UNIVERSITY of SAN CARLOS
SCIENTIA • VIRTUS • DEVOTIO

FIRST SEMESTER A.Y. 2021-2022

Name: Bebi Grace Balbuena **Teacher**: Mr. Godwin Monserate

Lab Activity: Using wireshark to view network traffic **Schedule**: MW

Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

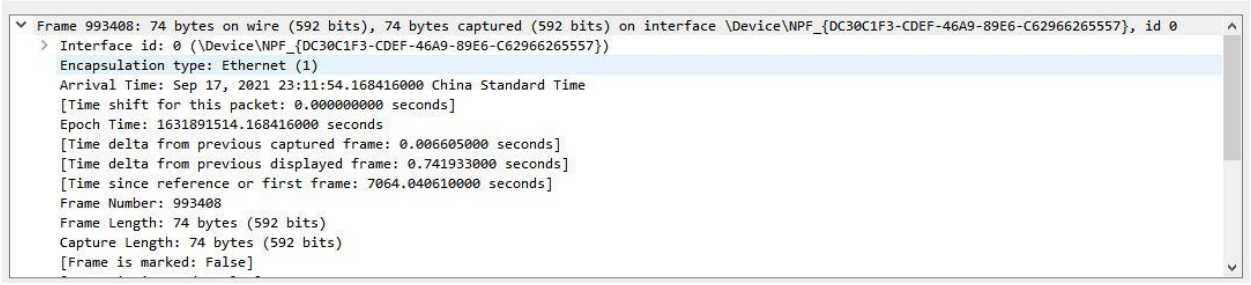
Local ICMP Data in Wireshark using: 192.168.0.60

```
C:\Users\pn.guest>ping 192.250.66.78

Pinging 192.250.66.78 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.250.66.78:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\pn.guest>
```

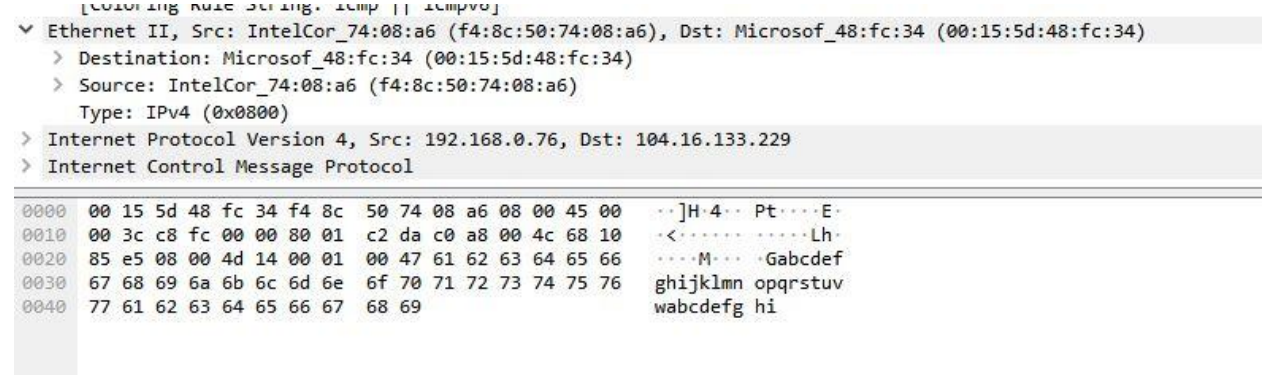
WireShark:

9928…	7060.990095	192.168.0.76	104.16.133.229	ICMP	74	Echo (ping) request id=0x0001, seq=68/17408, ttl=128 (reply in 992822)
9928…	7061.013843	104.16.133.229	192.168.0.76	ICMP	74	Echo (ping) reply id=0x0001, seq=68/17408, ttl=57 (request in 992814)
9930…	7062.011650	192.168.0.76	104.16.133.229	ICMP	74	Echo (ping) request id=0x0001, seq=69/17664, ttl=128 (reply in 993021)
9930…	7062.030109	104.16.133.229	192.168.0.76	ICMP	74	Echo (ping) reply id=0x0001, seq=69/17664, ttl=57 (request in 993017)
9932…	7063.027249	192.168.0.76	104.16.133.229	ICMP	74	Echo (ping) request id=0x0001, seq=70/17920, ttl=128 (reply in 993230)
9932…	7063.298677	104.16.133.229	192.168.0.76	ICMP	74	Echo (ping) reply id=0x0001, seq=70/17920, ttl=57 (request in 993208)
9934…	7064.040610	192.168.0.76	104.16.133.229	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (reply in 993415)
9934…	7064.075674	104.16.133.229	192.168.0.76	ICMP	74	Echo (ping) reply id=0x0001, seq=71/18176, ttl=57 (request in 993408)
1098…	7637.604798	192.168.0.76	192.250.66.78	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (no response found!)
1099…	7642.499873	192.168.0.76	192.250.66.78	ICMP	74	Echo (ping) request id=0x0001, seq=73/18688, ttl=128 (no response found!)
1100…	7647.515898	192.168.0.76	192.250.66.78	ICMP	74	Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (no response found!)
1100…	7652.513517	192.168.0.76	192.250.66.78	ICMP	74	Echo (ping) request id=0x0001, seq=75/19200, ttl=128 (no response found!)

Frame:



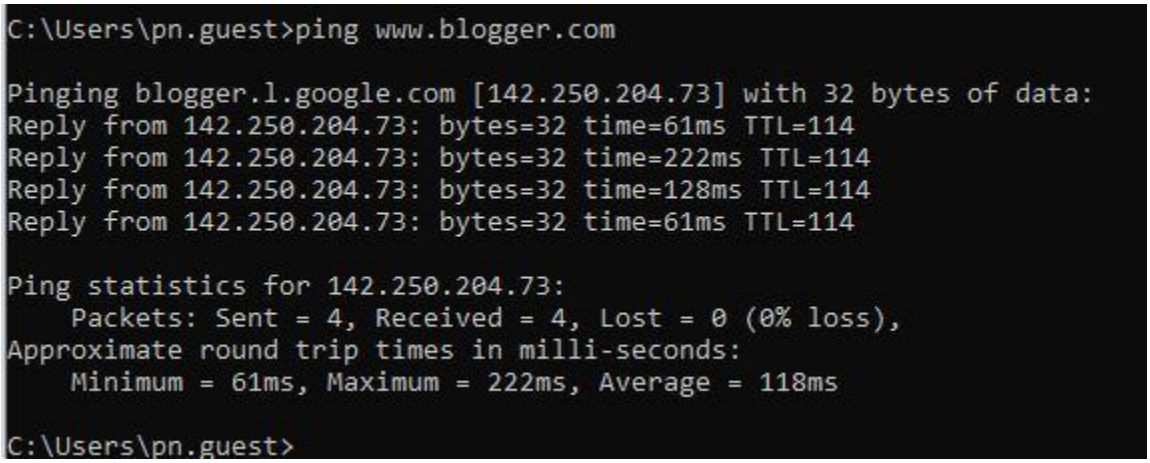
Source:

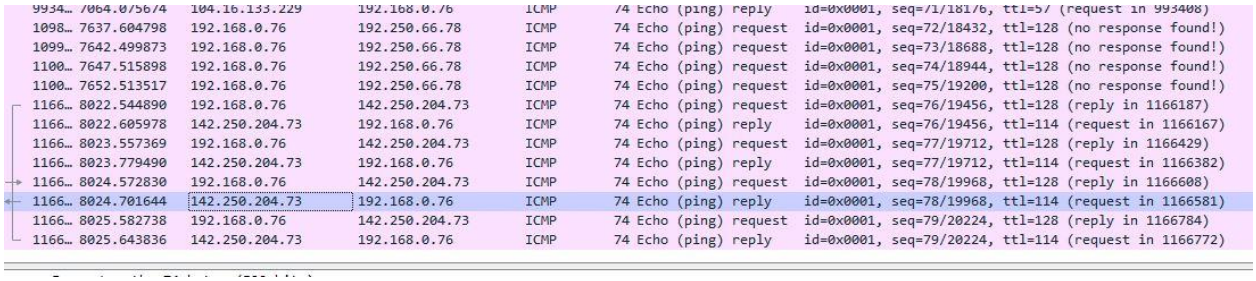


Answer:

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

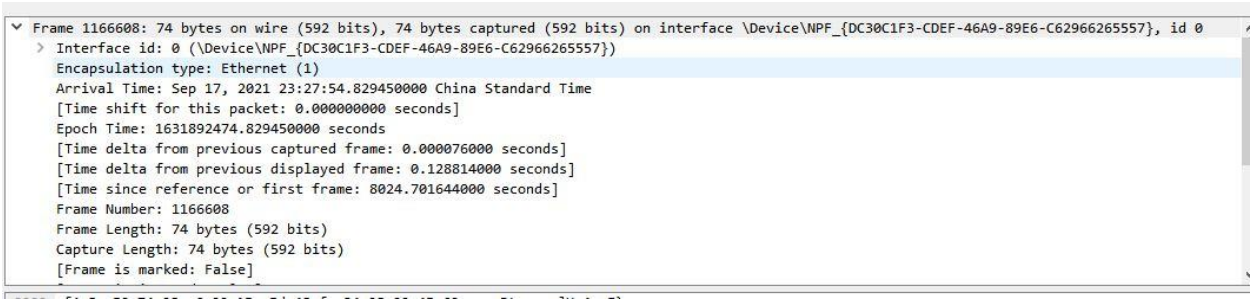
Capture and Analyze Remote ICMP Data in Wireshark using: Blogger.com (142.250.204.73)





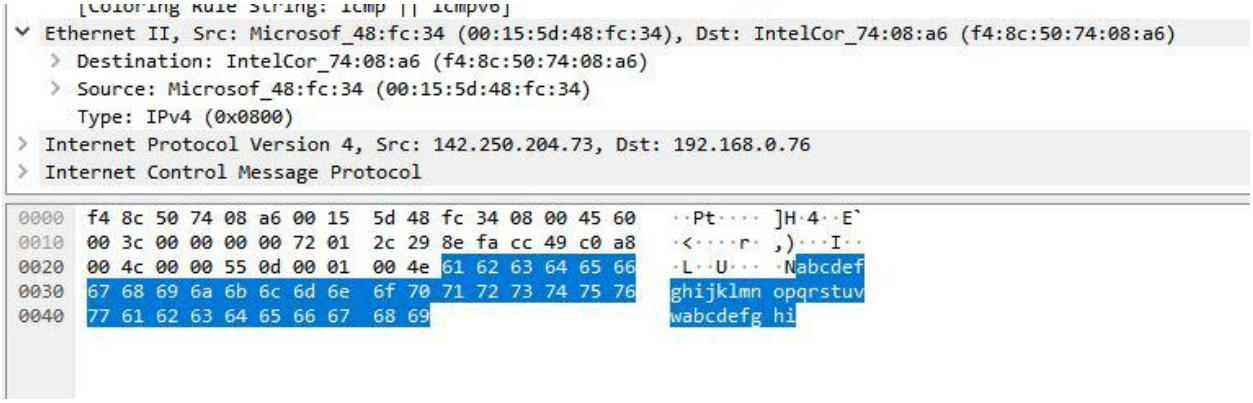
9934…	7064.075674	104.16.133.229	192.168.0.76	ICMP	74 Echo (ping) reply	id=0x0001, seq=71/18176, ttl=57 (request in 993408)
1098…	7637.604798	192.168.0.76	192.250.66.78	ICMP	74 Echo (ping) request	id=0x0001, seq=72/18432, ttl=128 (no response found!)
1099…	7642.499873	192.168.0.76	192.250.66.78	ICMP	74 Echo (ping) request	id=0x0001, seq=73/18688, ttl=128 (no response found!)
1100…	7647.515898	192.168.0.76	192.250.66.78	ICMP	74 Echo (ping) request	id=0x0001, seq=74/18944, ttl=128 (no response found!)
1100…	7652.513517	192.168.0.76	192.250.66.78	ICMP	74 Echo (ping) request	id=0x0001, seq=75/19200, ttl=128 (no response found!)
1166…	8022.544890	192.168.0.76	142.250.204.73	ICMP	74 Echo (ping) request	id=0x0001, seq=76/19456, ttl=128 (reply in 1166187)
1166…	8022.605978	142.250.204.73	192.168.0.76	ICMP	74 Echo (ping) reply	id=0x0001, seq=76/19456, ttl=114 (request in 1166167)
1166…	8023.557369	192.168.0.76	142.250.204.73	ICMP	74 Echo (ping) request	id=0x0001, seq=77/19712, ttl=128 (reply in 1166429)
1166…	8023.779490	142.250.204.73	192.168.0.76	ICMP	74 Echo (ping) reply	id=0x0001, seq=77/19712, ttl=114 (request in 1166382)
1166…	8024.572830	192.168.0.76	142.250.204.73	ICMP	74 Echo (ping) request	id=0x0001, seq=78/19968, ttl=128 (reply in 1166608)
1166…	8024.701644	142.250.204.73	192.168.0.76	ICMP	74 Echo (ping) reply	id=0x0001, seq=78/19968, ttl=114 (request in 1166581)
1166…	8025.582738	192.168.0.76	142.250.204.73	ICMP	74 Echo (ping) request	id=0x0001, seq=79/20224, ttl=128 (reply in 1166784)
1166…	8025.643836	142.250.204.73	192.168.0.76	ICMP	74 Echo (ping) reply	id=0x0001, seq=79/20224, ttl=114 (request in 1166772)

Frame:



```
Frame 1166608: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{DC30C1F3-CDEF-46A9-89E6-C62966265557}, id 0
  Interface id: 0 (\Device\NPF_{DC30C1F3-CDEF-46A9-89E6-C62966265557})
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 17, 2021 23:27:54.829450000 China Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1631892474.829450000 seconds
  [Time delta from previous captured frame: 0.000076000 seconds]
  [Time delta from previous displayed frame: 0.128814000 seconds]
  [Time since reference or first frame: 8024.701644000 seconds]
  Frame Number: 1166608
  Frame Length: 74 bytes (592 bits)
  Capture Length: 74 bytes (592 bits)
  [Frame is marked: False]
```

Source:



```
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Microsof_48:fc:34 (00:15:5d:48:fc:34), Dst: IntelCor_74:08:a6 (f4:8c:50:74:08:a6)
  Destination: IntelCor_74:08:a6 (f4:8c:50:74:08:a6)
  Source: Microsof_48:fc:34 (00:15:5d:48:fc:34)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 142.250.204.73, Dst: 192.168.0.76
Internet Control Message Protocol
```

```
0000  f4 8c 50 74 08 a6 00 15  5d 48 fc 34 08 00 45 60   ··Pt···· ]H·4··E`
0010  00 3c 00 00 00 00 72 01  2c 29 8e fa cc 49 c0 a8   ·<····r· ,)···I··
0020  00 4c 00 00 55 0d 00 01  00 4e 61 62 63 64 65 66   ·L··U··· ·Nabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

The transport layer provides a total end-to-end solution for reliable communications. TCP/IP relies on the transport layer to effectively control communications between two hosts. When an IP communication session must begin or end, the transport layer is used to build this connection. MAC addresses for remote hosts are not known on the local network, so the MAC address of the default-gateway is used. After the packet reaches the default-gateway router, the Layer 2 information is stripped from the packet and a new Layer 2 header is attached with the destination MAC address of the next hop router - IT.