Capturing and analyzing Bluetooth traffic using Wireshark

Course: Mobile, Multimedia and Security Course Code: UE19EC342

Semester: 6 Department: Electronics and Communication Engineering

Academic Year: 2021 -22 Campus: Electronic City Campus

PES University

Group Number 17

Group Name Vasl

Members

Mansoora S PES2UG19EC070

Nikhita Sridhar PES2UG19EC086

Nikshitha SV PES2UG19EC087

Course Instructor: Bivas Bhattacharya

**PROJECT IDEA**

Upcoming mobile applications are constantly improving their use of advanced devices features like sensors and short-range networks. In particular we have seen wide-ranging use of Bluetooth. Bluetooth is a wireless technology used to exchange data at short range with high frequency radio waves. In our project, we are analyzing the captured Bluetooth packets using Wireshark.

**DEMONSTRATION FEATURE**

In this project we are analyzing Bluetooth packets which are ideally done by using dedicated devices like Ubertooth One. Since not all own a sniffing device, we can obtain the results using the new feature introduced in Android 4.4. The feature is the ability to capture all Bluetooth HCL packets and save them to a file. After populating the captured file by running the application being tested, we can pull the file generated by Android into the external storage of the device and analyze it using Wireshark. This project was conducted without connecting it to other Bluetooth devices.

**BACKGROUND THEORY**

Bluetooth is a short-range wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances. It operates in the frequency range:  of 2.402 to 2.48 GHz. It is mainly used as an alternative to wired connections.

**THEORETICAL EXPECTATION**

In this project, we mainly analyze the HCI ACL packets.

Acl frames are used to transfer nonreal time data between nodes in a Bluetooth network.

**The purpose of ACL-**

Unicast connection between one node and another node

Multicast- Connection between a set or other node.

Acl provides a mechanism to send large PDUs between nodes by a fragmentation mechanism that supports transferring PDUs up to 64 bytes in size.

**PROCEDURE**

The bug report is downloaded from the Android device and analyzed on the laptop. To do this, first plug in your phone to your laptop using a USB cable, then we go to settings --> about phone --> build number

Click on it a few times and then enter the phone's pin, this will enable us to be the developer

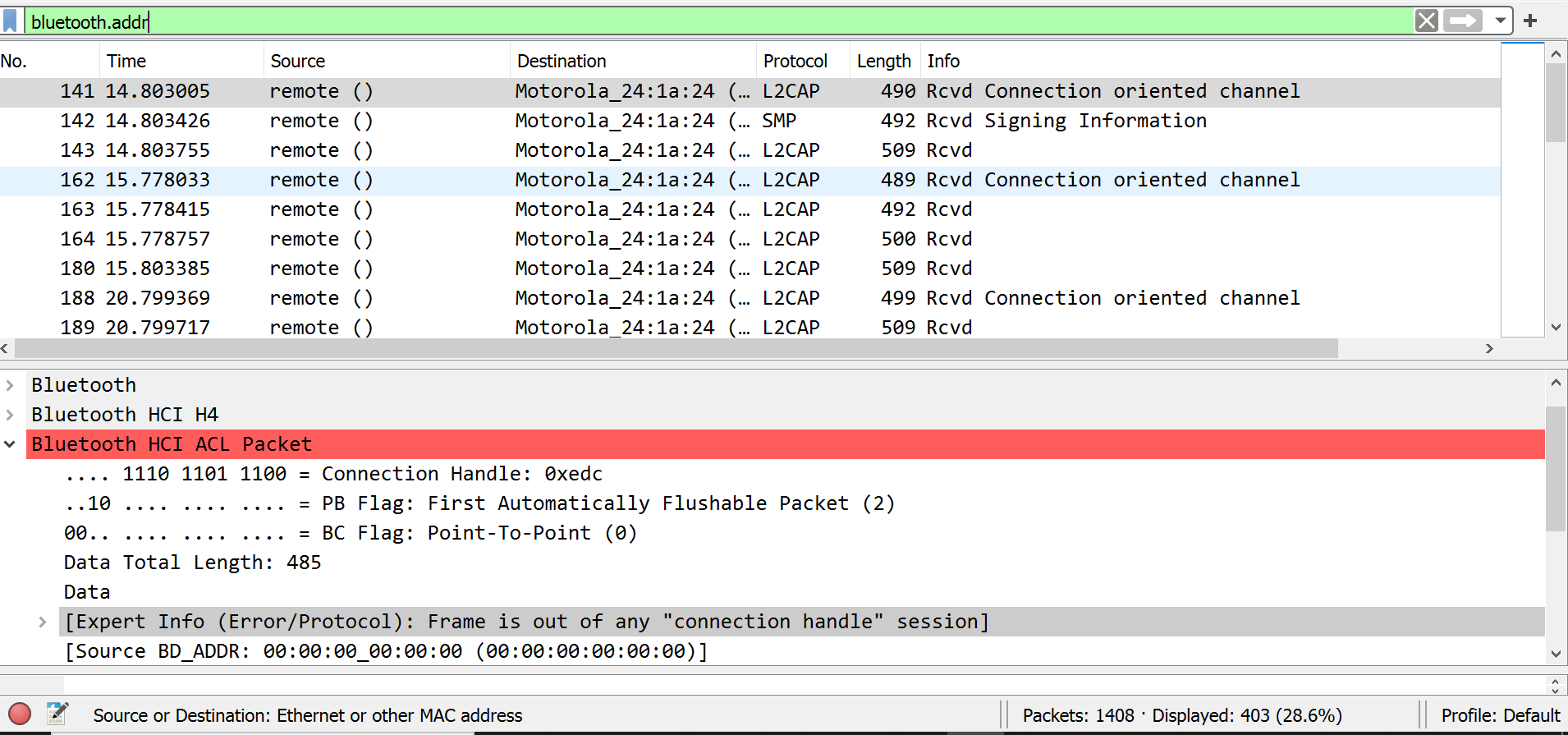
Now go to settings --> system --> developer options --> enable Bluetooth HCI snoop log --> enabled

This will enable the snoop log. Next, we need to enable USB debugging present in developer options.

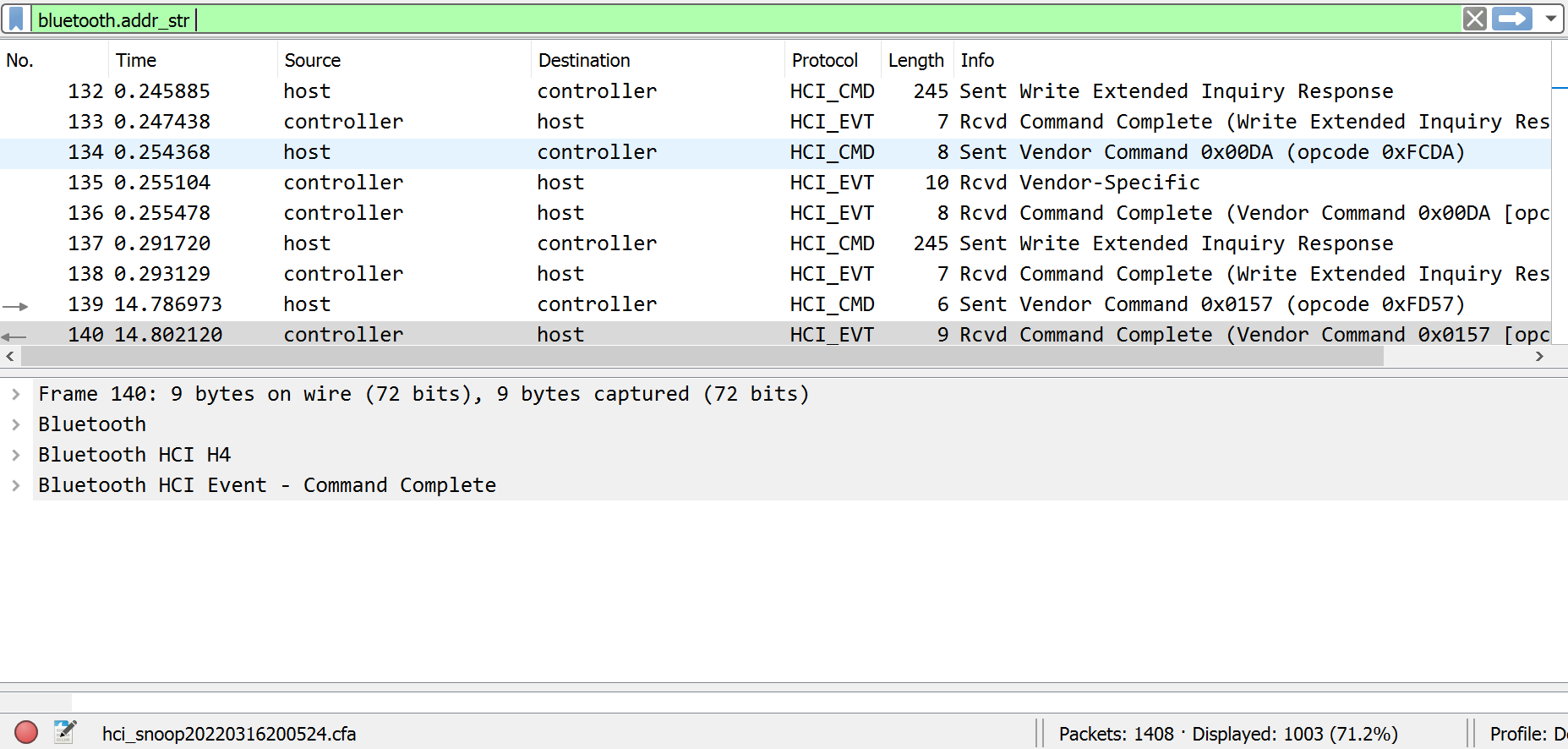
Turn off and on the Bluetooth device to reset the adaptor and finally download the full bug report present in developer options. We can also use the command prompt to get this bug report. A zip file is available to download and share. Extract the contents of this file onto your laptop and locate the CAF snoop file. This file is then opened on Wireshark and the analysis is performed

**OBSERVATION AND RESULTS**

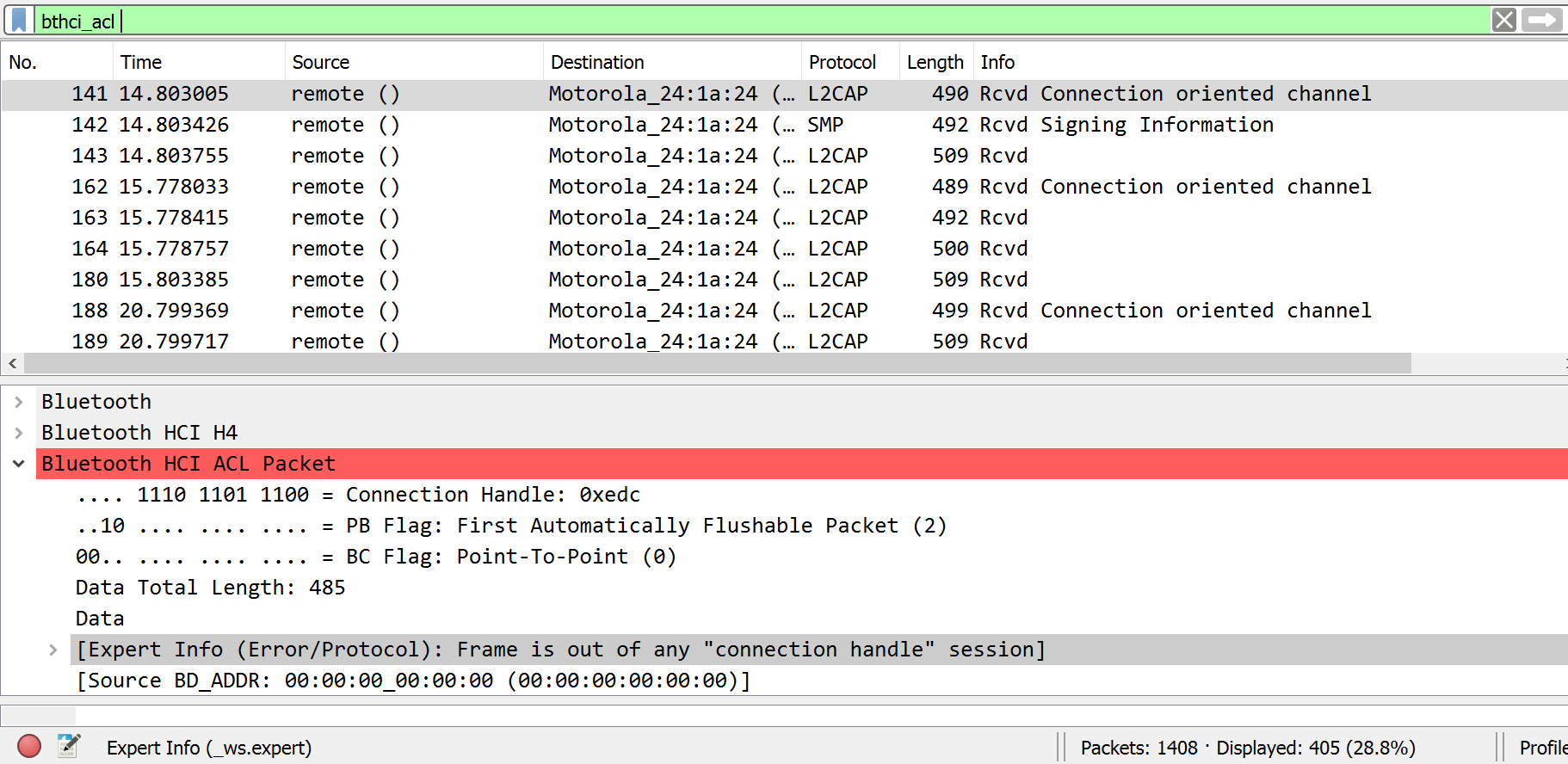
1) ***bluetooth.addr*** - gives the source and destination MAC or ethernet address. In this case source is remote and destination is Motorola



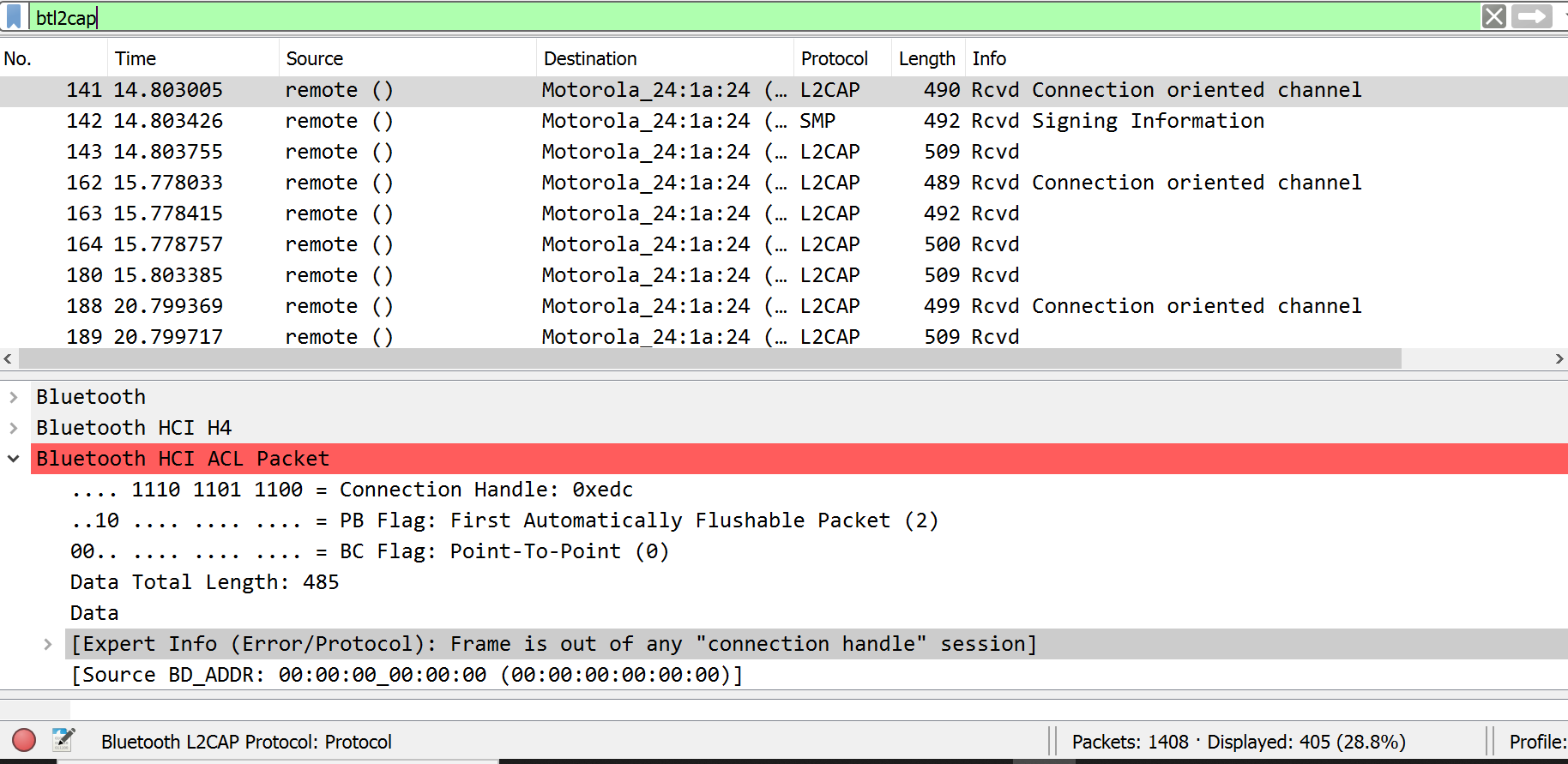
2) ***bluetooth.addr\_str*** - gives the character string with request and response commands



3) ***bthci\_acl*** - lists out the hci acl packets at the receiving end. Since this analysis was done without forming a connection to another Bluetooth device hence the source is shown as a remote source, and Expert Info shows Frame is out of any "connection handle" session



4) ***btl2cap*** - lists out the Logical Link Control and Adaptation Protocol packets, which is used to provide an interface for all the data applications that use the acl links



**CONCLUSION**

Bluetooth is mainly used as an alternative to wire connections, to exchange files between nearby portable devices. In this project we have captured the Bluetooth hcl acl packets on Android 4.4. This project is conducted without connecting to other Bluetooth devices. The captured file is extracted on to the pc. All the captured packets are being analyzed using various filters on WIreshark.