

**Network Traffic Analysis**

**Lab – Wireshark**

In this lab, we’ll be covering some fundamental Wireshark queries for analysis. This is a quick tour of some of the basic options, so don’t stress too much on the details and ask questions if you have them. Also, after you run a filter query, be sure you clear it by clicking the ‘x’ in the filter bar! Enjoy!



**Questions**

1. How many unique **IPv4 addresses** were in this capture?

(Select ‘Statistics’ → ‘Endpoints’)

Hint: What number is displayed on the IPv4 tab?

There were 192 unique IPv4 addresses.   
 -------------------------------------------------------------

1. How many packets are involved with **IP address 74.125.45.147** (source or destination)? (Use this filter: ip.addr == 74.125.45.147)

Hint: Just count the number (No.) of packets in the first column in Panel #1 or see the ‘Displayed’ number on the bottom right pane of your screen below.

11 packets are involved with IP address 74.125.45.147

------------------------------------------------------------------

1. How many packets were captured from host 209.85.239.20? How many ‘bytes’ were transferred? Two answers are required here.

(Use this filter: ip.addr == 209.85.239.20)

Hint: Just count the number of packets in Panel #1 or see the ‘Displayed’ number on the bottom right pane of your screen below. Also, look at Panel #2 – **Frame** 5822 – how many ‘bytes captured’ are identified?

89 packets were captured from host 209.85.239.20.

74 bytes were captured.

----------------------------------------------------------------------------------

1. Filter to show all the IP traffic that originated and was destined for the 192.168.0.0/24 network. What is the “**Destination IP**” address and “**Protocol**” identified for the **3rd packet**?

(Use this filter: ip.src == 192.168.0.0/24 && ip.dst == 192.168.0.0/24)

Hint: Count down from the top of Window #1 until you get to the 3rd packet and look at the 4th & 5th column.

Destination IP: 192.168.0.255 Protocol: NBNS

------------------------------------------------------------------

1. How many total **‘TCP’** conversations are captured?

(Select ‘Statistics’ → ‘Conversations’)

Hint: What number is displayed on the TCP tab?

432

------------------------------------------------------------------

1. What ‘**protocols’** were used in this capture? (Select ‘Statistics’→ ‘Protocol Hierarchy’) Hint: make sure no filters are applied. What are ALL the protocols identified under ‘Internet Protocol Version 4’?

User Datagram Protocol, Transmission Protocol, Internet Group Management Protocol, Internet Control Message Protocol, Address Resolution Protocol.

There were protocols within each of these protocols but wasn’t sure if these needed listed to.

------------------------------------------------------------------

1. What is the ‘physical address (MAC address)’ for the host 192.168.0.51? (Use this filter: ip.addr == 192.168.0.51) Hint: Look in Panel #2 - Ethernet II, Src:, what is the **Hex Number** identified, not the name of a company you may know?

da:9a:1d (00:0e:0c:da:9a:1d)

------------------------------------------------------------------

1. How many ‘**FTP sessions’** were established? (Use this filter: ftp)

Hint: Count the number of frames in column one or view the number ‘Displayed’ in the bottom right panel of your screen.

44

------------------------------------------------------------------

1. What was the **date** when FTP was first captured on the wire? (Use this filter: ftp) Hint: In Panel#2, click the arrow next to Frame and review the ‘**Arrival Time’**.

May 26, 2008

------------------------------------------------------------------

1. What was the ‘**name of the file’** that was downloaded during using FTP?

(Use this filter: ftp.request.command == RETR)

Hint: Look in the Info column in Panel#1 or in Panel#2 click the arrow next to File Transfer Protocol (FTP) or in Panel#3 look at the last column for a specific data file name.

RETR RPM-GPG-KEY.dag.txt

------------------------------------------------------------------