# COMP4336/9336 Mobile Data Networking

## Lab 1: Installation and familiarization of Wireshark

[*This is a self-study lab, i.e., you do not need to attend any lab in Week-1 and there is no lab submission for this lab*.]

## Objectives

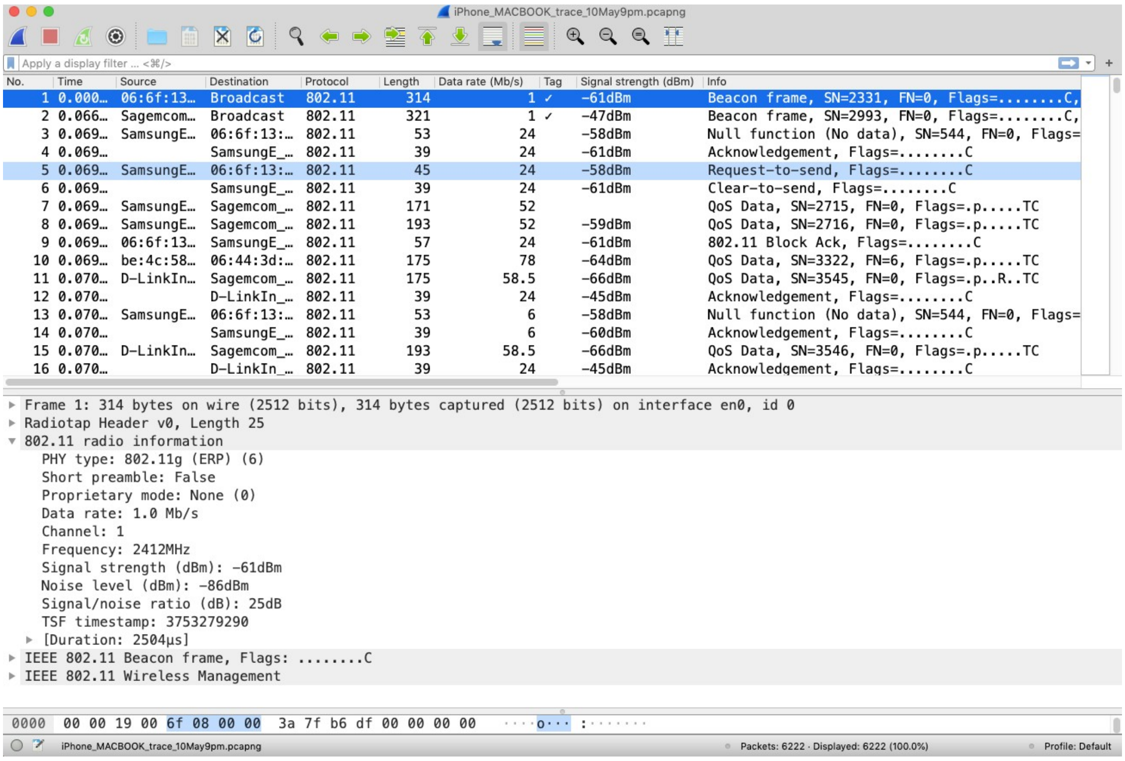
1. To install the freely available open source Wireshark tool in your laptop
2. To learn the basic features of Wireshark

## Wireshark overview

Wireshark [https://www.wireshark.org/] is an open source network packet capture and analysis tool used by millions of users worldwide. It is freely available to download for both Windows and MAC platforms, as well as Linux/Unix. Wireshark can be used to capture WiFi packets and inspect the wireless (radio) related aspects of data transmission, such as received signal strength, data rate of the transmission, and so on. This in turn allows us to deepen our understanding of many wireless and mobile data communication protocols and the fundamental theories behind them through hands-on experiments. Figure 1 shows a screenshot of Wireshark displaying some packet capture from WiFi and their radio related information.

Wireshark is a stable software with extensive on-line support, including

- user guide [https://www.wireshark.org/docs/wsug_html_chunked/],
- manual pages [https://www.wireshark.org/docs/wsug_html_chunked/],
- a detailed FAQ [https://www.wireshark.org/faq.html], and
- numerous YouTube videos posted by Wireshark experts and enthusiasts


iPhone_MACBOOK_trace_10May9pm.pcapng
Apply a display filter ... <⌘/>
iPhone_MACBOOK_trace_10May9pm.pcapng
Profile: Default

| No. | Time | Source | Destination | Protocol | Length | Data rate (Mb/s) | Tag | Signal strength (dBm) | Info |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.000… | 06:6f:13… | Broadcast | 802.11 | 314 | 1 | ✓ | -61dBm | Beacon frame, SN=2331, FN=0, Flags=........C, |
| 2 | 0.066… | Sagemcom… | Broadcast | 802.11 | 321 | 1 | ✓ | -47dBm | Beacon frame, SN=2993, FN=0, Flags=........C, |
| 3 | 0.069… | SamsungE… | 06:6f:13:… | 802.11 | 53 | 24 | | -58dBm | Null function (No data), SN=544, FN=0, Flags= |
| 4 | 0.069… | | SamsungE_… | 802.11 | 39 | 24 | | -61dBm | Acknowledgement, Flags=........C |
| 5 | 0.069… | SamsungE… | 06:6f:13:… | 802.11 | 45 | 24 | | -58dBm | Request-to-send, Flags=........C |
| 6 | 0.069… | | SamsungE_… | 802.11 | 39 | 24 | | -61dBm | Clear-to-send, Flags=........C |
| 7 | 0.069… | SamsungE… | Sagemcom_… | 802.11 | 171 | 52 | | | QoS Data, SN=2715, FN=0, Flags=.p.....TC |
| 8 | 0.069… | SamsungE… | Sagemcom_… | 802.11 | 193 | 52 | | -59dBm | QoS Data, SN=2716, FN=0, Flags=.p.....TC |
| 9 | 0.069… | 06:6f:13… | SamsungE_… | 802.11 | 57 | 24 | | -61dBm | 802.11 Block Ack, Flags=........C |
| 10 | 0.069… | be:4c:58… | 06:44:3d:… | 802.11 | 175 | 78 | | -64dBm | QoS Data, SN=3322, FN=6, Flags=.p.....TC |
| 11 | 0.070… | D-LinkIn… | Sagemcom_… | 802.11 | 175 | 58.5 | | -66dBm | QoS Data, SN=3545, FN=0, Flags=.p..R..TC |
| 12 | 0.070… | | D-LinkIn_… | 802.11 | 39 | 24 | | -45dBm | Acknowledgement, Flags=........C |
| 13 | 0.070… | SamsungE… | 06:6f:13:… | 802.11 | 53 | 6 | | -58dBm | Null function (No data), SN=544, FN=0, Flags= |
| 14 | 0.070… | | SamsungE_… | 802.11 | 39 | 6 | | -60dBm | Acknowledgement, Flags=........C |
| 15 | 0.070… | D-LinkIn… | Sagemcom_… | 802.11 | 193 | 58.5 | | -66dBm | QoS Data, SN=3546, FN=0, Flags=.p.....TC |
| 16 | 0.070… | | D-LinkIn_… | 802.11 | 39 | 24 | | -45dBm | Acknowledgement, Flags=........C |

```
▸ Frame 1: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface en0, id 0
▸ Radiotap Header v0, Length 25
▾ 802.11 radio information
    PHY type: 802.11g (ERP) (6)
    Short preamble: False
    Proprietary mode: None (0)
    Data rate: 1.0 Mb/s
    Channel: 1
    Frequency: 2412MHz
    Signal strength (dBm): -61dBm
    Noise level (dBm): -86dBm
    Signal/noise ratio (dB): 25dB
    TSF timestamp: 3753279290
  ▸ [Duration: 2504µs]
▸ IEEE 802.11 Beacon frame, Flags: ........C
▸ IEEE 802.11 Wireless Management

0000  00 00 19 00 6f 08 00 00  3a 7f b6 df 00 00 00 00   ····o··· :·······

Packets: 6222 · Displayed: 6222 (100.0%)
```

*Figure 1. WiFi capture in MacBook Air and display of radio information using Wireshark.*

## Your Tasks

1. Download and install the freely available Wireshark in your laptop [https://www.wireshark.org/download.html]. To have full access to Wireshark features, you may need to install it as administrator/root user. Windows users also need to install Microsoft Network Monitor 3.4 [https://www.microsoft.com/en-us/download/details.aspx?id=4865], which is necessary to capture WiFi packets.

2. By consulting the on-line manual, user guide, and tutorials, learn some of the important features of Wireshark, such as:
   - Capture live packets from the WiFi interface of your laptop
   - Display packets with radio-related information, such as received signal strength, data rate, WiFi beacon interval, etc.
   - Save captured packet trace into a file in different formats, such as pcap, and csv (pcap allows you to import the file into Wireshark for visual inspection, while csv allows you to import the data to tools such as Excel/Matlab/Python for statistical analysis and processing of the data)
   - Import previously captured packet traces, captured by Wireshark or other packet dump programs (e.g., Microsoft Network Monitor), from a file into Wireshark
   - Filter packets based on some criteria, such as display all WiFi packets transmitted from a particular WiFi access point
   - *Colorize* packet display based on filters
   - Create various *statistics*
   - Anything else that you find interesting …

Completing of these tasks will set you up for the next set of labs and the term project, which will make use of wireless packet captures and analysis.

**End of Lab 1**