ANNEX A · WIRESHARK: FIRST CAPTURE

Name: _____ Group G = _____ Date: _____

The rule: capture only your own machines and the lab. Never somebody else's traffic.

TASK 1 **Capture a ping into a file**

In `~/labs`, with your group number. Terminal 1 is pc1, terminal 2 is pc2, terminal 3 stays on the Ubuntu host.

```
G=3 containerlab deploy -t lan.clab.yml              # host
tcpdump -c 6 -i eth1 -w /tmp/ping.pcap arp or icmp   # pc2: saves 6 frames
ping -c 2 10.G.0.12                                  # pc1
docker cp clab-lan-pc2:/tmp/ping.pcap .              # host: copy it out of pc2
wireshark ping.pcap &                                # host
```

DONE WHEN tcpdump said `6 packets captured` and Wireshark shows a list of six lines.

TASK 2 **The packet list (top pane)**

Frames in total: _____ Protocols in the Protocol column: _____ and _____

Info of frame 1: _____ Its destination: _____

Source column: frames 1–2 show a _____ address; frames 3–6 show an _____ address.

DONE WHEN you can say which frame is the question, which is the answer, and which four are the ping.

TASK 3 **Open frame 3, layer by layer (middle pane)**

Click frame 3. Open each line with its arrow and copy the values.

Line in Wireshark	Source	Destination	Field that names what is inside
Ethernet II			Type:
Internet Protocol Version 4			Protocol:
Internet Control Message Protocol	Type: (request or reply?)		—

Frame 3 is _____ bytes on the wire. IPv4 `Total Length`: _____ So the Ethernet header is _____ bytes.

`Time to Live`: _____ Click frame 4. ICMP `Type`: _____ What changed in the addresses?

_____

Click `Source Address` inside IPv4 and look at the bottom pane. The four bytes that light up:

_____

DONE WHEN the table is full and those four hex bytes, converted to decimal, are the IP address of pc1.

TASK 4 **Display filters (the bar above the list)**

Type each filter, press Enter, count the lines. Clear the bar between filters.

Filter	Frames shown	Which frame numbers
`arp`		
`icmp`		
`eth.dst == ff:ff:ff:ff:ff:ff`		
`icmp.type == 8`		
`ip.addr == 10.G.0.12` (your G)		

The last filter does not show frames 1 and 2, although they talk about that address. Why?

_____

DONE WHEN the bar was green five times and the last question has an answer with the word “header”.

TASK 5 **Extra: your real card, live (only if your teacher says capture is enabled)**

In Wireshark: Capture → Options, choose the wired card, Start. In a host terminal: `ping -c 2 1.1.1.1`. Stop the capture (red square). Filter `icmp`. Open the first request.

Destination IP: _____ Destination MAC: _____

Run `ip neigh` on the host. That MAC belongs to: _____

DONE WHEN you can explain why the frame is not addressed to the machine that owns 1.1.1.1.

Clean up: close Wireshark, `exit` in pc1 and pc2, `containerlab destroy -t lan.clab.yml --cleanup`.

EXIT TICKET **Circle one answer. Alone, no notes.**

1. In Wireshark, where do you see one line per layer for the selected frame?
a) The packet list **b)** The packet details
c) The packet bytes **d)** The filter bar

2. Which field of the Ethernet II header says that an IPv4 packet is inside?
a) Destination **b)** Source
c) Time to Live **d)** Type

3. Why does the filter `ip.addr == 10.G.0.12` hide the ARP frames?
a) An ARP frame has no IP header **b)** ARP frames are encrypted
c) ARP uses a different cable **d)** The filter is wrong

4. What does Wireshark do to the network while it captures?
a) It slows it down **b)** It blocks other users
c) Nothing: it only listens **d)** It sends ARP requests