Christopher Bazyani

Practical Cyber Security

Unit 4

Packet Sniffing - TCP UDP

**Capture a UDP Trace**

Entering the udp filter after the capture

Graphical user interface, text, application

Description automatically generated

**Inspecting the UDP Trace**

Selecting different packets in the trace and browsing the expanded UDP header

Text

Description automatically generated

**Open the TCP Trace**

Using the trace-tcp provided and opening it on Wireshark

Text

Description automatically generated

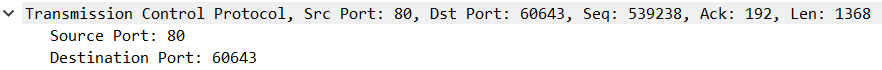
**Inspecting the TCP Trace**

Selecting a long packet anywhere in the middle of your trace whose protocol is listed as TCP and expanding the TCP protocol section in the middle panel.

Graphical user interface, text, application, table

Description automatically generated

Exploring the source and destination ports



Sequence number field



Acknowledgement number field



Flags field

Text

Description automatically generated

Checksum



Options

Text

Description automatically generated

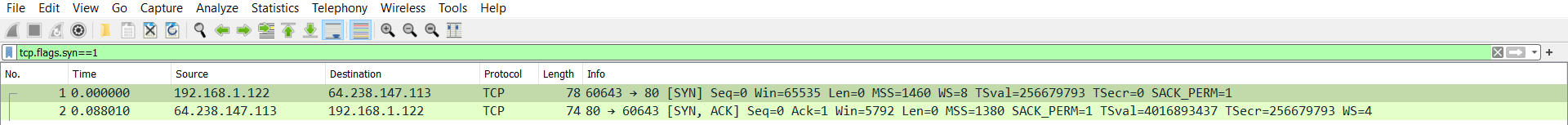
TCP Payload



**TCP Connection Setup/Teardown**

Seeing the Three-way handshake by finding the TCP segment with the SYN flag. The SYN flag is noted in the Info column and can also search for packets with the SYN flag on using the

filter expression “tcp.flags.syn==1”.



Clearing the trace using the “x” button next to the packet filter button would end up like this

Text

Description automatically generated