# Aim: To capture and analyse packets using a network monitoring tool

Network Monitoring Tool: Wireshark

Wireshark is the world’s foremost and widely-used network protocol analyser. It lets you see what is happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

Packet Analysis:

## Protocol: [TCP] Transmission Control Protocol

Frame (Packet) Number: 298216

Time: 09:23:18.443586

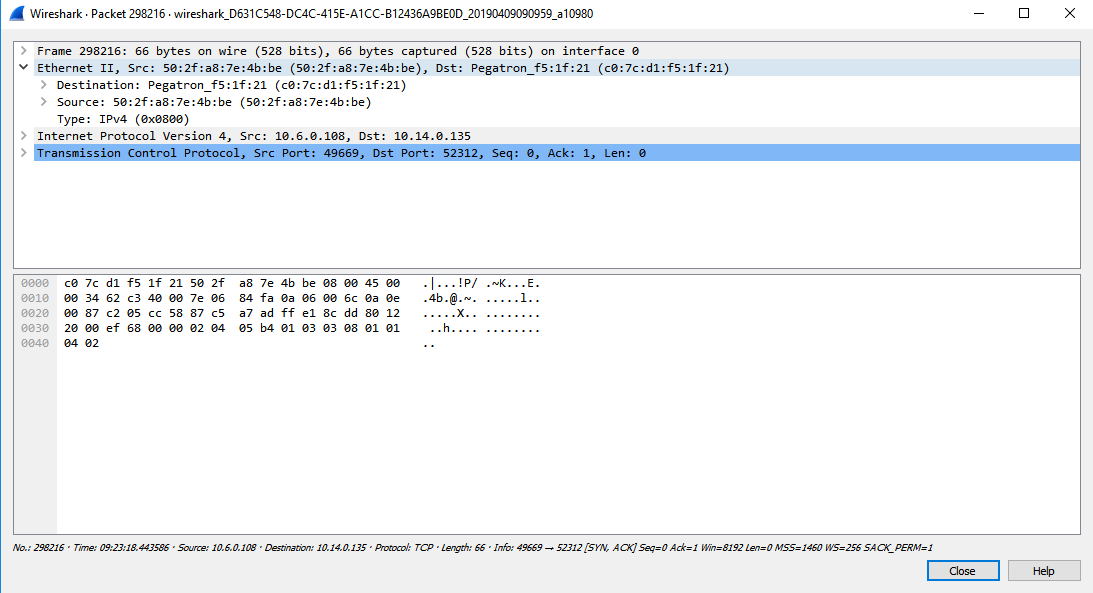
Source IP: 10.6.0.108:52312

Destination IP: 10.14.0.135:49669

Source MAC: 50:2f:a8:7e:4b:be

Destination MAC: c0:7c:d1:f5:1f:21

Length: 66



## Protocol: [UDP] User Datagram Protocol

Frame (Packet) Number: 298326

Time: 09:23:19.014648

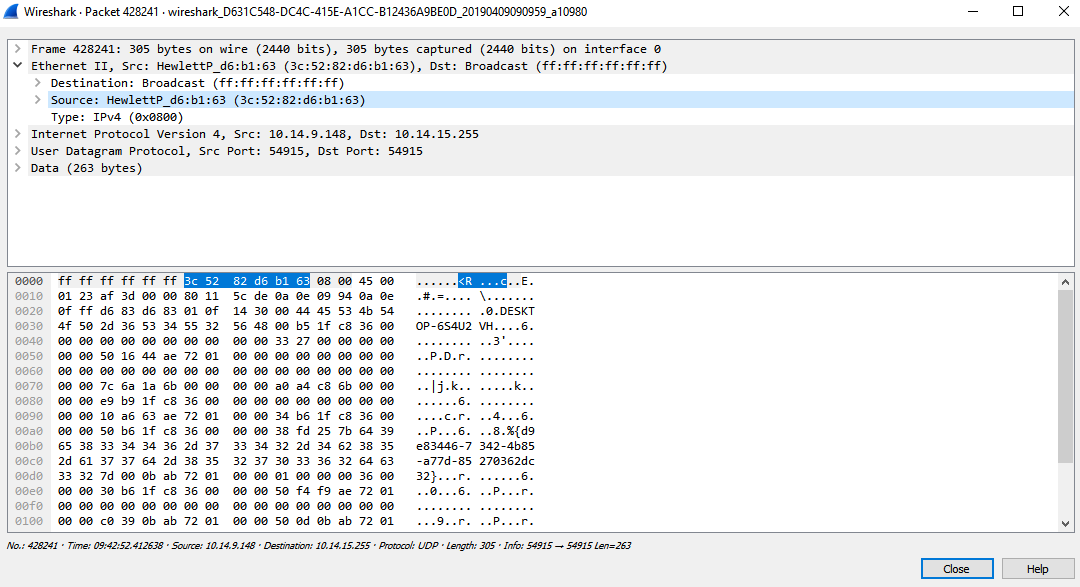
Source IP: 0.0.0.0:68

Destination IP: 255.255.255.255:67

Source MAC: c0:7c:d1:f5:1f:21

Destination MAC: ff:ff:ff:ff:ff:ff

Length: 342



## Protocol: [ICMP] Internet Control Message Protocol

Frame (Packet) Number: 377512

Time: 09:31:15.823585

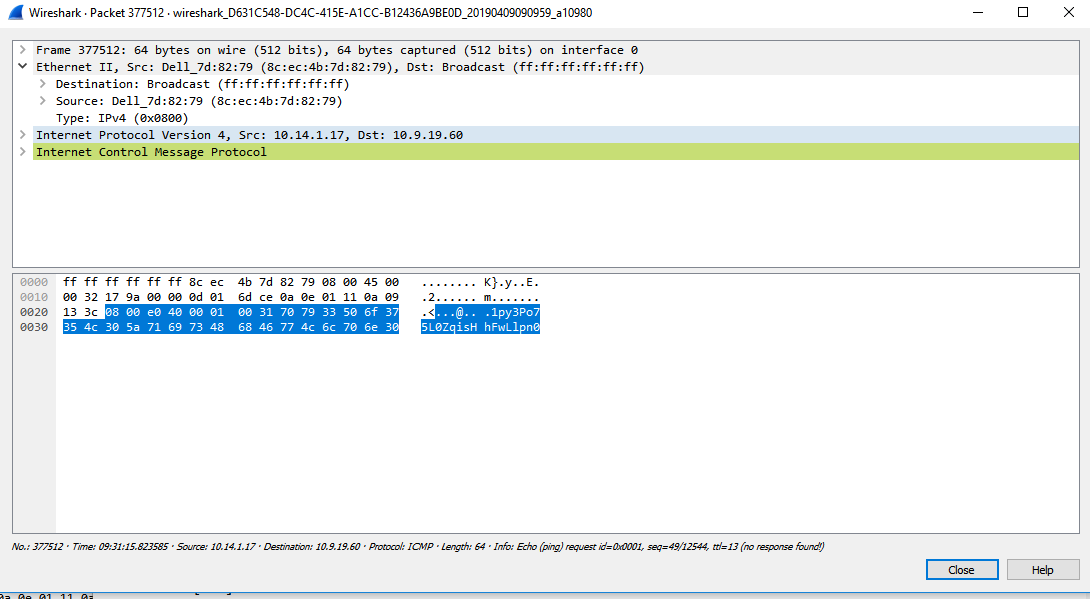
Source IP: 10.14.1.17

Destination IP: 10.9.19.60

Source MAC: 8c:ec:4b:7d:82:79

Destination MAC: ff:ff:ff:ff:ff:ff

Length: 64



## Protocol: [ARP] Address Resolution Protocol

Frame (Packet) Number: 318

Time: 09:10:04.394096

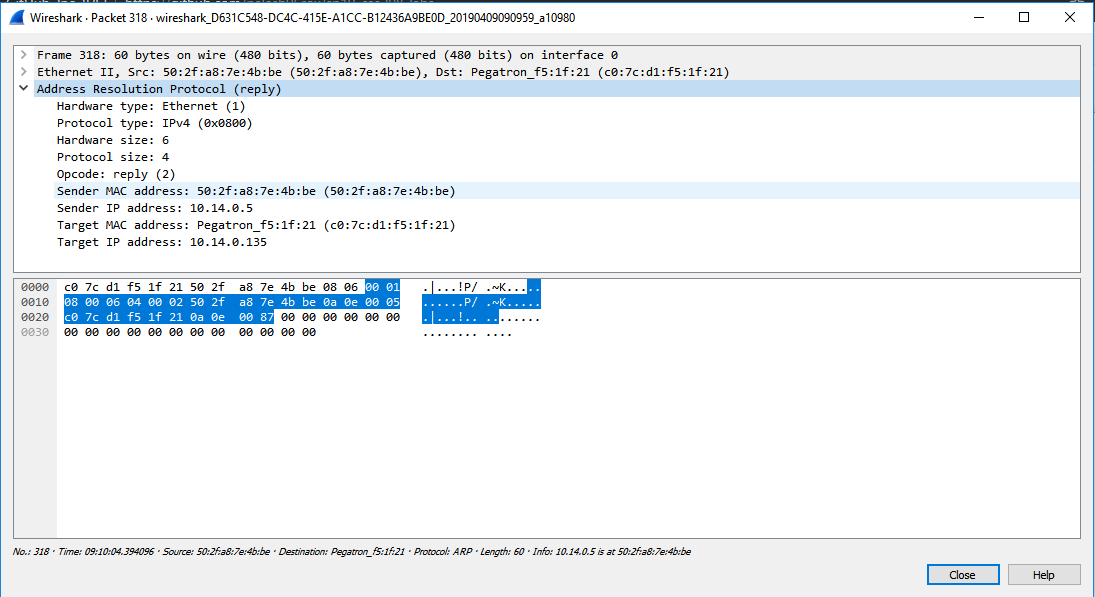
Source IP: 10.14.0.5

Destination IP: 10.14.0.135

Source MAC: 50:2f:a8:7e:4b:be

Destination MAC: c0:7c:d1:f5:1f:21

Length: 60



## Protocol: [DHCP]

Frame (Packet) Number: 298326

Time: 09:23:19.014648

Source IP: 0.0.0.0:68

Destination IP: 255.255.255.255:67

Source MAC: c0:7c:d1:f5:1f:21

Destination MAC: ff:ff:ff:ff:ff:ff

Length: 342

