Submission - LAB 3: ICMP / Fragmentation

Please submit during this lab session or else at next week's lab session.

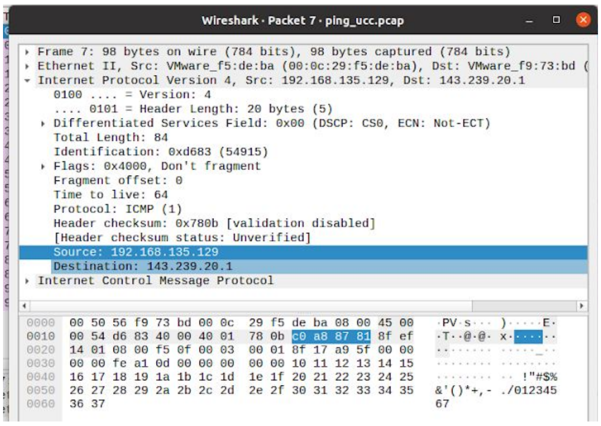
Student name: Nathan Crowley

Student ID: 118429092

1. ICMP and Ping

You should answer the following questions:

1. What is the IP address of the source host? What is the IP address of the destination host?
    - Source: 192.168.135.129
    - Destination: 143.239.20.1



Wireshark · Packet 7 · ping_ucc.pcap

```
▸ Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▸ Ethernet II, Src: VMware_f5:de:ba (00:0c:29:f5:de:ba), Dst: VMware_f9:73:bd (
▾ Internet Protocol Version 4, Src: 192.168.135.129, Dst: 143.239.20.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xd683 (54915)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x780b [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.135.129
    Destination: 143.239.20.1
▸ Internet Control Message Protocol

0000  00 50 56 f9 73 bd 00 0c  29 f5 de ba 08 00 45 00   ·PV·s··· )·····E·
0010  00 54 d6 83 40 00 40 01  78 0b c0 a8 87 81 8f ef   ·T··@·@· x·······
0020  14 01 08 00 f5 0f 00 03  00 01 8f 17 a9 5f 00 00   ········ ·····_··
0030  00 00 fe a1 0d 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

2. Why is it that an ICMP packet does not have source and destination port numbers?
    - ICMP does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes.
    - ICMP = Internet Control Message Protocol, is an error-reporting protocol network devices, like routers, use to generate error messages to the source IP address when network problems *prevent* delivery of IP packets.
    - Each ICMP packet has a "Type" and a "Code".
    - Example: Type 8 and Code 0 is the ICMP "echo request".

2. ICMP and Traceroute

- sudo traceroute -n -I -m 5 www.ucc.ie:
    - **"-n"** disables intermediary node hostname lookup.
    - **"-I"** forces ICMP probes.
    - **"-m 5"** sets the maximum TTL to 5.
    - This command will send 3 packets with TTL=1, 3 packets with TTL=2 and 3 packets with TTL=3 and so on.
- sudo traceroute -n -T -p 34567 -m 5 www.ucc.ie:
    - **"-T"** forces TCP probes.
    - **"-p 34567"** sets the destination default HTTP port a web server usually operates on, and "www.ucc.ie" is the web server.
- sudo traceroute -n -T -p 80 -m 5 www.ucc.ie:
    - **"-p 80"** will send probes to destination port 80, which is the default HTTP port a web server operates on, and "www.ucc.ie" is the web server.

1. XExamine the three ICMP packets sent by www.ucc.ie as a response to the UDP probes to port 34567. Compare them to the responses sent by www.ucc.ie as a response to the TCP probes to port 80. How are they different?
    - www.ucc.ie = IP 143.239.20.1
    -

2. Examine the last three ICMP packets sent by www.ucc.ie as a response to the ICMP probes. How are these packets different from the ICMP error packets? Why are they different?
    - They are ICMP packet type 0 (echo reply) compared to type 11 (time-to-live-exceeded).
    - These differ as the packers have completed as they made it to the destination IP.

3. Imagine you are a network administrator. You don’t want to give any information about your network map, so you want to allow ping, but block incoming traceroute ICMP from the Internet. How do you think you could discern between the two? Do you think it would be easier to identify and block the traceroute request or the reply messages? Explain your answer.
    - The difference between ping and traceroute is that ping messages only use type 0(echo reply) and type 8(echo request).
    - And you could filter out the type 11 (time exceeded) and block them.

4. After running this experiment, how do you think that a port scanner works like? (A port scanner finds all the "open" ports of a network host for UDP and TCP - “open” ports are called the ones that a service listens to and responds from) i.e. how you determine which ports are “open” and which are “closed”.
    - Port scanners are used to sweep a whole network block or a single target to check if any port is alive. It sends an ICMP echo request (Type 8) to the target, if the response is an ICMP reply, then the port is alive.
    - **TCP:**
        - Port is open if a **SYN** packet gets a **SYN-ACK** reply from the target.
        - Port is closed if a **RST** packet is returned.
    - **UPD:**
        - Port is open if there is **no response** (something is blocking the ICMP).
        - Port is closed if the sender receives a response (**ICMP port unreachable**).