Wireshark Assignment 3

Mustafa Gönen 2264547

1. What are the IP numbers of attacker, victim, user and OVS machines, respectively?

Client ID	Interfaces	IP Numbers
victim	Interface-0	10.10.1.1
attacker	Interface-3	10.10.2.2
user	Interface-5	10.10.3.2
OVS	Interface-1	10.10.1.2
OVS	Interface-2	10.10.2.1
OVS	Interface-4	10.10.3.1

2. Why an ICMP message does not need to have source and destination port numbers?

Because, Internet Control Message (ICMP) doesn't use a port. ICMP is an echo-reply protocol not a communication protocol. In addition to this, it was designed to communicate Network-Network-Layer information between hosts and routers, not between application layer processes.

3. List the Wireshark sequence numbers of the first 5 request packets with their corresponding reply packets (if any).

Seq Number	Request Number (BE)	Reply Number (BE)
7 (BE) – 1792(LE)	8	9
12 (BE) – 3072 (LE)	11	12
8 (BE) – 2048 (LE)	16	17
13 (BE) - 3328 (LE)	19	20
9 (BE) – 2304 (LE)	22	23

4. a) Examine the first ping request packet with its corresponding reply packet. What are the ICMP type and code numbers of each (request and reply) packets?

Request P	ICMP Type	ICMP Code	Checksum	Seq Nu.	Identifier

8	8(echo (ping))	0	0x6364 - 25444	7(BE) (0x0007)
				1792(LE) (0x0700)
					4807(BE) - 0x12c7
					50962(LE) - 0xc712

Reply P	ICMP Type	ICMP Code	Checksum	Seq Nu.	Identifier

9	0(echo (ping))	0	0x6b64 - 27492	7(BE) (0x0007)
				1792(LE) (0x0700)
					4807(BE) - 0x12c7
					50962(LE) - 0xc712

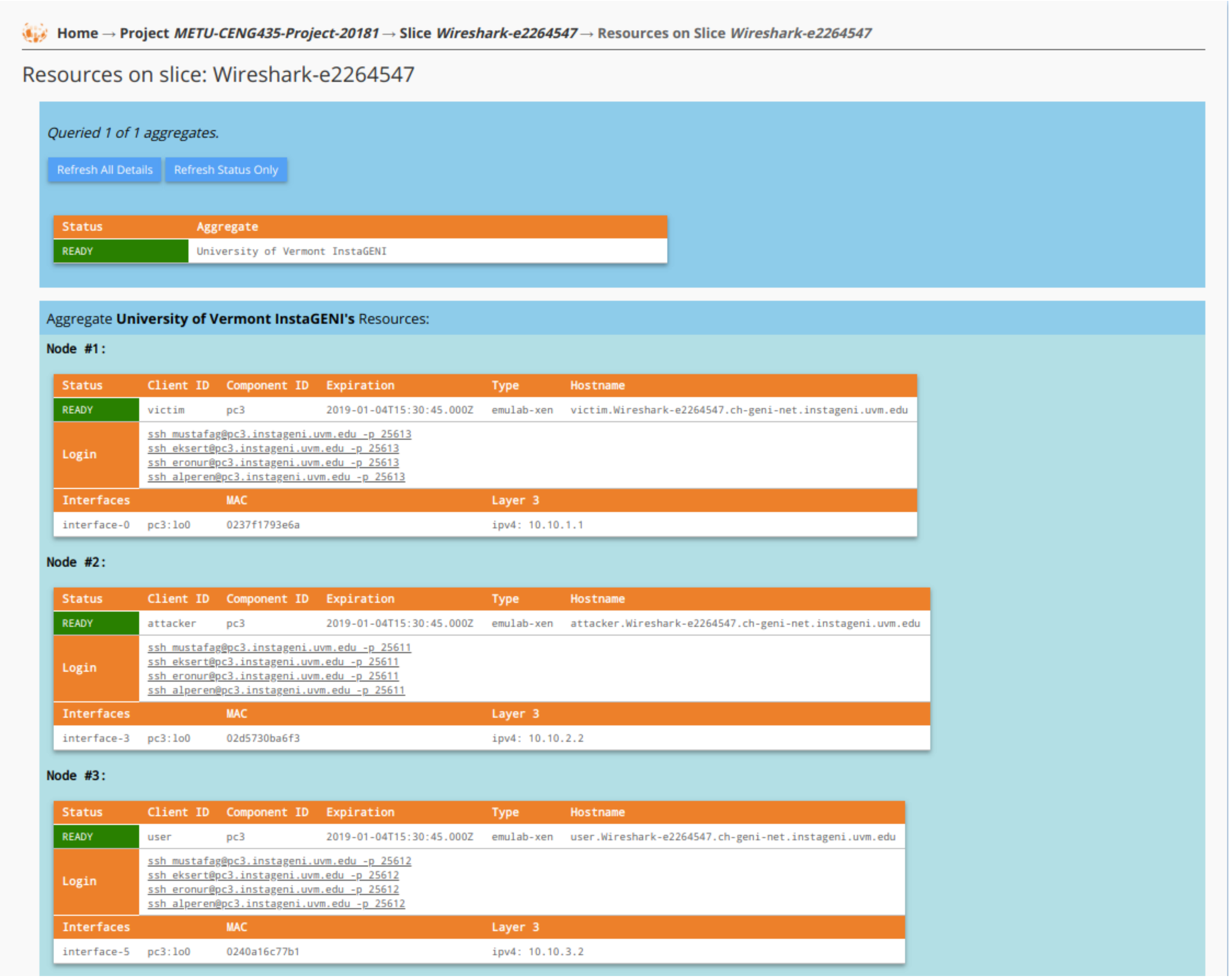
b) How many bytes are the checksum, sequence number and identifier fields?

Checksum → 2 bytes
Identifier Fields → 2 bytes
Seq Number → 2 bytes

5. Specify the TTL values of packets by means of source - destination address pairs and comment on the similarities and differences among TTL values.

The TTL (Time to live) value refers to the time that a packet travels on the Internet. This value decreases once when passing through each device. Because the ping sent to the victim from the attacker passes through the OVS router, it drops from 64 to 63. However, since the ping passed from the user to the OVS router does not pass through any router, the TTL value remains at the initial value of 64.

6. Put the screenshot of graphical illustration of resources and Details page (which opens by clicking "Details" at the bottom) in GENI Platform.



Home → Project *METU-CENG435-Project-20181* → Slice *Wireshark-e2264547* → Resources on Slice *Wireshark-e2264547*
Refresh All Details
Refresh Status Only

Resources on slice: Wireshark-e2264547

Queried 1 of 1 aggregates.

Status	Aggregate
READY	University of Vermont InstaGENI

Aggregate **University of Vermont InstaGENI's** Resources:

Node #1:

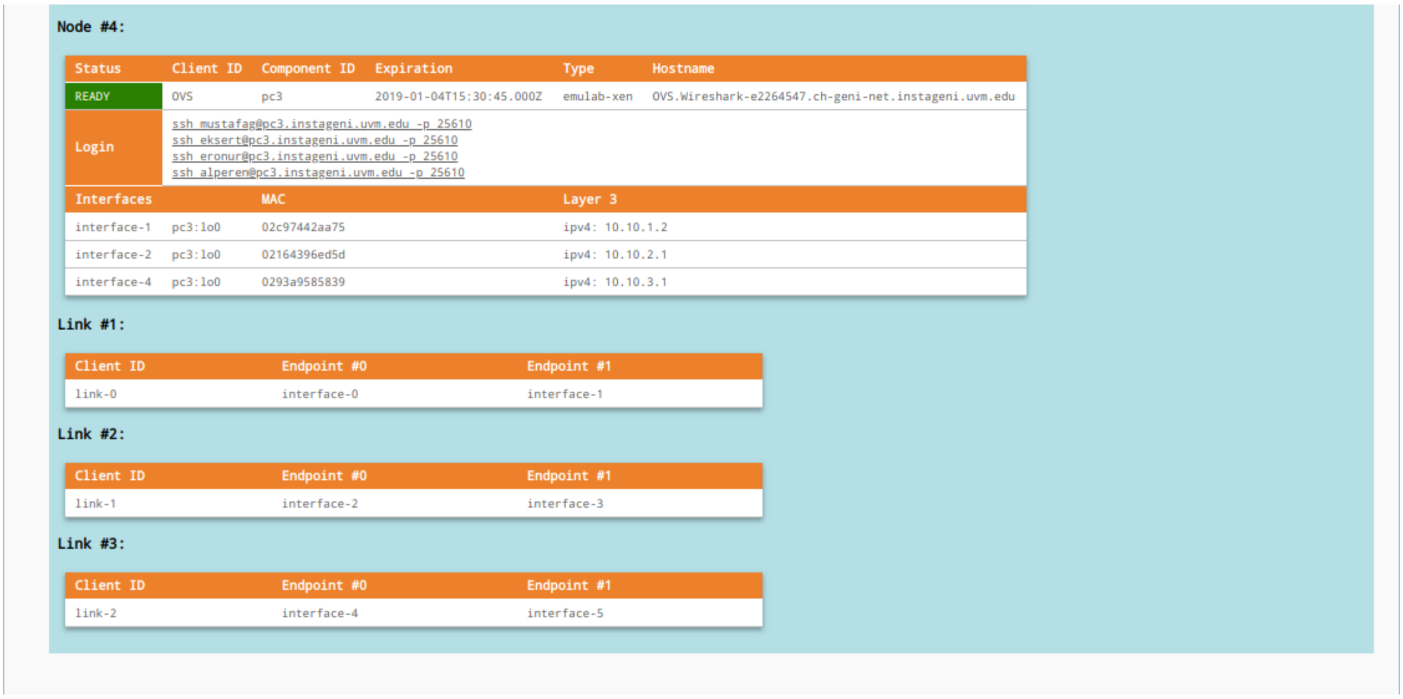
Status	Client ID	Component ID	Expiration	Type	Hostname
READY	victim	pc3	2019-01-04T15:30:45.000Z	emulab-xen	victim.Wireshark-e2264547.ch-geni-net.instageni.uvm.edu
Login	ssh mustafag@pc3.instageni.uvm.edu -p 25613 ssh ekserl@pc3.instageni.uvm.edu -p 25613 ssh eronur@pc3.instageni.uvm.edu -p 25613 ssh alperen@pc3.instageni.uvm.edu -p 25613				
Interfaces		MAC		Layer 3	
interface-0	pc3:lo0	0237f1793e6a		ipv4: 10.10.1.1	

Node #2:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	attacker	pc3	2019-01-04T15:30:45.000Z	emulab-xen	attacker.Wireshark-e2264547.ch-geni-net.instageni.uvm.edu
Login	ssh mustafag@pc3.instageni.uvm.edu -p 25611 ssh ekserl@pc3.instageni.uvm.edu -p 25611 ssh eronur@pc3.instageni.uvm.edu -p 25611 ssh alperen@pc3.instageni.uvm.edu -p 25611				
Interfaces		MAC		Layer 3	
interface-3	pc3:lo0	02d5730ba6f3		ipv4: 10.10.2.2	

Node #3:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	user	pc3	2019-01-04T15:30:45.000Z	emulab-xen	user.Wireshark-e2264547.ch-geni-net.instageni.uvm.edu
Login	ssh mustafag@pc3.instageni.uvm.edu -p 25612 ssh ekserl@pc3.instageni.uvm.edu -p 25612 ssh eronur@pc3.instageni.uvm.edu -p 25612 ssh alperen@pc3.instageni.uvm.edu -p 25612				
Interfaces		MAC		Layer 3	
interface-5	pc3:lo0	0240a16c77b1		ipv4: 10.10.3.2	



Node #4:

Status	Client ID	Component ID	Expiration	Type	Hostname
READY	OVS	pc3	2019-01-04T15:30:45.000Z	emulab-xen	OVS.Wireshark-e2264547.ch-geni-net.instageni.uvm.edu
Login	ssh mustafag@pc3.instageni.uvm.edu -p 25610 ssh eksert@pc3.instageni.uvm.edu -p 25610 ssh eronur@pc3.instageni.uvm.edu -p 25610 ssh alperen@pc3.instageni.uvm.edu -p 25610				
Interfaces		**MAC**		**Layer 3**	
interface-1	pc3:lo0	02c97442aa75		ipv4: 10.10.1.2	
interface-2	pc3:lo0	02164396ed5d		ipv4: 10.10.2.1	
interface-4	pc3:lo0	0293a9585839		ipv4: 10.10.3.1	

Link #1:

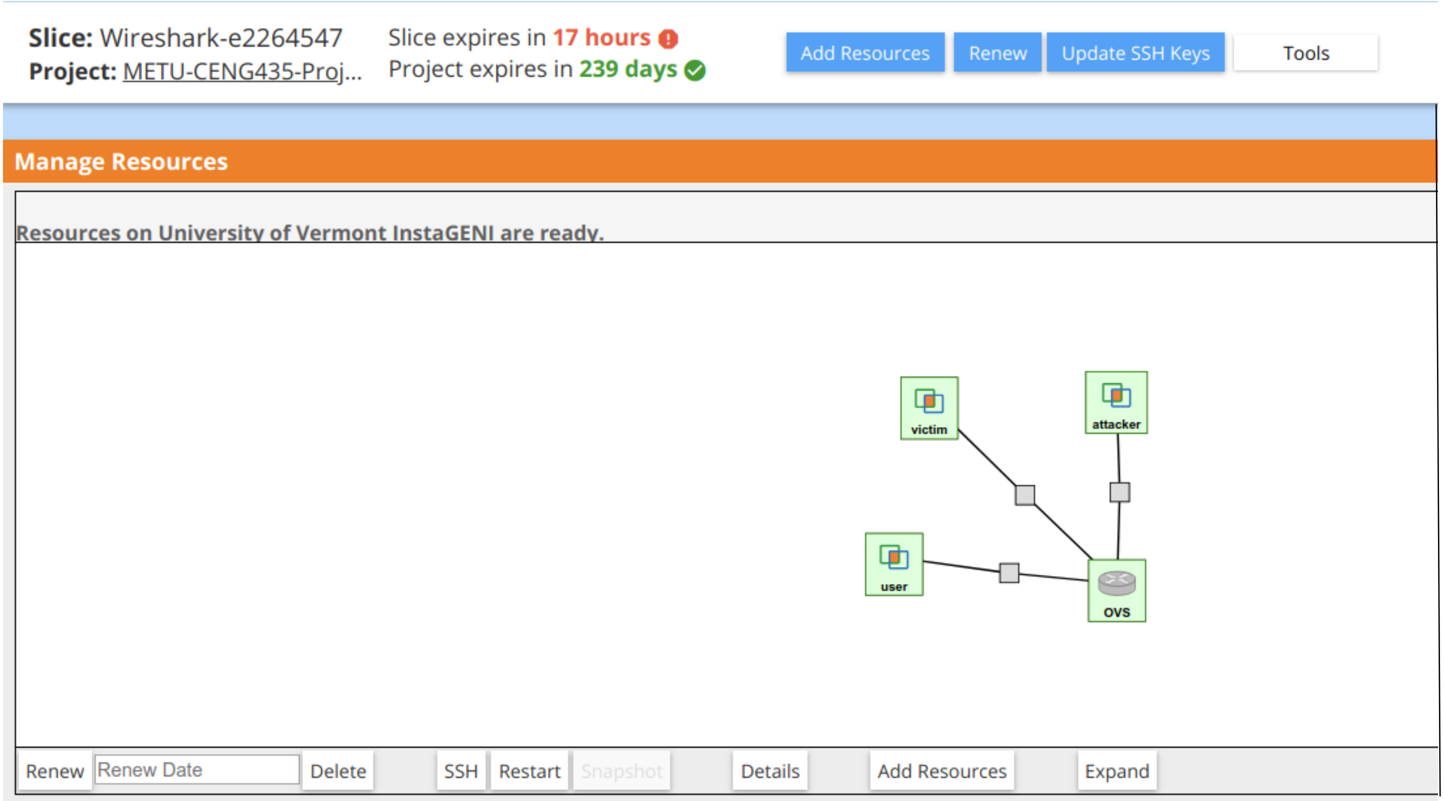
Client ID	Endpoint #0	Endpoint #1
link-0	interface-0	interface-1

Link #2:

Client ID	Endpoint #0	Endpoint #1
link-1	interface-2	interface-3

Link #3:

Client ID	Endpoint #0	Endpoint #1
link-2	interface-4	interface-5



Slice: Wireshark-e2264547
Project: METU-CENG435-Proj...

Slice expires in **17 hours**
Project expires in **239 days**

Manage Resources

Resources on University of Vermont InstaGENI are ready.