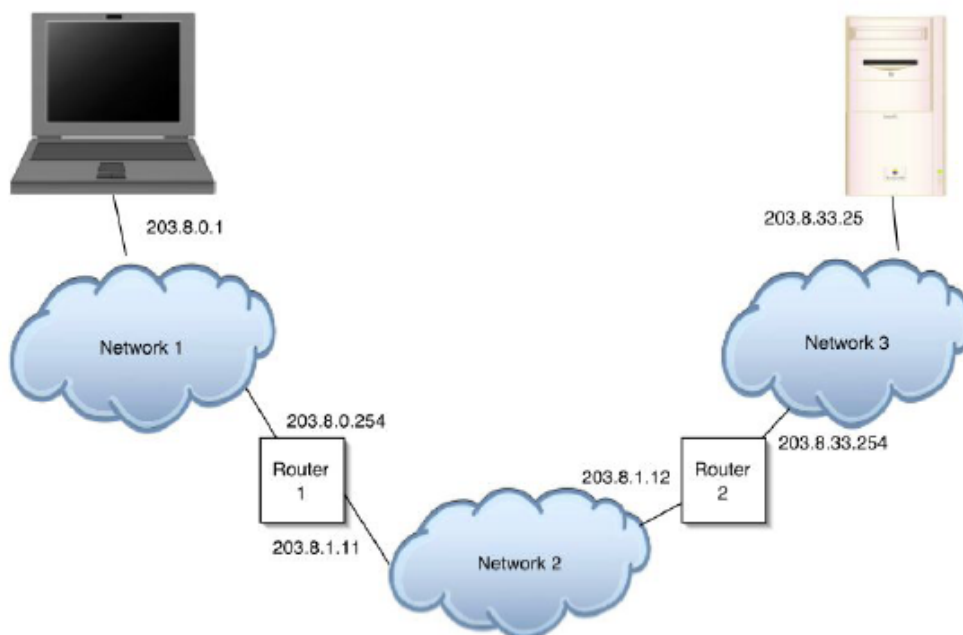


EE4014 Activities on Packet Analysis

A. http-google101.pcapng

1. Use Wireshark to open the trace file “http-google101.pcapng”.
2. You can sort the Packet List pane by clicking on the desired column heading. E.g. click on “Source” column heading.
3. What IP Addresses are found in this trace file?
4. What application protocols are in used?
5. You can change the location of columns by clicking and dragging on a column heading to move it left or right.
6. You can Right-Click on Column Headings to Hide, Display, Rename, Remove Columns.
7. Right-click on any packet in the Packet List pane to see what’s available (right-click functionality includes apply filters, colourise traffic, reassemble traffic (follow streams), and more).
8. Click on a packet in the Packet List pane, Wireshark shows the details for that packet.
9. In the Packet Details pane, you can click on the + indicators to expand sections of the frames. Or you can right-click on the + indicators to expand an entire frame (Expand All) or just one collapsed section (Expand Subtrees).
10. Go to the Packet Bytes Pane, it shows the contents of the frame in hex and ASCII formats. If you highlight a field in the Packet Details pane, Wireshark also highlights the location of that field and the bytes contained in that field in the Packet Bytes pane.

B. Frames and Packets



Frames are captured in the above 3 networks at the same time. Open capture files network1.pcapng, network2.pcapng, and network3.pcapng at the same time.

1. In Frame 1 of network1.pcapng, what are the IP addresses of the IP packet as carried in the frame?
2. Is the same IP packet as mentioned above found in network2.pcapng and network3.pcapng? If so, what are the frame numbers in these two trace files (of the frames that carry the same IP packet).
3. How can you confirm that your answer in 2. is correct?

4. Fill in the following table for the frames and the packet as discussed above:

In Network 1		In Network 2		In Network 3	
Frame #		Frame #		Frame #	
Source IP address		Source IP address		Source IP address	
Destination IP address		Destination IP address		Destination IP address	
Source MAC address		Source MAC address		Source MAC address	
Destination MAC address		Destination MAC address		Destination MAC address	

- Will the IP address of the packet change in network1, network2, and network3?
- Will the MAC address of the packet change in network1, network2, and network3?
- What kind of devices are using the 6 MAC addresses in the table?
- Is the IP packet as carried in network1 *exactly* the same as that in network2?
- If no, what have been changed. Check out the same IP packet in network3.

C. [http-google101.pcapng](#)

- Open trace file “http-google101.pcapng”. This is a typical web browsing session.
- In Frame 1 and Frame 2, what application protocol is in used? What is the IP address of the DNS server? What is requested? What result is returned?
- What is done in Frame 3 and Frame 4?
- What is done in Frames 5,6,7?
- What is requested in Frame 8? What is the meaning of “1.1”?
- What response is made in Frame 10?
- What is requested in Frame 36?
- In Frames 231,232 and 233, why another DNS request is performed?