In the lab and lecture we looked at the process of connecting a device to a WPA2 network and the 4-Way handshake where the encryption keys are exchanged with Wireshark. For homework 6, use the provided pcap file (`hw6.pcap`) to answer the following questions (*one of the answer sheets can be used*) on the connection process and 4-way handshake.

1) What is the SSID of the network the device is connecting to? **[0.25 pts]**

2) Answer the following based on the 4-way handshake:
- What is the ANonce? **[0.25 pts]**
- What is the SNonce? **[0.25 pts]**
- What is the client's (station/device connecting to the network) MAC address? **[0.25 pts]**
- What is the AP's MAC address? **[0.25 pts]**
- What is the MIC in Message 2? **[0.25 pts]**

Use `hw6_temp.py` (and/or Wireshark) to help you answer the following questions.

3) Given the passphrase for the network is "S0mething$imple" (without the ""), what is the PMK/PSK for the network? **[0.5 pts]**
The following link can also be used to calculate the PMK/PSK or to check that your calculation is correct: https://www.wireshark.org/tools/wpa-psk.html

4) Answer the following based on the encryption keys **[2 pts]**
- What is the PTK for the connection? ***[0.25]***
- What is the KCK for the connection? ***[0.125]***
- What is the KEK for the connection? ***[0.125]***
- What is the TK for the connection? ***[0.125]***

  The following marks are assigned for modifications done to the hw6_temp.py script.
  - PMK calculation ***[0.25]***
  - PTK calculation ***[0.75]***
  - Finding KCK ***[0.125]***
  - Finding KEK ***[0.125]***
  - Finding TK ***[0.125]***

Total Points [4 pts]

Bonus Section
A few websites were visited during the connection, but login details were entered on one site.
- Which website had the log in details? **[0.5 pts]**
  - Hint: Use Wireshark and enter the password in the decryption key list
- What was the name that was entered? **[0.5 pts]**
- What was the email address that was entered? **[0.5 pts]**
- What was password that was entered? **[0.5 pts]**

Due Date: Check Moodle for date
Late Submission Deadline: Check Moodle for date (usually 1 week after due date)
Submission Files: The modified **python script** and **a file** with the answers to questions 1 to 4
Location: Moodle Homework6 link