

Kierunek: CBE	Nazwa zajęć: LABORATORIUM SIECI BEZPRZEWODOWYCH		Ocena:
Nr. ćwiczenia: 1	Tytuł ćwiczenia: Bezpieczeństwo systemów Bluetooth Classic oraz Bluetooth Low Energy		
Termin: Piątek 11:15 gr. P	Data wykonania ćwiczenia: 17.10.2025	Nr. grupy: 1	
Osoby wykonujące ćwiczenie:		Podpisy:	
Adam Wiktor			
Kacper Powolny			
Mateusz Jakoniuk			
Sprawozdanie wykonał:		Adam Wiktor	
Data wykonania sprawozdania:		23.10.2025	
Sprawozdanie sprawdził:		dr. inż. Michał Kowal	

Oświadczam, że zapoznałem/łam się ze niniejszym sprawozdaniem i uważam je za poprawnie wykonane:

.....

Oświadczam/y iż poniższe sprawozdanie zostało wykonane przeze mnie/nas samodzielnie:



Jakoniuk

Powolny

.....

Cel ćwiczenia

1. Zgłębienie aspektów bezpieczeństwa systemów Bluetooth Classic oraz Bluetooth Low Energy.
2. Zapoznanie się z metodami ataku na system Bluetooth.
3. Zrozumienie podatności systemu Bluetooth.
4. Zapoznanie się z narzędziami do testowania bezpieczeństwa sieci Bluetooth zawartych w systemie Kali Linux.

Wykorzystany sprzęt i oprogramowanie

1. Dwa komputery z systemem operacyjnym Kali Linux.
2. Laptop z systemem operacyjnym Arch Linux.
3. Dwa adaptory Bluetooth.
4. Słuchawki SteelSeries Arctis Nova 5X.
5. Telefon Pixel 8 Pro.
6. Telefon iPhone.
7. Oprogramowanie zawarte w systemie operacyjnym Kali Linux.

Przebieg ćwiczenia

Rekonesans

```
sudo hciconfig
```

hci0: DOWN, adapter należy włączyć.

```
sudo hciconfig hci0 up
```

Ze względu na błąd (RF-KILL 132) musieliśmy dodatkowo wykonać komendę - `rfkill unblock bluetooth`, po wykonaniu tych dwóch:

hci0: UP RUNNING.

```
sudo hcitool scan
```

Scanning... Pierwszy skan nie zwrócił niczego, ale później udało się znaleźć urządzenia:

- **20:AF:1B:0B:07:CE SteelSeries Arctis Nova 5X**
- **5C:33:7B:F7:4F:7D Pixel 8 Pro**
- **08:C8:C2:73:E1:0D Adapter Bluetooth – Kali Linux**
- **28:C1:A0:3D:06:72 iPhone (Kacper)**

W kolejnych zadaniach skupimy się na pierwszych trzech urządzeniach.

```
sudo hcitool info <adres MAC>
```

```
Requesting information ...
```

```
BD Address: 20:AF:1B:0B:07:CE
```

```
OUI Company: SteelSeries ApS (20-AF-1B)
```

```
Device Name: SteelSeries Arctis Nova 5X
```

```
LMP Version: 5.3 (0xc) LMP Subversion: 0x8773
```

```
Manufacturer: Realtek Semiconductor Corporation (93)
```

```
Features page 0: 0xff 0xff 0xff 0xfa 0xdb 0xfd 0x7b 0x87
```

```
<3-slot packets> <5-slot packets> <encryption> <slot offset>  
<timing accuracy> <role switch> <hold mode> <sniff mode>  
<park state> <RSSI> <channel quality> <SCO link> <HV2 packets>  
<HV3 packets> <u-law log> <A-law log> <CVSD> <paging scheme>  
<power control> <transparent SCO> <broadcast encrypt>  
<EDR ACL 2 Mbps> <enhanced iscan> <interlaced iscan>  
<interlaced pscan> <inquiry with RSSI> <extended SCO>  
<EV4 packets> <EV5 packets> <AFH cap. perip.>  
<AFH cls. perip.> <LE support> <3-slot EDR ACL>  
<5-slot EDR ACL> <pause encryption> <AFH cap. central>  
<AFH cls. central> <EDR eSCO 2 Mbps> <EDR eSCO 3 Mbps>  
<3-slot EDR eSCO> <extended inquiry> <LE and BR/EDR>  
<simple pairing> <encapsulated PDU> <err. data report>  
<non-flush flag> <LSTO> <inquiry TX power> <EPC>  
<extended features>
```

```
Features page 1: 0x03 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
Features page 2: 0x20 0x08 0x00 0x00 0x00 0x00 0x00 0x00
```

```
→ ~ sudo hcitool info 5C:33:7B:F7:4F:7D
```

```
Requesting information ...
```

```
BD Address: 5C:33:7B:F7:4F:7D
```

```
OUI Company: Google, Inc. (5C-33-7B)
```

```
Device Name: Pixel 8 Pro
```

```
LMP Version: 5.4 (0xd) LMP Subversion: 0x8113
```

```
Manufacturer: Broadcom Corporation (15)
```

```
Features page 0: 0xbf 0xfe 0x8f 0xfe 0xdb 0xff 0x7b 0x87
```

```
<3-slot packets> <5-slot packets> <encryption> <slot offset>  
<timing accuracy> <role switch> <sniff mode> <RSSI>  
<channel quality> <SCO link> <HV2 packets> <HV3 packets>  
<u-law log> <A-law log> <CVSD> <paging scheme> <power control>  
<transparent SCO> <broadcast encrypt> <EDR ACL 2 Mbps>  
<EDR ACL 3 Mbps> <enhanced iscan> <interlaced iscan>  
<interlaced pscan> <inquiry with RSSI> <extended SCO>  
<EV4 packets> <EV5 packets> <AFH cap. perip.>  
<AFH cls. perip.> <LE support> <3-slot EDR ACL>  
<5-slot EDR ACL> <sniff subrating> <pause encryption>  
<AFH cap. central> <AFH cls. central> <EDR eSCO 2 Mbps>  
<EDR eSCO 3 Mbps> <3-slot EDR eSCO> <extended inquiry>  
<LE and BR/EDR> <simple pairing> <encapsulated PDU>  
<err. data report> <non-flush flag> <LSTO> <inquiry TX power>  
<EPC> <extended features>
```

```
Features page 1: 0x0b 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

```
Features page 2: 0x33 0x0f 0x00 0x00 0x00 0x00 0x00 0x00
```

```

→ ~ sudo hcitool info 08:C8:C2:73:E1:0D
Requesting information ...
  BD Address: 08:C8:C2:73:E1:0D
  OUI Company: GN Audio A/S (08-C8-C2)
  Device Name: kali
  LMP Version: 4.0 (0x6) LMP Subversion: 0x2031
  Manufacturer: Cambridge Silicon Radio (10)
  Features page 0: 0xff 0xff 0x8f 0xfe 0xdb 0xff 0x5b 0x87
    <3-slot packets> <5-slot packets> <encryption> <slot offset>
    <timing accuracy> <role switch> <hold mode> <sniff mode>
    <park state> <RSSI> <channel quality> <SCO link> <HV2 packets>
    <HV3 packets> <u-law log> <A-law log> <CVSD> <paging scheme>
    <power control> <transparent SCO> <broadcast encrypt>
    <EDR ACL 2 Mbps> <EDR ACL 3 Mbps> <enhanced iscan>
    <interlaced iscan> <interlaced pscan> <inquiry with RSSI>
    <extended SCO> <EV4 packets> <EV5 packets> <AFH cap. perip.>
    <AFH cls. perip.> <LE support> <3-slot EDR ACL>
    <5-slot EDR ACL> <sniff subrating> <pause encryption>
    <AFH cap. central> <AFH cls. central> <EDR eSCO 2 Mbps>
    <EDR eSCO 3 Mbps> <3-slot EDR eSCO> <extended inquiry>
    <LE and BR/EDR> <simple pairing> <encapsulated PDU>
    <non-flush flag> <LSTO> <inquiry TX power> <EPC>
    <extended features>
  Features page 1: 0x03 0x00 0x00 0x00 0x00 0x00 0x00 0x00

```

Wynik 1-3: hcitool info dla słuchawek, telefonu i laptopa

Poza adresem MAC widać dodatkowo informacje o producencie, nazwę urządzenia, wersję protokołu LMP (służącego do zarządzania połączeniami Bluetooth), a także „Features page”, o których można więcej poczytać w specyfikacji standardu Bluetooth.

```
sudo hcitool inq
```

```

→ ~ sudo hcitool inq
Inquiring ...
  08:C8:C2:73:E1:0D      clock offset: 0x751a      class: 0x6c010c
  5C:33:7B:F7:4F:7D      clock offset: 0x5cf6      class: 0x5a420c
  20:AF:1B:0B:07:CE      clock offset: 0x23ff      class: 0x240418

```

Wynik 4: hcitool inq wykonany w pobliskiej sieci – widoczny kolejno laptop, telefon i słuchawki

Komenda zwraca listę urządzeń Bluetooth w zasięgu wraz z ich adresem MAC – dokładnie te same, co opisaliśmy wcześniej. Obok tych fizycznych adresów widać clock offset (potrzebny do synchronizacji) oraz klasę – opisuje ona typ urządzenia, lecz zwracana jest ona jako liczba szesnastkowa.

```
sudo btscanner
```

btscanner pokazuje bardzo podobne informacje o tych samych trzech urządzeniach, ale jest interaktywny. Dodatkowo, ten program „tłumaczy” nazwy klas na rzeczywiste typy urządzeń – laptop, słuchawki, telefon. Po wybraniu urządzenia, można dokonać jego dokładniejszej analizy, podobnej do tej przedstawionej w hcitool info. Widoczne są jednak jeszcze inne informacje, takie jak „First seen”, „Last seen”, „Vulnerable to”, „Services”. Z niewyjaśnionego jednak powodu to narzędzie nie było w stanie dokonać poprawnej analizy

sluchawek SteelSeries – zwrócone zostało n/a zamiast rzeczywistych informacji, które zostały znalezione przez poprzedni program.

Time	Address	Clk off	Class	Name
2025/10/17 11:51:13	08:C8:C2:73:E1:0D	0x7510	0x6c010c	kali
2025/10/17 11:51:10	5C:33:7B:F7:4F:7D	0x5ced	0x5a420c	Pixel 8 Pro
2025/10/17 11:51:11	20:AF:1B:0B:07:CE	0x23f7	0x240418	SteelSeries Arctis Nova 5X

Poniżej można zobaczyć dokładne opisy trzech urządzeń, na których się skupiliśmy.

RSSI:	+0	LQ:	000	TXPWR:	Cur	+0
Address:	08:C8:C2:73:E1:0D					
Found by:	00:01:95:7D:ED:BD					
OUI owner:						
First seen:	2025/10/17 11:50:30					
Last seen:	2025/10/17 11:51:51					
Name:	kali					
Vulnerable to:						
Clk off:	0x7510					
Class:	0x6c010c					
	Computer/Laptop					
Services:	Rendering,Capturing,Audio,Telephony					
HCI Version						

LMP Version: 4.0 (0x6) LMP Subversion: 0x2031						
Manufacturer: Cambridge Silicon Radio (10)						
HCI Features						

Features:	0xff 0xff 0x8f 0xfe					
<3-slot packets> <5-slot packets> <encryption> <slot offset>						
<timing accuracy> <role switch> <hold mode> <sniff mode> <park state>						
<RSSI> <channel quality> <SCO link> <HV2 packets> <HV3 packets>						
<u-law log> <A-law log> <CVSD> <paging scheme> <power control>						
<transparent SCO> <broadcast encrypt> <EDR ACL 2 Mbps>						
<EDR ACL 3 Mbps> <enhanced iscan> <interlaced iscan>						
<interlaced pscan> <inquiry with RSSI> <extended SCO> <EV4 packets>						
<EV5 packets> <AFH cap. perip.> <AFH cls. perip.> <LE support>						
<3-slot EDR ACL> <5-slot EDR ACL> <sniff subrating>						
<pause encryption> <AFH cap. central> <AFH cls. central>						
<EDR eSCO 2 Mbps> <EDR eSCO 3 Mbps> <3-slot EDR eSCO>						
<extended inquiry> <LE and BR/EDR> <simple pairing>						
<encapsulated PDU> <non-flush flag> <LST0> <inquiry TX power> <EPC>						
<extended features>						

Wynik 5: opis laptopa Kali Linux wykonany btscanner

RSSI: +0 LQ: 000 TXPWR: Cur +0
Address: 5C:33:7B:F7:4F:7D
Found by: 00:01:95:7D:ED:BD
OUI owner:
First seen: 2025/10/17 11:50:03
Last seen: 2025/10/17 11:51:49
Name: Pixel 8 Pro
Vulnerable to:
Clk off: 0x5cee
Class: 0x5a420c
Phone/Smart phone
Services: Reserved, Networking, Capturing, Object Transfer, Telephony

HCI Version

LMP Version: 5.4 (0xd) LMP Subversion: 0x8113

Manufacturer: Broadcom Corporation (15)

HCI Features

Features: 0xbf 0xfe 0x8f 0xfe

<3-slot packets> <5-slot packets> <encryption> <slot offset>
<timing accuracy> <role switch> <sniff mode> <RSSI> <channel quality>
<SCO link> <HV2 packets> <HV3 packets> <u-law log> <A-law log> <CVSD>
<paging scheme> <power control> <transparent SCO> <broadcast encrypt>
<EDR ACL 2 Mbps> <EDR ACL 3 Mbps> <enhanced iscan> <interlaced iscan>
<interlaced pscan> <inquiry with RSSI> <extended SCO> <EV4 packets>
<EV5 packets> <AFH cap. perip.> <AFH cls. perip.> <LE support>
<3-slot EDR ACL> <5-slot EDR ACL> <sniff subrating>
<pause encryption> <AFH cap. central> <AFH cls. central>
<EDR eSCO 2 Mbps> <EDR eSCO 3 Mbps> <3-slot EDR eSCO>
<extended inquiry> <LE and BR/EDR> <simple pairing>
<encapsulated PDU> <err. data report> <non-flush flag> <LST0>
<inquiry TX power> <EPC> <extended features>

Wynik 6: opis telefonu Pixel wykonany btscanner

```
RSSI:      +0    LQ: 000    TXPWR: Cur   +0
Address:    20:AF:1B:0B:07:CE
Found by:   00:01:95:7D:ED:BD
OUI owner:
First seen: 2025/10/17 11:50:01
Last seen:  2025/10/17 11:52:14
Name:       SteelSeries Arctis Nova 5X
Vulnerable to:
Clk off:    0x23f7
Class:      0x240418
            Audio-Video/Headphones
Services:   Rendering,Audio

HCI Version
-----
LMP Version: n/a (n/a) LMP Subversion: n/a
Manufacturer: n/a (n/a)

HCI Features
-----
Features:    n/a n/a n/a n/a
```

Wynik 7: niekompletny opis słuchawek SteelSeries wykonany btscanner

```
sudo l2ping <adres MAC>
```

Ping wykonany na wszystkie urządzenia zakończył się sukcesem – odpowiadają ode na pakiety.

```
Ping: 20:AF:1B:0B:07:CE from 00:01:95:7D:ED:BD (data size 44) ...
44 bytes from 20:AF:1B:0B:07:CE id 0 time 13.82ms
44 bytes from 20:AF:1B:0B:07:CE id 1 time 30.17ms
44 bytes from 20:AF:1B:0B:07:CE id 2 time 7.40ms
44 bytes from 20:AF:1B:0B:07:CE id 3 time 7.12ms
44 bytes from 20:AF:1B:0B:07:CE id 4 time 7.59ms
44 bytes from 20:AF:1B:0B:07:CE id 5 time 9.95ms
```

```
→ ~ sudo l2ping 5C:33:7B:F7:4F:7D
Ping: 5C:33:7B:F7:4F:7D from 00:01:95:7D:ED:BD (data size 44) ...
44 bytes from 5C:33:7B:F7:4F:7D id 0 time 104.46ms
44 bytes from 5C:33:7B:F7:4F:7D id 1 time 116.28ms
44 bytes from 5C:33:7B:F7:4F:7D id 2 time 84.82ms
44 bytes from 5C:33:7B:F7:4F:7D id 3 time 91.92ms
```



```
→ ~ sudo l2ping 08:C8:C2:73:E1:0D
Ping: 08:C8:C2:73:E1:0D from 00:01:95:7D:ED:BD (data size 44) ...
44 bytes from 08:C8:C2:73:E1:0D id 0 time 12.88ms
44 bytes from 08:C8:C2:73:E1:0D id 1 time 50.88ms
44 bytes from 08:C8:C2:73:E1:0D id 2 time 62.08ms
44 bytes from 08:C8:C2:73:E1:0D id 3 time 30.91ms
```

Wynik 8: l2ping wykonany dla słuchawek, telefonu i laptopa

```
sudo sdptool browse <adres MAC>
```

sdptool, jak nazwa wskazuje, służy do aktywowania protokołu SDP (Service Discovery Protocol) do analizowania dostępnych urządzeń Bluetooth i odpalonych na nich serwisach. Na każdym z urządzeń można zauważyć serwisy (znajdzone lub nieznajdzone – PnP, RecHandle) oraz powiązane z nimi protokoły (L2CAP, AVCTP, ATT).

```
→ ~ sudo sdptool browse 20:AF:1B:0B:07:CE
Browsing 20:AF:1B:0B:07:CE ...
Service RecHandle: 0x10001
Service Class ID List:
  "PnP Information" (0x1200)
Language Base Attr List:
  code_IS0639: 0x656e
  encoding: 0x6a
  base_offset: 0x100
Profile Descriptor List:
  "PnP Information" (0x1200)
  Version: 0x0103

Browsing 20:AF:1B:0B:07:CE ...
Service Search failed: Invalid argument
Service RecHandle: 0x10002
Service Class ID List:
  "Audio Sink" (0x110b)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 25
  "AVDTP" (0x0019)
    uint16: 0x0103
Profile Descriptor List:
  "Advanced Audio" (0x110d)
    Version: 0x0104

Service RecHandle: 0x10003
Service Class ID List:
  "AV Remote" (0x110e)
  "AV Remote Controller" (0x110f)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 23
  "AVCTP" (0x0017)
    uint16: 0x0104
Profile Descriptor List:
  "AV Remote" (0x110e)
    Version: 0x0106
```

```
→ ~ sudo sdptool browse 5C:33:7B:F7:4F:7D
Browsing 5C:33:7B:F7:4F:7D ...
Service RecHandle: 0x10000
Service Class ID List:
  "Generic Attribute" (0x1801)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 31
  "ATT" (0x0007)
    uint16: 0x0001
    uint16: 0x0009

Service RecHandle: 0x10001
Service Class ID List:
  "Generic Access" (0x1800)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 31
  "ATT" (0x0007)
    uint16: 0x0014
    uint16: 0x001a

Service Name: Advanced Audio Source
Service RecHandle: 0x10003
Service Class ID List:
  "Audio Source" (0x110a)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 25
  "AVDTP" (0x0019)
    uint16: 0x0103
Profile Descriptor List:
  "Advanced Audio" (0x110d)
    Version: 0x0104
```



```

→ ~ sudo sdptool browse 08:C8:C2:73:E1:0D
Browsing 08:C8:C2:73:E1:0D ...
Service RecHandle: 0x10000
Service Class ID List:
"PnP Information" (0x1200)
Profile Descriptor List:
"PnP Information" (0x1200)
Version: 0x0103

Browsing 08:C8:C2:73:E1:0D ...
Service Search failed: Invalid argument
Service Name: Generic Access Profile
Service Provider: BlueZ
Service RecHandle: 0x10001
Service Class ID List:
"Generic Access" (0x1800)
Protocol Descriptor List:
"L2CAP" (0x0100)
PSM: 31
"ATT" (0x0007)
uint16: 0x0001
uint16: 0x0005

Service Name: Generic Attribute Profile
Service Provider: BlueZ
Service RecHandle: 0x10002
Service Class ID List:
"Generic Attribute" (0x1801)
Protocol Descriptor List:
"L2CAP" (0x0100)
PSM: 31
"ATT" (0x0007)
uint16: 0x0006
uint16: 0x000f

```

Wynik 9: analiza sdptool browse słuchawek, telefonu i laptopa

sudo bettercap

Pozwala on na analizę wielu typów ruchu bezprzewodowego, ale działa również dla Bluetooth. Po uruchomieniu szukane są urządzenia – jest ich więcej niż 3, które wcześniej analizowaliśmy.

```

→ ~ sudo bettercap
bettercap v2.41.3 (built for linux amd64 with go1.25.1 X:nodwarf5) [type 'help' for a list of commands]

10.230.200.0/24 > 10.230.200.80 » [12:00:35] [sys.log] [war] executable netstat not found in $PATH
10.230.200.0/24 > 10.230.200.80 » [12:00:35] [sys.log] [war] Could not detect gateway.
10.230.200.0/24 > 10.230.200.80 » ble.recon on
BLE » [12:00:45] [ble.device.new] new BLE device detected as 4B:2C:40:D4:51:64 (Apple, Inc.) -74 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 0A:26:70:44:C6:B4 (Microsoft) -51 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 62:8A:96:89:C1:52 (Apple, Inc.) -64 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 13:E2:49:55:82:F8 (Microsoft) -61 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 5C:E2:1C:F3:74:28 (Apple, Inc.) -54 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as E4:27:D2:70:7C:AB (Apple, Inc.) -66 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 73:77:9B:CA:D3:B9 (Apple, Inc.) -63 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 1C:76:49:46:52:96 (Microsoft) -71 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 20:AF:1B:0B:07:CE (SteelSeries ApS) -54 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 4C:F1:59:4A:3C:91 (Apple, Inc.) -71 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 6D:6E:B7:C4:BC:3A (Sony Corporation) -45 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 63:A3:13:3A:12:E9 (Apple, Inc.) -72 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 64:80:66:A0:57:03 (Apple, Inc.) -68 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 62:E8:E7:27:D8:A1 (Apple, Inc.) -64 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 3D:59:0C:D7:9C:CD (Microsoft) -69 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as CD:CF:E5:CA:1A:58 (Apple, Inc.) -83 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 03:90:7C:69:62:B2 (Microsoft) -68 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as C7:BF:E4:0B:C2:A4 (Apple, Inc.) -76 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 7C:2D:3D:03:33:C3 (Apple, Inc.) -65 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 62:03:8D:B6:C3:55 (Apple, Inc.) -70 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 65:4B:AC:25:A2:88 (Apple, Inc.) -79 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 79:84:AF:88:84:01 (Apple, Inc.) -63 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 52:46:9A:81:40:56 (Apple, Inc.) -75 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as 57:3B:3E:6A:2E:34 (Apple, Inc.) -79 dBm.
BLE » [12:00:45] [ble.device.new] new BLE device detected as D9:E1:25:17:00:C3 (Apple, Inc.) -64 dBm.
BLE » [12:00:46] [ble.device.new] new BLE device detected as EB:74:EB:6F:74:19 (Apple, Inc.) -70 dBm.
BLE » [12:00:46] [ble.device.new] new BLE device detected as 16:FF:58:34:C3:7E -73 dBm.
BLE » [12:00:46] [ble.device.new] new BLE device detected as E2:7D:61:B2:7B:24 (Apple, Inc.) -56 dBm.
BLE » [12:00:46] [ble.device.new] new BLE device detected as 41:43:28:AE:A5:BF (Apple, Inc.) -55 dBm.
BLE » [12:00:46] [ble.device.new] new BLE device detected as DD:68:D1:BC:B2:0F (Apple, Inc.) -64 dBm.
BLE » [12:00:46] [ble.device.new] new BLE device detected as C4:F7:FC:19:F9:A0 (Apple, Inc.) -80 dBm.
BLE » [12:00:46] [ble.device.new] new BLE device detected as EA:73:54:CF:08:6B (Apple, Inc.) -75 dBm.
BLE » [12:00:46] [ble.device.new] new BLE device detected as F1:F0:FB:0E:A1:BA (Apple, Inc.) -69 dBm.

```

Wynik 10: bettercap uruchomiony w sali laboratoryjnej

```
ble.recon on -> ble.recon off -> ble.show
```

Po włączeniu skanowania `ble.recon` on i odczekaniu kilku minut, można zobaczyć wyniki skanu. Podstawowe informacje o urządzeniach są wyświetlone w wygodny sposób, posortowane według jakości sygnału wyrażonej w dBm.

RSSI	MAC	Name	Vendor	Flags	Connect	Seen
-50 dBm	50:91:c6:f7:79:87		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✗	12:12:25
-51 dBm	59:1e:23:48:3f:3f		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:25
-51 dBm	e2:7d:61:b2:7b:24		Apple, Inc.		✗	12:12:21
-54 dBm	79:99:40:78:d1:ae		Sony Corporation		✓	12:12:25
-55 dBm	d9:e1:25:17:00:c3		Apple, Inc.		✗	12:12:23
-56 dBm	0a:ad:40:95:c9:74		Microsoft		✗	12:12:25
-59 dBm	1e:e0:e5:36:1f:b9		Microsoft		✗	12:12:25
-62 dBm	4b:2c:40:d4:51:64		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:25
-64 dBm	1a:ea:93:ac:bc:07		Microsoft		✗	12:12:25
-65 dBm	41:eb:01:a9:9a:0f	LE_WH-1000XMS	Sony Corporation		✓	12:11:59
-66 dBm	3f:5f:8e:82:ad:97		Microsoft		✗	12:12:25
-67 dBm	79:de:2b:3f:8c:61		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:10
-67 dBm	c2:cd:6e:f9:14:6b		Apple, Inc.		✗	12:12:25
-67 dBm	fe:4b:a7:94:b6:33		Apple, Inc.		✗	12:12:25
-68 dBm	20:af:1b:0b:07:ce	SteelSeries Arctis Nova SX	SteelSeries ApS		✓	12:12:25
-68 dBm	4e:1b:05:96:95:92		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:25
-68 dBm	5a:96:ce:b6:13:c1		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:25
-68 dBm	dd:68:d1:bc:b2:0f		Apple, Inc.		✗	12:12:17
-68 dBm	f6:73:e3:3b:7b:42		Apple, Inc.		✗	12:12:23
-69 dBm	db:31:dd:06:79:a8		Apple, Inc.		✗	12:12:25
-69 dBm	e2:e3:35:8a:8c:f1		Apple, Inc.		✗	12:12:21
-70 dBm	76:02:c1:9b:d3:35		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:25
-71 dBm	69:6e:a9:0f:d9:3d		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✗	12:12:25
-72 dBm	65:4b:ac:25:a2:88		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:25
-72 dBm	f1:f0:fb:0e:a1:ba		Apple, Inc.		✗	12:12:24
-73 dBm	f1:07:42:f3:c2:0f		Apple, Inc.		✗	12:12:25
-74 dBm	48:82:46:a4:87:ff		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:25
-74 dBm	72:08:e9:13:c2:65		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:23
-74 dBm	c2:ef:88:bb:91:33		Apple, Inc.		✗	12:12:24
-75 dBm	23:b3:b1:82:8f:6d				✗	12:12:25
-76 dBm	f9:ce:0b:5b:32:ce		Apple, Inc.		✗	12:12:24
-77 dBm	64:9f:28:98:df:dd		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:24
-77 dBm	74:3e:c1:3e:65:be		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:25
-77 dBm	cd:56:90:84:af:1e		Apple, Inc.		✗	12:12:22
-77 dBm	f6:38:d8:40:7b:4b		Apple, Inc.		✓	12:12:18
-79 dBm	19:d0:6d:15:f9:51		Microsoft		✗	12:12:25
-79 dBm	63:a3:13:3a:12:e9		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:11:55
-80 dBm	de:0a:7b:d9:84:34		Apple, Inc.		✗	12:12:20
-82 dBm	62:8a:96:89:c1:52		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✗	12:12:23
-83 dBm	74:63:89:60:ad:d4		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:24
-85 dBm	79:84:af:88:84:01		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	12:12:23
-89 dBm	c4:f7:fc:19:f9:a0		Apple, Inc.		✗	12:12:22
-92 dBm	08:89:72:3b:93:34				✗	12:12:14
-96 dBm	23:d8:3b:9c:30:c7		Microsoft		✗	12:12:21

Wynik 11: Analiza ruchu sieciowego narzędziem ble

```
ble.enum <adres MAC>
```

Próbowano wykonać enumerację dla słuchawek SteelSeries, lecz z nie udało się naprawić problemu z timeout.

```
10.230.200.0/24 > 10.230.200.80 » ble.enum 20:af:1b:0b:07:ce
[12:41:07] [sys.log] [inf] ble.recon connecting to 20:af:1b:0b:07:ce ...
10.230.200.0/24 > 10.230.200.80 » [12:41:12] [sys.log] [war] ble.recon
connection timeout
10.230.200.0/24 > 10.230.200.80 » ble.enum 20:af:1b:0b:07:ce
[12:41:36] [sys.log] [inf] ble.recon connecting to 20:af:1b:0b:07:ce ...
10.230.200.0/24 > 10.230.200.80 » [12:41:41] [sys.log] [war] ble.recon
connection timeout
10.230.200.0/24 > 10.230.200.80 » ble.enum 20:af:1b:0b:07:ce
[12:41:44] [sys.log] [inf] ble.recon connecting to 20:af:1b:0b:07:ce ...
10.230.200.0/24 > 10.230.200.80 » [12:41:49] [sys.log] [war] ble.recon
connection timeout
```

Wynik 12: Nieudana analiza słuchawek przy pomocy narzędzia ble

`sudo bettercap -eval "ui on"` – skan urządzeń BLE, porównanie z `ble.enum`

```
→ ~ sudo bettercap -eval "ui on"
bettercap v2.41.3 (built for linux amd64 with go1.25.1 X:nodwarf5) [type 'help'
for a list of commands]

[12:43:27] [sys.log] [war] executable netstat not found in $PATH
[12:43:27] [sys.log] [war] Could not detect gateway.
[12:43:27] [sys.log] [inf] ui starting api.rest as a requirement for ui
[12:43:27] [sys.log] [inf] api.rest api server starting on http://127.0.0.1:8081
10.230.200.0/24 > 10.230.200.80 » [12:43:27] [sys.log] [inf] ui web ui starting
on http://127.0.0.1:8080
```

RSSI	MAC	Name	Vendor	Flags	Connectable	Services	Seen
-70	75:5E:D6:5D:7E:7E	OPPO Enco Air3 Pro	unknown	LE + BR/EDR (controller)	✓	🔊	12:45:48
-70	48:EF:6D:D7:FC:23	LE_WH-1000XM5	unknown	none	✓	🔊	12:46:20
-70	5E:74:F5:08:4D:FA		Microsoft	none	✗	🔊	12:46:21
-70	5E:74:F5:08:4D:FA		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✗	🔊	12:46:16
-70	20:AF:1B:0B:07:CE		SteelSeries ApS	none	✗	🔊	12:46:21
-70	D9:8D:0D:A6:4E:77		Apple, Inc.	none	✗	🔊	12:46:20
-70	74:E7:4E:73:44:23		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	🔊	12:46:21
-70	06:2C:A0:52:31:0E		Microsoft	none	✗	🔊	12:46:20
-70	C9:D1:01:01:B8:68		Apple, Inc.	none	✗	🔊	12:46:20
-70	12:39:33:85:53:93		Microsoft	none	✗	🔊	12:46:18
-70	C2:01:83:30:34:85		Apple, Inc.	none	✗	🔊	12:46:20
-70	6F:09:30:89:71:16		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	🔊	12:46:21
-70	FC:84:9B:06:62:8E		Apple, Inc.	none	✗	🔊	12:46:20
-70	C5:3F:1C:36:09:3B		Apple, Inc.	none	✗	🔊	12:46:13
-70	9F:F3:7C:99:04:74		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	🔊	12:46:21
-70	CB:66:09:30:6C:1C		Apple, Inc.	none	✗	🔊	12:46:20
-70	04:D4:96:17:85:6D		Microsoft	none	✗	🔊	12:46:21
-70	64:72:8C:D1:E2:50		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	🔊	12:46:20
-70	4E:38:8D:A4:F2:32		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✓	🔊	12:46:20
-70	4E:38:8D:A4:F2:32		Apple, Inc.	LE + BR/EDR (controller), LE + BR/EDR (host)	✗	🔊	12:46:21

Wynik 13: analiza przy pomocy bettercap z UI

Wynik jest bardzo podobny do analizy przy pomocy `ble.show`, ale nie widać dokładnej wartości w dBm.

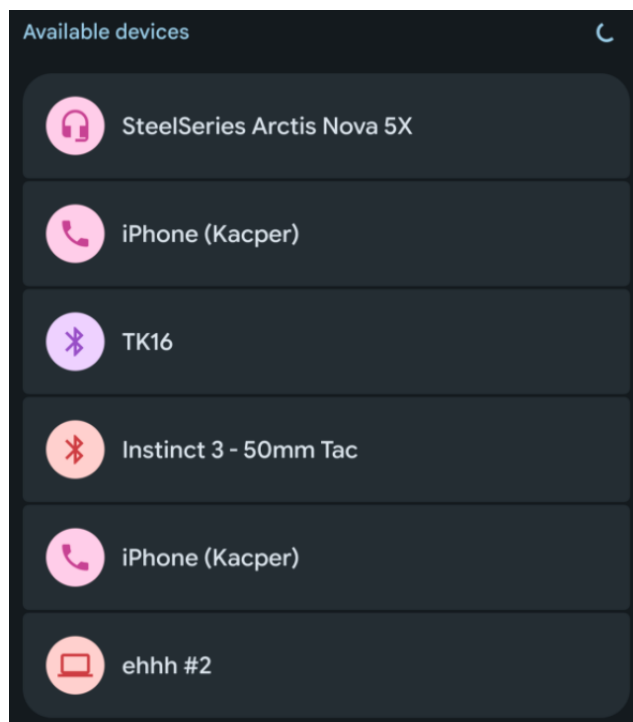
Spoofing Bluetooth Devices

Jako cel obraliśmy słuchawki telefon iPhone (Kacper). Ponownie zostało użyte narzędzie `btscanner`, żeby zdobyć informacje. Po wykonaniu poleceń, Kali Linux podszywający się pod telefon Kacpra pojawił się w możliwych połączeniach Bluetooth.

```
(student@kali)-[~]
$ sudo bluetoothctl system-alias 'iPhone (Kacper)'
Changing iPhone (Kacper) succeeded

(honey@kali)-[~]
$ sudo hciconfig -a
hci1: Type: Primary Bus: USB
      BD Address: 28:C1:A0:3D:06:72 ACL MTU: 310:10 SCO MTU: 64:8
      UP RUNNING
      RX bytes:1286 acl:0 sco:0 events:61 errors:0
      TX bytes:4355 acl:0 sco:0 commands:60 errors:0
      Features: 0xff 0xff 0x8f 0xfe 0xdb 0xff 0x5b 0x87
      Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
      Link policy: RSWITCH HOLD SNIFF PARK
      Link mode: PERIPHERAL ACCEPT
      Name: 'iPhone (Kacper)'
      Class: 0x7a020c
      Service Classes: Networking, Capturing, Object Transfer, Audio, Telep
      Device Class: Phone, Smart phone
      HCI Version: 4.0 (0x6) Revision: 0x2031
      LMP Version: 4.0 (0x6) Subversion: 0x2031
      Manufacturer: Cambridge Silicon Radio (10)
```

Laptop 1: Zmiana aliasu na laptopie i jego klasy

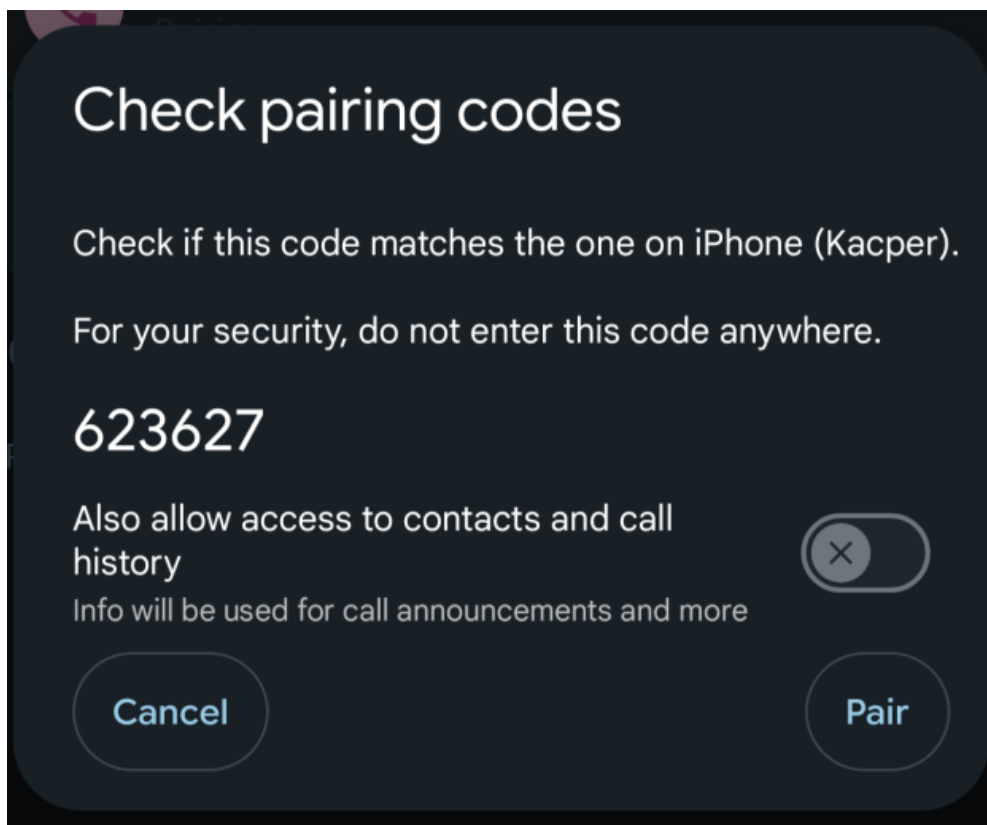


Telefon 1: Kali Linux podszywający się pod telefon

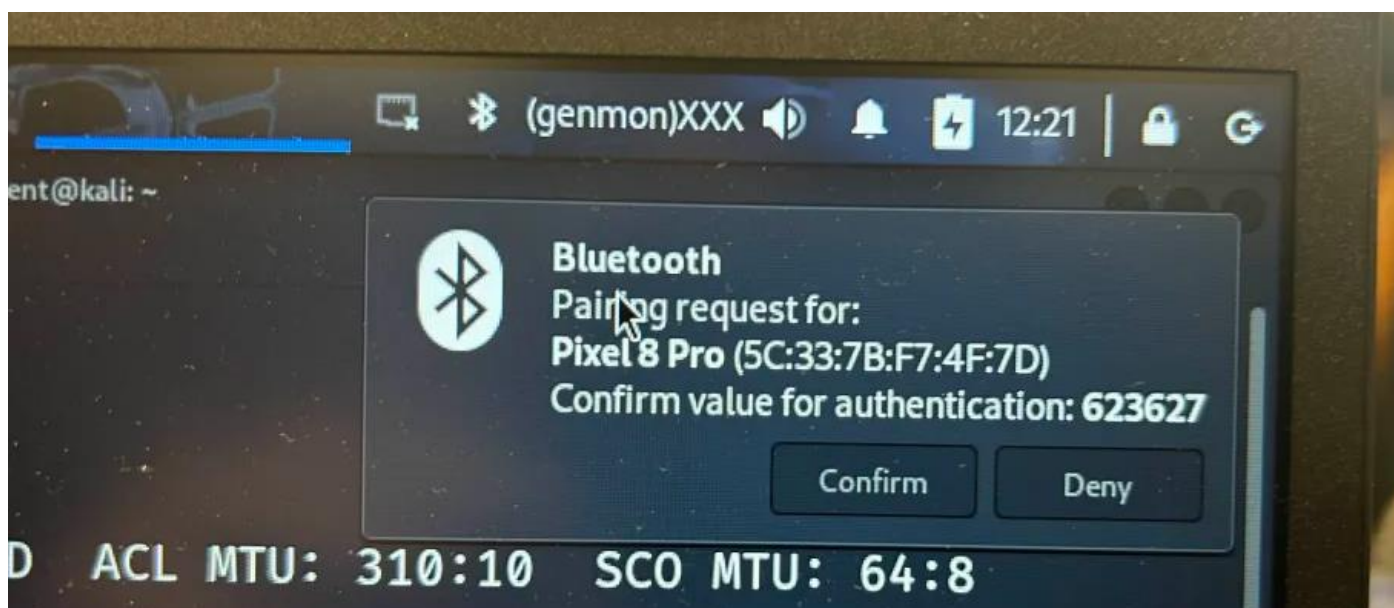
Skan pokazuje, że rzeczywiście są dwa teoretycznie takie same urządzenia, ale o innym adresie MAC.

Time	Address	Clk off	Class	Name
2025/10/17 12:07:29	00:01:95:7D:ED:BD	0x6354	0x7c010c	ehhh #2
2025/10/17 12:08:36	08:C8:C2:73:E1:0D	0x585b	0x6c010c	iPhone (Kacper)
2025/10/17 12:08:48	5C:33:7B:F7:4F:7D	0x4029	0x5a420c	Pixel 8 Pro
2025/10/17 12:08:48	28:C1:A0:3D:06:72	0x7ad0	0x7a020c	iPhone (Kacper)
2025/10/17 12:08:48	20:AF:1B:0B:07:CE	0x2379	0x240418	SteelSeries Arctis Nova 5X

Po zmianie adresu MAC na Kali Linuxie, widać było tylko jedno urządzenie – iPhone (Kacper), do którego podłączono się telefonem Pixel.



Telefon 2: Połączenie z podstawionym urządzeniem

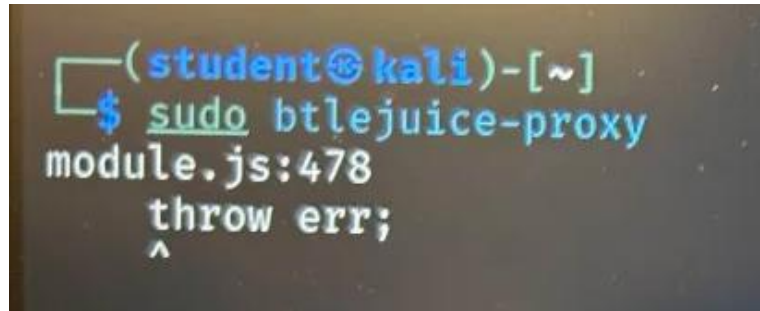


Laptop 2: Widok ze strony podstawionego urządzenia

Atak Man-in-the-Middle

Server proxy został uruchomiony na pierwszym Kali Linuxie po próbach naprawy – niestety program ostatni raz był aktualizowany około 7 lat temu.

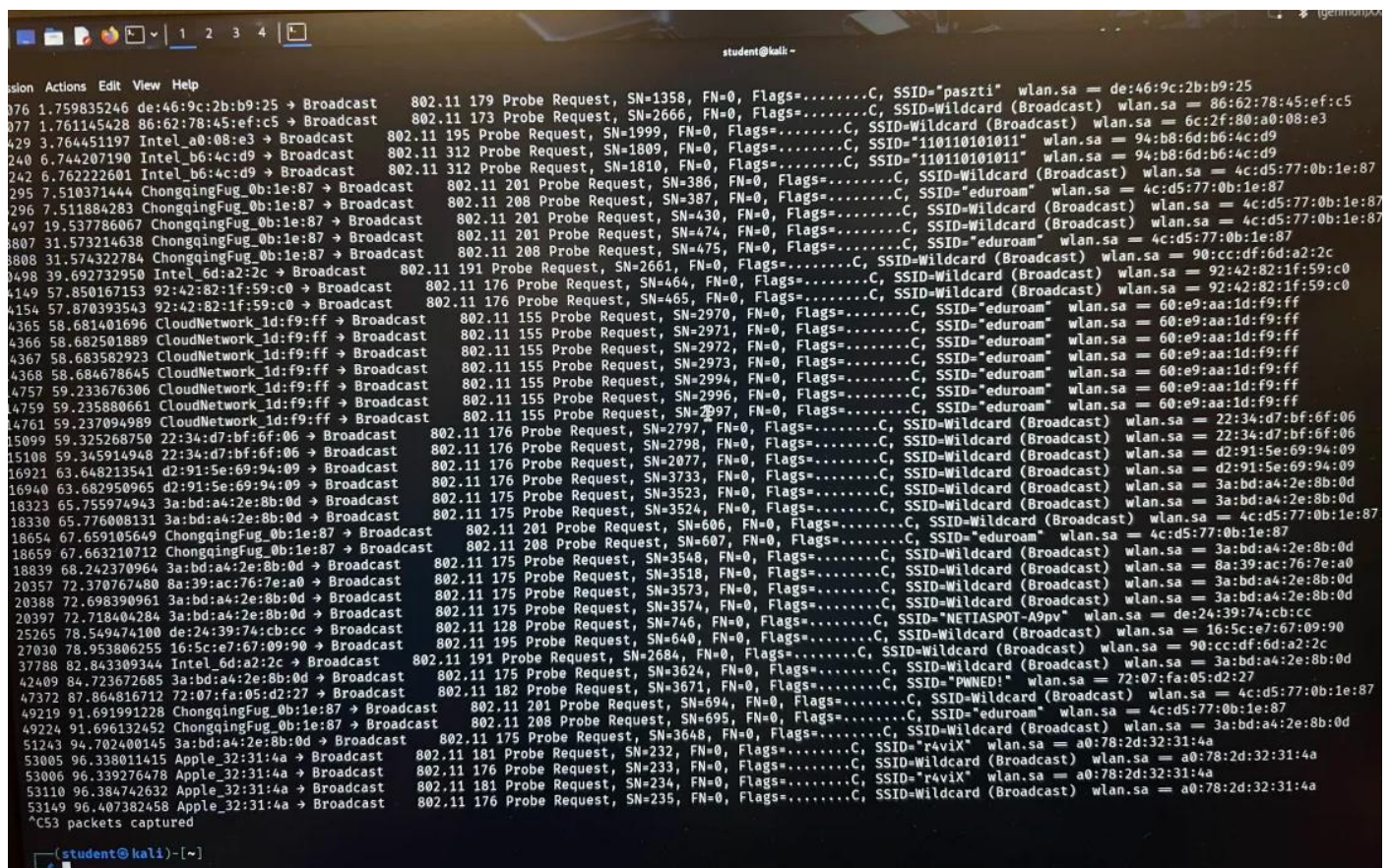
Drugi Kali Linux połączył się z proxy, o czym został powiadomiony serwer. Na localhost:8080 próbowano wybrać cel, ale wtedy otrzymaliśmy nieznany błąd na proxy.



Error 1: Błąd btblejuice-proxy zgłaszany w trakcie zajęć

Bluetooth Off-by-One

Po zatrzymaniu procesów wpływających na interfejs bezprzewodowy (905 wpa_supplicant), włączono tryb monitorowania na karcie bezprzewodowej wlan0. Po użyciu narzędzia tshark nie udało się jednak znaleźć adresów MAC spełniających warunek off-by-one. Następnie wyłączony został tryb monitorowania.



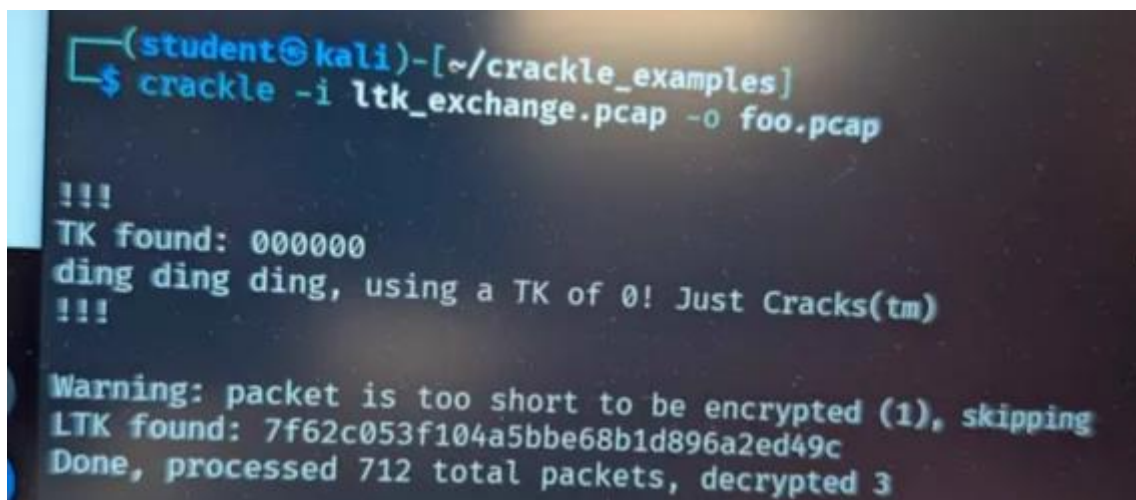
Error 2: Nieznalezienie urządzeń spełniające warunek z zadania

bluetooth_tools nie zostało wgrane na nasze maszyny z Kali Linux, zatem nie byliśmy w stanie dokończyć zadania.

Bluetooth Low Energy TK Cracking

Po pobraniu plików z eportalu zostały wykonane komendy:

```
crackle -i ltk_...
```

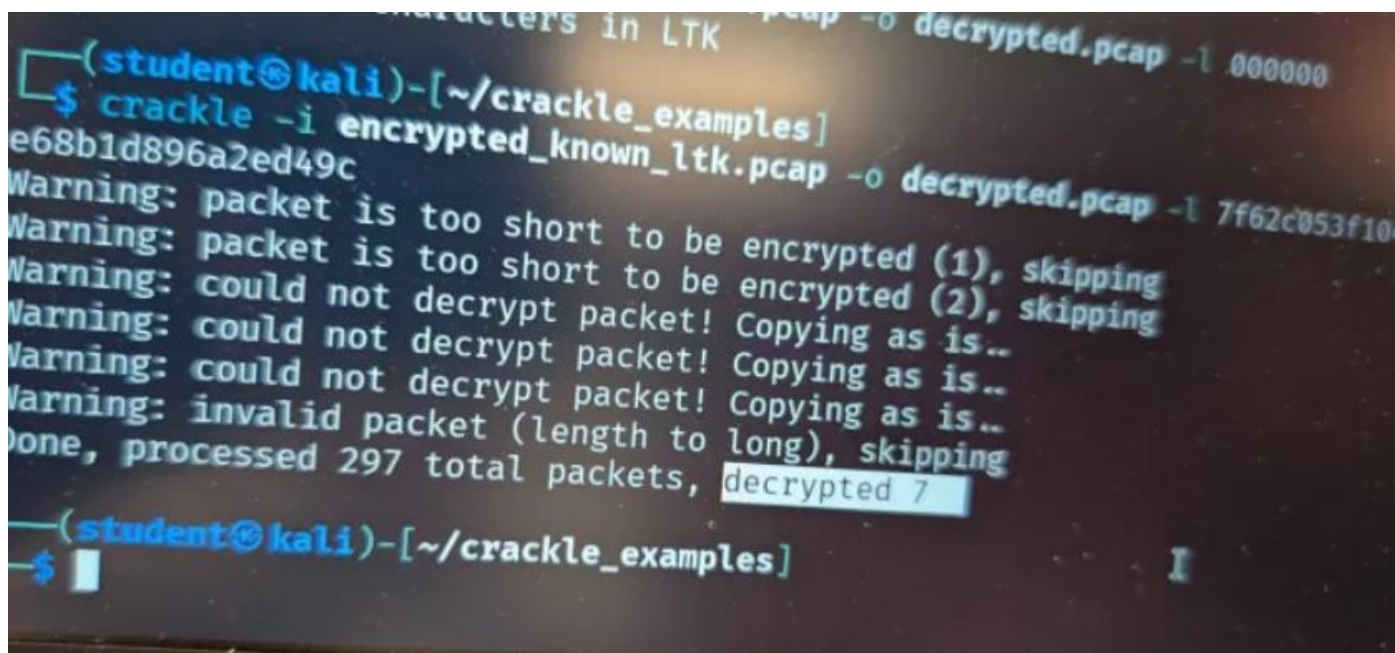


Wynik 14: odzyskanie klucza TK i LTK z transmisji sieciowej

TK found: 000000

LTK found: 7f62c...

```
crackle -i encrypted_known_ltk...
```



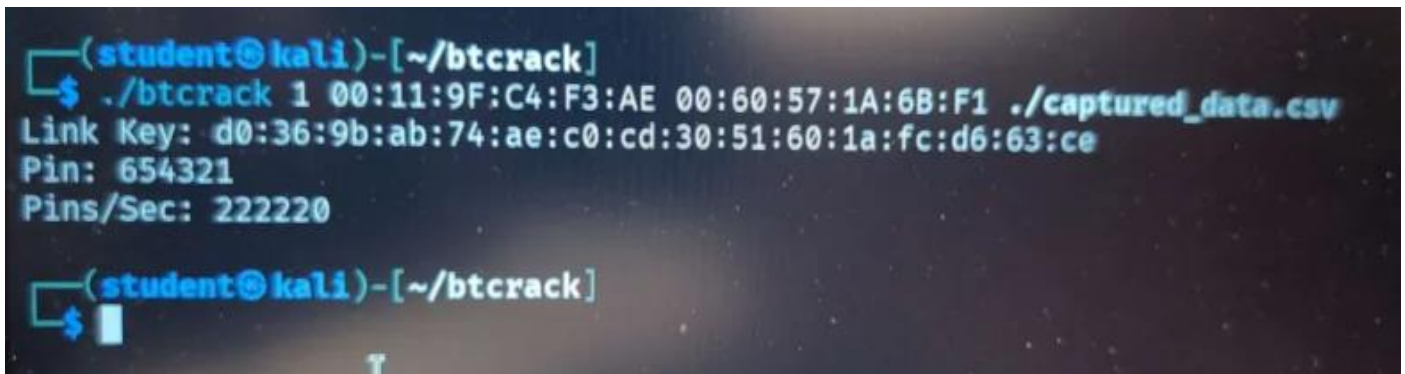
Wynik 15: deszyfracja pakietów odnalezionym kluczem LTK

Decrypted: 7

Udało się odszyfrować ruch sieciowy zgodnie z instrukcją.

Classic PIN Attack

Narzędziem **btcrack** zostały zcrackowane przechwycone dane do złamania klucza LK i kodu PIN, w wyniku tego zostały wyeksportowane informacje:

A terminal window screenshot showing the execution of the btcrack tool. The prompt is (student@kali)-[~/btcrack]. The command entered is ./btcrack 1 00:11:9F:C4:F3:AE 00:60:57:1A:6B:F1 ./captured_data.csv. The output shows the Link Key as d0:36:9b:ab:74:ae:c0:cd:30:51:60:1a:fc:d6:63:ce, the Pin as 654321, and Pins/Sec as 222220. The prompt then returns to (student@kali)-[~/btcrack].

```
(student@kali)-[~/btcrack]  
$ ./btcrack 1 00:11:9F:C4:F3:AE 00:60:57:1A:6B:F1 ./captured_data.csv  
Link Key: d0:36:9b:ab:74:ae:c0:cd:30:51:60:1a:fc:d6:63:ce  
Pin: 654321  
Pins/Sec: 222220  
  
(student@kali)-[~/btcrack]  
$
```

PIN: 654321

Link Key: 222220

Wnioski, obserwacje i analiza

Lorem ipsum dolor sit amet, consectetur adipiscing elit. In placerat neque sit amet felis tincidunt bibendum eget id odio. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Ut ac purus dictum, convallis magna vitae, malesuada risus. Pellentesque gravida dolor a porta ultrices. Quisque sit amet vulputate dolor. Curabitur eleifend vel augue in aliquam. Cras vitae fermentum tortor. Morbi sed lectus dapibus ex vestibulum tempus. Suspendisse eu urna enim. Donec eget erat lorem.