Problem 1

Suppose an application generates chunks of 60 bytes of data, each chunk gets encapsulated in a TCP segment, and then an IP datagram.

1. What percentage of each datagram will be overhead, and what percentage will be application data?
2. What would be the overhead if each TCP segment include 100 of application chunks (i.e., 100×60 bytes), assuming the maximum size of an IP packet is 500 bytes and sending such big TCP payload would require fragmentation.

1. Since there is 40 bytes if header, the overhead is 40/60+40 = 0.4. Application data is 0.6
2. I will not consider header as overhead here.
Overhead is 500 - 100 = 400 due to fragmentation.

Problem 2

Consider the router trying to send the following IP packet:

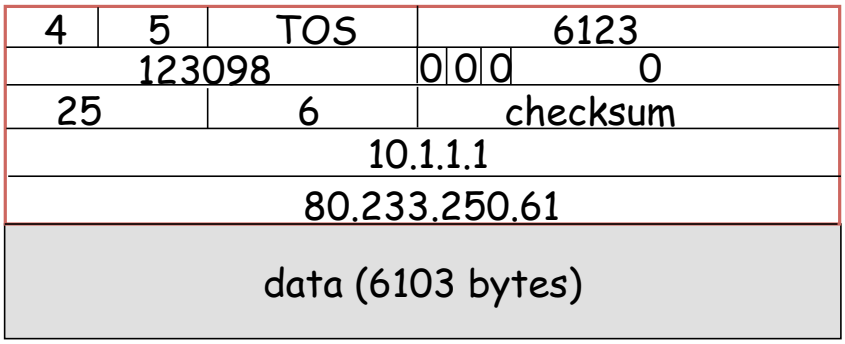


Figure 1: An IP packet.

Assuming that the maximum transmission unit that can be transferred over the link is 1400 bytes. For each of the fragment show the header length, total length, identification, flags, fragment offset, TTL, protocol fields, and IP payload size.

Write your answer using the table below

Header length	Total length	Identification	Flags	Fragment offset	TTL	Protocol	Data size
20 bytes	1400 bytes	123098	001	0	24	6	1376 bytes
20 bytes	1400 bytes	123098	001	172	23	6	1376 bytes
20 bytes	1400 bytes	123098	001	344	22	6	1376 bytes
20 bytes	1400 bytes	123098	001	516	21	6	1376 bytes
20 bytes	620 bytes	123098	000	688	20	6	600 bytes

Problem 3

Calculate the network mask, the number of bits of the network, the number of endpoint addresses in the network (excluding special addresses), the network address, and the broadcast address of the network for the following:

1. 131.179.196.0/24
2. 169.232.34.48/30
3. 196.22.136.0/21
4. 93.181.192.0, netmask 255.255.224.0
5. 10.128.0.0, netmask 255.192.0.0

1.
network mask: 255.255.255.0. first 24 bits are high, others are low: 11111111.11111111.11111111.0000.
number of bits of the network: 32 since it's ipv4
number of endpoint addresses: 2**(32 - 24) - 2 = 254
network address: 131.179.196.0
10000011.10110011.11000100.00000000
broadcast address:131.179.196.240
10000011.10110011.11000100.11110000
2.
network mask: 255.255.255.252. first 30 bits are high, others are low: 11111111.11111111.11111111.11111100.
number of bits of the network: 32
number of endpoint addresses: 2**(32 - 30) - 2 = 2
network address: 169.232.34.48
10101001.11101000.00100010.00110000
broadcast address: 169.232.34.51
10101001.11101000.00100010.00110011
3.
network mask: 255.255.248.0. first 21 bits are high, others are low: 11111111.11111111.11111000.0000.
number of bits of the network: 32
number of endpoint addresses: 2**(32 - 21) - 2 = 2046
network address:196.22.136.0
11000100.00010110.10001000.00000000
broadcast address:196.22.143.255
11000100.00010110.10001111.11111111
4.
network mask: 255.255.254.0. first 23 bits are high, others are low: 11111111.11111111.11111110.0000.
number of bits of the network: 32
number of endpoint addresses: 2**(32 - 23) - 2 = 510
network address: 93.181.192.0
01011101.10110101.11000000.00000000
broadcast address: 93.181.193.255
01011101.10110101.11000001.11111111
5.
network mask: 255.192.0.0. first 10 bits are high, others are low: 11111111.11000000.00000000.0000.
number of bits of the network: 32
number of endpoint addresses: 2**(32 - 10) - 2 = 4194302
network address: 10.128.0.0
00001010.10000000.00000000.00000000
broadcast address: 10.191.255.255
00001010.10111111.11111111.11111111

Problem 4

Why is the IP header checksum recalculated at every router?

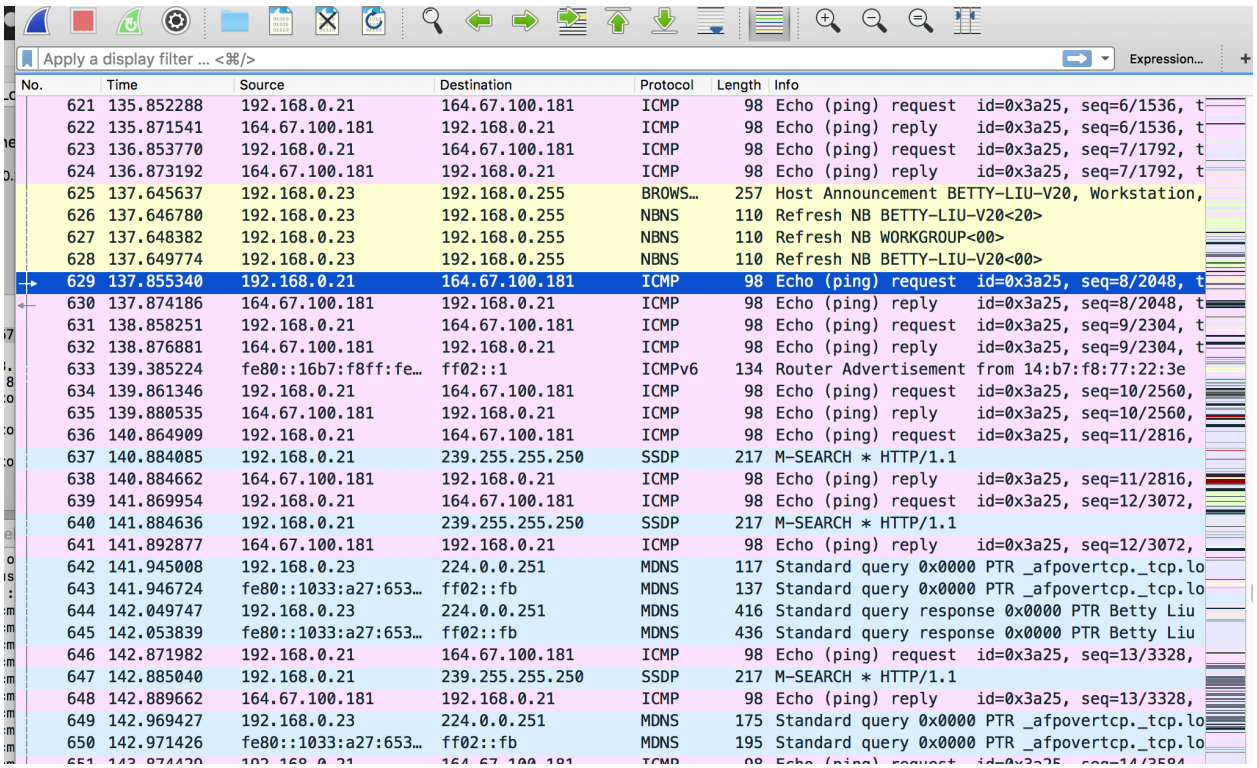
Checksum is calculated at every router because datagram needs to be discarded if the data is corrupted, so in order to minimize incorrect information, incorrect data needs to be detected as soon as possible. Checking checksum at every router ensures early detection of incorrect data. Also, some fileds in the header such as time to live changes at every router, so checksum needs to be performed before header is processed.

Problem 5

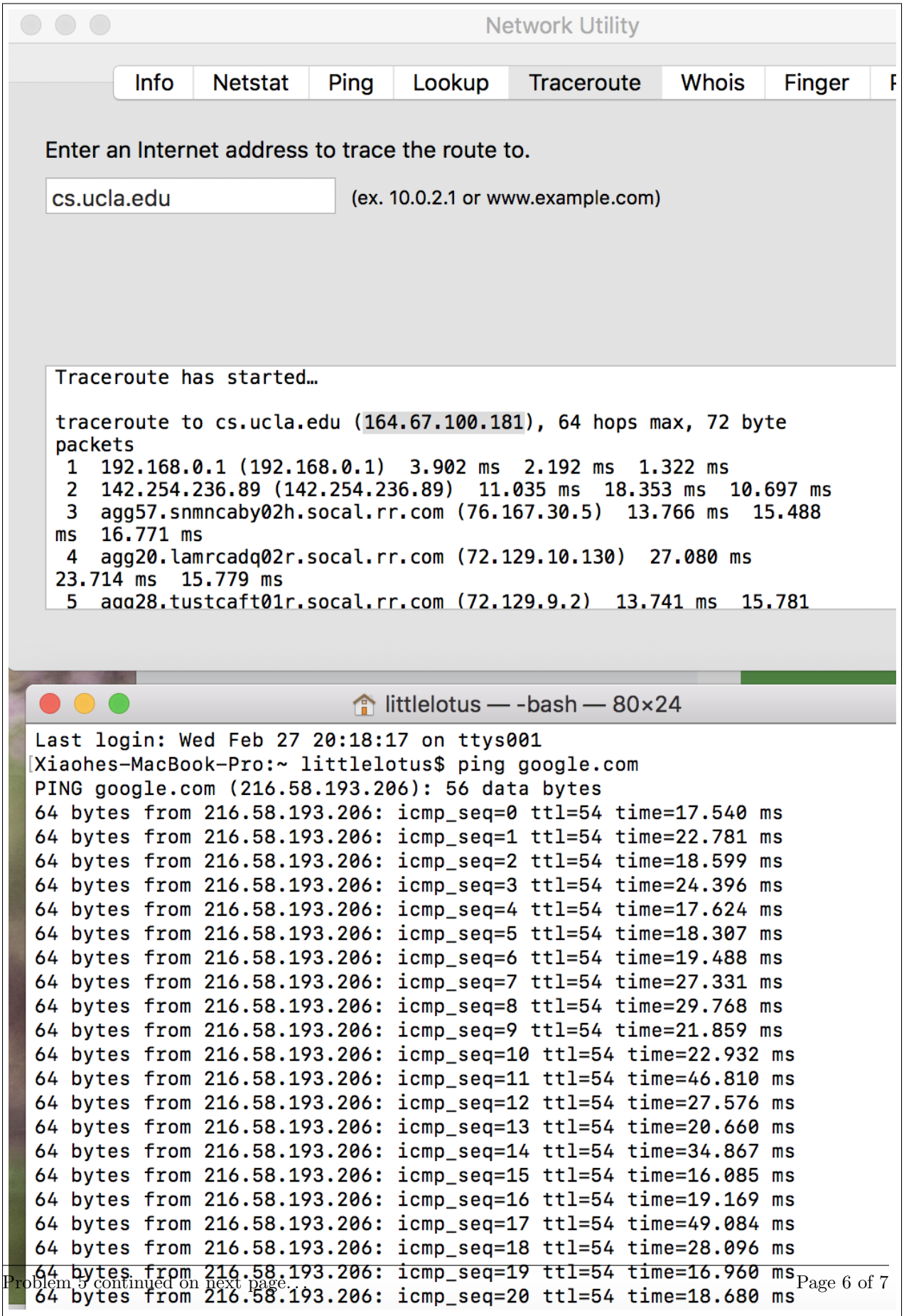
Install *Wireshark* (`https://www.wireshark.org/`). Then, (i) start capturing a packet trace from your network interface, (ii) open a web browser, (iii) go to `https://www.cs.ucla.edu/`, (iv) and then stop capturing the trace.

Investigate any TCP packet from your network interface to the UCLA CS web server. What is the IP address of your network interface? What is the IP address of www.cs.ucla.edu? Provide the screenshot that shows the IP addresses in the investigated packet.

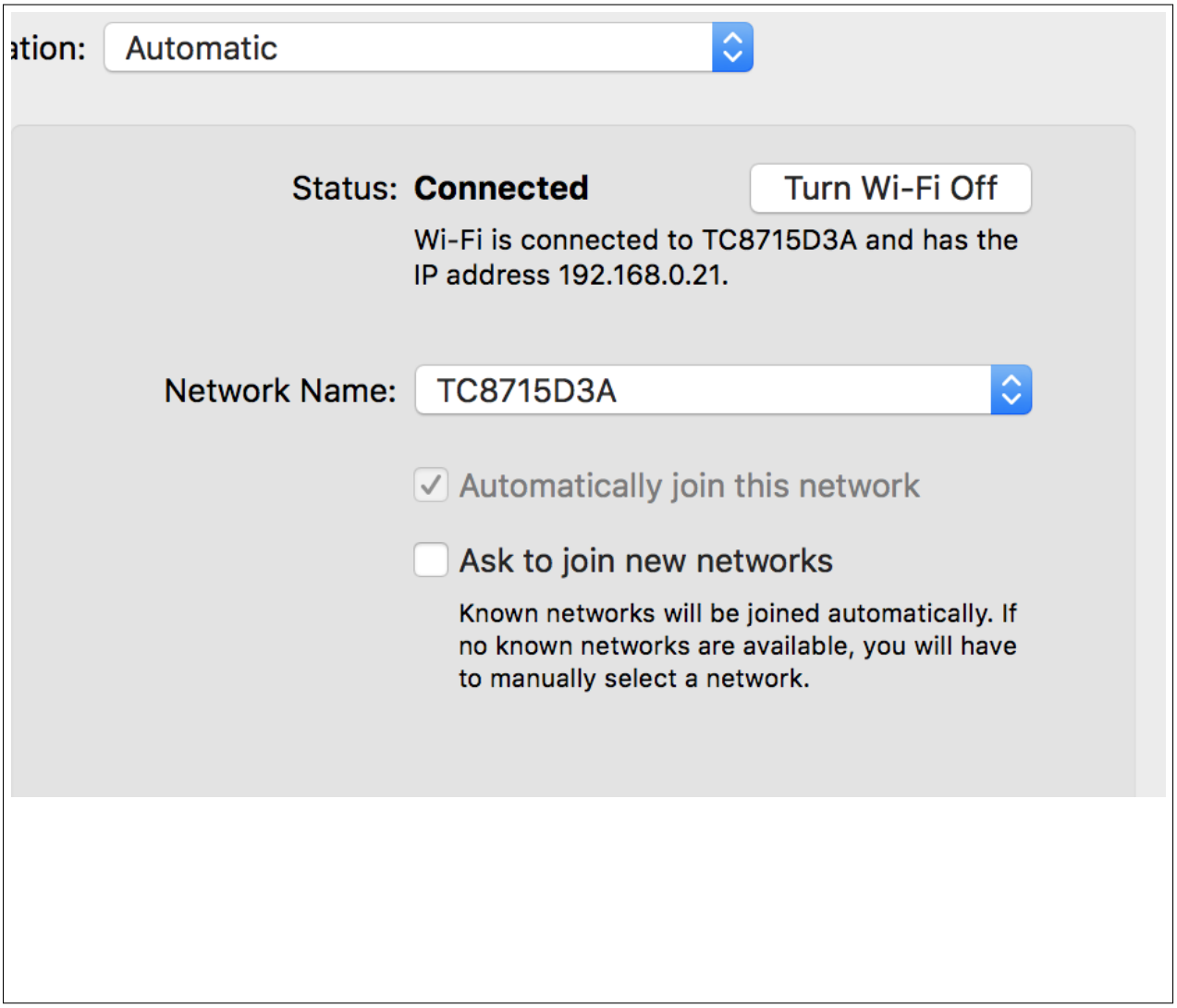
My network interface IP address is 192.168.0.21
The IP address of ucla cs website is: 164.67.100.181



Problem 5 continued on next page. . .



Problem 5 continued on next page...


ation:
Automatic
Status: Connected
Turn Wi-Fi Off
Wi-Fi is connected to TC8715D3A and has the IP address 192.168.0.21.
Network Name:
TC8715D3A
Automatically join this network
Ask to join new networks
Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.