**Introduction to Ethical Hacking**

**Assignment - Network Analysis**

**Weighting 60%**

**Due 14th April 2021 via Blackboard 5:30pm**

Answer the following questions

Open the file **IEHAssign1.pcapng** and answer the following questions.

1. Describe and explain multiple filters used to identify packets communicating with the device **Dell\_45:49**. Use a detailed diagram to show the communication between the main devices? **(10 marks)**
2. Give a detailed description of the following packets, include filters and diagrams to help explain these packets.
   1. 295 and 302
   2. 560
   3. 4154
   4. 9525 **(20 marks)**
3. Describe the protocols and port numbers used in devices where the most packets were sent and received. **(5 marks)**
4. What filter will return 1197 packets. Describe the type of traffic and the communication. Use an advanced Wireshark feature to identify traffic between two devices. **(20 marks)**
5. Describe and list the filters which have helped you to remove broadcast or unwanted traffic. **(5 marks)**
6. Use at least two colourisation rules to help identify key packets in the capture file.

**(10 marks)**

1. Use an IO Graph and include two filters from the questions above to highlight key traffic.

**(10 marks)**

Write a short report (2000 words) on the type of activity carried out by the DELL\_45 computer?

Your report should include a range of Wireshark features which you have used. **(20 marks)**

Use Harvard style referencing within your report.

Please submit a turnitin report with this assignment.

Your assignment must be uploaded to Blackboard by the end of business on the **9th of April 2021**.