**IT430: Lab 04 – PCAP Data Analysis II**

Names: Cooper Walshe, Owen Pitchford

Alphas: 256666, 255076

External source  
Class notes

Honor

We wrote the code on my own except the help from the external source listed above. Moreover, we didn’t copy any part of the code from other midshipmen.

Initials: CW and TOP

Challenges

We originally didn’t think about getting rid of the padding on some packets which caused an issue but we figured it out.

The bit manipulation required some thinking but we also figured it out.

What we learned and what was interesting to us

(Specify what you learned and what was interesting to you)

We learned how to convert between bytes to ints and bytes to hex. And also how to slice apart a PCAP file to get exactly what we need from it.

We learned the flag code 0x018 was used when a message is sent. The push and ack flag are set.

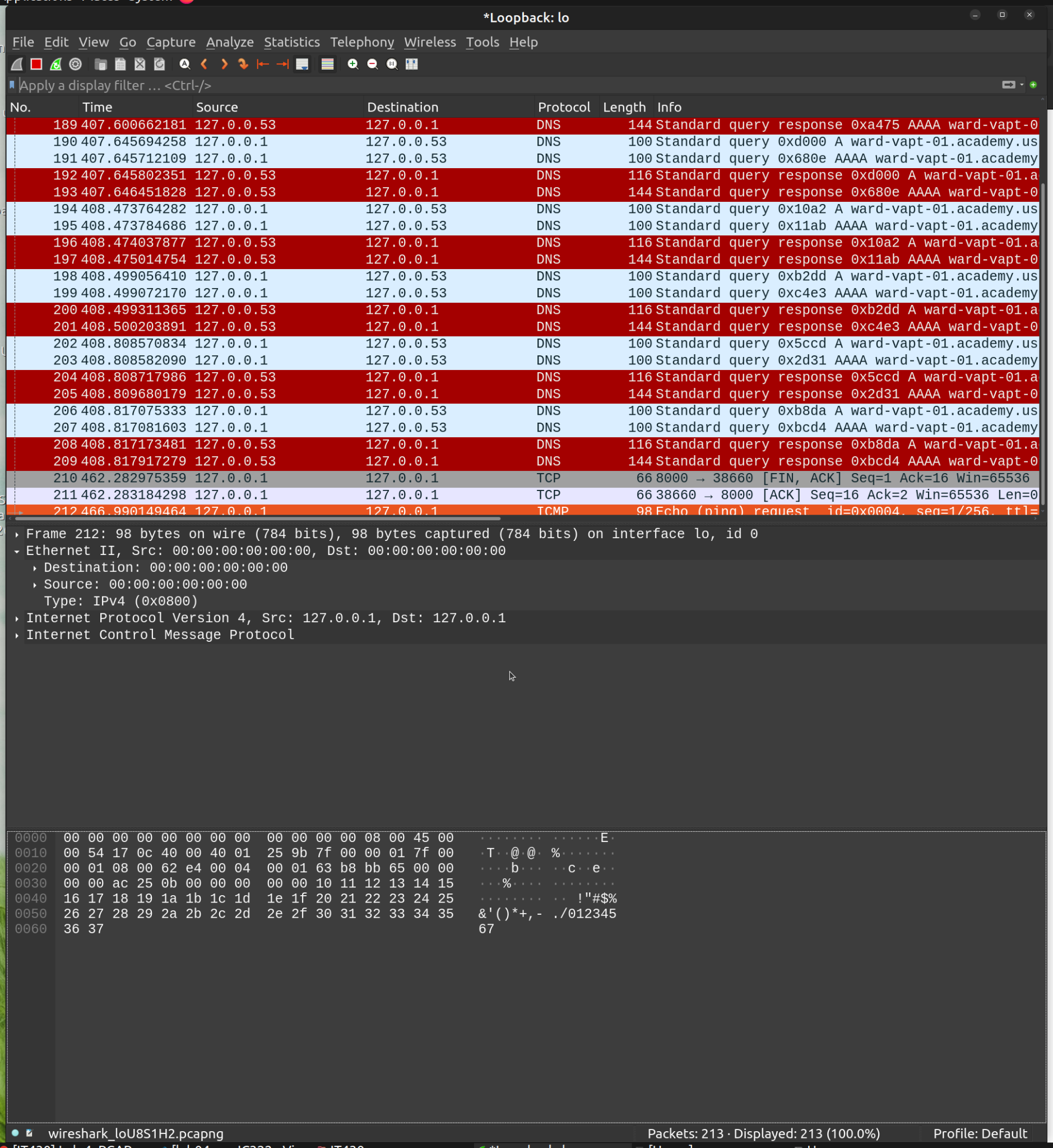
How much work each of did (0: nothing, 10: everything)

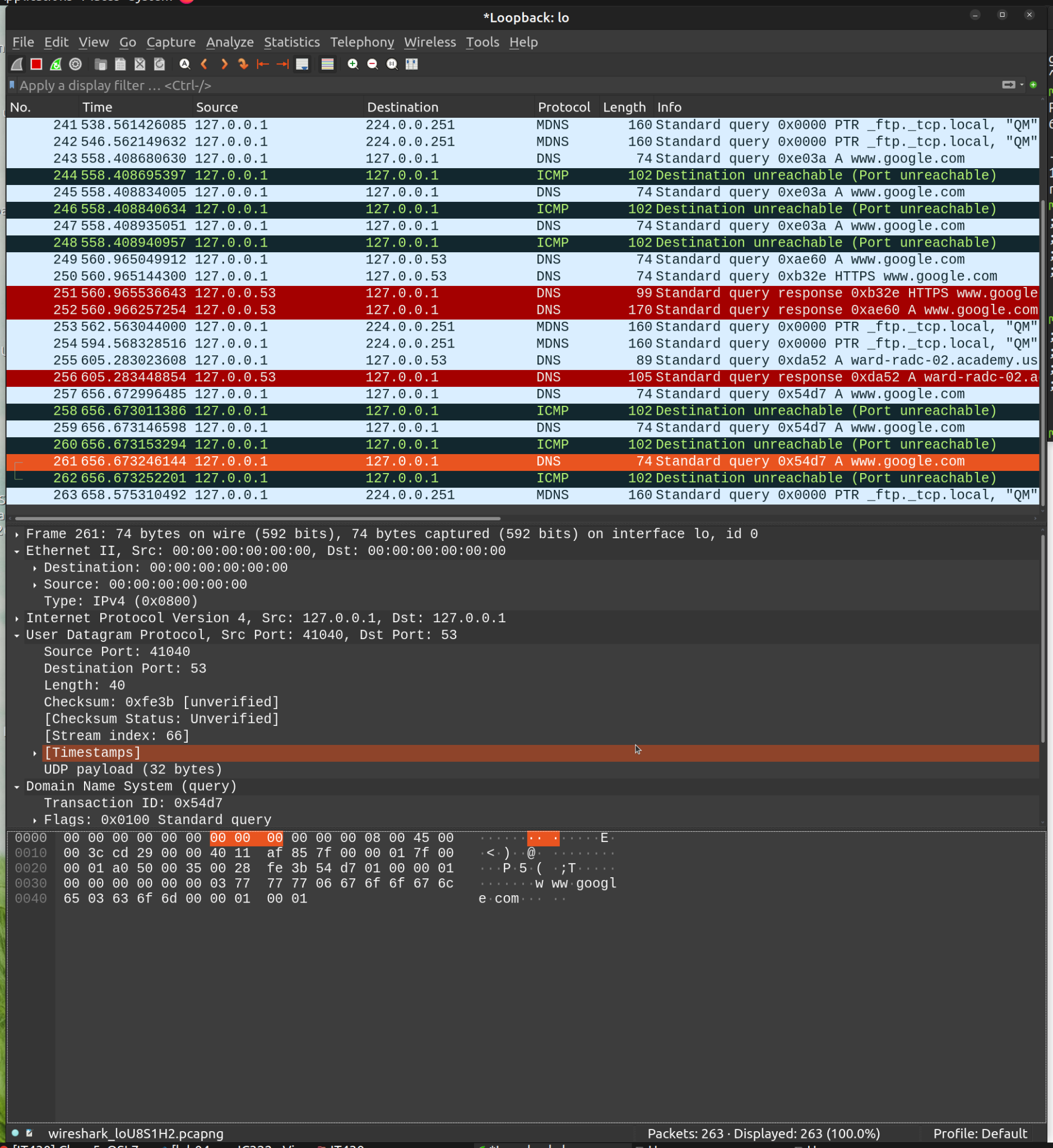
- Owen: 5

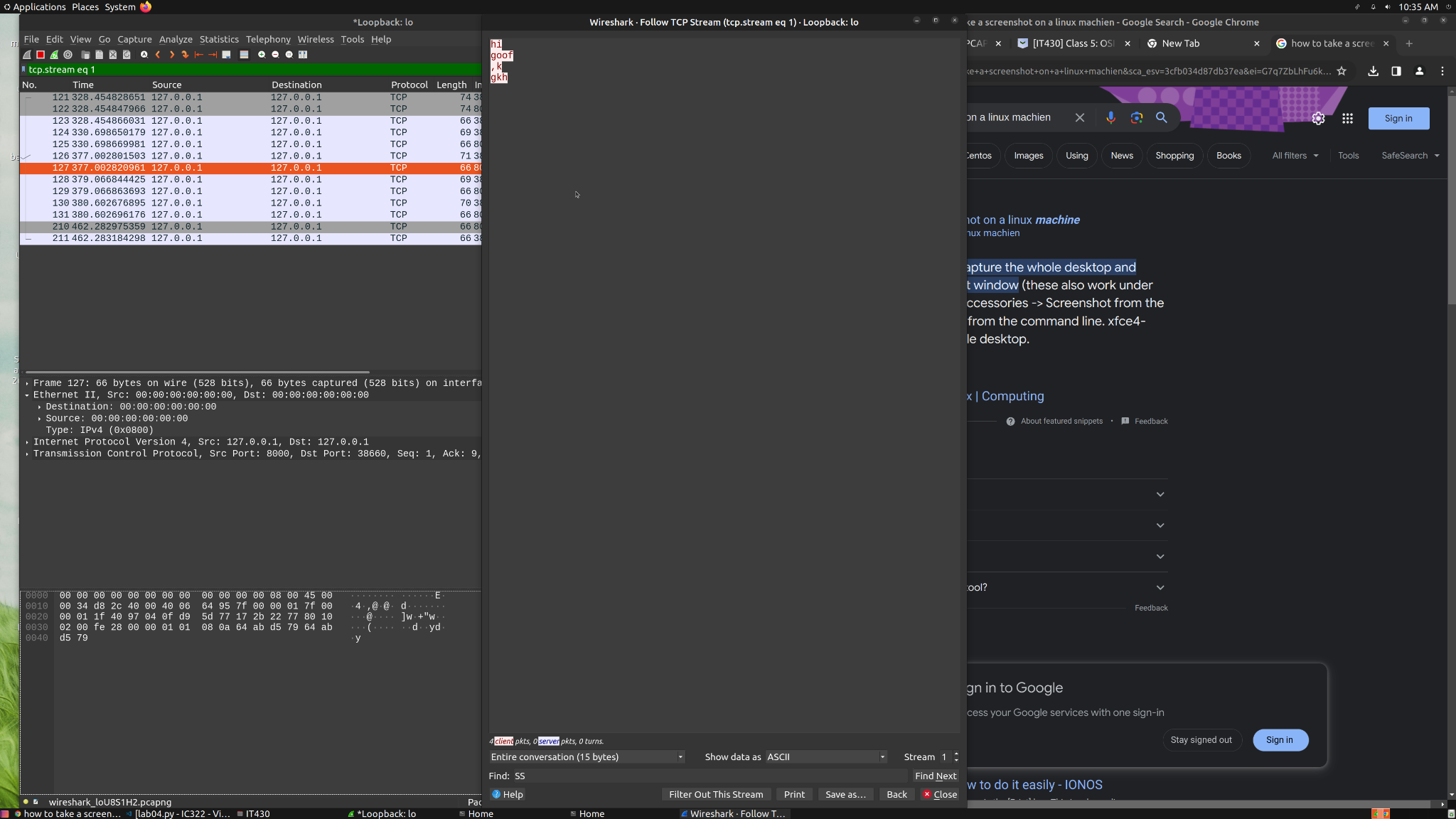
- Cooper: 5

# **Part 1**

(For each part of the lab, give your work -- attach code, screen captures, explanations and answers as necessary)







# **Part 2**

def showpkts\_IP(data):

data = data[24:] #Get rid of global header

while(data):

#Get rid of excess packet header

data = data[12:]

#Find the packet length

pkt\_len = int.from\_bytes(data[0:4], "little")

#Get rid of that packet length

data = data[4:]

#Turn only that packet to hex

tempData = ([f"{i:02x}" for i in data[0:pkt\_len]])

print("Dst-MAC=", getAdr(tempData))

tempData= tempData[6:]

print("Src-MAC=", getAdr(tempData))

tempData= tempData[8:]

verIHL= tempData[0]

IHL = int(verIHL, 16)%16

print("IHL=", IHL)

tempData = tempData[2:]

totalLength = int(tempData[0]+tempData[1], 16)

print("Total Length=", totalLength)

tempData = tempData[2:]

#junk

tempData = tempData[5:]

protocol = int(tempData[0], 16)

tempData = tempData[3:]

print("Src-IP=", getIP(tempData))

tempData = tempData[4:]

print("Dst-IP=", getIP(tempData))

tempData = tempData[4:]

getData(tempData[:totalLength - (IHL\*4)])

data = data[pkt\_len:]

print('')

def getData(bigData):

#Format the data properly

print("data:")

for index, element in enumerate(bigData, start=1):

print(element, end='')

#End line

if index%16==0: print('')

# middle separation

elif index%8==0: print(" ", end='')

#No change

else: print(" ", end='')

def getIP(data2):

IP = ""

for index, element in enumerate(data2[0:4], start = 1):

element = str(int(element, 16))

IP = (IP + element)

if(index != 4):

IP = IP + "."

return IP

def getAdr(data2):

dstMac =""

for index, element in enumerate(data2[0:6], start = 1):

dstMac = (dstMac + element)

if(index != 6):

dstMac = dstMac + ":"

return dstMac

# 

# **Part 3:**

def showpkts\_TCP(data, ip1, ip2):

#Get rid of global header

data = data[24:]

while(data):

#Get rid of excess packet header

data = data[12:]

#Find the packet length

pkt\_len = int.from\_bytes(data[0:4], "little")

#Get rid of that packet length

data = data[4:]

#Turn only that packet to hex

tempData = ([f"{i:02x}" for i in data[0:pkt\_len]])

tempData= tempData[23:]

protocol = int(tempData[0], 16)

#skip if not TCP

if(protocol != 6):

data = data[pkt\_len:]

continue

tempData = tempData[3:]

src\_ip = getIP(tempData)

tempData = tempData[4:]

dst\_ip = getIP(tempData)

tempData = tempData[4:]

src\_port = int(tempData[0] + tempData[1], 16)

dst\_port = int(tempData[2] + tempData[3], 16)

offset = (int(tempData[12], 16) >> 4) \* 4 #bit manipulation for offset

flags = int(tempData[12][1] + tempData[13], 16)

tempData = tempData[offset:]

if(ip1 == src\_ip and ip2 == dst\_ip or ip1 == dst\_ip and ip2 == src\_ip):

msg = bytes.fromhex(" ".join(tempData))

if flags == 0x018:

print(f"{src\_ip}({src\_port}) -> {dst\_ip}({dst\_port}) :")

print(f" {msg}")

data = data[pkt\_len:]

# 

# **Part 4:**

Western firms such as Google, Facebook, and Twitter have recently stepped away from the Chinese market over concerns that the Chinese government is using their services in an unethical way. For example, China not only required Google to have a censored version of their search engine, but they also hacked into their program that ran wire taps for the FBI. By seeing their list of wiretaps, they could know if their spies were made or not. This is not uncommon. There are repeated cyber attacks launched by Chinese entities that have no regard for decent cyberspace practices and no attempt to hide their origin. According to the reading, China believes that the country is at war with the west and therefore attacks in cyberspace are permitted.

An interesting pattern that I see is that everytime a country or an organization acts with aggression towards Chinese practices, then the Chinese government launches a cyber attack. This is seen with Tibet, Australia, and the US. Other than clear cyber attacks, there is the issue with Huawei and cyber equipment. The US and UK have banned Huawei’s routers, but China is still using them in outreach programs to developing countries. It’s scary to think about much of the world using Huawei technology when it’s so easy for China to hack in and get the data.

Russia, like China, believes that they are currently in a struggle with the west (primarily the US and the EU). Instead of using cyberattacks to steal trade secrets and spy on people, Russia is using cyber attacks to disrupt social order. An example of this is their NotPetya attack which would restrict the user’s access to data on their computer and require payment for their files. In reality, the data was already lost and the only way to get data back was to restore a backup. This attack affected many large name companies and in some cases resulted in 300 million in losses for single organizations. An interesting part of the reading talks about how Russia can use the cyber attacks to shut off power stations and what not, but their actual goal is to influence voters and create a distrust in institutions. The reading points out that this is working in a way with Brexit, and many EU countries opting for authoritarian regimes. I would also argue that their disinformation campaign has created a distrust in the American voting system. This can be seen with the drama that unfolded in the 2020 election.

Russia and China are the two biggest offenders in cyberspace, however, almost all malicious governments engage in cyber attacks. It is beginning to seem like countries are using cyberspace to push their agenda on to others without the fear of it being deemed an act of war. As the attacks get bigger and bigger, I’m sure at some point an attack will cross the line for a country and turn kinetic. The reading closes with mentioning that there isn’t as much of a blanket of anonymity in the cyber realm that people think. Attacks have perpetrators, and perpetrators are brought to justice.