

Part 1:

- 1) The result is the output "Xavier CS web server is up". The wireshark packet capture shows the Echo Request of Type 8, Code 0:

```
▼ Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0xf20c [correct]
  [Checksum Status: Good]
  Identifier (BE): 1720 (0x06b8)
  Identifier (LE): 47110 (0xb806)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  [Response frame: 6]
  Timestamp from icmp data: Nov 12, 2020 20:25:21.000000000 EST
  [Timestamp from icmp data (relative): 0.927496490 seconds]
```

as well as the Echo Reply of Type 0, Code 0:

```
▼ Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xfa0c [correct]
  [Checksum Status: Good]
  Identifier (BE): 1720 (0x06b8)
  Identifier (LE): 47110 (0xb806)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  [Request frame: 5]
  [Response time: 34.092 ms]
  Timestamp from icmp data: Nov 12, 2020 20:25:21.000000000 EST
```

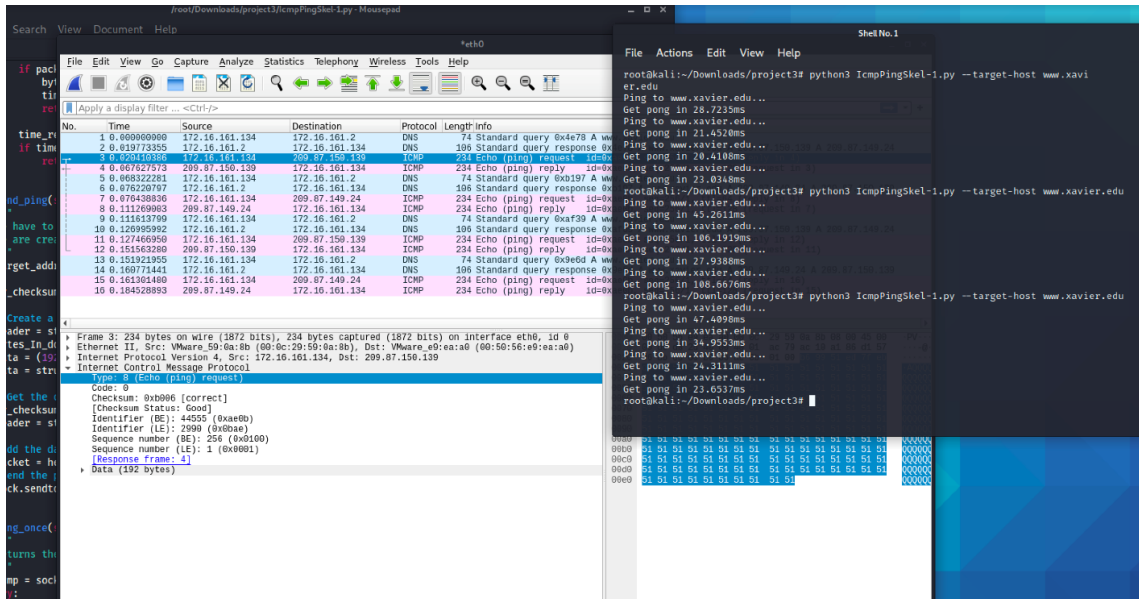
- 2) Within the code, it appears that the command "ping -c 1 www.xavier.edu" is split up and ran within the subprocess.check_call function, and if there is any error output the stdout/stderr will capture the value in bytecode, and the subprocess.check_call method will call subprocess.CalledProcessError if the value returned is not 0.

Part 2:

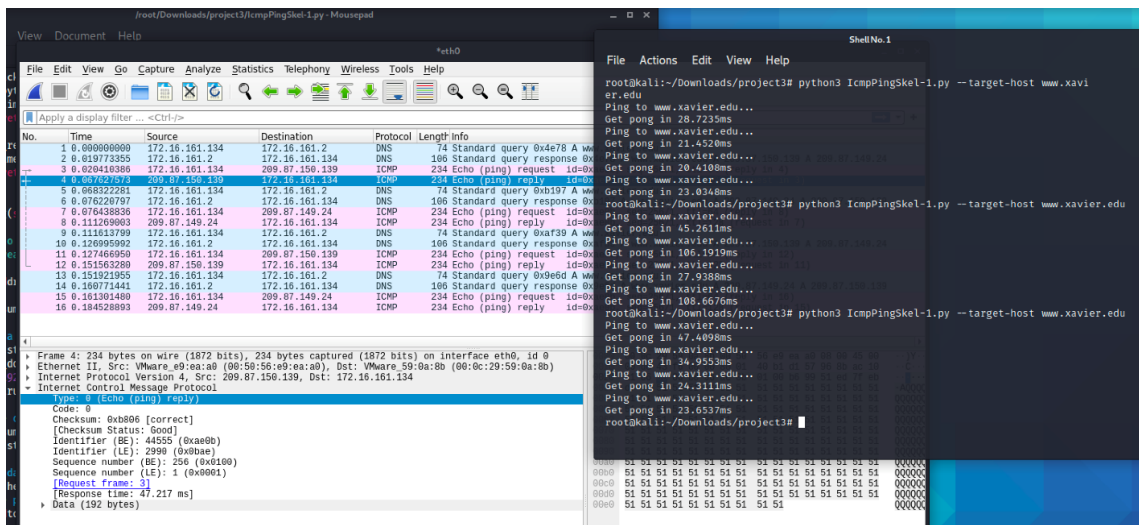
Completed Code with comments submitted in canvas.

Part 3:

- 1) ICMP Request Packet: Type 8, Code 0. This matches the packet we created in the program as the ICMP type is the same.



- 2) ICMP Reply Packet: Type 0, Code 0. We did not get a warning within this packet



- 3) The ICMP Packet data is very similar to the dummy ICMP data we created on the Python program because the Typing is the same.