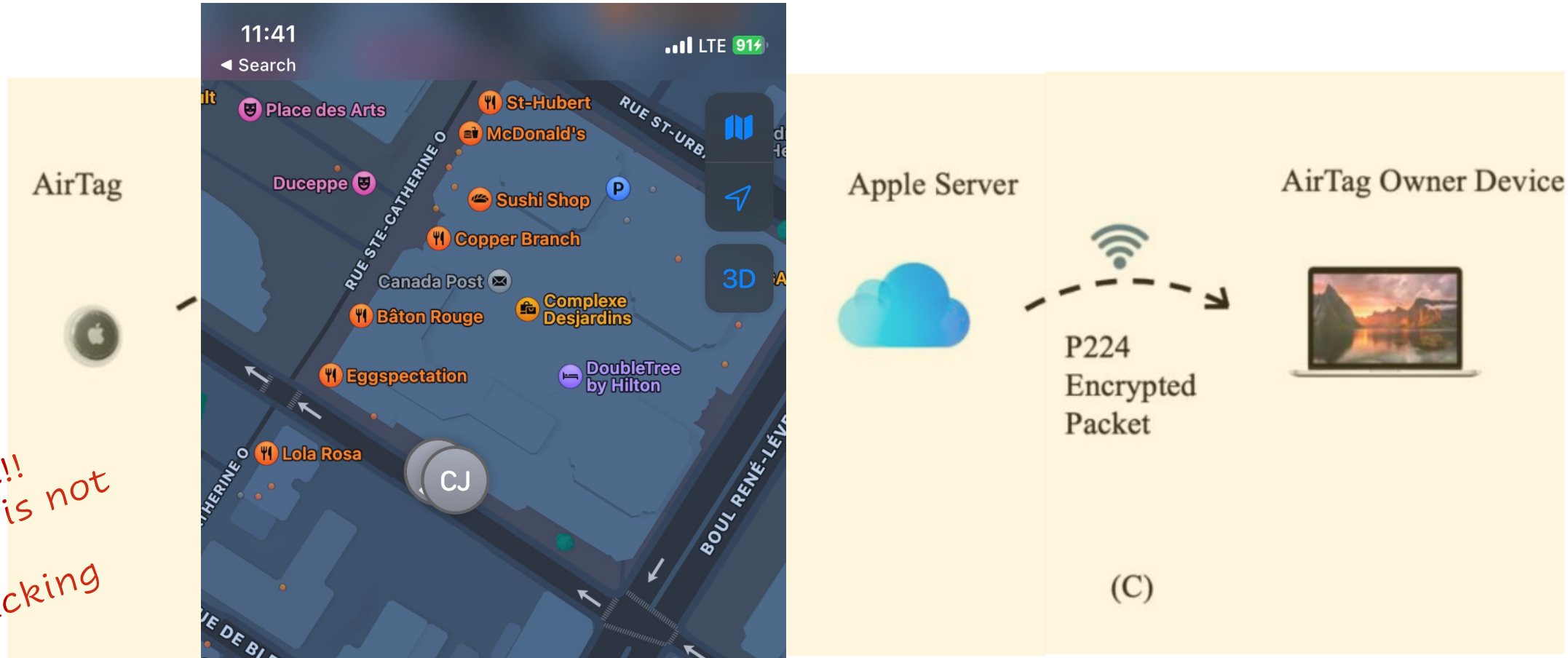
airtag

Apple Server

Can download and unlock with Private Key

Continuity Protocol Explained

It's not a bug, it's a feature!

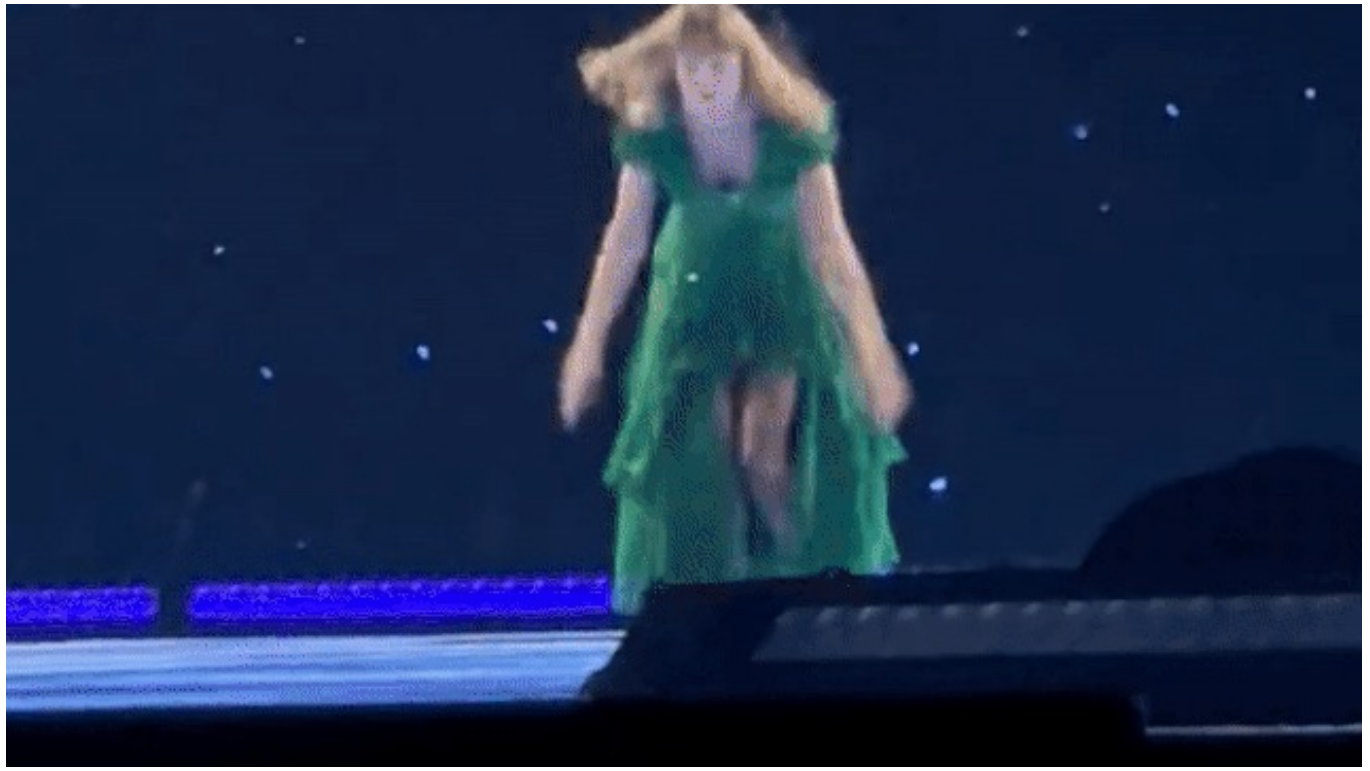


NOTE!! This is not live tracking

If at 3:00p y to a user who claimed they were at the Hilton Hotel, the or near the Hilton Hotel at the same time.

What the heck is P224- ECIES?!

- Let’s take a deep dive into encryption (photo cred @replover4eva)



P-224 Encryption in General

- Recall the Diffie Hellman key exchange, and the ability to generate a shared secret
- P-224 Elliptic Curve Diffie Hellman (ECDH) is similar, with more parameters

The "domain parameters" are already agreed upon (*p, a, b, G, n, h*) and the curve is represented by the formula:

$$y^2 = x^3 - 3x + 18958286285566608000408668544493926415504680968679321075787234672564$$

and (*p, a, b, G, n, h*) are defined as follows:

```
p = 26959946667150639794667015087019630673557916260026308143510066298881
a = -3
b = 18958286285566608000408668544493926415504680968679321075787234672564
G= (19277929113566293071110308034699488026831934219452440156649784352033,
19926808758034470970197974370888749184205991990603949537637343198772)
n = 26959946667150639794667015087019625940457807714424391721682722368061
h=1
```

(FIPS 186-4 Digital Standard)

P-224 ECIES

- “Elliptic Curve Integrated Encryption Scheme”
- Supposed to be Even More Secure™ and protect against chosen-plaintext and chosen-ciphertext attacks
- ECIES integrates additional features such as message authentication codes (MAC) and key derivation functions (KDF) into the protocol, as well as a symmetric encryption scheme for faster encryption times
- This is introduced in a 2009 paper (Daniel R. L. Brown. Standards for Efficient Cryptography 1 (SEC 1). 2009. https://www.secg.org/sec1-v2.pdf)

- In the AirTag implementation, the KDF used is ANSI-X9.63-KDF and the MAC scheme used is SHA-256. The symmetric key scheme ENC is AES-128-GCM.
- It is important to note that given an elliptic curve and an x-coordinate on that curve, the y-coordinate can be trivially calculated, so usually only the x-coordinate is shared in practical implementations

Continuity Protocol Explained

It's not a bug, it's a feature!

The AirTag and owner device must collaboratively generate a 28 byte Master public key P, (comprised of key pair public p_0 and private d_0) as well a 32 byte key Secret Key Separated (SKS)

(if you want to know more, there's bonus slides at the end, but basically, they use math to each generate P without either actually sending P over the channel, much like most shared secret generation)

The master key P and SKS are used to generate a derivative key PW_i, defined by key pairs public p_i and private d_i

Every 15 minutes, a new key pair public p_i and private d_i are generated, and the new p_i value is what is beaconed

All the math

1) ephemeral key is generated (extraction)

$SKS_i = KDF(SKS_{i-1}, \text{“update”}, 32)$

2) expansion of key pair

$(u_i , v_i) = KDF(SKS_i , \text{“diversify”}, 72)$

3) Reduce into P-224 valid scalars

$u_i = u_i \pmod{q-1} + 1$ (where q is the order of the base point G of the P-224 elliptic curve.)

$v_i = v_i \pmod{q-1} + 1$

4) Generate p_i and d_i

$d_i = (d_0 * u_i) + v_i$

$p_i = (d_i * G)$

Where * is the dot product, G is the point generator and the original public key is (d_0, p_0)

Continuity Protocol Explained

It's not a bug, it's a feature!

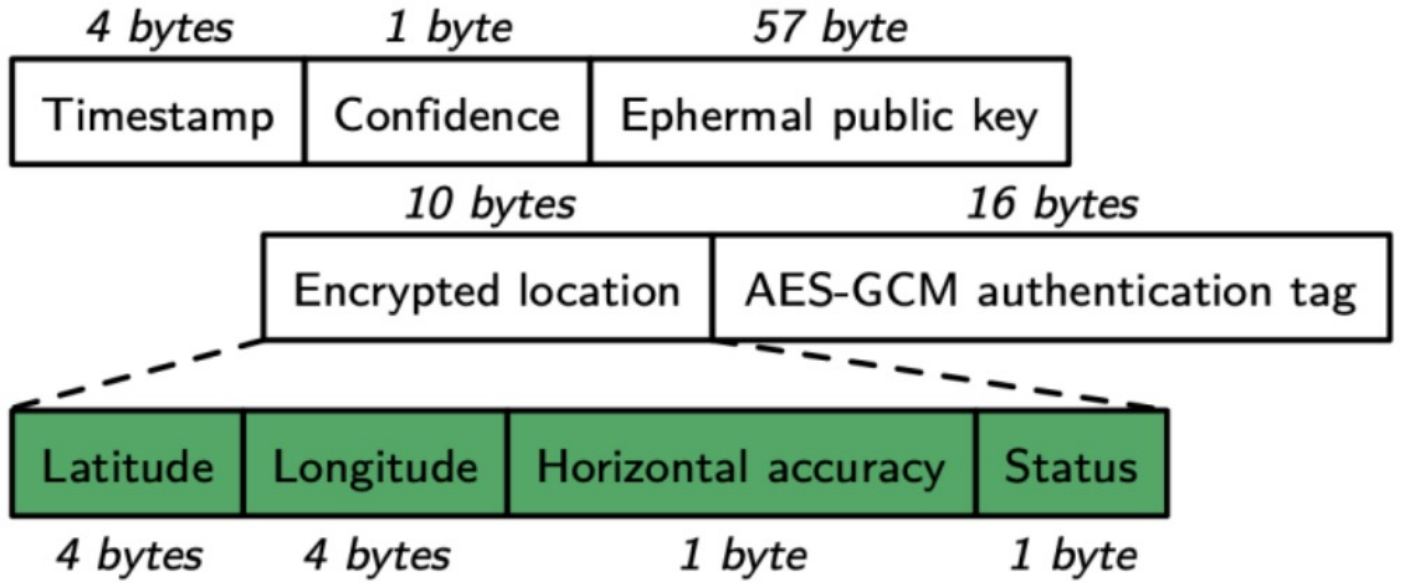


Fig. 2. Binary format of a location report.

(from TU Darmstadt paper)

s its own ephemeral key

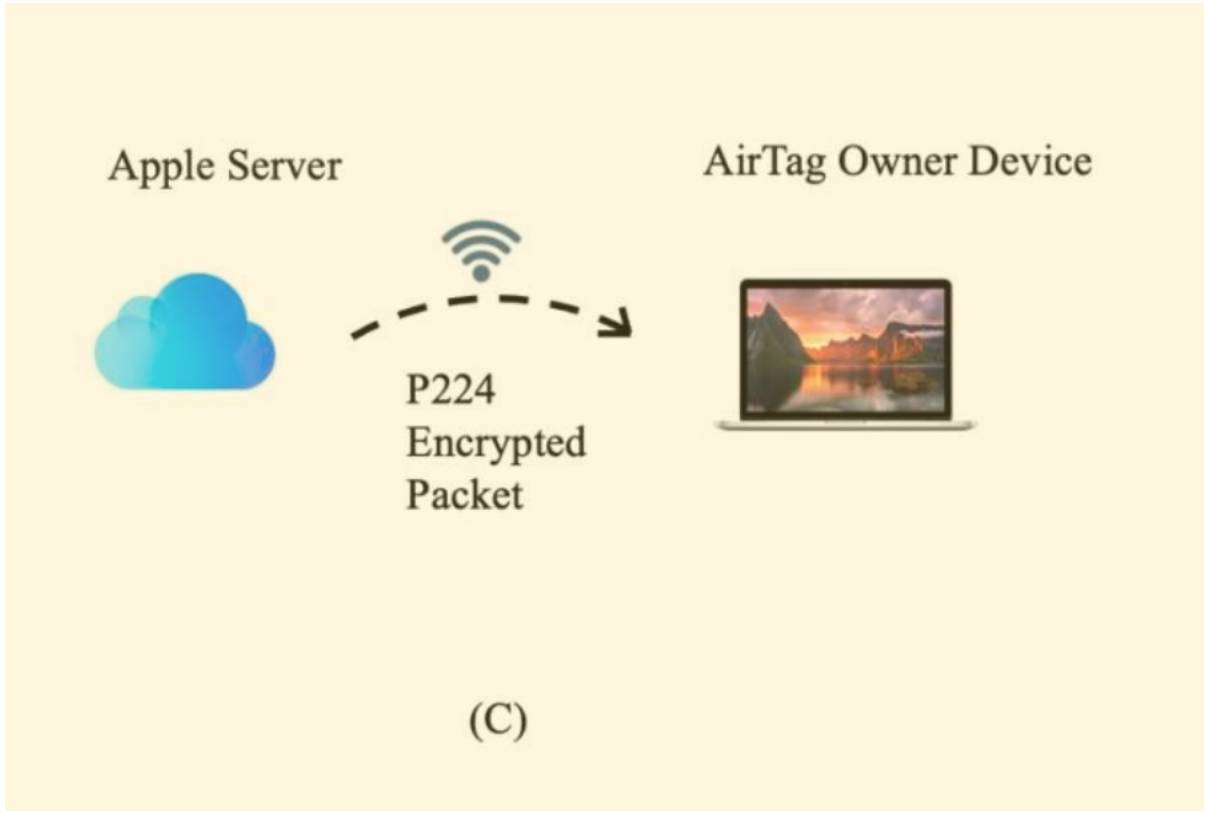
ey p_i, it uses ECDH to
et –> SharedKeyFinder

n ephemeral key
e", 32)

come a 16 byte
CM. The last 16 bytes of
n vector (IV). This is an

Continuity Protocol Explained

It's not a bug, it's a feature!



- The Apple Servers store the locations reports as key value pairs (SHA256(p_i), 88 byte location report)
- You can request a location report as long as you know the hash
- The owner device collaboratively generated (p_0,d_0), so calculating p_i and SHA256(p_i) is trivial.
- Also, because the owner device can recalculate all of the private keys from the airtag as well, it will calculate the corresponding private key d_i for public key p_i, then using the ephemeral public key , the owner can calculate the shared secret SKF. Using the known KDF function, the owner can then calculate SKF', which becomes e' and IV, and was used to AES- 128 encrypt the original payload, and since AES is symmetric, this will decrypt that location report as well.

Bluetooth Limitations

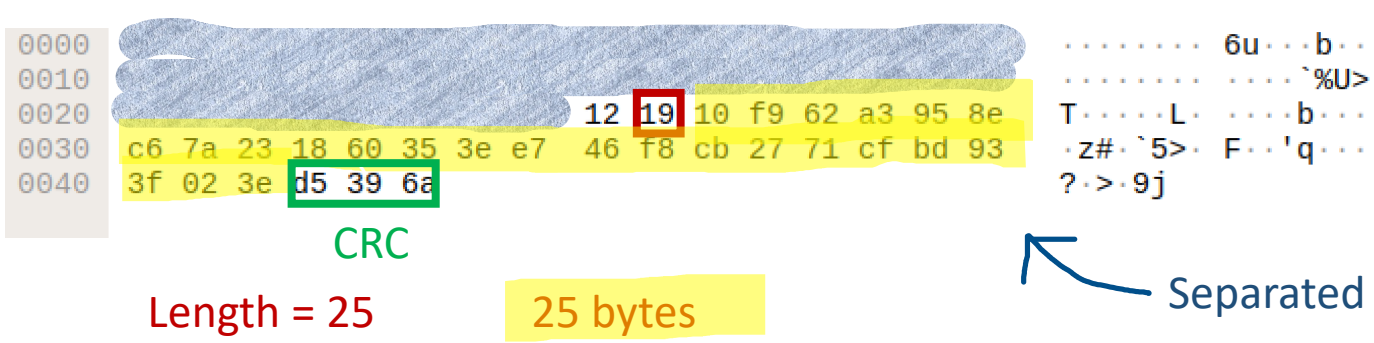
- Small Packet Size vs Strong Encryption Need
  - MTU recommendation is 512 bytes (that's including header info and payload)
  - In practice this is much smaller! And for Bluetooth low energy EVEN smaller (max recommended payload only 27 bytes)
  - BUT we want to use strong encryption, and a P-224 key of 224 bits is equivalent to an RSA key of 2048 bits
  - So Apple does something a little creative here....

Continuity Protocol Explained

It's not a bug, it's a feature!

0	7 8	15 16	23 24	31
Access Address - 0x8E89BED6				
Packet Header				
Advertising Address - xx:xx:xx:xx:xx:xx				
Length / Type - 0x01 / Flags (Optional)				Length
Type - 0xFF	Company ID - 0x004C			Apple Type
Apple Length	Variable Length Apple Data			Apple Type
Apple Length	Variable Length Apple Data			

Apple BLE Frame Format

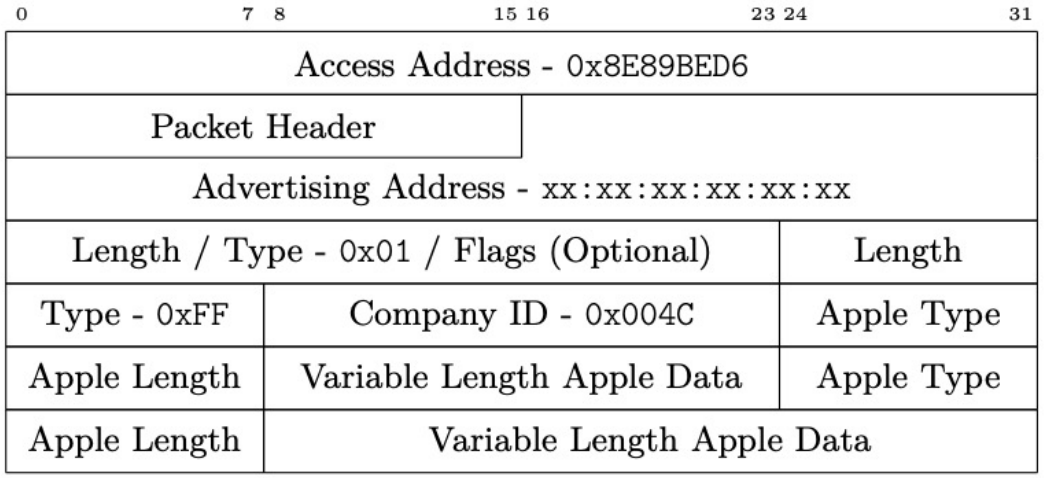


Creative Key Storage

It's not a bug, it's a feature!

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Separated



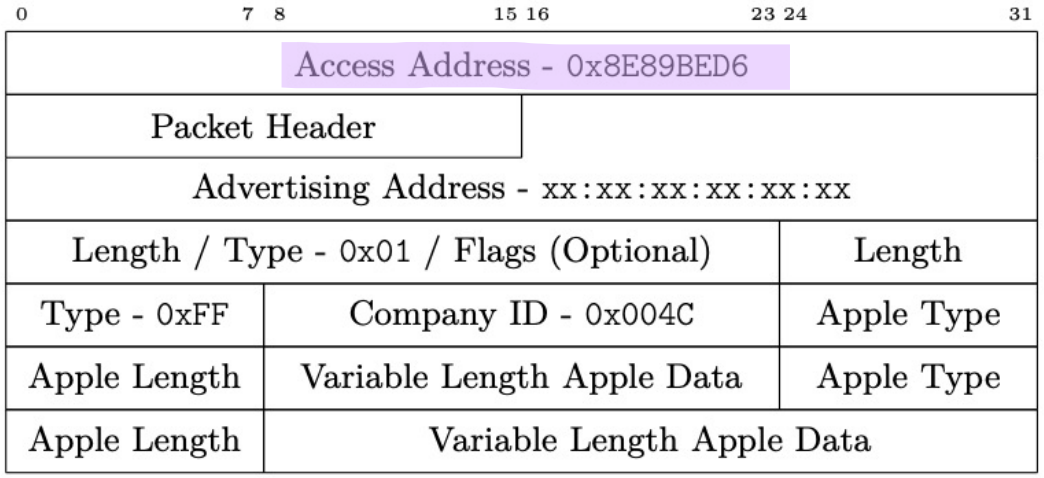
Apple BLE Frame Format

Creative Key Storage

It's not a bug, it's a feature!

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Separated



Apple BLE Frame Format

Creative Key Storage

It's not a bug, it's a feature!

```
0000   00 00 18 00 fb 00 00 00   36 75 0c 00 00 62 09 00    ........ 6u...b..
0010   98 85 d7 0b 17 0a 16 00   d6 be 89 8e 60 25 55 3e    ........ ....`%U>
0020   54 07 14 d9 1e ff 4c 00   12 19 10 f9 62 a3 95 8e    T.....L. ....b...
0030   c6 7a 23 18 60 35 3e e7   46 f8 cb 27 71 cf bd 93    .z#.`5>. F..'q...
0040   3f 02 3e d5 39 6a                                   ?.>.9j
```

Separated

0 7	8 15	16 23	24 31
Access Address - 0x8E89BED6			
Packet Header			
Advertising Address - xx:xx:xx:xx:xx:xx			
Length / Type - 0x01 / Flags (Optional)			Length
Type - 0xFF	Company ID - 0x004C		Apple Type
Apple Length	Variable Length Apple Data		Apple Type
Apple Length	Variable Length Apple Data		

Apple BLE Frame Format

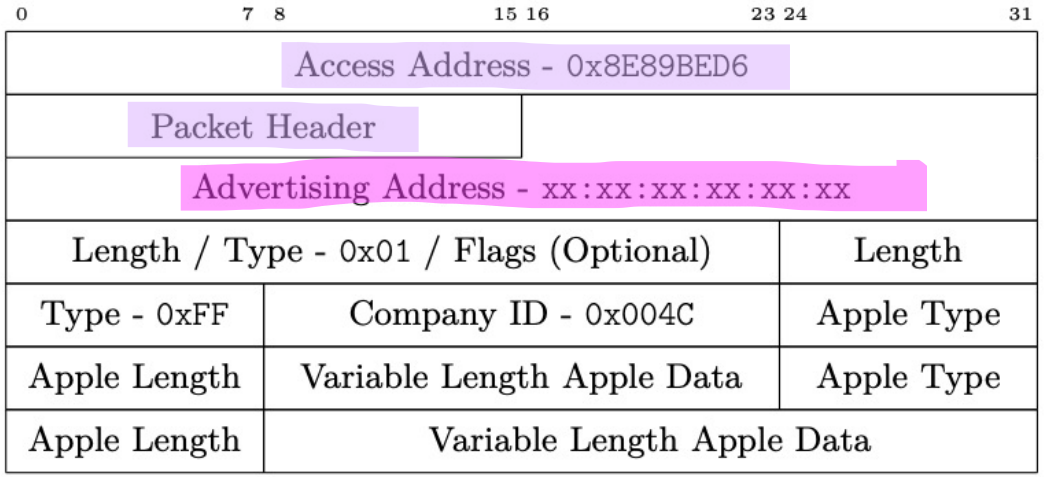
Creative Key Storage

It's not a bug, it's a feature!

28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Separated



Bytes 0-5

Apple BLE Frame Format

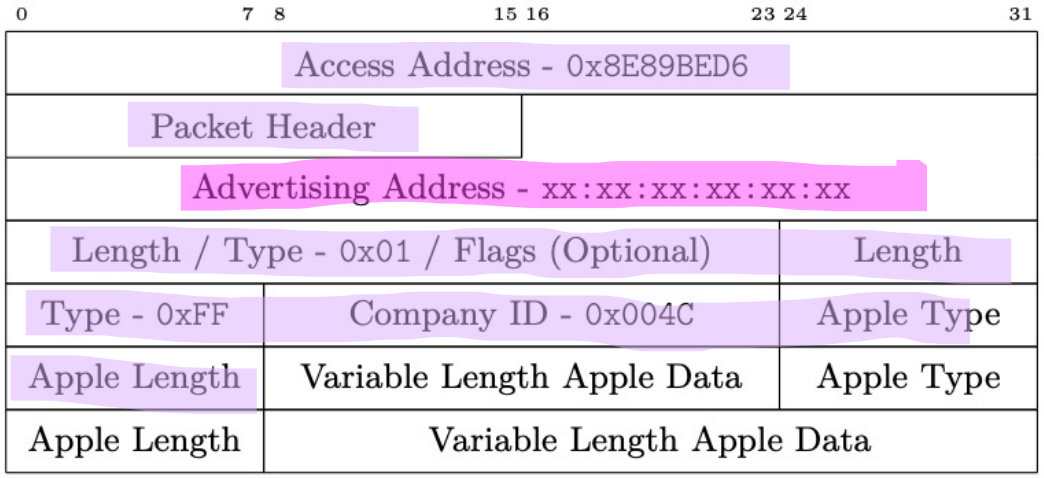
Creative Key Storage

It's not a bug, it's a feature!

28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Separated



Bytes 0-5

Apple BLE Frame Format

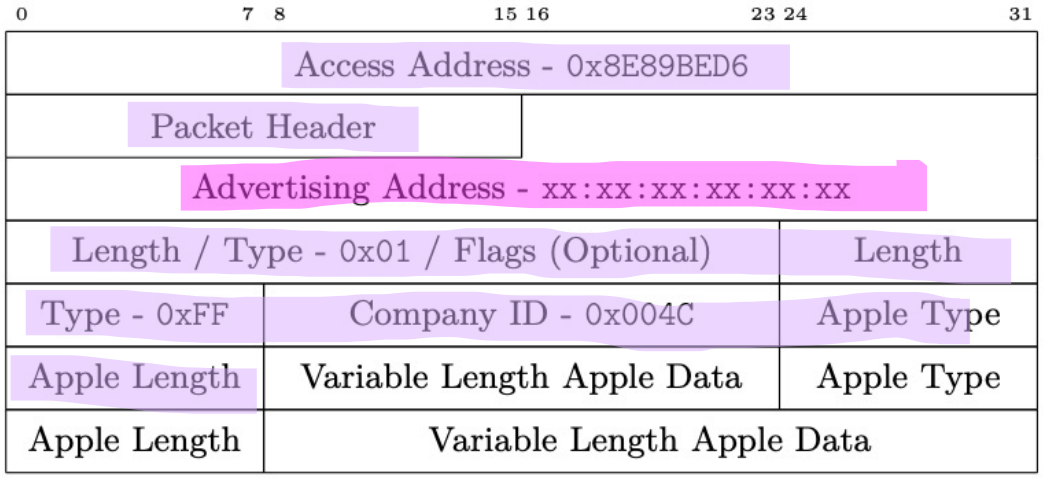
Creative Key Storage

It's not a bug, it's a feature!

28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Separated



Bytes 0-5

Apple BLE Frame Format

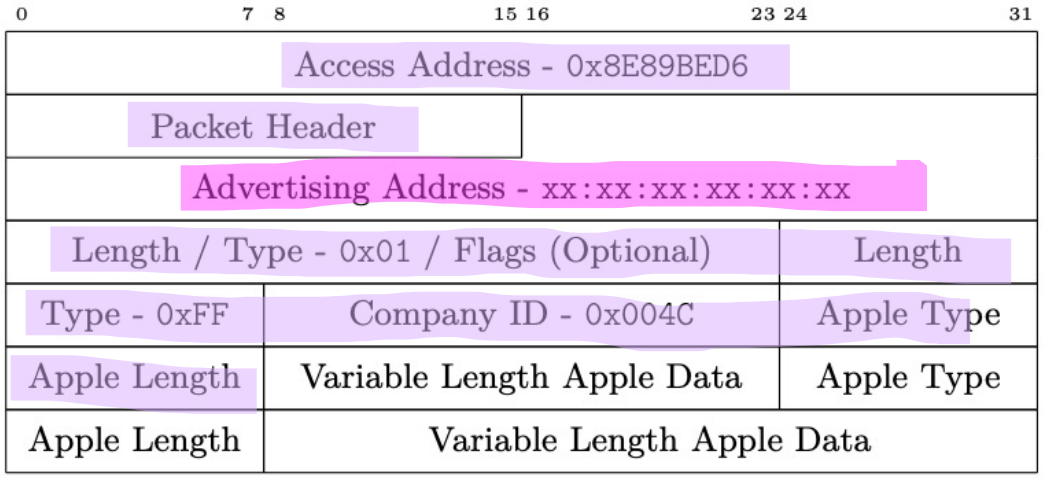
Creative Key Storage

It's not a bug, it's a feature!

28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Separated



Bytes 0-5

Apple BLE Frame Format

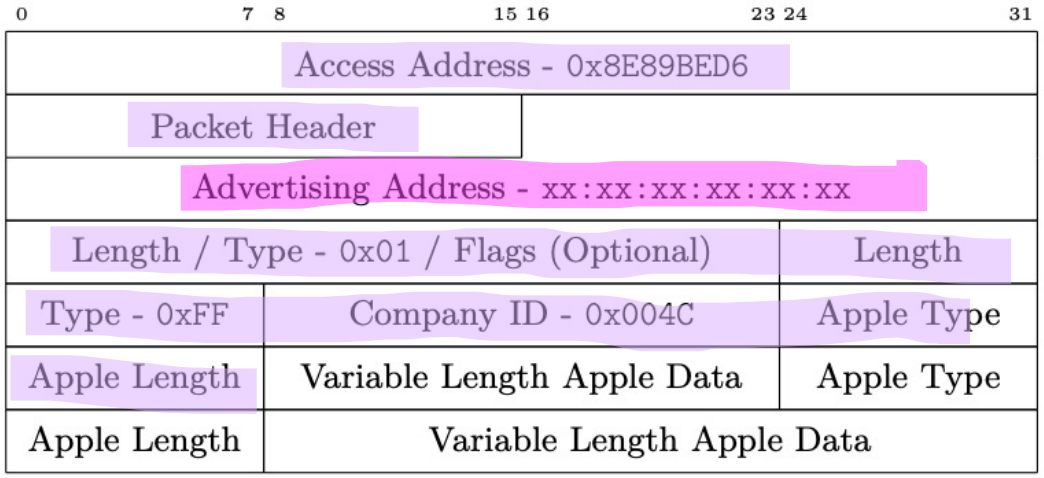
Creative Key Storage

It's not a bug, it's a feature!

28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Separated



Bytes 0-5

Bytes 6-27

Apple BLE Frame Format

Creative Key Storage

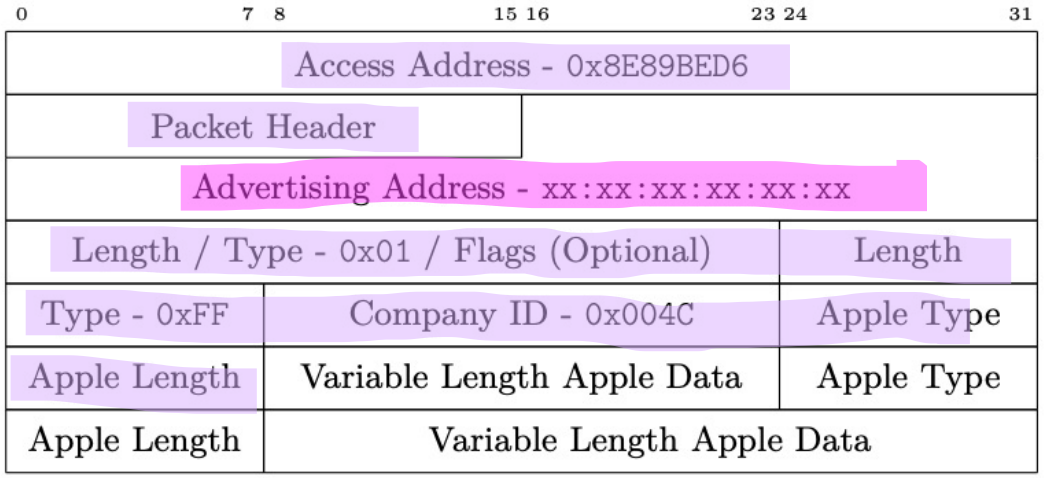
It's not a bug, it's a feature!

28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Hint

Separated



Bytes 0-5

Bytes 6-27

Apple BLE Frame Format

Creative Key Storage

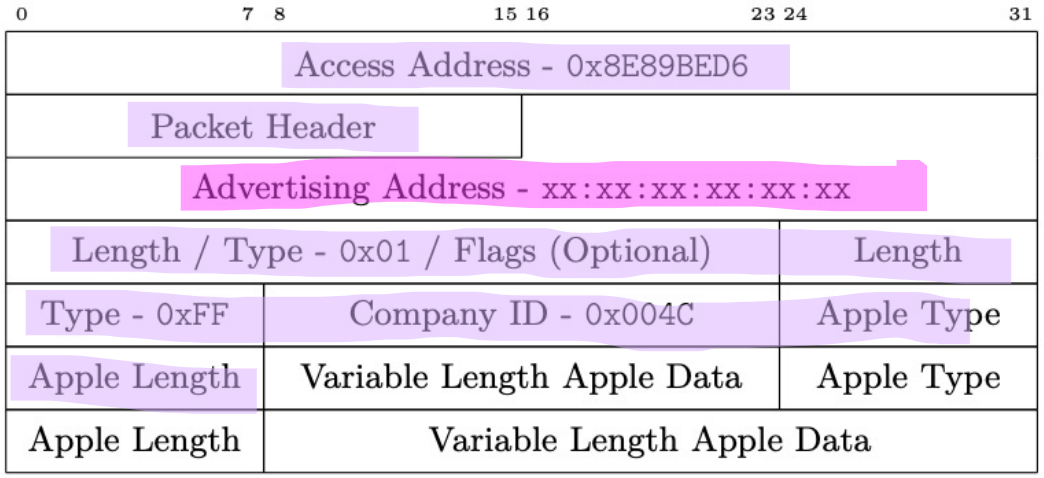
It's not a bug, it's a feature!

28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Hint

Separated



Bytes 0-5

Bytes 6-27

Apple BLE Frame Format

Creative Key Storage

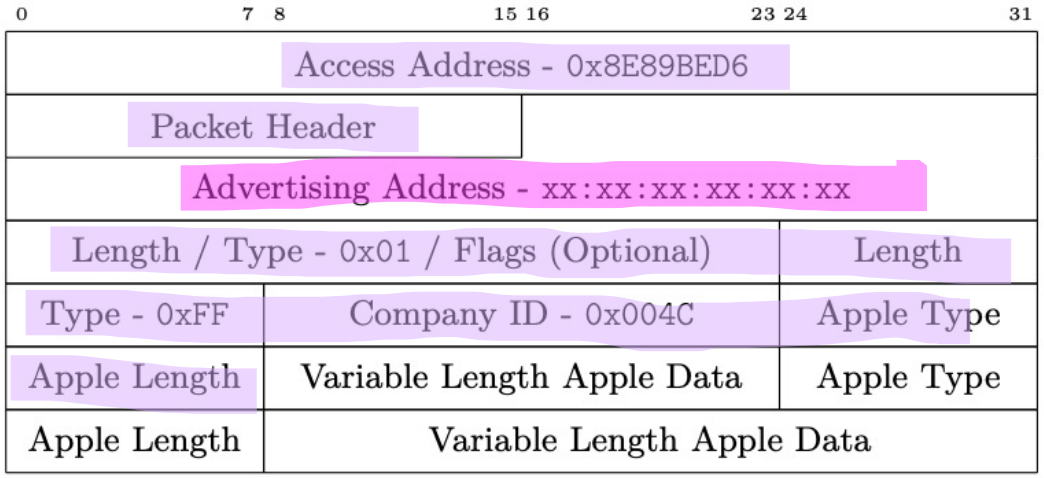
It's not a bug, it's a feature!

28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Hint

Separated



Bytes 0-5

Bytes 6-27

d	9
1101	1001

Apple BLE Frame Format

Creative Key Storage

It's not a bug, it's a feature!

28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Public Key

Hint

Separated

Bits

0	7	8	15	16	23	24	31
Access Address - 0x8E89BED6							
Packet Header							
Advertising Address - xx:xx:xx:xx:xx:xx							
Length / Type - 0x01 / Flags (Optional)							Length
Type - 0xFF			Company ID - 0x004C				Apple Type
Apple Length			Variable Length Apple Data				Apple Type
Apple Length			Variable Length Apple Data				

Bytes 0-5

Bytes 6-27

d	9
1101	1001

Apple BLE Frame Format

Creative Key Storage

It's not a bug, it's a feature!

28 byte key

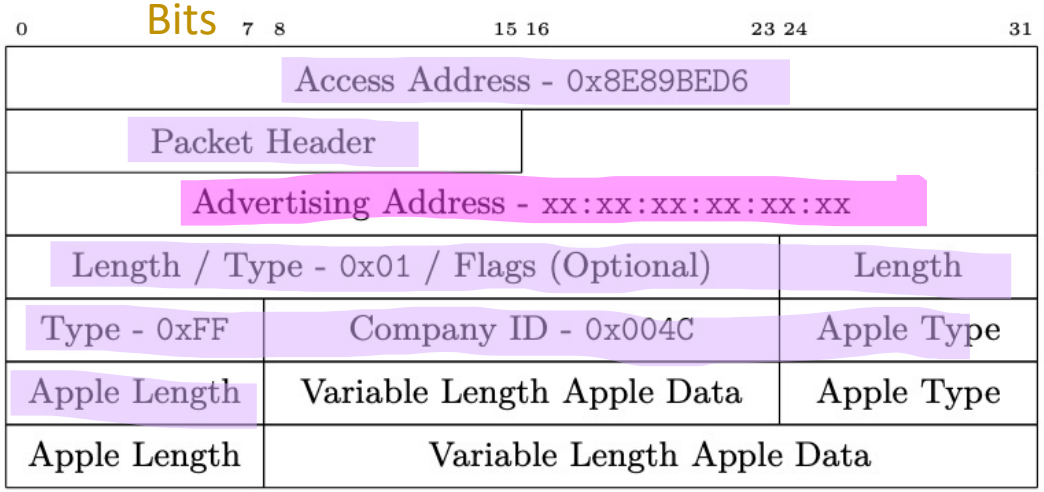
```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Public Key

Hint

Separated

Bits



Bytes 0-5

Bytes 6-27

d	9
1101	1001

→0010→10→1001→9

Final PubKey:

Apple BLE Frame Format

Creative Key Storage

It's not a bug, it's a feature!

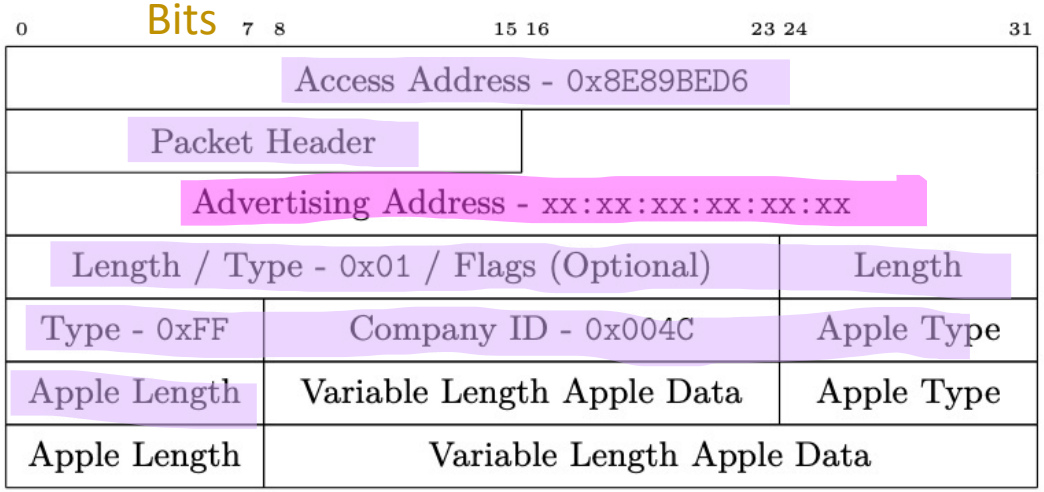
28 byte key

```
0000  00 00 18 00 fb 00 00 00  36 75 0c 00 00 62 09 00   ........ 6u...b..
0010  98 85 d7 0b 17 0a 16 00  d6 be 89 8e 60 25 55 3e   ........ ....`%U>
0020  54 07 14 d9 1e ff 4c 00  12 19 10 f9 62 a3 95 8e   T.....L. ....b...
0030  c6 7a 23 18 60 35 3e e7  46 f8 cb 27 71 cf bd 93   .z#.`5>. F..'q...
0040  3f 02 3e d5 39 6a                                 ?.>.9j
```

Public Key

Hint

Separated



Bytes 0-5

Bytes 6-27

d	9
1101	1001

→0010→10→1001→9

Final PubKey:

991407543e55f962a3958e
c67a231860353ee746f8cb2771cfbd933f

Apple BLE Frame Format

References

[1] Hardwick, Tim. “Apple Announces AirTag Tracking Devices Starting at $29 Each. *MacRumors,* 20 Apr. 2021, https://www.macrumors.com/2021/04/20/apple-unveils-airtags-tracking-devices/.

[2] “AirTag.” *Apple,* Apr. 2021, https://www.apple.com/airtag/.

[3] “Create Innovative Accessories.” *Apple.* 2021,https://mfi.apple.com/.

[4] Goldheart, Sam. “AirTag Teardown: Yeah, This Tracks” *IFixit,* 1 May 2021, https://www.ifixit.com/News/50145/airtag-teardown-part-one-yeah-this-tracks.

[5] “NRF52832.” Nordic Semiconductor, https://www.nordicsemi.com/products/nrf52832.

[6] NIST. “Digital Signature Standard (DSS).” *Federal Information Processing Standards Publication*, 2013, https://doi.org/10.6028/nist.fips.186-4.

[7] Guillaume Celosia, Mathieu Cunche. Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism. MobiQuitous 2019 - 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Dec 2019, Houston, United States. pp.1-10, ff10.1145/3360774.3360777ff. ffhal-02394629f

[8] Afaneh, Mohammad. “Bluetooth Addresses & Privacy in Bluetooth Low Energy.” *Novel Bits*, 6 Apr. 2020, https://novelbits.io/Bluetooth-address-privacy-ble/.

[9] *Great Scott Gadgets*, https://greatscottgadgets.com/ubertoothone/.

[10] Bluetooth SIG. Bluetooth Core Specification Version 5.2. Tech. rep. 2019.

[11] Heinrich, Alexander, et al. “Who Can *Find My* Devices? Security and Privacy of Apple’s Crowd-Sourced Bluetooth Location Tracking System.” *Proceedings on Privacy Enhancing Technologies*, vol. 2021, no. 3, 2021, pp. 227–245., https://doi.org/10.2478/popets-2021-0045.

More References

[12] “Find My Network Accessory Specification.” *Apple.* Version Release R1. 2020. url: https://developer.apple.com/ find-my/.
[13] Kassem Fawaz, Kyu-Han Kim, and Kang G Shin. 2016. Protecting Privacy of BLE Device Users. In 25th USENIX Security Symposium (*USENIX Security 16*). 1205–1221.
[14] Celosia, Guillaume, and Mathieu Cunche. “Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols.” *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 1, 2020, pp. 26–46., https://doi.org/10.2478/popets-2020-0003.
[15] “Throughput with Bluetooth Low Energy Technology.” Version 4.0 Bluetooth API Documentation. *Silicon Labs*, June 2022, https://docs.silabs.com/Bluetooth/4.0/general/system-and- performance/throughput-with-Bluetooth-low-energy-technology.
[16] Derhgawen, Ashish. “Maximizing BLE Throughput Part 4: Everything You Need to Know.” *Punch Through*, 16 Nov. 2020, https://punchthrough.com/ble-throughput-part-4/.
[17] “Size Considerations for Public and Private Keys.” Documentation, *IBM*, 27 May 2021, https://www.ibm.com/docs/en/zos/2.4.0?topic=certificates-size-considerations-public-private-keys. [18] Jeremy Martin, Douglas Alpuche, Kristina Bodeman, Lamont Brown, Ellis Fenske, Lucas Foppe, Travis Mayberry, Erik Rye, Brandon Sipes, and Sam Teplov. “Handoff All Your Privacy: A Review of Apple’s Bluetooth Low Energy Implementation.” In: (2019). doi: 10.2478/popets-2019- 0057.

More References

[18] Douglas Alpuche, Kristina Bodeman, Lamont Brown, Ellis Fenske, Lucas Foppe, Travis Mayberry, Erik Rye, Brandon Sipes, and Sam Teplov. “Handoff All Your Privacy: A Review of Apple’s Bluetooth Low Energy Implementation.” In: (2019). doi: 10.2478/popets-2019- 0057.

[19] Travis Mayberry, Ellis Fenske, Dane Brown, Jeremy Martin, Christine Fossaceca, Erik C. Rye, Sam Teplov, and Lucas Foppe. 2021. Who Tracks the Trackers? Circumventing Apple’s Anti- Tracking Alerts in the Find My Network. In Proceedings of the 20th Workshop on Privacy in the Electronic Society (WPES ’21), November 15, 2021, Virtual Event, Republic of Korea. *ACM*, New York, NY, USA, 6 pages. https://doi.org/10.1145/3463676.3485616

[20] Daniel R. L. Brown. Standards for Efficient Cryptography 1 (SEC 1). 2009. https://www.secg.org/sec1-v2.pdf

[21] “Apple Platform Security.” *Apple.* 2020. url: https : / / support.apple.com/guide/security/ (Alternate Link).https://github.com/0xmachos/Apple-Platform-Security-Guides/blob/master/2020- spring-apple-platform-security-guide.pdf

[22] *Wireshark · Go Deep.*, https://www.wireshark.org/.

[25] Diffie and M. E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, Vol. 22, No. 6, 1976, pp. 644-654. https://ee.stanford.edu/~hellman/publications/24.pdf

[26] “Elliptic-Curve Diffie–Hellman.” *Wikipedia*, Wikimedia Foundation, 9 Nov. 2022, https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman.

[27] “P-224.” *Standard Curve Database*, 2020, https://neuromancer.sk/std/nist/P-224.

More References

[28] “Chapter 3 - An Introduction To Cryptography”.Editor(s): Dale Liu, Max Caceres, Tim Robichaux, Dario V. Forte, Eric S. Seagren, Devin L. Ganger, Brad Smith, Wipul Jayawickrama, Christopher Stokes, Jan Kanclirz, Next Generation SSH2 Implementation,Syngress,2009,
Pages 41-64,https://doi.org/10.1016/B978-1-59749-283-6.00003-9. (https://www.sciencedirect.com/topics/computer-science/plaintext-attack)

[29] Ryan K.L. Ko, Kim-Kwang Raymond Choo,Chapter 1 -The Cloud Security Ecosystem.Syngress, 2015,Pages 1-14,https://doi.org/10.1016/B978-0-12-801595-7.00001-X. (https://www.sciencedirect.com/topics/computer-science/el-gamal)

[30] NIST. “Digital Identity Guidelines”. *Special Publication*, 2017, https://doi.org/10.6028/NIST.SP.800-63b

[31] Abdel Hakeem SA, Kim H. Centralized Threshold Key Generation Protocol Based on Shamir Secret Sharing and HMAC Authentication. Sensors (Basel). 2022 Jan 3;22(1):331. doi: 10.3390/s22010331

[32] Alexander Heinrich, Niklas Bittner, and Matthias Hollick. 2022. AirGuard - Protecting Android Users from Stalking Attacks by Apple Find My Devices.

[33] NIST. “Recommendation for Key-Derivation Methods in Key-Establishment Schemes”. *Special Publication*, 2018, https://doi.org/10.6028/NIST.SP.800-56Cr1

[34] Ireland, David. “AES-GCM Authenticated Encryption.” *CryptoSys PKI Pro Manual*, DI Management Services Pty Limited, 10 Sept. 2022, https://www.cryptosys.net/pki/manpki/pki_aesgcmauthencryption.html.

[35] Daniel J. Bernstein and Tanja Lange. SafeCurves: choosing safe curves for elliptic-curve cryptography. 1 Jan 2017. https://safecurves.cr.yp.to.

[36] Giry, Damien. “Cryptographic Key Length Recommendation.” *BlueKrypt*, 24 May 2020, https://www.keylength.com/en/4/.

her hax
PODCAST

Questions?

christine@herhaxpodcast.com
@x71n3 on Twitter

AirTag + Owner Device Key Exchange

- Assume an a priori securely established Bluetooth communications channel (During the Bluetooth pairing procedure, the two devices use an a priori Apple server key (written into the firmware of both devices) [12]to encrypt these initial transmissions)
- Collaborative Key Generation Steps (From the Original FindMy Specification)
    - "AirTag Accessory Alice" must generate a P-224 scalar *s* and a random 32 byte value *r*, then concatenates *s* with *r*, and calculates a value *c1* by calculating the SHA-256 of *s* concatenated with *r*.
    - "Owner Device Bob" also generates a P-224 scalar, *s'*, and a random 32 byte value *r'*. However, Bob then uses generational point *G* to generate *S'*, where *S' = G * s'*, where * indicates the dot product. Note, this is quite similar to the calculation for Bob's public key in the section above. Bob's iDevice can then send *c2* which is a set containing {S', r'}.
    - Now, S' is also point on the curve P-224, because it was created from G, the generational point. AirTag Accessory Alice verifies this. The AirTag will be the first to compute the Master public key P. Using S' from the Owner device, the formula is P = S' +s * G. Remember, P is never sent over the channel, so instead, the AirTag sends c3 = {s, r}

AirTag + Owner Device Key Exchange (cont)

- Collaborative Key Generation Steps (cont)
  - Next, the owner device does a bit of verification, first, verifying that s is a valid P-224 scalar, and then computing the SHA-256 hash of s concatenated with r. The AirTag sent this value initially with c1, so the owner device compares its own calculation to c1, and aborts if they are not equal. Now, the owner device can independently compute the Master key P with the formula P = S' +s * G and the private key d with the formula d = s +s'(mod q), where q is the order of the base point G of the P-224 elliptic curve.
  - At this point, the AirTag and the owner device (Alice and Bob) each have generated P without sending it over the channel. Using P, each can independently compute SKN and SKS as the 64 byte output of the KDF function ANSI-X9.63-KDF(x(P), r concatenated with r'). The SKN is the first 32 bytes of this value and SKS the last 32 bytes.