Christopher Bazyani

Practical Cyber Security

Unit 5

Packet Sniffing – 802.11

**Inspect an 802.11 Trace**

Inspecting number 16 data frame, which carries packets across 802.11 networks



Graphical user interface, text, application

Description automatically generated

Inspecting the protocol layers recorded with the frame for these protocols by looking in middle panel

Graphical user interface, text, application

Description automatically generated

IEEE 802.11 is the bits of the 802.11 data frame

Text

Description automatically generated

Data is a record containing the frame payload data as shown

Graphical user interface

Description automatically generated

Expanding the IEEE 802.11 record of the data frame and inspect the details of the various header fields

Frame control

Text

Description automatically generated

Duration

Text

Description automatically generated

BSS Identifier, Source Address, Destination Address

A picture containing text, orange

Description automatically generated

Fragment and sequence number



Frame check sequence



WEP field

Graphical user interface, text

Description automatically generated

Expanding the Flags field to see the details in it

Text

Description automatically generated

**802.11 Physical Layer**

Finding the frequency by expanding the Radiotap header of any frame and looking for Channel frequency

Channel frequency is 2462 MHz or 2.462 GHz. It is known as 802.11b/g channel 11



Adding two new display columns for the TX Rate and RSSI by going to the Preferences panel and selecting Columns

A picture containing text, screenshot, indoor

Description automatically generated

The columns in my figure are called Rate, with a field of type IEEE 802.11 TX Rate, and RSSI, with a field type of IEEE 802.11 RSSI

A screenshot of a video game

Description automatically generated with low confidence

**802.11 Link Layer**

Navigating to the conversation types

Graphical user interface, text, application, email

Description automatically generated

Then selecting the IEEE 802.11 conversation

Graphical user interface, application, table

Description automatically generated

Filtering to see only data frames, I entered the expression “wlan.fc.type==2” into the filter

box above the list of frames in the top panel. Clicking on the Type subfield tells us in the status display at bottom that Wireshark knows this field by the name wlan.fc.type. Thus, the expression to filter for Data frames with Type value 2 is “wlan.fc.type==”data frame”” or “wlan.fc.type==2”

Graphical user interface, text

Description automatically generatedI can now see how many data frames are in the trace and what is the most common subtype of data frame

Graphical user interface, text, application

Description automatically generated

I can now see there are 1783 Data frames or 48% of the total (3731) frames

