**ETHICAL HACKING – II**

**LAB ASSIGNMENT 2**

### \*\*Bluetooth Packet Analysis Without Physical Hardware Using Simulation Tools\*\*

If you don’t have access to Bluetooth hardware or sniffing devices like Ubertooth One, you can simulate Bluetooth packet analysis using virtual environments or pre-captured datasets.

### \*\*1. Prerequisites\*\*  
1. \*\*Wireshark Installed\*\*:  
   - Download and install Wireshark from [Wireshark's website](<https://www.wireshark.org/).>

A screenshot of a computer

Description automatically generated

2. \*\*Pre-Captured Bluetooth Traffic Files\*\*:  
   - Download Bluetooth `.pcap` files from online repositories like:  
     - [Wireshark Sample Captures](<https://wiki.wireshark.org/SampleCaptures).>  
     - [PacketTotal](<https://packettotal.com/).>  
   - Examples include:  
     - Files with L2CAP, HCI, and ATT traffic.  
     - Bluetooth Low Energy (BLE) captures for IoT devices

A screenshot of a computer

Description automatically generated

3. \*\*Virtualized Environment (Optional)\*\*:  
   - Use simulation tools to emulate Bluetooth behavior (e.g., Bluetooth emulators in Android SDK or IoT development platforms).

### \*\*2. Steps to Simulate Bluetooth Packet Analysis\*\*

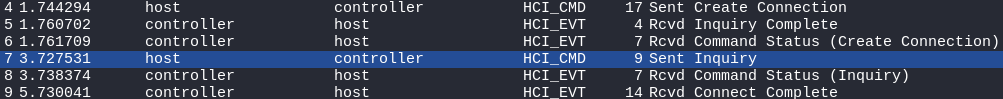
#### \*\*Step 1: Load Pre-Captured Files\*\*  
1. \*\*Open Wireshark\*\*:  
   - Launch Wireshark on your system.  
   - Click \*\*File > Open\*\*, and load a pre-captured `. pcap` file containing Bluetooth traffic.

A screenshot of a computer

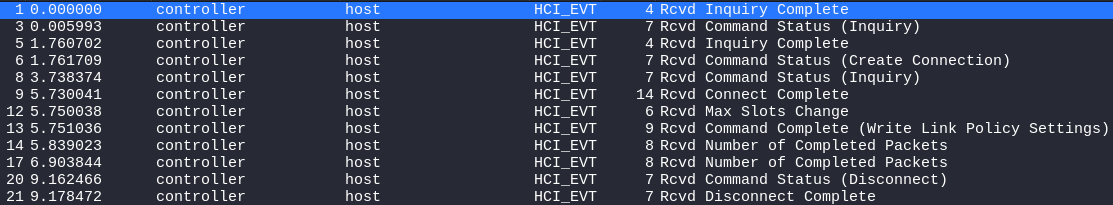
Description automatically generated

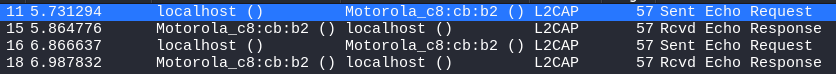
2. \*\*Analyze Sample Captures\*\*:  
   - Look for files with examples of:  
     - Device discovery.

  
     - Pairing process (HCI packets).

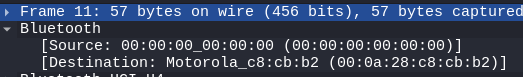
  
     - BLE communication (GATT/ATT protocols).

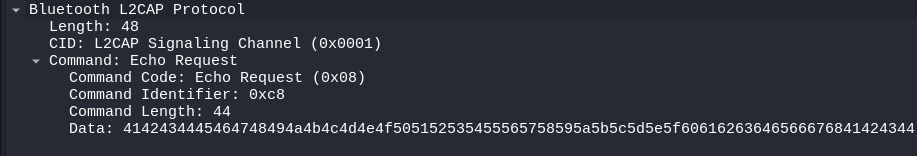
#### \*\*Step 2: Apply Bluetooth Protocol Filters\*\*  
1. \*\*Common Filters\*\*:  
   - `bthci\_evt`: HCI event packets, such as connection requests or status updates.

  
   - `btl2cap`: L2CAP traffic, which manages data between devices.

  
   - `btatt`: Attribute Protocol traffic for BLE devices.  
   - `btcommon`: General Bluetooth traffic, including discovery

2. \*\*Analyze Specific Traffic\*\*:  
   - Inspect protocol-specific fields:  
     - Device MAC addresses.

  
     - Connection handles.  
     - Data payloads in L2CAP or ATT packets.



#### \*\*Step 3: Simulate Activities\*\*  
1. \*\*Device Discovery\*\*:  
   - Look for HCI Inquiry and Inquiry Response packets:  
     - `bthci\_evt.inquiry\_result`: Lists devices discovered in the scan.

  
   - Observe details such as device names, class, and MAC addresses.

****

2. \*\*Pairing Process\*\*:  
   - Analyze pairing handshake using Secure Simple Pairing (SSP):  
     - Look for key exchange packets in HCI traffic (`bthci\_evt.link\_key\_notification`).

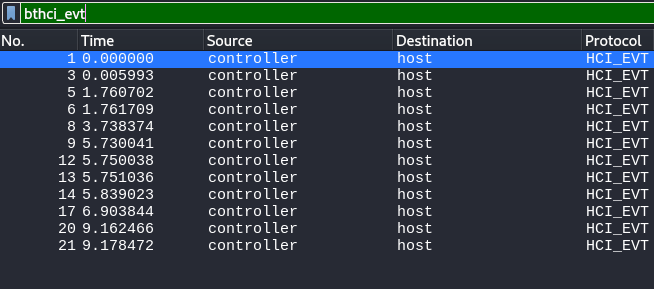
3. \*\*Data Exchange\*\*:  
   - Examine BLE-specific data transfers:  
     - Use `btatt` filters to inspect GATT operations like reading or writing characteristics.

#### \*\*Step 4: Use Simulated Bluetooth Environments\*\*  
If you prefer to simulate traffic dynamically:  
1. \*\*Android Emulator\*\*:  
   - Use the Android Studio Emulator to simulate Bluetooth activities like pairing or file transfers.  
   - Capture the resulting traffic with Wireshark on your host machine.

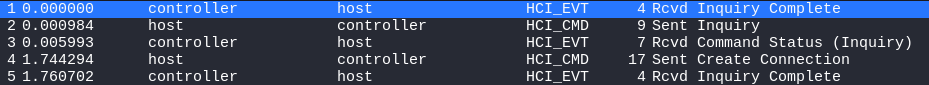
2. \*\*IoT Development Kits\*\*:  
   - Tools like Nordic Semiconductor’s nRF Connect SDK offer BLE simulation.  
   - Emulate BLE communication and capture traffic in virtualized environments.

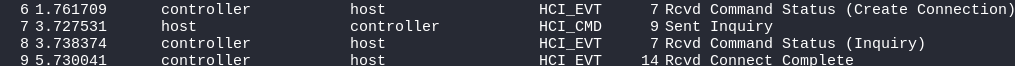
### \*\*3. Practical Exercises\*\*

#### \*\*Exercise 1: Analyze HCI Inquiry and Pairing\*\*  
- Objective: Understand how Bluetooth devices discover each other and establish connections.  
- Task:  
  - Load a capture with `bthci\_evt` packets.



  - Identify Inquiry and Response packets.

  
  - Trace the pairing process.



#### \*\*Exercise 2: Examine L2CAP Traffic\*\*  
- Objective: Study data transmission protocols.  
- Task:  
  - Use a capture with `btl2cap` traffic.

A screenshot of a computer

Description automatically generated  
  - Analyze the payload structure and device communication.

A black background with white text

Description automatically generated

#### \*\*Exercise 3: Investigate BLE GATT Operations\*\*  
- Objective: Explore Bluetooth Low Energy communication.  
- Task:  
  - Filter `btatt` traffic to see characteristic reads/writes.  
  - Identify the UUIDs of services and attributes.

### \*\*4. Benefits of This Approach\*\*  
1. \*\*Accessibility\*\*:  
   - No need for specialized hardware or real devices.  
   - Can be done entirely on a laptop or desktop.

2. \*\*Cost-Effective\*\*:  
   - Free tools and sample captures are readily available.

3. \*\*Safe and Controlled\*\*:  
   - No risk of intercepting unauthorized or sensitive real-world traffic.

### \*\*5. Challenges and Solutions\*\*  
1. \*\*Limited Realism\*\*:  
   - Pre-captured files may not replicate dynamic interactions.  
   - \*\*Solution\*\*: Use virtualized tools like Android emulators for interactivity.

2. \*\*Lack of Hardware-Specific Features\*\*:  
   - Some advanced Bluetooth attacks require physical sniffers.  
   - \*\*Solution\*\*: Focus on understanding theoretical concepts and protocol analysis.

### \*\*6. Wrap-Up\*\*  
This method allows students to learn Bluetooth hacking basics and security analysis without the need for physical hardware. By studying pre-captured files and simulating interactions in virtual environments, learners can gain practical insights into Bluetooth communication and vulnerabilities in a safe, cost-effective manner.