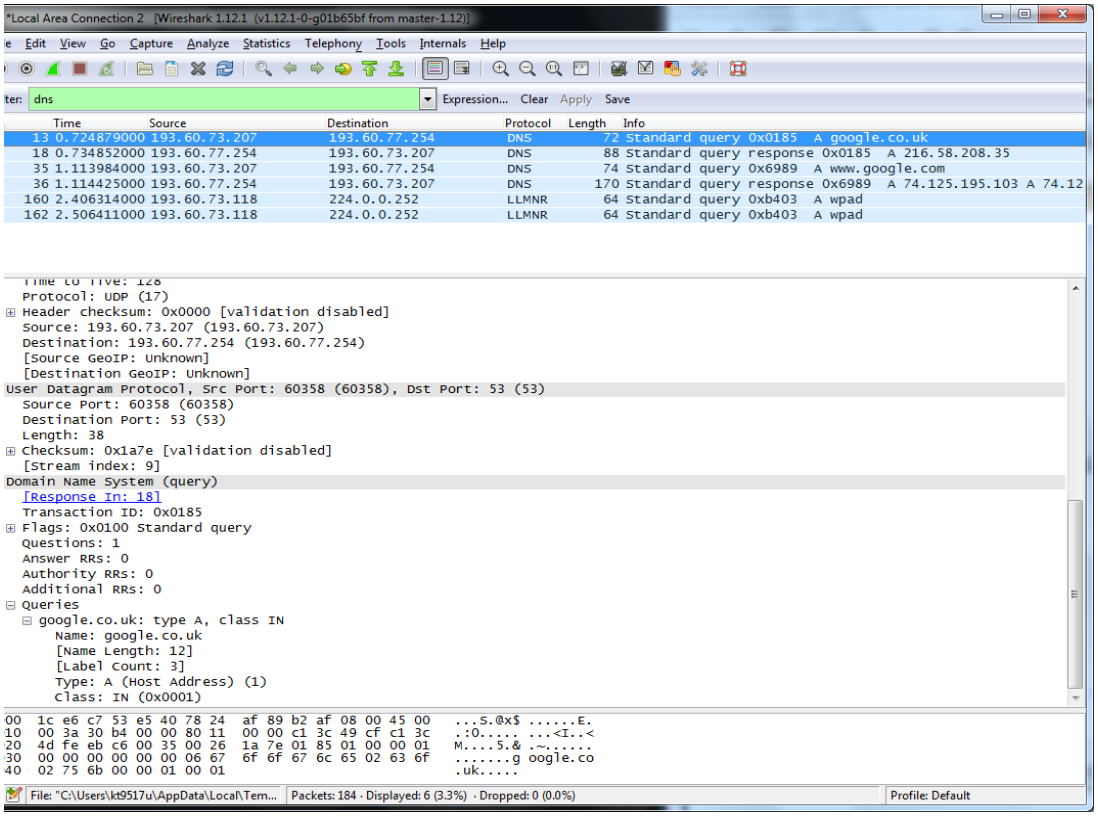
Packet Sniffing - Marking Scheme

	Registration Number	Surname	Forename	% Contribution
Student 1	000839875	Turon	Kacper	25
Student 2	000874782	Basharat	Usman	25
Student 3	000878481	Kallon	Kevin	25
Student 4	000871936	Young	Jack	25

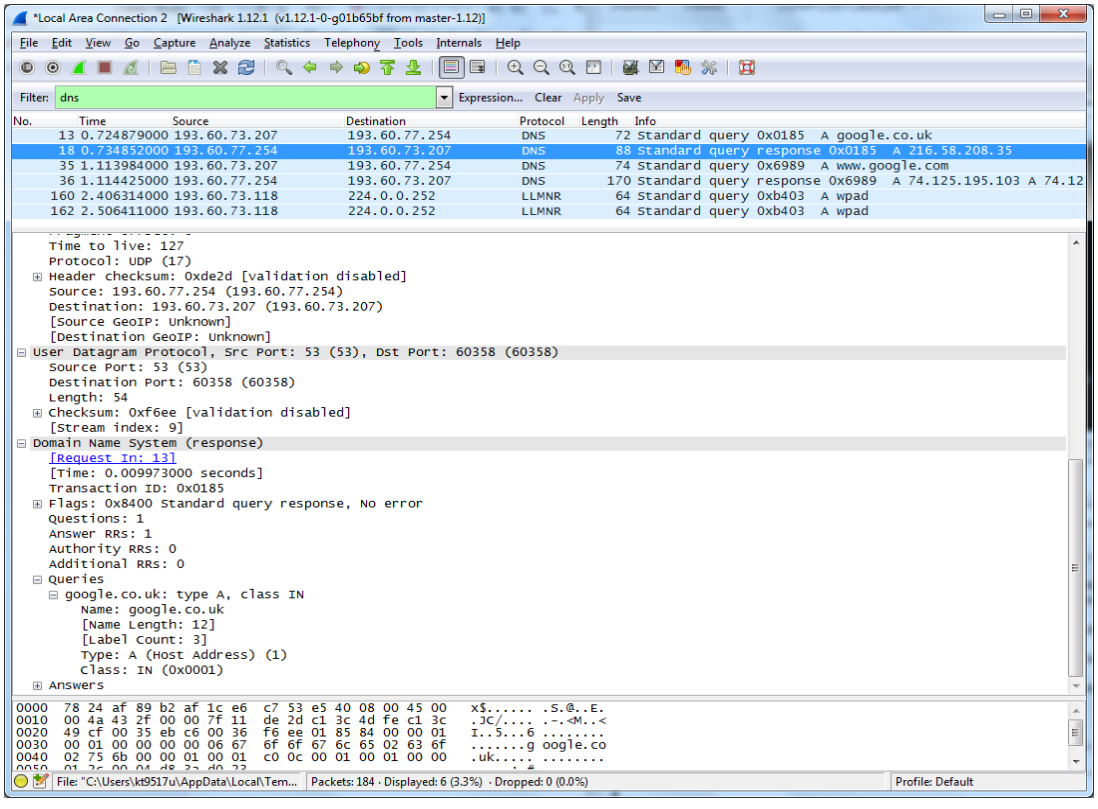
Task	Mark	Grade
Task 1 - Capture a HTTP Request Sequence	40	
Task 2 - Capture a Chat Session	30	
Task 3 - Capture an FTP Session	30	
Total	100	

Packet Sniffing

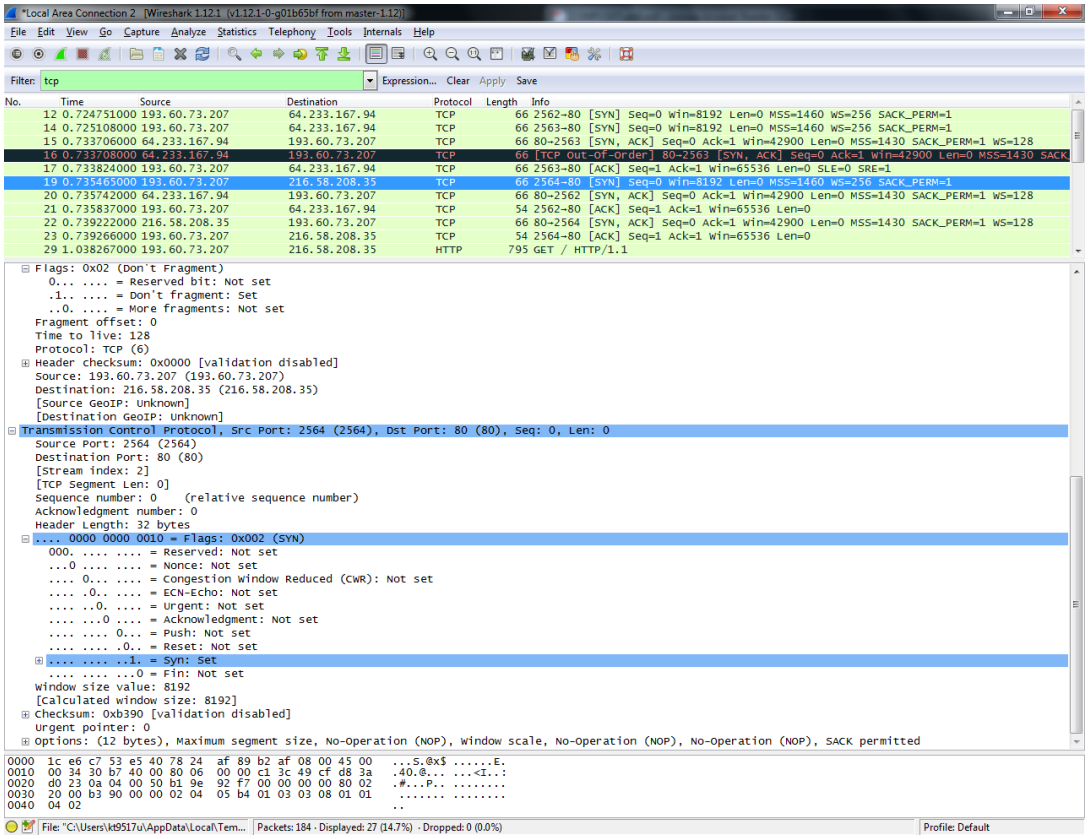
Task 1



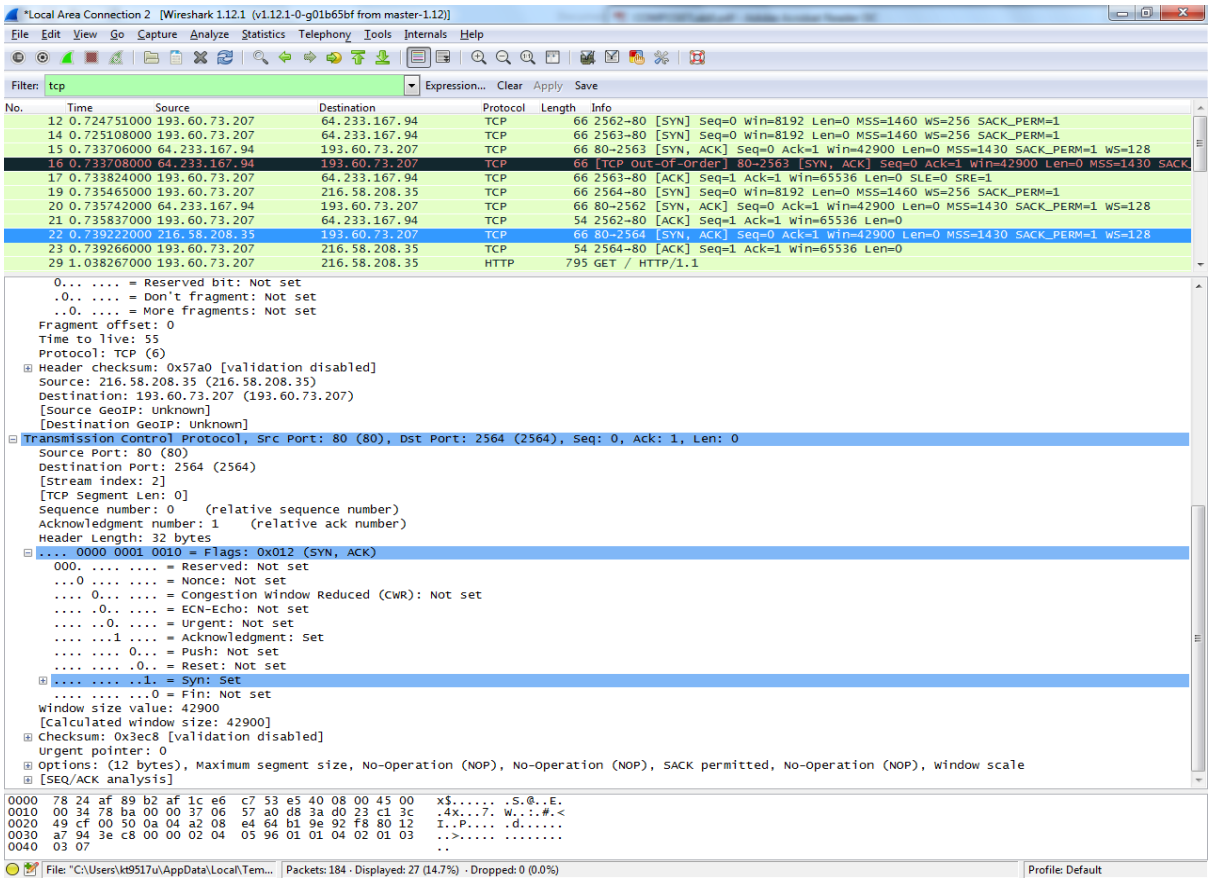
DNS request for the IP address that corresponds to the URL



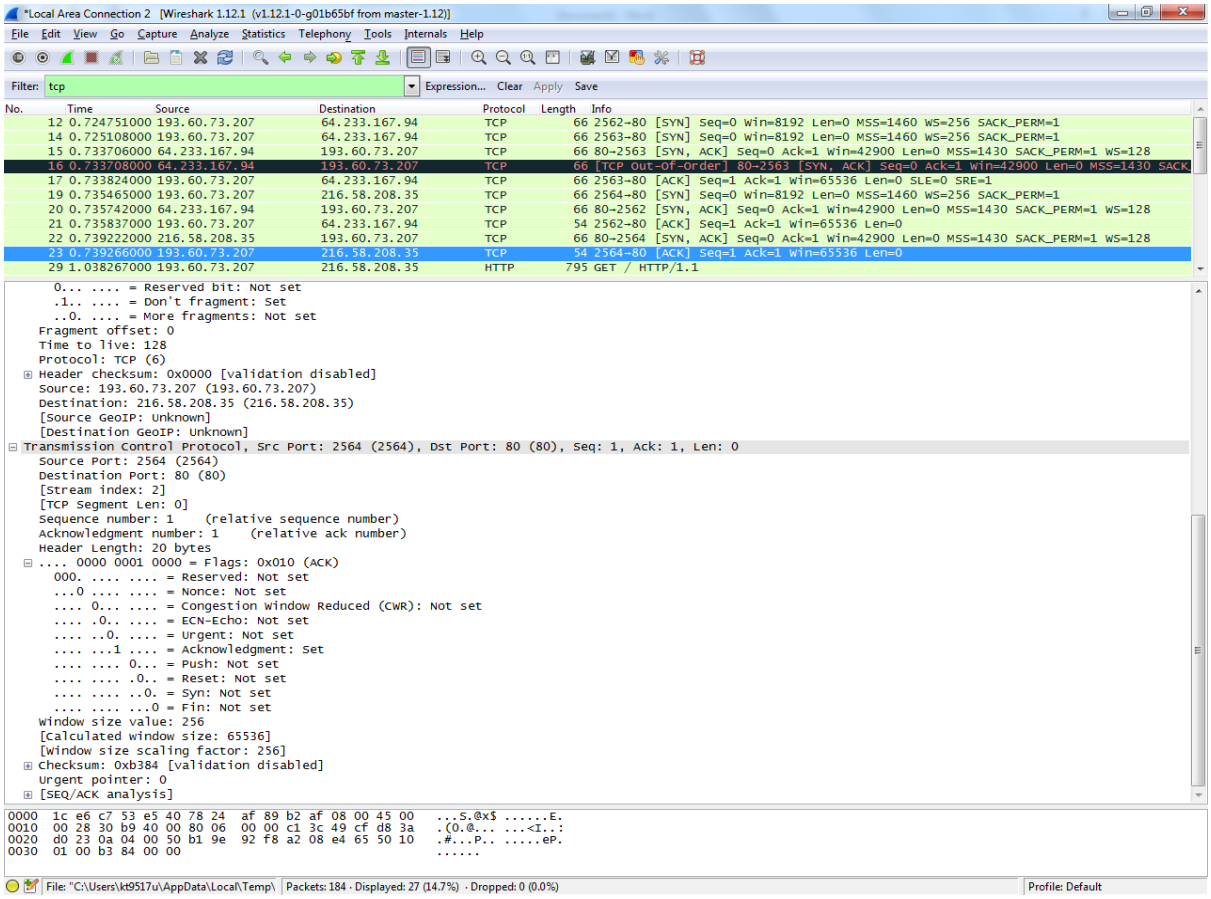
DNS response returned with the IP address clearly seen



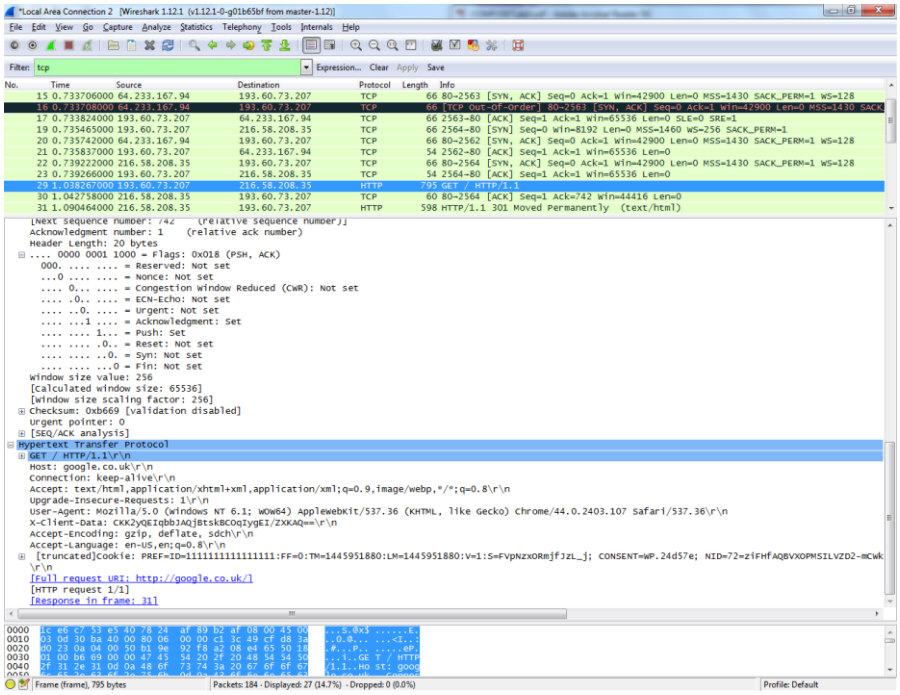
HTTP – TCP starting the 3-way handshake (SYN bit =1) – note sequence numbers



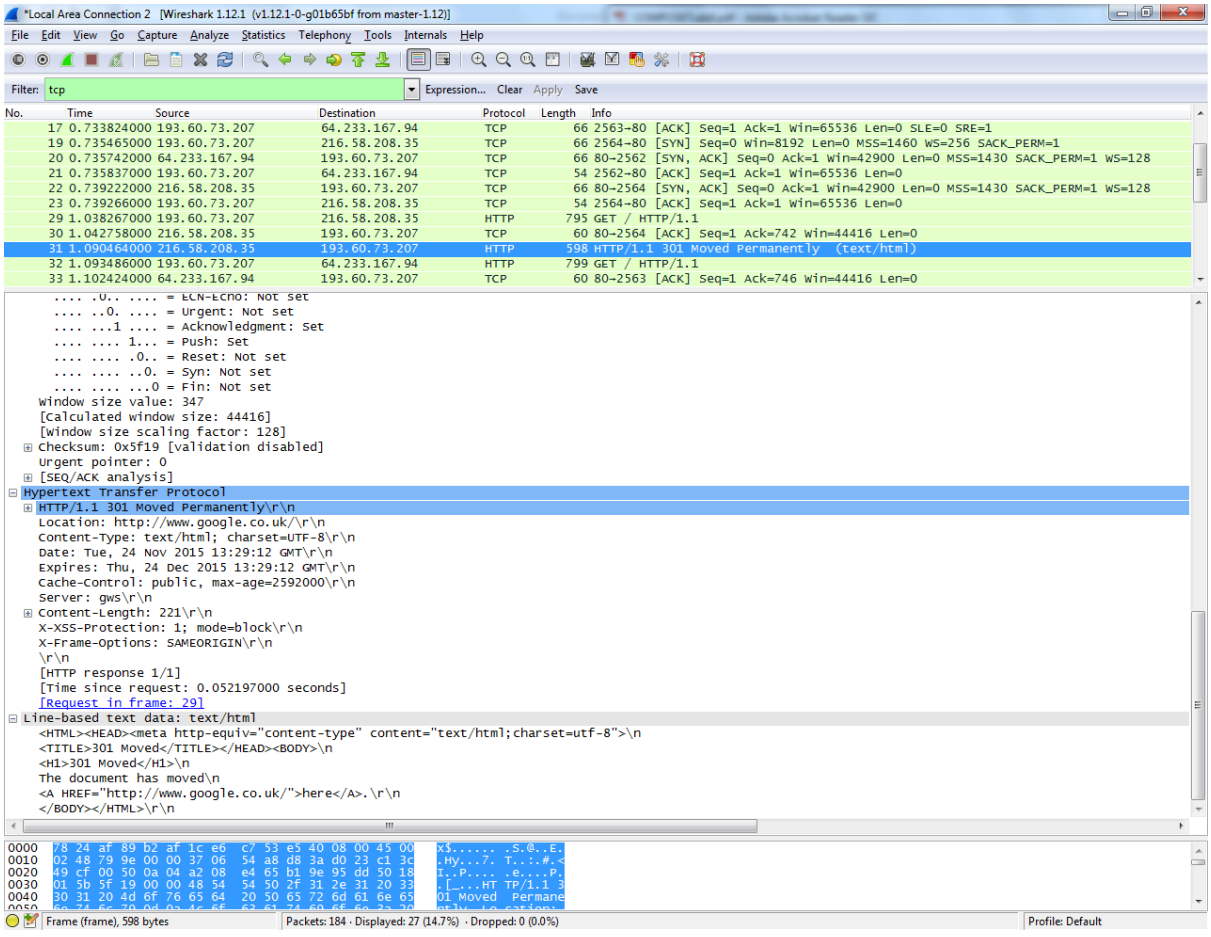
HTTP – TCP response from server (port 80) (SYN bit =1, ACK bit = 1)



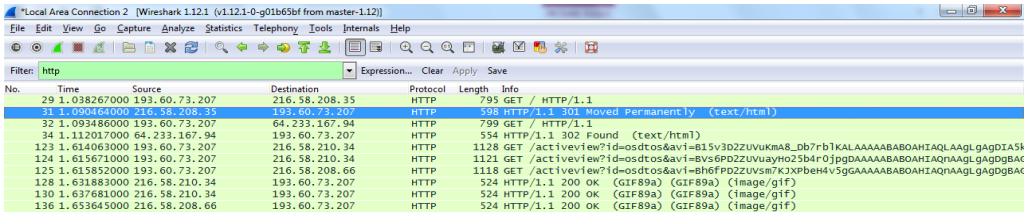
HTTP – TCP acknowledgement to the server (ACK bit =1) – look at seq numbers again now browser starts to request web pages

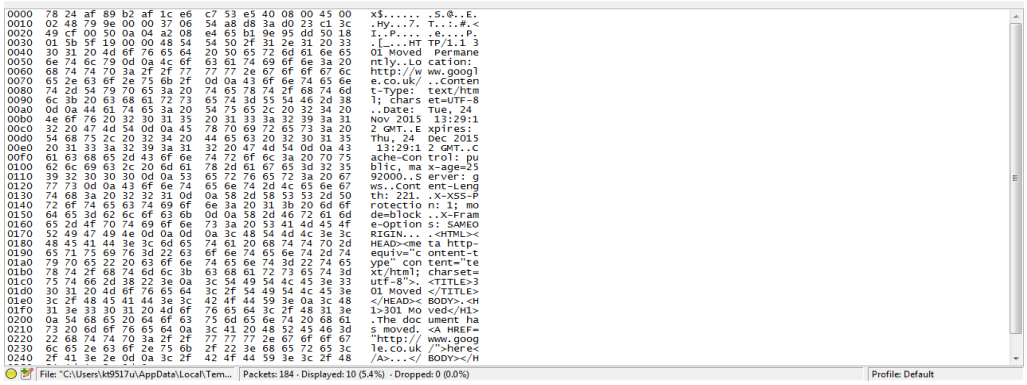


HTTP GET - which the request to retrieve the web page



HTTP returned with data – this will be the header for the web page





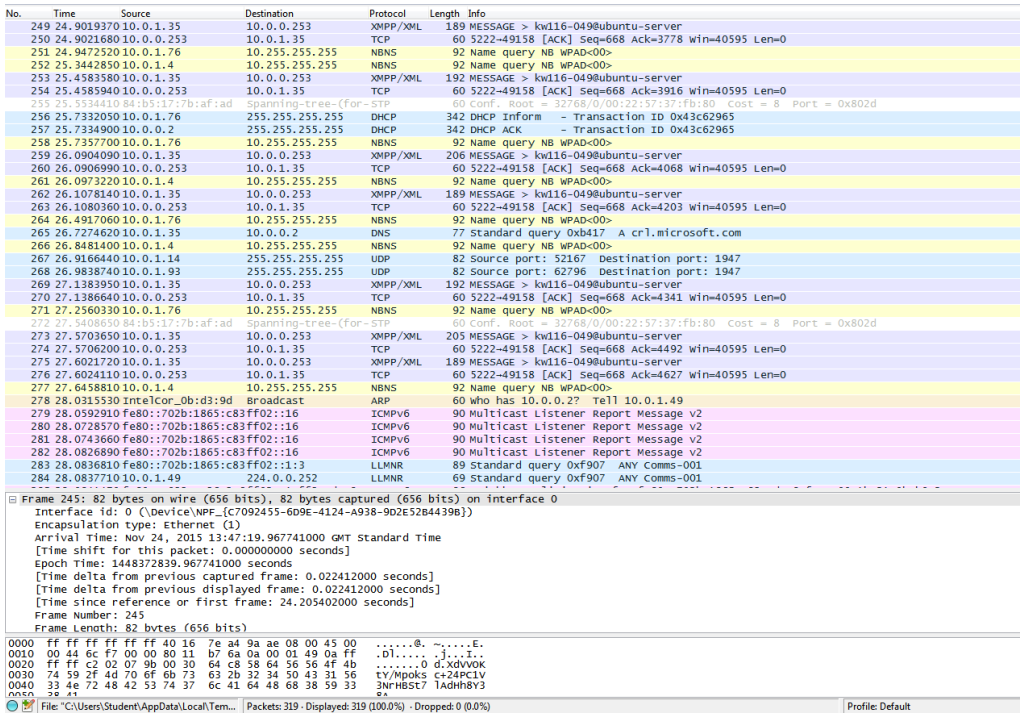
HTTP data packets each with Hyper Text Mark Up Language (HTML) code in it – the data to display the Web page

Task 2

Protocols found

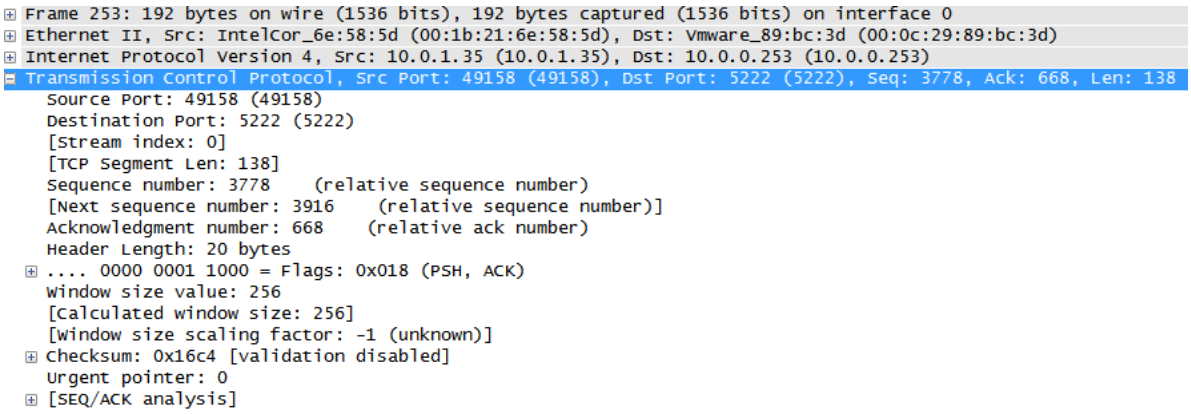
A) List different protocols captured

- NBNS
- ARP
- DNS
- LLMNR
- XMPP/XML
- TCP
- ARP
- LOOP
- UDP
- DHCPv6
- BROWSER
- ICMP
- DHCP
- ICMPv6
- SSDP



B) What is the protocol that delivers the chat packet?
XMPP/XML

C) What ports are involved in the chat messaging?
Src port: 49158 DST port: 5222



D) What else can you find out about the chat protocol?
MESSAGE [id=”purple3cad42c5” type=”chat” chatstate=”composing”]
Id: purple3cad42c5
To:kw116-049@ubuntu-server
Type: chat
CHATSTATE: composing

```
XMPP Protocol
  MESSAGE [id="purple3cad42c5" type="chat" chatstate="composing"]
      id: purple3cad42c5
      to: kw116-049@ubuntu-server
      type: chat
      CHATSTATE: composing
```

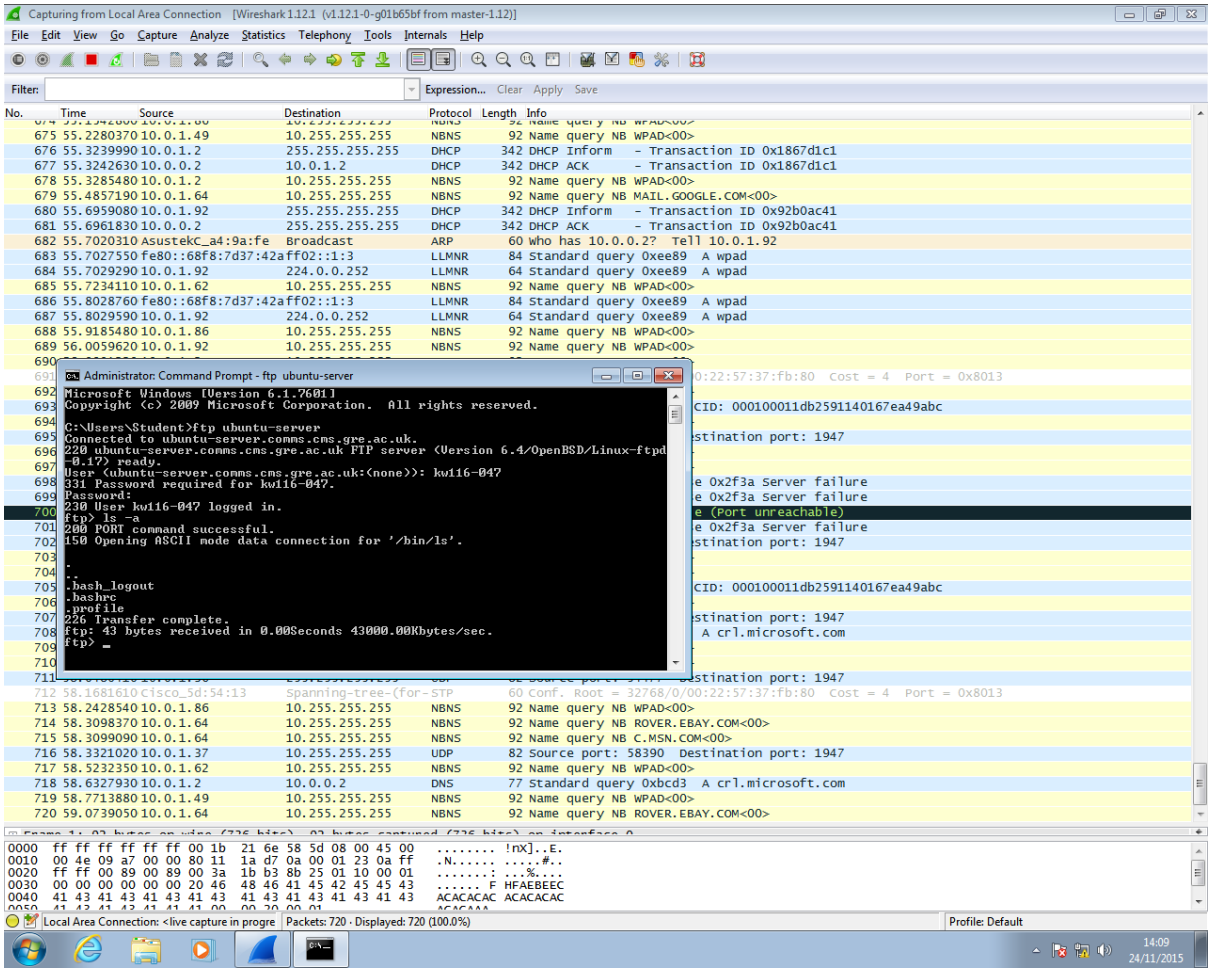
E) Why is the source IP address always the same regardless of which buddy you are chatting with?

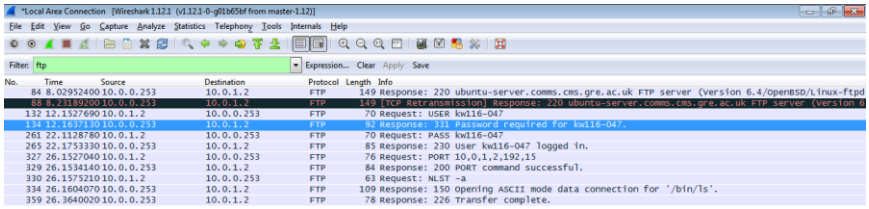
The message is being transmitted from the same computer regardless of which user it is being sent to.

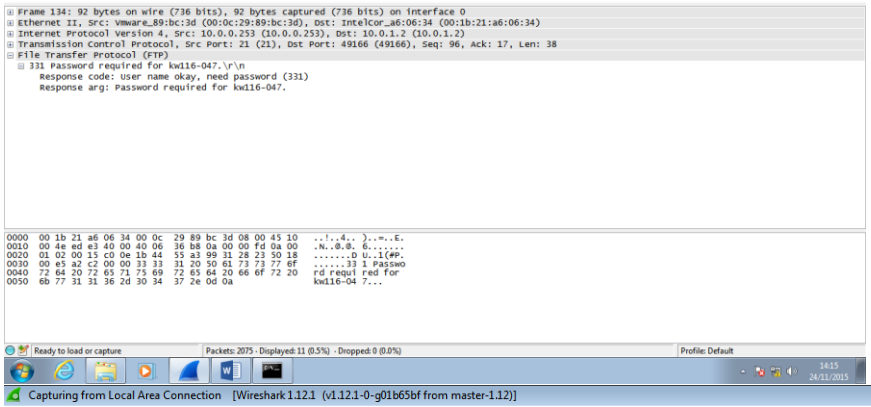
F) Open one of your captured packets by double clicking on it and open the jabber part of the packet. What is the chat message?

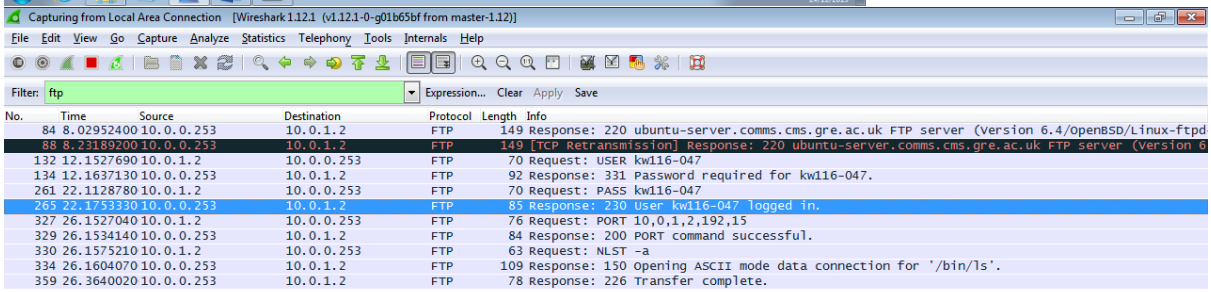
The message received was, “I’m not here right now”

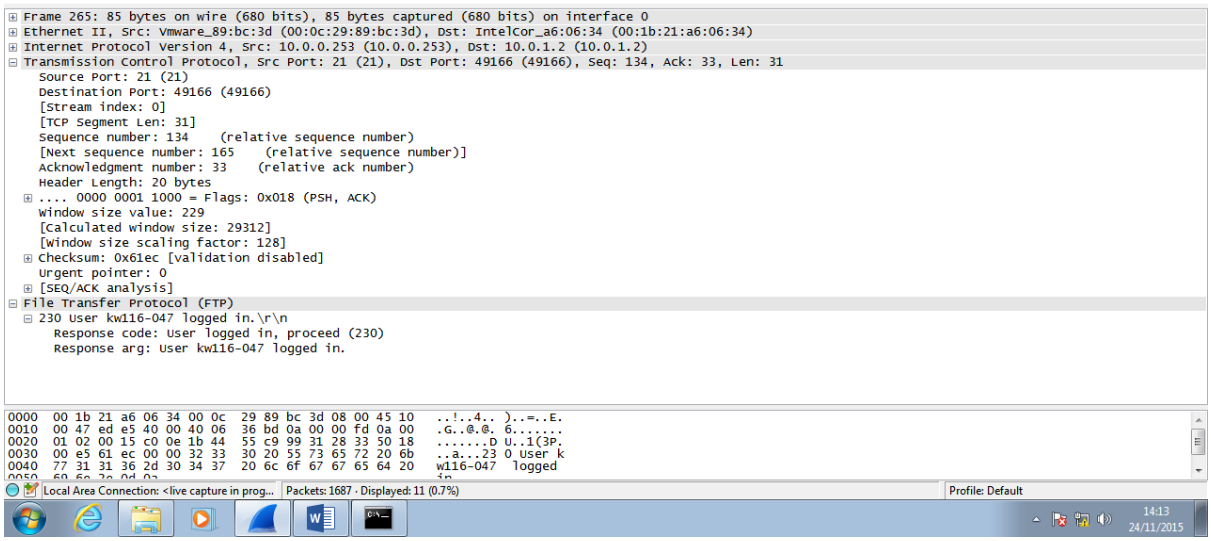
Task 3

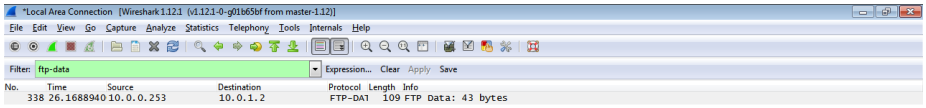


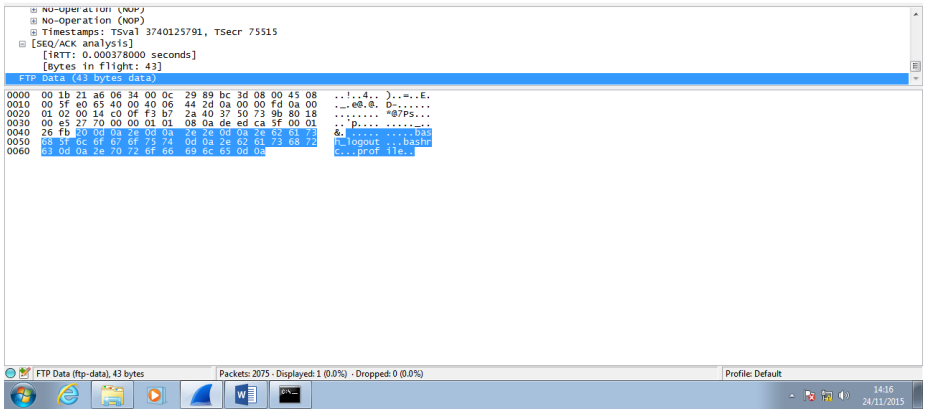

*Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ftp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
84 8.02952400 10.0.0.253 10.0.1.2 FTP 149 Response: 220 ubuntu-server.comms.cms.gre.ac.uk FTP server (Version 6.4/OpenBSD/Linux-ftpd
88 8.23189200 10.0.0.253 10.0.1.2 FTP 149 [TCP Retransmission] Response: 220 ubuntu-server.comms.cms.gre.ac.uk FTP server (Version 6
132 12.1527690 10.0.1.2 10.0.0.253 FTP 70 Request: USER kw116-047
134 12.1637130 10.0.0.253 10.0.1.2 FTP 92 Response: 331 Password required for kw116-047.
261 22.1128780 10.0.1.2 10.0.0.253 FTP 70 Request: PASS kw116-047
265 22.1753330 10.0.0.253 10.0.1.2 FTP 85 Response: 230 User kw116-047 logged in.
327 26.1527040 10.0.1.2 10.0.0.253 FTP 76 Request: PORT 10,0,1,2,192,15
329 26.1534140 10.0.0.253 10.0.1.2 FTP 84 Response: 200 PORT command successful.
330 26.1575210 10.0.1.2 10.0.0.253 FTP 63 Request: NLST -a
334 26.1604070 10.0.0.253 10.0.1.2 FTP 109 Response: 150 Opening ASCII mode data connection for '/bin/ls'.
359 26.3640020 10.0.0.253 10.0.1.2 FTP 78 Response: 226 Transfer complete.

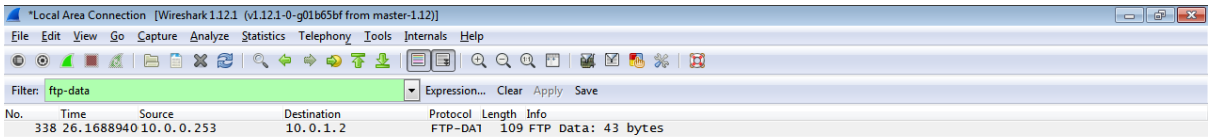

Frame 134: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
Ethernet II, Src: Vmware_89:bc:3d (00:0c:29:89:bc:3d), Dst: IntelCor_a6:06:34 (00:1b:21:a6:06:34)
Internet Protocol Version 4, Src: 10.0.0.253 (10.0.0.253), Dst: 10.0.1.2 (10.0.1.2)
Transmission Control Protocol, Src Port: 21 (21), Dst Port: 49166 (49166), Seq: 96, Ack: 17, Len: 38
File Transfer Protocol (FTP)
331 Password required for kw116-047.\r\n
Response code: User name okay, need password (331)
Response arg: Password required for kw116-047.
0000 00 1b 21 a6 06 34 00 0c 29 89 bc 3d 08 00 45 10 ..!..4..)..=..E.
0010 00 4e ed e3 40 00 40 06 36 b8 0a 00 00 fd 0a 00 .N..@.@. 6.......
0020 01 02 00 15 c0 0e 1b 44 55 a3 99 31 28 23 50 18 ....D U..1(#P.
0030 00 e5 a2 c2 00 00 33 33 31 20 50 61 73 73 77 6f ......33 1 Passwo
0040 72 64 20 72 65 71 75 69 72 65 64 20 66 6f 72 20 rd requi red for
0050 6b 77 31 31 36 2d 30 34 37 2e 0d 0a kw116-04 7...
Ready to load or capture
Packets: 2075 · Displayed: 11 (0.5%) · Dropped: 0 (0.0%)
Profile: Default

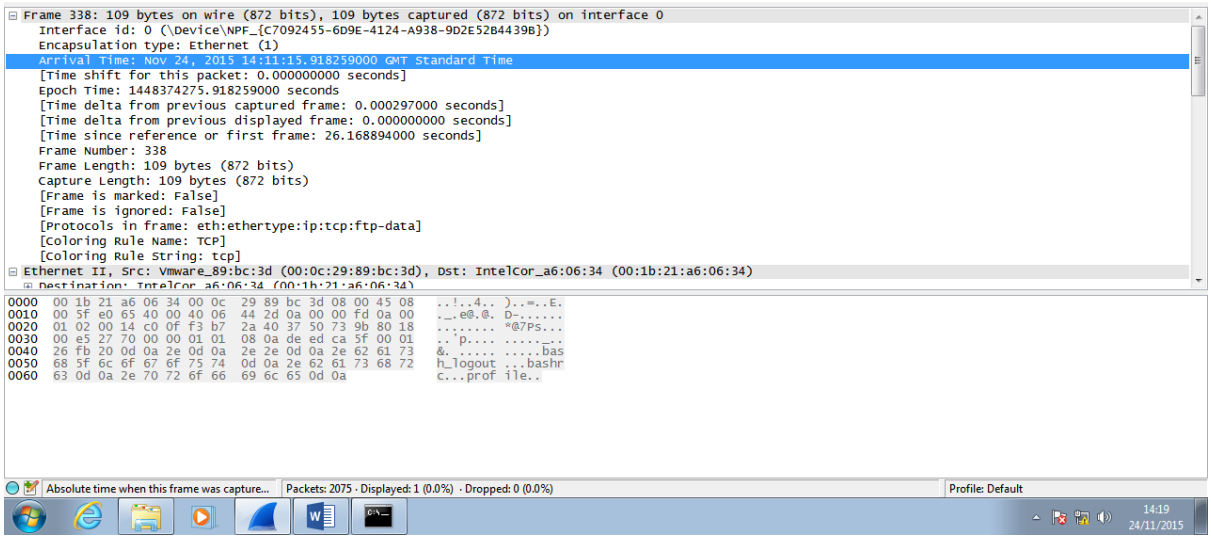

Capturing from Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ftp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
84 8.02952400 10.0.0.253 10.0.1.2 FTP 149 Response: 220 ubuntu-server.comms.cms.gre.ac.uk FTP server (Version 6.4/OpenBSD/Linux-ftpd
88 8.23189200 10.0.0.253 10.0.1.2 FTP 149 [TCP Retransmission] Response: 220 ubuntu-server.comms.cms.gre.ac.uk FTP server (Version 6
132 12.1527690 10.0.1.2 10.0.0.253 FTP 70 Request: USER kw116-047
134 12.1637130 10.0.0.253 10.0.1.2 FTP 92 Response: 331 Password required for kw116-047.
261 22.1128780 10.0.1.2 10.0.0.253 FTP 70 Request: PASS kw116-047
265 22.1753330 10.0.0.253 10.0.1.2 FTP 85 Response: 230 User kw116-047 logged in.
327 26.1527040 10.0.1.2 10.0.0.253 FTP 76 Request: PORT 10,0,1,2,192,15
329 26.1534140 10.0.0.253 10.0.1.2 FTP 84 Response: 200 PORT command successful.
330 26.1575210 10.0.1.2 10.0.0.253 FTP 63 Request: NLST -a
334 26.1604070 10.0.0.253 10.0.1.2 FTP 109 Response: 150 Opening ASCII mode data connection for '/bin/ls'.
359 26.3640020 10.0.0.253 10.0.1.2 FTP 78 Response: 226 Transfer complete.

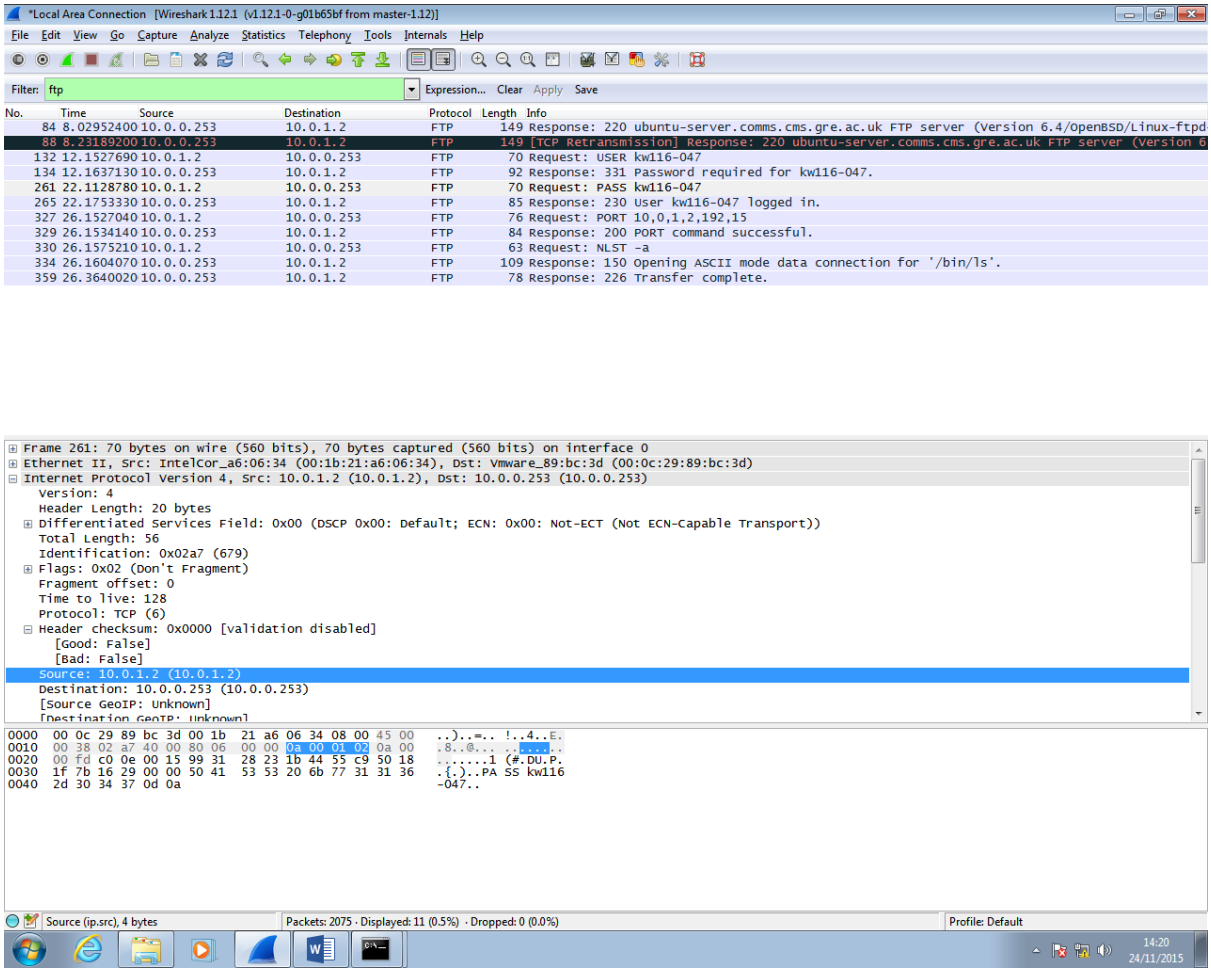

Frame 265: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
Ethernet II, Src: Vmware_89:bc:3d (00:0c:29:89:bc:3d), Dst: IntelCor_a6:06:34 (00:1b:21:a6:06:34)
Internet Protocol Version 4, Src: 10.0.0.253 (10.0.0.253), Dst: 10.0.1.2 (10.0.1.2)
Transmission Control Protocol, Src Port: 21 (21), Dst Port: 49166 (49166), Seq: 134, Ack: 33, Len: 31
Source Port: 21 (21)
Destination Port: 49166 (49166)
[Stream index: 0]
[TCP Segment Len: 31]
Sequence number: 134 (relative sequence number)
[Next sequence number: 165 (relative sequence number)]
Acknowledgment number: 33 (relative ack number)
Header Length: 20 bytes
.... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
Window size value: 229
[Calculated window size: 29312]
[Window size scaling factor: 128]
Checksum: 0x61ec [validation disabled]
Urgent pointer: 0
[SEQ/ACK analysis]
File Transfer Protocol (FTP)
230 User kw116-047 logged in.\r\n
Response code: User logged in, proceed (230)
Response arg: User kw116-047 logged in.
0000 00 1b 21 a6 06 34 00 0c 29 89 bc 3d 08 00 45 10 ..!..4..)..=..E.
0010 00 47 ed e5 40 00 40 06 36 bd 0a 00 00 fd 0a 00 .G..@.@. 6.......
0020 01 02 00 15 c0 0e 1b 44 55 c9 99 31 28 33 50 18 ....D U..1(3P.
0030 00 e5 61 ec 00 00 32 33 30 20 55 73 65 72 20 6b ..a...23 0 User k
0040 77 31 31 36 2d 30 34 37 20 6c 6f 67 67 65 64 20 w116-047 logged
Local Area Connection: <live capture in prog...
Packets: 1687 · Displayed: 11 (0.7%)
Profile: Default
14:13
24/11/2015


*Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ftp-data
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
338 26.1688940 10.0.0.253 10.0.1.2 FTP-DAT 109 FTP Data: 43 bytes


No-Operation (NOP)
No-Operation (NOP)
Timestamps: TSval 3740125791, TSecr 75515
[SEQ/ACK analysis]
[iRTT: 0.000378000 seconds]
[Bytes in flight: 43]
FTP Data (43 bytes data)
0000 00 1b 21 a6 06 34 00 0c 29 89 bc 3d 08 00 45 08 ..!..4..)..=..E.
0010 00 5f e0 65 40 00 40 06 44 2d 0a 00 00 fd 0a 00 ._.e@.@. D-......
0020 01 02 00 14 c0 0f f3 b7 2a 40 37 50 73 9b 80 18 .... *@7Ps...
0030 00 e5 27 70 00 00 01 01 08 0a de ed ca 5f 00 01 ..'p.... ....._..
0040 26 fb 20 0d 0a 2e 0d 0a 2e 2e 0d 0a 2e 62 61 73 &. ....bas
0050 68 5f 6c 6f 67 6f 75 74 0d 0a 2e 62 61 73 68 72 h_logout ...bashr
0060 63 0d 0a 2e 70 72 6f 66 69 6c 65 0d 0a c...prof ile..
FTP Data (ftp-data), 43 bytes
Packets: 2075 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
14:16
24/11/2015


*Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ftp-data
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
338 26.1688940 10.0.0.253 10.0.1.2 FTP-DAT 109 FTP Data: 43 bytes


Frame 338: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
Interface id: 0 (\Device\NPF_{C7092455-6D9E-4124-A938-9D2E52B4439B})
Encapsulation type: Ethernet (1)
Arrival Time: Nov 24, 2015 14:11:15.918259000 GMT Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1448374275.918259000 seconds
[Time delta from previous captured frame: 0.000297000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 26.168894000 seconds]
Frame Number: 338
Frame Length: 109 bytes (872 bits)
Capture Length: 109 bytes (872 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:ftp-data]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Vmware_89:bc:3d (00:0c:29:89:bc:3d), Dst: IntelCor_a6:06:34 (00:1b:21:a6:06:34)
Destination: IntelCor_a6:06:34 (00:1b:21:a6:06:34)
0000 00 1b 21 a6 06 34 00 0c 29 89 bc 3d 08 00 45 08 ..!..4..)..=..E.
0010 00 5f e0 65 40 00 40 06 44 2d 0a 00 00 fd 0a 00 ._.e@.@. D-......
0020 01 02 00 14 c0 0f f3 b7 2a 40 37 50 73 9b 80 18 .... *@7Ps...
0030 00 e5 27 70 00 00 01 01 08 0a de ed ca 5f 00 01 ..'p.... ....._..
0040 26 fb 20 0d 0a 2e 0d 0a 2e 2e 0d 0a 2e 62 61 73 &. ....bas
0050 68 5f 6c 6f 67 6f 75 74 0d 0a 2e 62 61 73 68 72 h_logout ...bashr
0060 63 0d 0a 2e 70 72 6f 66 69 6c 65 0d 0a c...prof ile..
Absolute time when this frame was capture...
Packets: 2075 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
14:19
24/11/2015



ftp shows everything that happen within protocol. ftp command channel

ftp-data shows the data that was sent. ftp is data channel