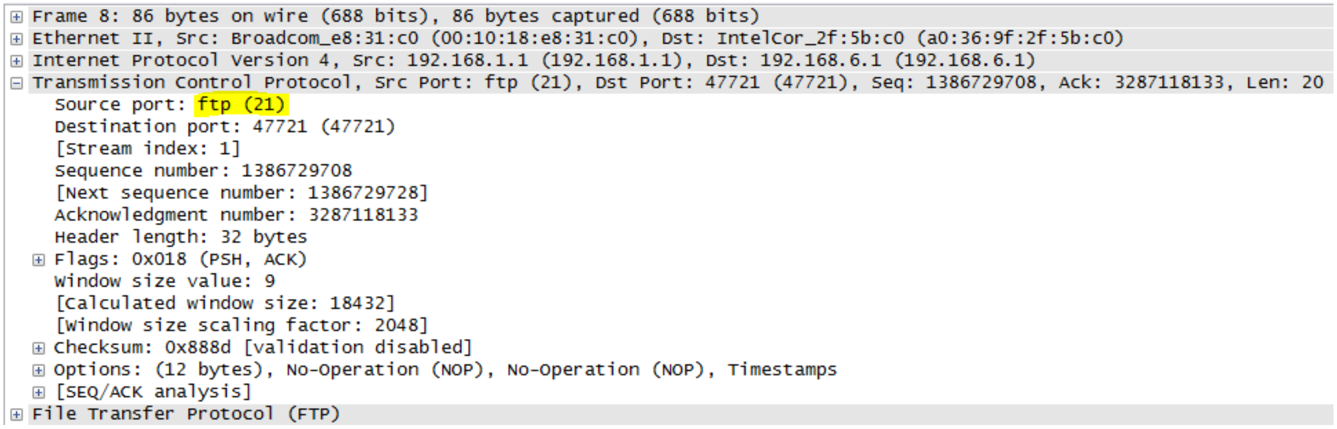
Name: Kyomin Ku

UPI: kku031

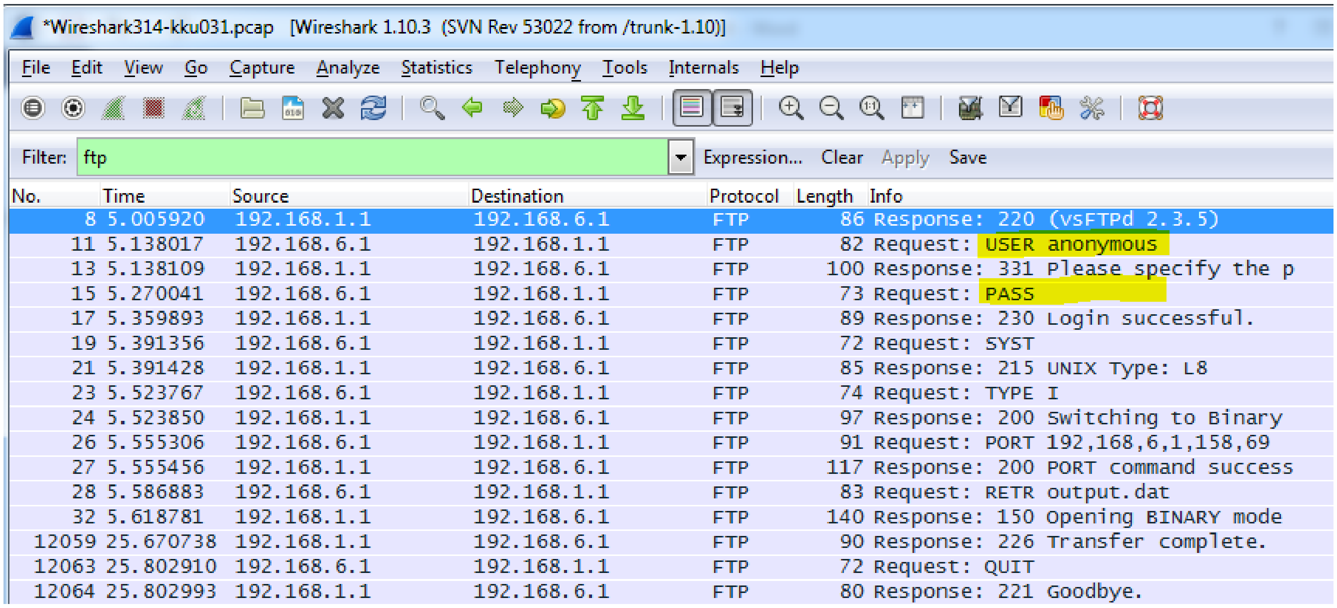
A: The FTP Protocol

1. 21



```
⊞ Frame 8: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
⊞ Ethernet II, Src: Broadcom_e8:31:c0 (00:10:18:e8:31:c0), Dst: IntelCor_2f:5b:c0 (a0:36:9f:2f:5b:c0)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.6.1 (192.168.6.1)
⊟ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 47721 (47721), Seq: 1386729708, Ack: 3287118133, Len: 20
    Source port: ftp (21)
    Destination port: 47721 (47721)
    [Stream index: 1]
    Sequence number: 1386729708
    [Next sequence number: 1386729728]
    Acknowledgment number: 3287118133
    Header length: 32 bytes
  ⊞ Flags: 0x018 (PSH, ACK)
    Window size value: 9
    [Calculated window size: 18432]
    [Window size scaling factor: 2048]
  ⊞ Checksum: 0x888d [validation disabled]
  ⊞ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ⊞ [SEQ/ACK analysis]
⊞ File Transfer Protocol (FTP)
```

2. Usercode: anonymous, and there is no password.

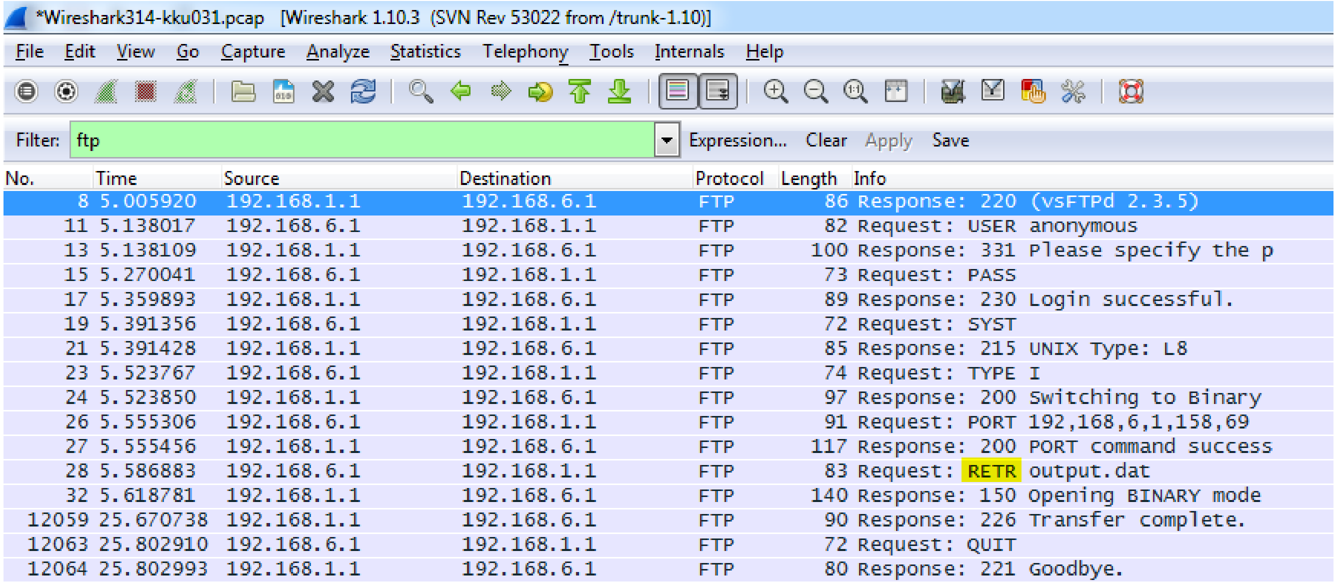


Filter: ftp

```
No.     Time       Source        Destination   Protocol Length Info
    8 5.005920    192.168.1.1   192.168.6.1   FTP        86 Response: 220 (vsFTPd 2.3.5)
   11 5.138017    192.168.6.1   192.168.1.1   FTP        82 Request: USER anonymous
   13 5.138109    192.168.1.1   192.168.6.1   FTP       100 Response: 331 Please specify the p
   15 5.270041    192.168.6.1   192.168.1.1   FTP        73 Request: PASS
   17 5.359893    192.168.1.1   192.168.6.1   FTP        89 Response: 230 Login successful.
   19 5.391356    192.168.6.1   192.168.1.1   FTP        72 Request: SYST
   21 5.391428    192.168.1.1   192.168.6.1   FTP        85 Response: 215 UNIX Type: L8
   23 5.523767    192.168.6.1   192.168.1.1   FTP        74 Request: TYPE I
   24 5.523850    192.168.1.1   192.168.6.1   FTP        97 Response: 200 Switching to Binary
   26 5.555306    192.168.6.1   192.168.1.1   FTP        91 Request: PORT 192,168,6,1,158,69
   27 5.555456    192.168.1.1   192.168.6.1   FTP       117 Response: 200 PORT command success
   28 5.586883    192.168.6.1   192.168.1.1   FTP        83 Request: RETR output.dat
   32 5.618781    192.168.1.1   192.168.6.1   FTP       140 Response: 150 Opening BINARY mode
12059 25.670738   192.168.1.1   192.168.6.1   FTP        90 Response: 226 Transfer complete.
12063 25.802910   192.168.6.1   192.168.1.1   FTP        72 Request: QUIT
12064 25.802993   192.168.1.1   192.168.6.1   FTP        80 Response: 221 Goodbye.
```

3. BINARY transmits raw bytes of the file being transferred. Hence the file could be transferred in its exact original form.

4. RETR

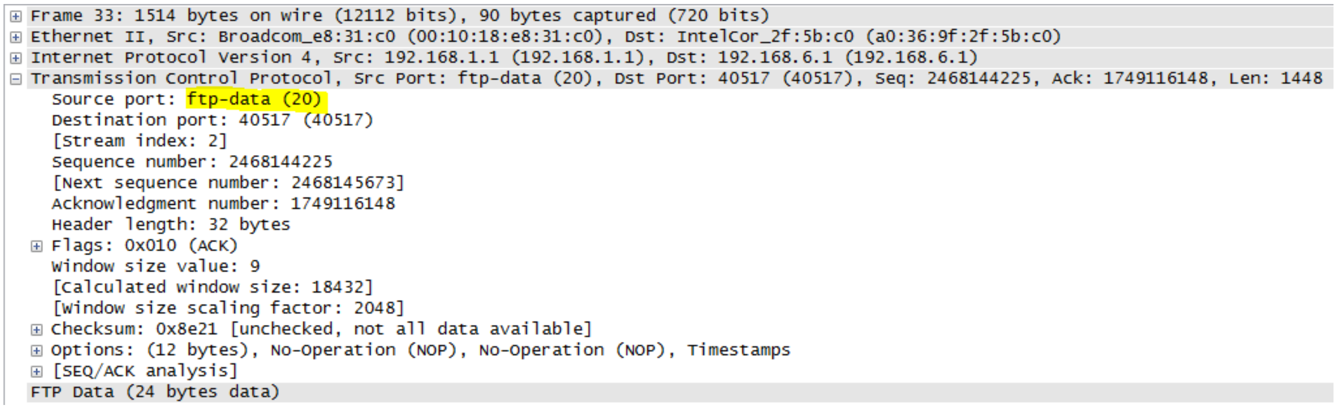


Filter: ftp

```
No.      Time       Source        Destination    Protocol Length Info
    8 5.005920  192.168.1.1   192.168.6.1    FTP        86 Response: 220 (vsFTPd 2.3.5)
   11 5.138017  192.168.6.1   192.168.1.1    FTP        82 Request: USER anonymous
   13 5.138109  192.168.1.1   192.168.6.1    FTP       100 Response: 331 Please specify the p
   15 5.270041  192.168.6.1   192.168.1.1    FTP        73 Request: PASS
   17 5.359893  192.168.1.1   192.168.6.1    FTP        89 Response: 230 Login successful.
   19 5.391356  192.168.6.1   192.168.1.1    FTP        72 Request: SYST
   21 5.391428  192.168.1.1   192.168.6.1    FTP        85 Response: 215 UNIX Type: L8
   23 5.523767  192.168.6.1   192.168.1.1    FTP        74 Request: TYPE I
   24 5.523850  192.168.1.1   192.168.6.1    FTP        97 Response: 200 Switching to Binary
   26 5.555306  192.168.6.1   192.168.1.1    FTP        91 Request: PORT 192,168,6,1,158,69
   27 5.555456  192.168.1.1   192.168.6.1    FTP       117 Response: 200 PORT command success
   28 5.586883  192.168.6.1   192.168.1.1    FTP        83 Request: RETR output.dat
   32 5.618781  192.168.1.1   192.168.6.1    FTP       140 Response: 150 Opening BINARY mode
12059 25.670738 192.168.1.1   192.168.6.1    FTP        90 Response: 226 Transfer complete.
12063 25.802910 192.168.6.1   192.168.1.1    FTP        72 Request: QUIT
12064 25.802993 192.168.1.1   192.168.6.1    FTP        80 Response: 221 Goodbye.
```

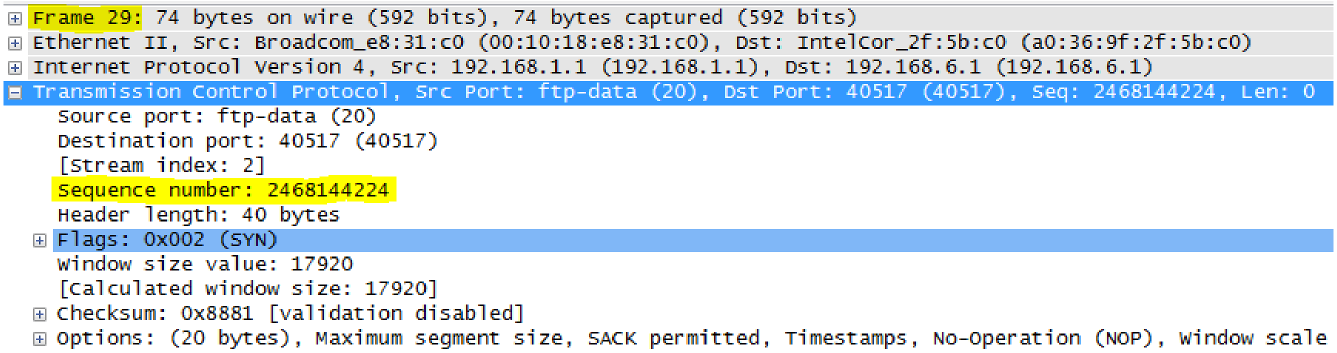
B: Data bytes transmitted by TCP

5a. 20



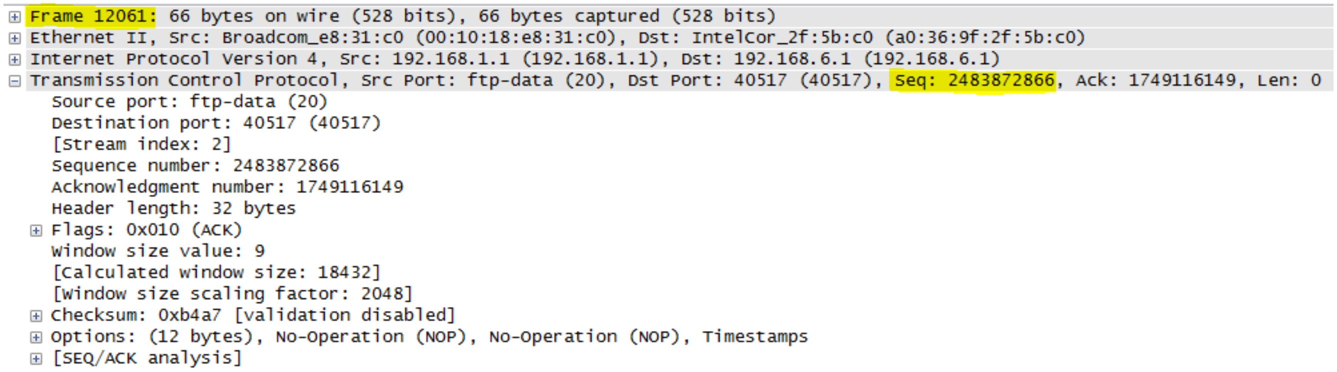
```
⊞ Frame 33: 1514 bytes on wire (12112 bits), 90 bytes captured (720 bits)
⊞ Ethernet II, Src: Broadcom_e8:31:c0 (00:10:18:e8:31:c0), Dst: IntelCor_2f:5b:c0 (a0:36:9f:2f:5b:c0)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.6.1 (192.168.6.1)
⊟ Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 40517 (40517), Seq: 2468144225, Ack: 1749116148, Len: 1448
    Source port: ftp-data (20)
    Destination port: 40517 (40517)
    [Stream index: 2]
    Sequence number: 2468144225
    [Next sequence number: 2468145673]
    Acknowledgment number: 1749116148
    Header length: 32 bytes
  ⊞ Flags: 0x010 (ACK)
    Window size value: 9
    [Calculated window size: 18432]
    [Window size scaling factor: 2048]
  ⊞ Checksum: 0x8e21 [unchecked, not all data available]
  ⊞ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ⊞ [SEQ/ACK analysis]
  FTP Data (24 bytes data)
```

5b. Packet number: 29, Sequence number: 2468144224



```
⊞ Frame 29: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: Broadcom_e8:31:c0 (00:10:18:e8:31:c0), Dst: IntelCor_2f:5b:c0 (a0:36:9f:2f:5b:c0)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.6.1 (192.168.6.1)
⊟ Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 40517 (40517), Seq: 2468144224, Len: 0
    Source port: ftp-data (20)
    Destination port: 40517 (40517)
    [Stream index: 2]
    Sequence number: 2468144224
    Header length: 40 bytes
  ⊞ Flags: 0x002 (SYN)
    Window size value: 17920
    [Calculated window size: 17920]
  ⊞ Checksum: 0x8881 [validation disabled]
  ⊞ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
```

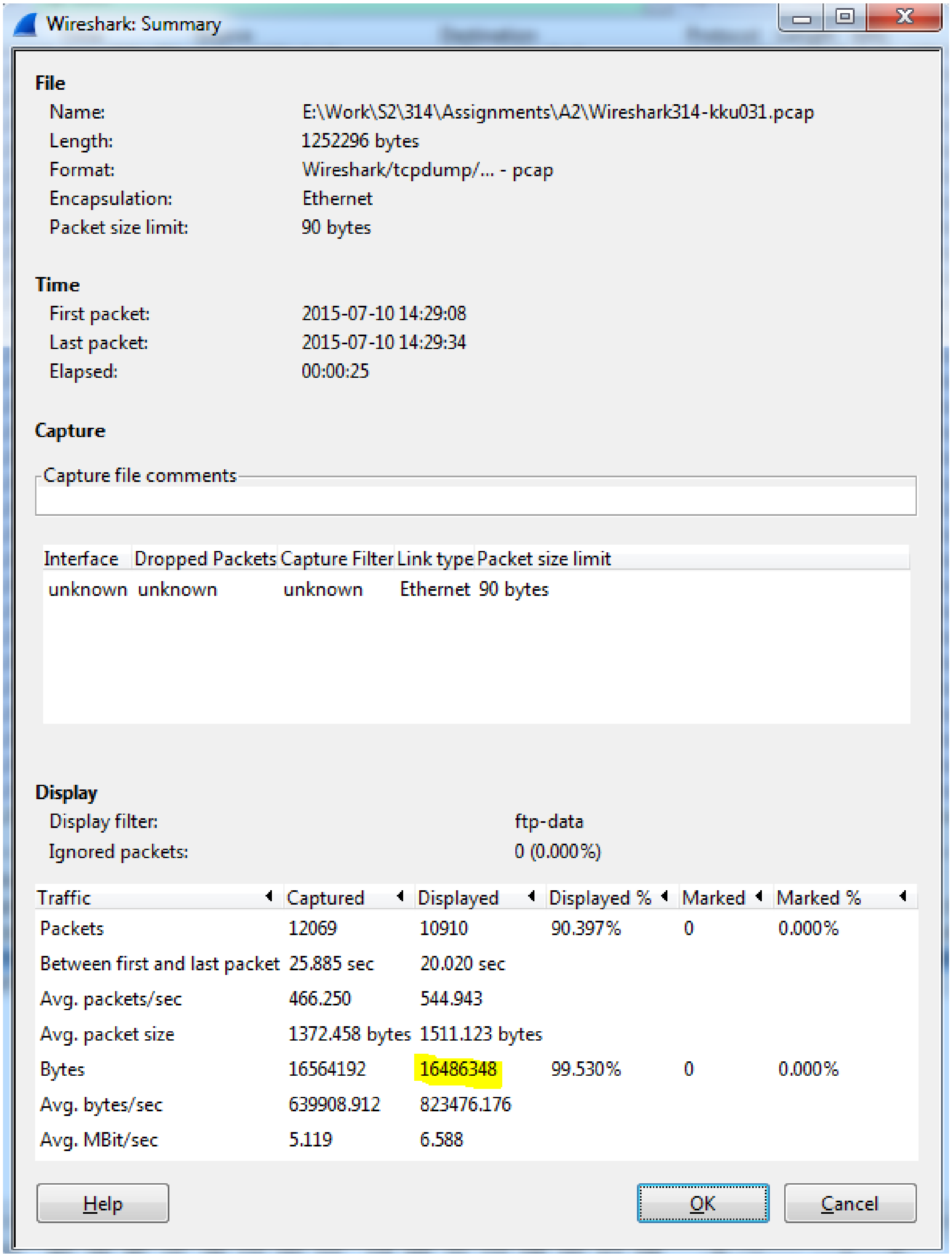
5c. Packet number: 12061, Sequence number: 2483872866



```
⊞ Frame 12061: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
⊞ Ethernet II, Src: Broadcom_e8:31:c0 (00:10:18:e8:31:c0), Dst: IntelCor_2f:5b:c0 (a0:36:9f:2f:5b:c0)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.6.1 (192.168.6.1)
⊟ Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: 40517 (40517), Seq: 2483872866, Ack: 1749116149, Len: 0
    Source port: ftp-data (20)
    Destination port: 40517 (40517)
    [Stream index: 2]
    Sequence number: 2483872866
    Acknowledgment number: 1749116149
    Header length: 32 bytes
  ⊞ Flags: 0x010 (ACK)
    Window size value: 9
    [Calculated window size: 18432]
    [Window size scaling factor: 2048]
  ⊞ Checksum: 0xb4a7 [validation disabled]
  ⊞ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ⊞ [SEQ/ACK analysis]
```

5d. (2483871809 - 2468144225) - 2 = 15727582 bytes

5e. 16486348 bytes



File

Name:	E:\Work\S2\314\Assignments\A2\Wireshark314-kku031.pcap
Length:	1252296 bytes
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Packet size limit:	90 bytes

Time

First packet:	2015-07-10 14:29:08
Last packet:	2015-07-10 14:29:34
Elapsed:	00:00:25

Capture

Capture file comments

Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	90 bytes

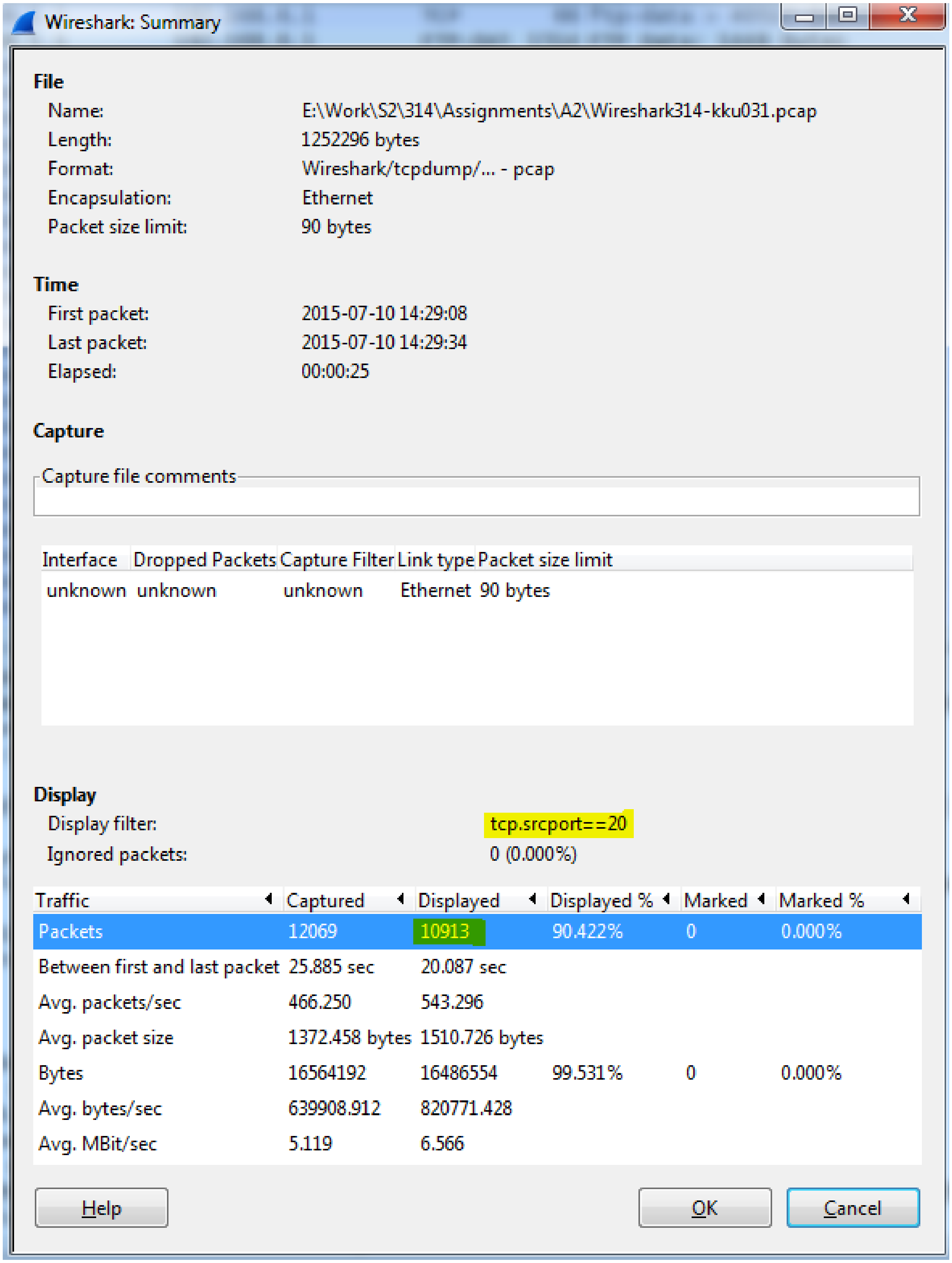
Display

Display filter:	ftp-data
Ignored packets:	0 (0.000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	12069	10910	90.397%	0	0.000%
Between first and last packet	25.885 sec	20.020 sec			
Avg. packets/sec	466.250	544.943			
Avg. packet size	1372.458 bytes	1511.123 bytes			
Bytes	16564192	16486348	99.530%	0	0.000%
Avg. bytes/sec	639908.912	823476.176			
Avg. MBit/sec	5.119	6.588			

C: Packets retransmitted by TCP

6a. 10913



File

Name: E:\Work\S2\314\Assignments\A2\Wireshark314-kku031.pcap
Length: 1252296 bytes
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Packet size limit: 90 bytes

Time

First packet: 2015-07-10 14:29:08
Last packet: 2015-07-10 14:29:34
Elapsed: 00:00:25

Capture

Capture file comments

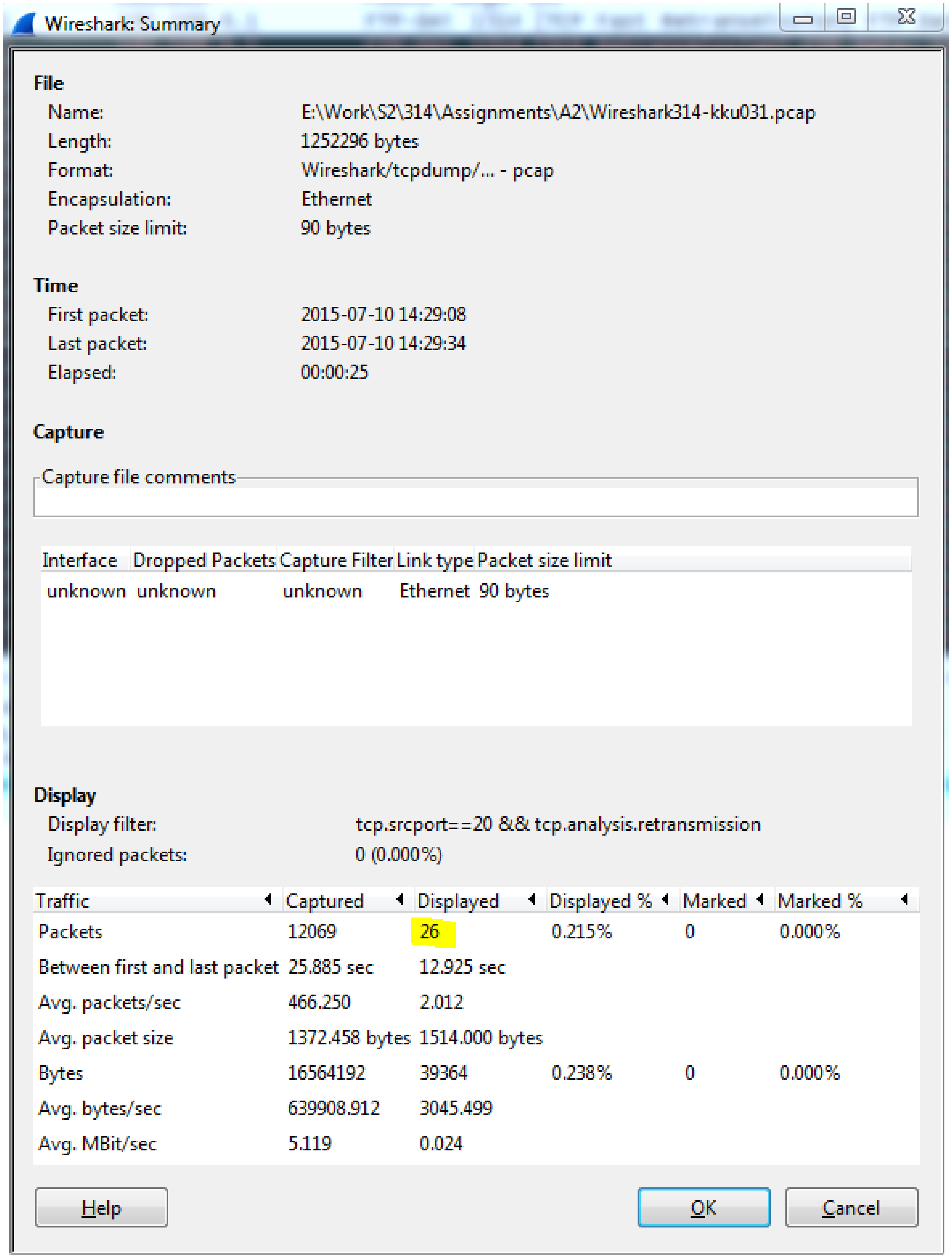
Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	90 bytes

Display

Display filter: tcp.srcport==20
Ignored packets: 0 (0.000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	12069	10913	90.422%	0	0.000%
Between first and last packet	25.885 sec	20.087 sec			
Avg. packets/sec	466.250	543.296			
Avg. packet size	1372.458 bytes	1510.726 bytes			
Bytes	16564192	16486554	99.531%	0	0.000%
Avg. bytes/sec	639908.912	820771.428			
Avg. MBit/sec	5.119	6.566			

6b. 26



Wireshark: Summary

File

Name:	E:\Work\S2\314\Assignments\A2\Wireshark314-kku031.pcap
Length:	1252296 bytes
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Packet size limit:	90 bytes

Time

First packet:	2015-07-10 14:29:08
Last packet:	2015-07-10 14:29:34
Elapsed:	00:00:25

Capture

Capture file comments

Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	90 bytes

Display

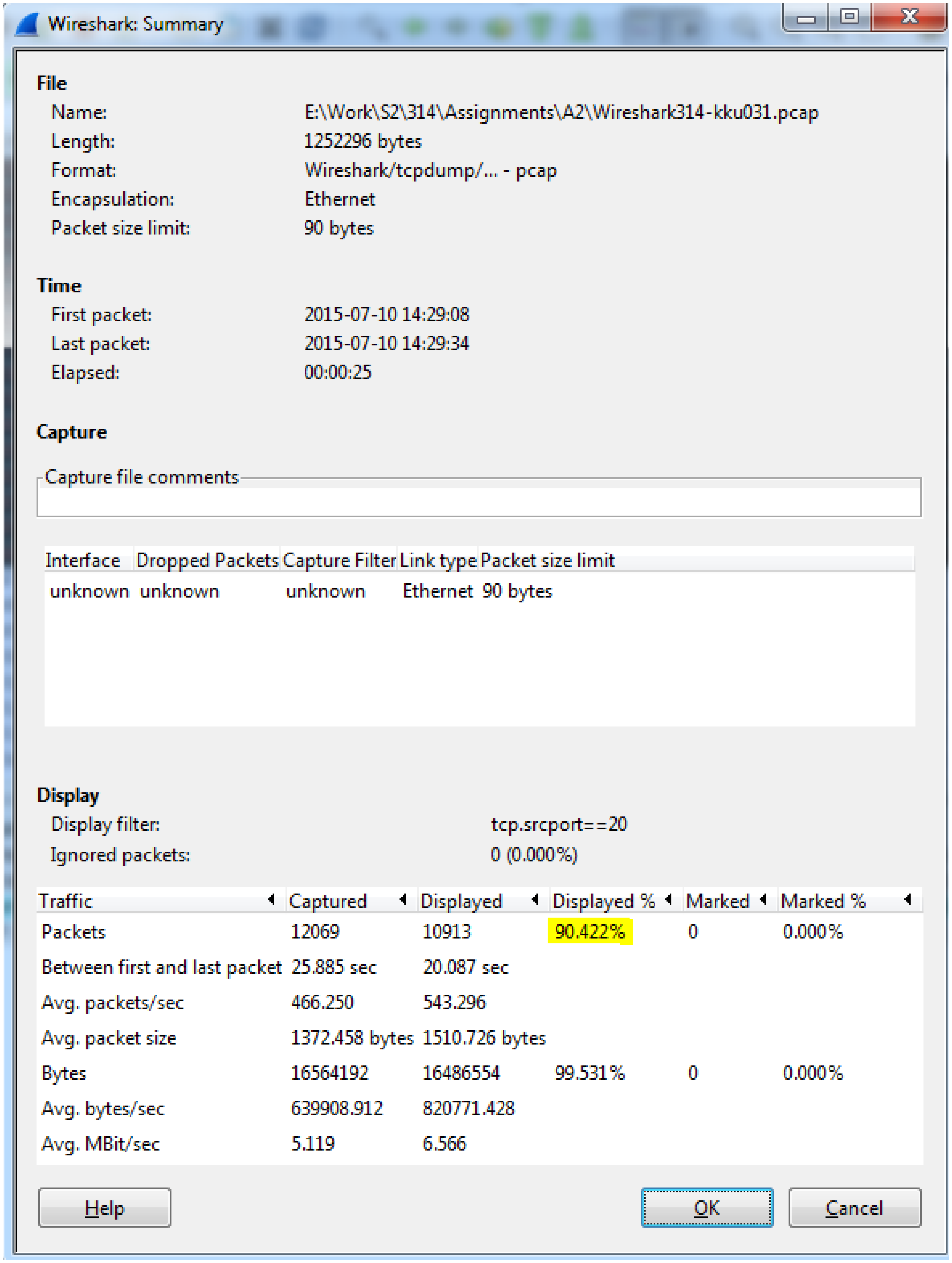
Display filter:	tcp.srcport==20 && tcp.analysis.retransmission
Ignored packets:	0 (0.000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	12069	26	0.215%	0	0.000%
Between first and last packet	25.885 sec	12.925 sec			
Avg. packets/sec	466.250	2.012			
Avg. packet size	1372.458 bytes	1514.000 bytes			
Bytes	16564192	39364	0.238%	0	0.000%
Avg. bytes/sec	639908.912	3045.499			
Avg. MBit/sec	5.119	0.024			

6c. Regardless of the sequence and acknowledge numbers, dropping/blocking packets are not possible in Wireshark. Instead, it shows/decodes any packet which is captured. Wireshark does not consider using checksum or IP id in recognising a packet retransmission.

It recognises a packet retransmission with a comparison that shows the difference between the sequence numbers and the expected sequence number from the last packet of the conversation into the same direction. The arrangement is placed by packet order.

6d.



File

Name:	E:\Work\S2\314\Assignments\A2\Wireshark314-kku031.pcap
Length:	1252296 bytes
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Packet size limit:	90 bytes

Time

First packet:	2015-07-10 14:29:08
Last packet:	2015-07-10 14:29:34
Elapsed:	00:00:25

Capture

Capture file comments

Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	90 bytes

Display

Display filter:	tcp.srcport==20
Ignored packets:	0 (0.000%)

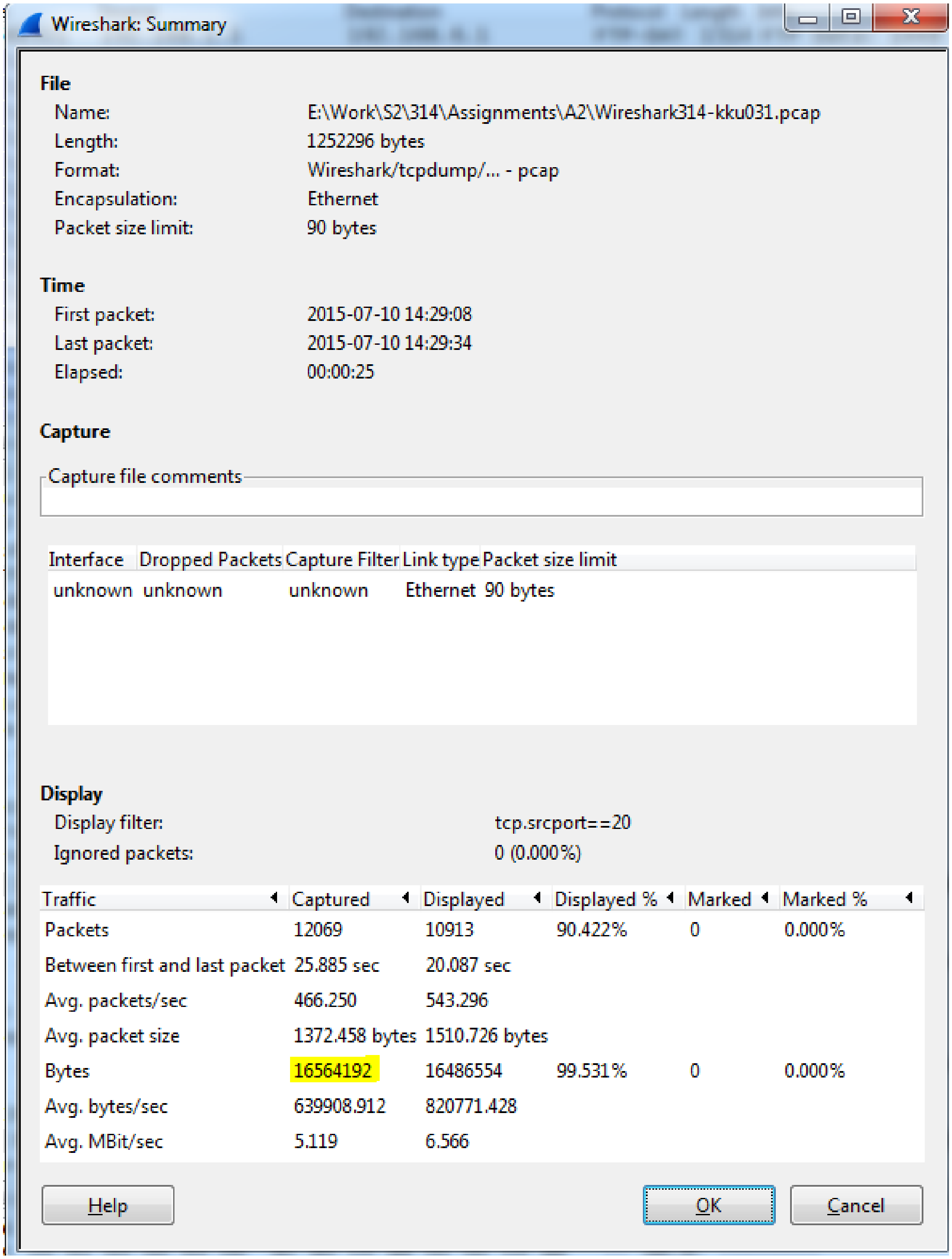
Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	12069	10913	90.422%	0	0.000%
Between first and last packet	25.885 sec	20.087 sec			
Avg. packets/sec	466.250	543.296			
Avg. packet size	1372.458 bytes	1510.726 bytes			
Bytes	16564192	16486554	99.531%	0	0.000%
Avg. bytes/sec	639908.912	820771.428			
Avg. MBit/sec	5.119	6.566			

90.422% is the percentage of the displayed packet. Therefore the observed packet loss percentage for this trace file would be:

100% - 90.422% = **9.578%**

D: Protocol overhead

7a. 16564192 bytes



File

Name: E:\Work\S2\314\Assignments\A2\Wireshark314-kku031.pcap
Length: 1252296 bytes
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Packet size limit: 90 bytes

Time

First packet: 2015-07-10 14:29:08
Last packet: 2015-07-10 14:29:34
Elapsed: 00:00:25

Capture

Capture file comments

Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	90 bytes

Display

Display filter: tcp.srcport==20
Ignored packets: 0 (0.000%)

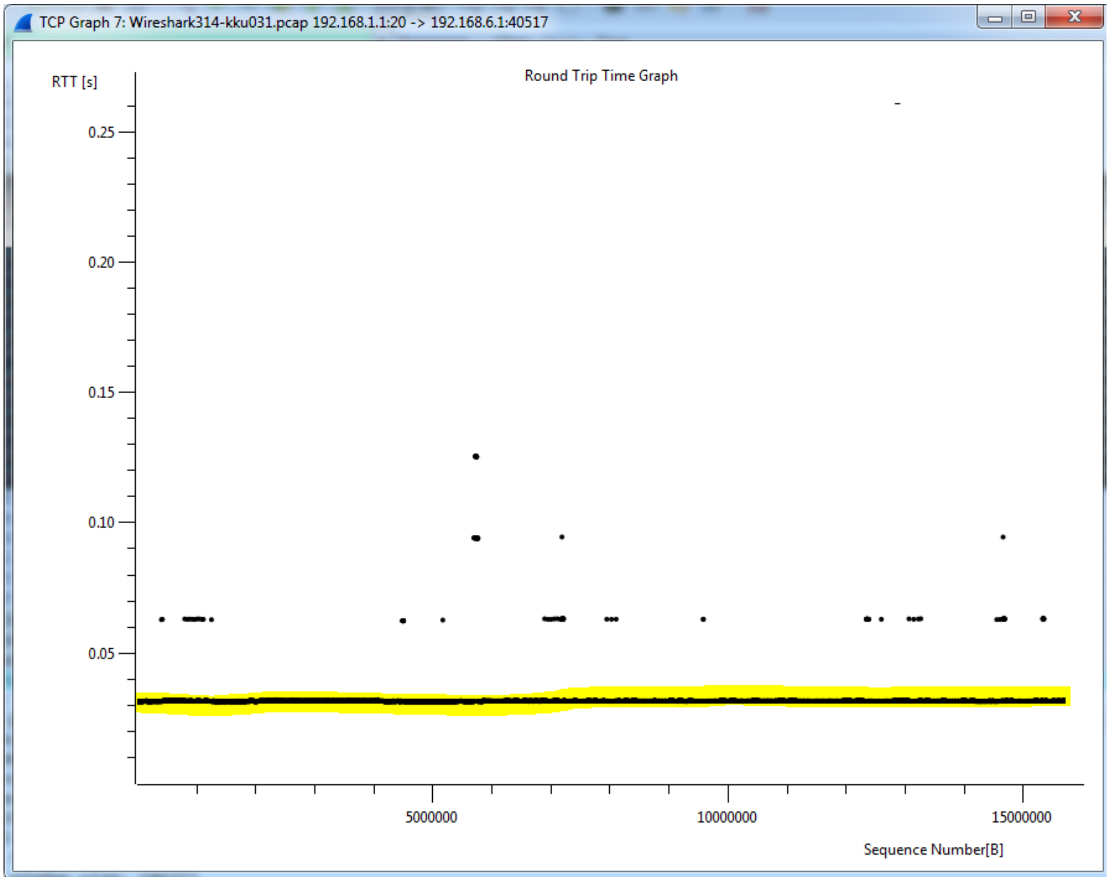
Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	12069	10913	90.422%	0	0.000%
Between first and last packet	25.885 sec	20.087 sec			
Avg. packets/sec	466.250	543.296			
Avg. packet size	1372.458 bytes	1510.726 bytes			
Bytes	16564192	16486554	99.531%	0	0.000%
Avg. bytes/sec	639908.912	820771.428			
Avg. MBit/sec	5.119	6.566			

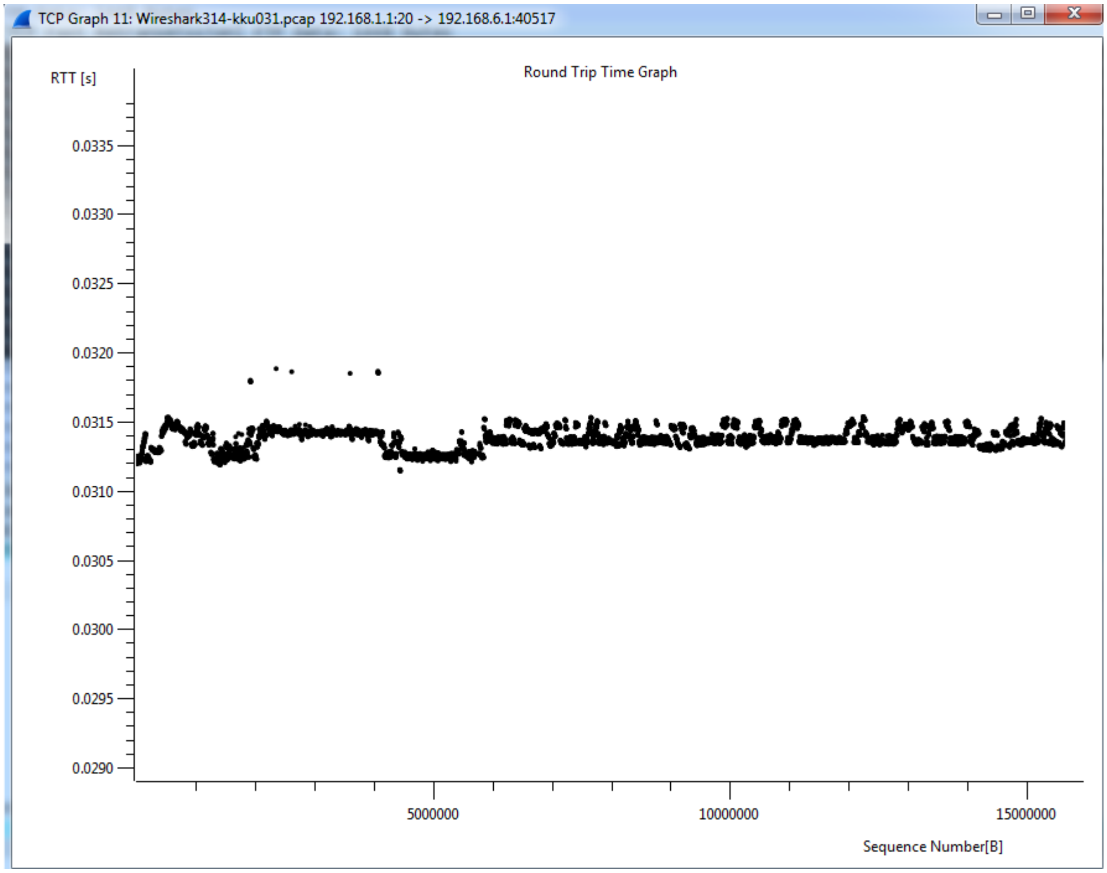
7b. In this case, 66 bytes is the overhead for a TCP packet. There are 10913 packets in total, hence 66 * 10913 = 720258.

720258 bytes is the total overhead, therefore 720258/16486554*100 = **4.37%** (2dp) gives the percentage of “protocol overhead” for this file transfer.

7c. Overhead is everything except the actual data. Frame length is 1514 bytes whereas actual data is 1448 bytes. This gives a leftover of 66 bytes, the overhead. Out of 66 bytes, 32 bytes is from by the TCP header length, 20 bytes is from the IP header length and the rest of it is from the Ethernet layer.

E: Round-trip time





According to the Round Trip Time graphs (screen shots) above, the most common RTT for packets is 0.0313s = 31.3ms (3 sf)