# COMP 40660: Advances in Wireless Networking

School of Computer Science, University College Dublin, Ireland
Spring 2023

# Assignment 3: Wireshark

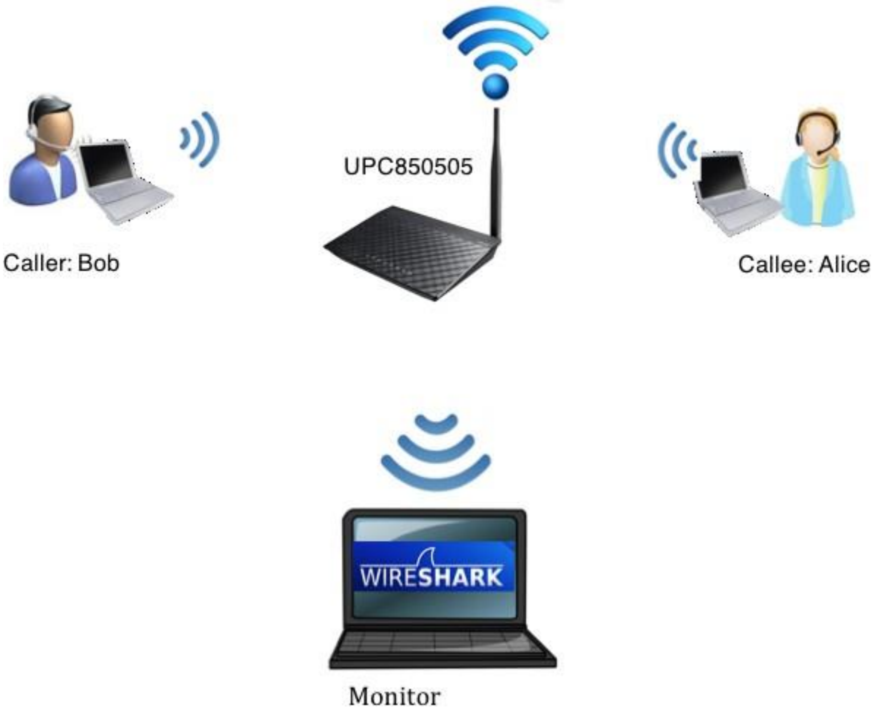
This assignment is worth 10% of the overall grade.

**Important note:** For this assignment, you will need to download, or downgrade to, or use **version 1.10.6 of Wireshark**. If you have not done so already (for the Wireless Exercises), do the following:

- go to https://www.wireshark.org/download.html
- Scroll down to the **older releases.**
- Then choose one link from the platforms listed in the **Go Spelunking** section
- Select one of the links e.g.: "Wireshark Foundation (https, us)"
- Select **win32/** or **win64/** for Windows machines, **src/** for Linux machines, or **osx/** for Mac machines,
- then select **all-versions/** and download **version 1.10.6**

For Assignment 2, download from **assignment_3_capture_file** from *Brightspace.*

As shown in the figure below, a VoIP call is taking place between Bob and Alice, through the UPC850505 access point. The black laptop has its wireless card in monitor mode on the same channel that the UPC850505 access point (and other networks) is/are operating on and thus, can capture frames containing packets relating to the VoIP call.



Open up the capture file, **assignment_3_capture_file.pcap**, using Wireshark, taking care not to upgrade (even if prompted) from version 1.10.6.

**Note**: use RFC3261 (https://tools.ietf.org/html/rfc3261 or https://datatracker.ietf.org/doc/html/rfc3261) to understand the response codes of the signaling protocol in use.

**Provide answers to the following questions, correctly numbering each of your answers.**

**Questions:**

**Q1** For the given VoIP call trace file, specify what signaling protocol is used to establish the VoIP call (Hint: Use the **Telephony** menu.)

**Q2** Specify for the VoIP call: the start time, stop time, and the state of the call.

**Q3** What are the unique IDs (i.e., the protocol addresses) of the caller and the callee? (See the RFC for details)

**Q4** What is the initial speaker's IP address (i.e., the IP of the user that initiated the call)?

**Q5** Take a screenshot of the signaling flow diagram between Bob and Alice.

**Q6** From the signaling flow you obtained in the previous question, what is the signaling status code for **Trying**?

**Q7** What is the source & destination ports used for the VoIP call signaling?

**Q8** What filter would only display (Real-Time Transport Protocol) packets, the packets that carry the voice packets?

**Q9** What adjustment would have to be made to the filter to exclude the *version 0* packets.

**Q10** What is the entire duration of the call, from the first **voice** packet to the last **voice** packet? You must provide evidence to support your answer in the form of a screenshot.

**Q11** What is the average packet size of the packets that carry the voice traffic?

**Q12** What is the channel type, channel number, and bandwidth of the VoIP call channel that has been monitored in this capture? (Hint: look in *Radiotap Header* packet-header)
You must provide evidence to support your answer in the form of a screenshot.

**Q13** What is the spectrum of the frequency band this channel is tuned to?
You must provide evidence to support your answer in the form of a screenshot.

**Q14** What are the MAC addresses of Bob, Alice, and the AP device? Take a screenshot to illustrate your answer.

**Q15** Why does each signaling message appear at least twice?
(Hint: check the values of the source, destination, receiver, and transmitter MAC addresses)

**Q16** Why do some signaling messages appear more than twice? (Hint: check the flags of the *Frame Control Field*)
Take a screenshot to illustrate your answer.

**Q17** There are **two** different cases in which signaling messages appear more than twice. Explain the difference between the two cases.

**Q18** What is the Wireshark filter you need to use to show only the signaling packets captured for this VoIP call (i.e., non-voice packets)?
How many packets match this filter?
Take a screenshot to show the packets displayed.

**Q19** What refinement to the filter in the previous question could you apply to remove most duplicate packet entries?

**Q20** What is BSSID of current access point? Which WLAN does it belong to?

**Q21** What filter is required to display only **beacon** frames from the **UPC850505** WLAN?

**Q22** For frames carrying RTP traffic from 192.168.1.10, what is the percentage of the frame that is VoIP payload? Also, specify the **audio codec** used in the VoIP call. (Hint: Look inside the Real-Time Transport Protocol packet-header)

**Q23** Frame 5011 contains a Real-time Transport Control Protocol (RTCP) packet. Looking inside the packet body under the **Source 1** entry, and its associated sub-entries, what is the purpose of this type of packet?
Take a screenshot of the Source 1 entry.

**Q24** Briefly discuss the purpose of using the SDP protocol in conjunction with RTP.

**Q25** Using the signaling flow diagram from Q5, identify the signaling message sent by Alice after which the actual call starts. What is the packet number for this message?

**Q26** After the signaling message identified in the previous question, the actual VoIP call starts. What is the transport protocol used for the VoIP call?
Specify the Layer 4 protocol used.

**Q27** Select a beacon frame belonging to the WLAN that you found in Q20.
In the *IEEE 802.11 wireless LAN management* packet-header, in *Tagged Parameters*, in *Tag: Vender Specific Microsoft WMM/WME: Parameter Element*, you will see the values for ECWmin and ECWmax for the different access categories (ACs).
Using your knowledge of the 802.11 frame exchange process and the CSMA/CA mechanism, explain how ECWmin and ECWmax are incorporated into the frame transmission process.

**Q28** What are the values of ECWmin and ECWmax for each of the access categories? You must provide evidence to support your answer in the form of a screenshot.

**Q29** Find a frame carrying RTP VoIP traffic and look for an entry relating to QoS in the 802.11 MAC header.
Explain whether or not the appropriate QoS value / AC is being used.
You must provide evidence to support your answer in the form of a screenshot.

**Q30** Identify the signaling message used to terminate the session between Bob and Alice. What are the packet numbers for this message?
Which user ended the call (Bob or Alice)?

**Q31** How many RTP streams are used during this VoIP call? For each of them, specify the SSRC value.
(Hint: Use the **Telephony** menu).
You must provide evidence to support your answer in the form of a screenshot.

**Q32** For each stream found in the previous question, what is the **max Delay** (Delta), **max Jitter**, and **mean Jitter**?

**Q33** Using the **Telephony** menu, select **VoIP calls**, select the call. Then, click the **Player** button, and then the **Decode** button to decode the VoIP stream.
What is the duration (in seconds) for each RTP stream identified? Select **Play**, to hear the VoIP call, and state the contents of this call. (Hint: tick the box beside the call you want to play)

**Q34** Using the I/O Graph, plot three graphs on the same plot:

The 1st graph must show the **signaling** messages The 2nd graph must show the **RTP** packets.
The 3rd graph must show **all** packets.

Settings:
X Axis
Tick Interval: 0.1 sec
Pixels per tick: 10
Y Axis
Scale: 200

**Submission deadline: 11.59PM on 27th March 2023**

---

*End of the assignment*

---