

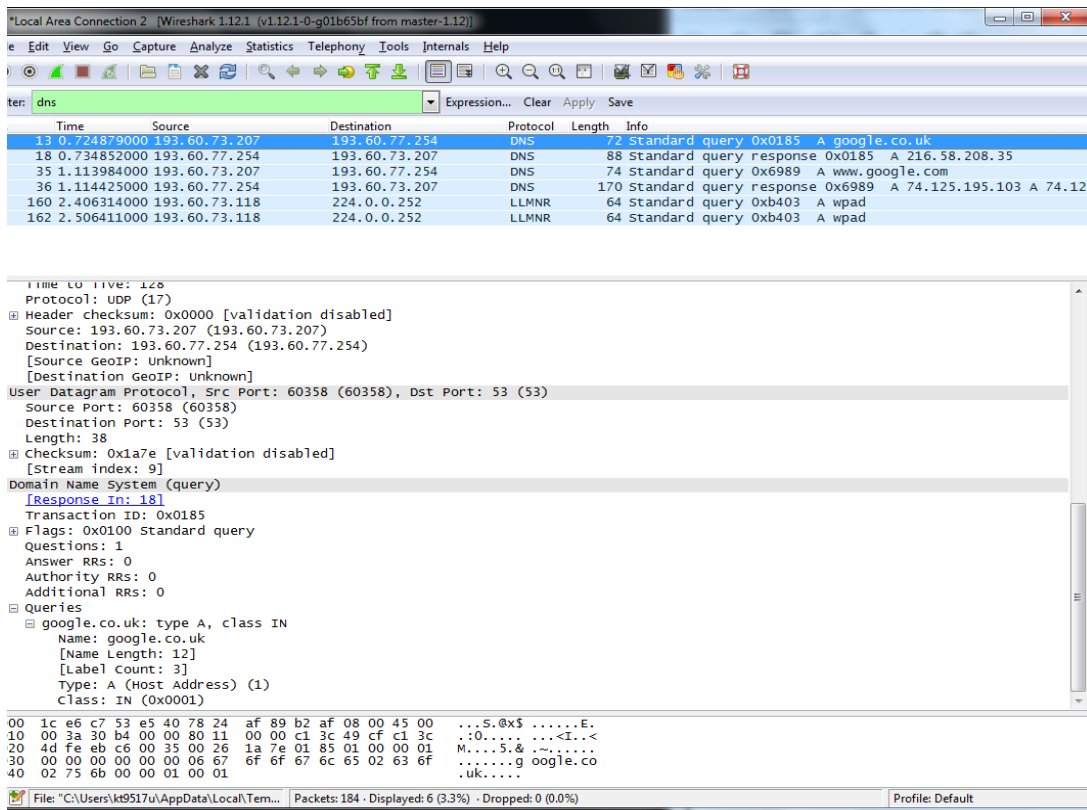
Packet Sniffing - Marking Scheme

	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

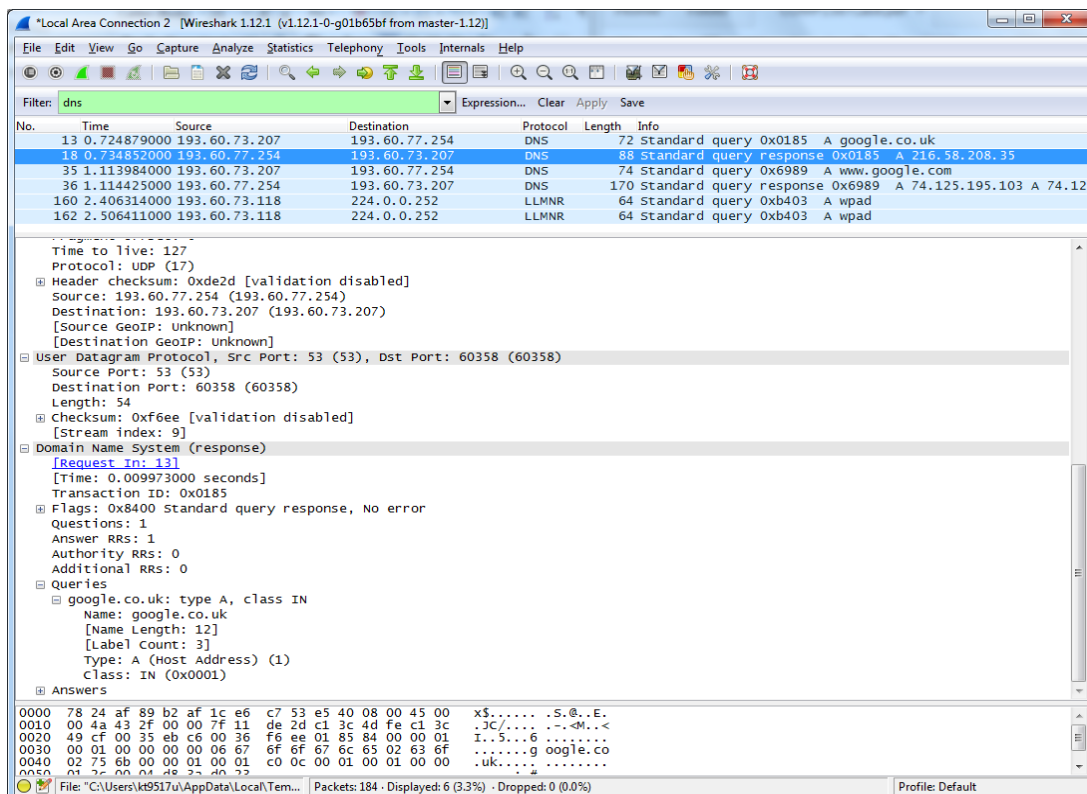
Task	Mark	Grade
Task 1 - Capture a HTTP Request Sequence	40	
Task 2 - Capture a Chat Session	30	
Task 3 - Capture an FTP Session	30	
Total	100	

[Packet Sniffing](#)

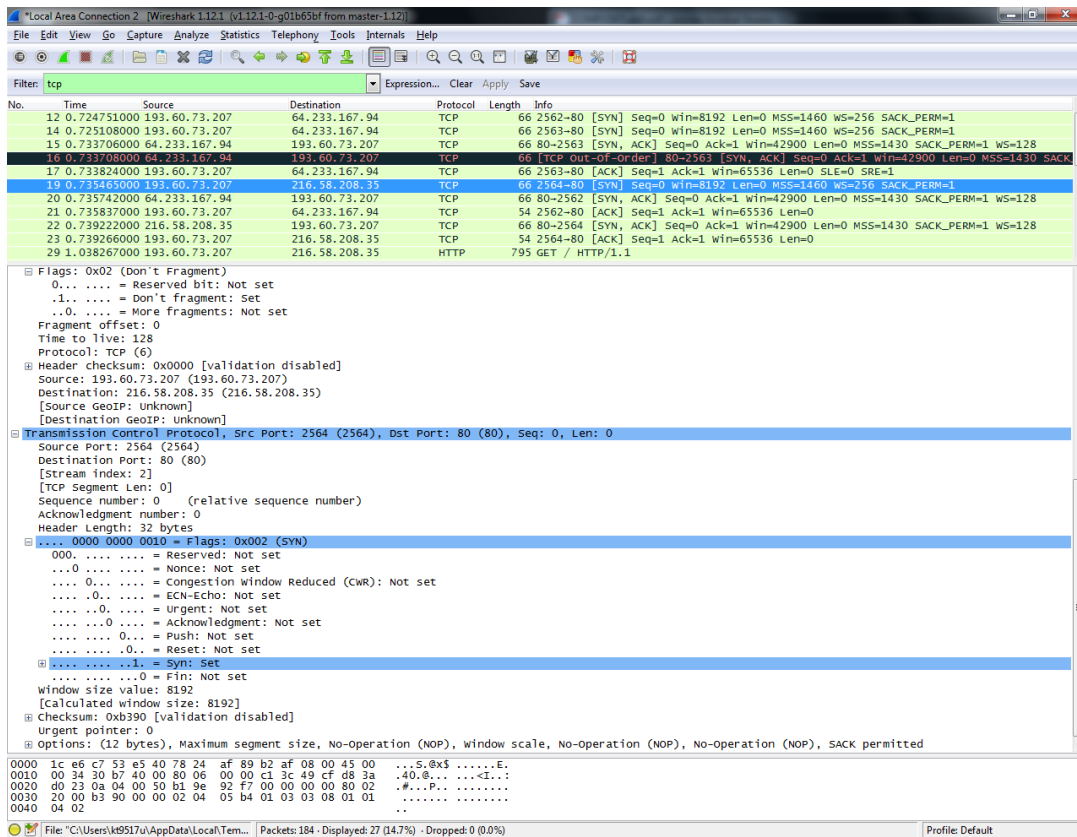
Task 1



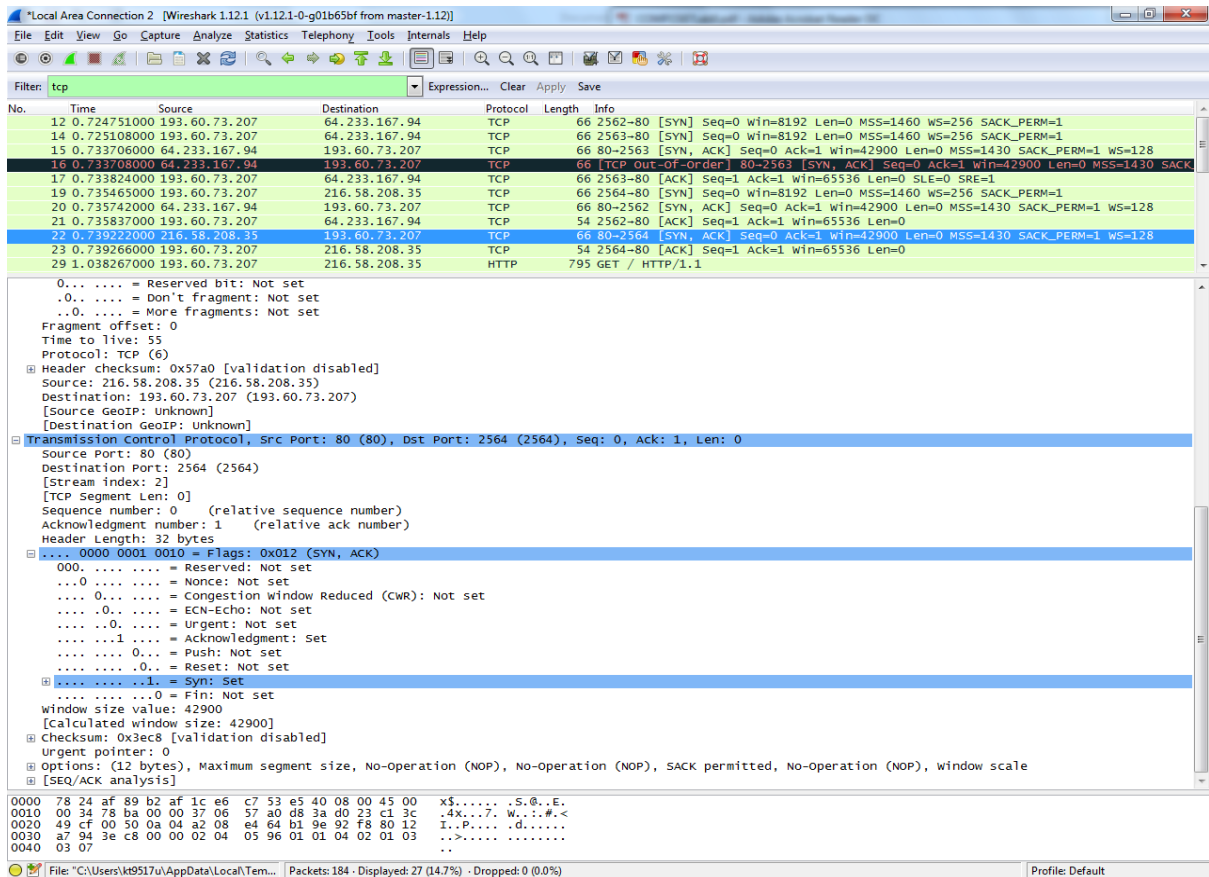
DNS request for the IP address that corresponds to the URL



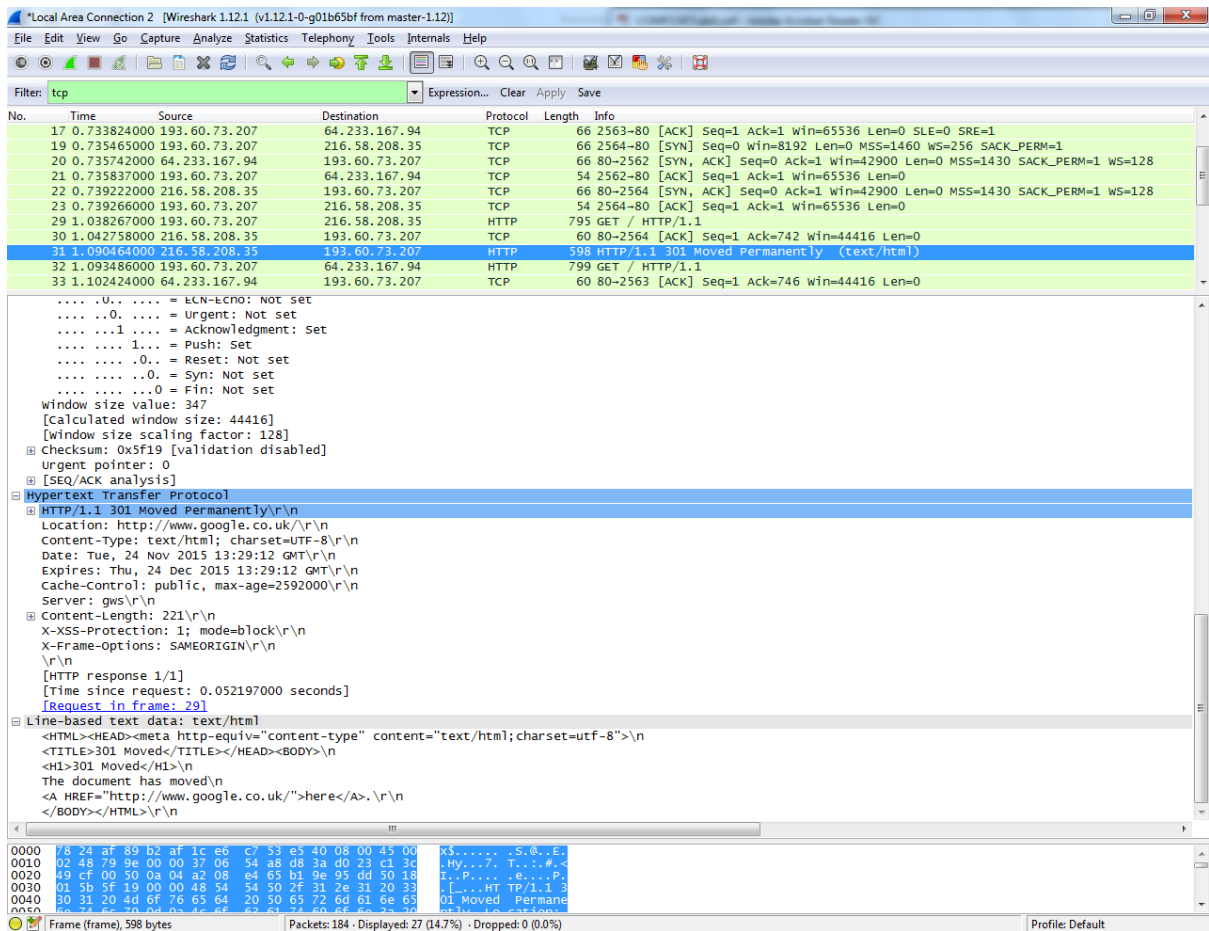
DNS response returned with the IP address clearly seen



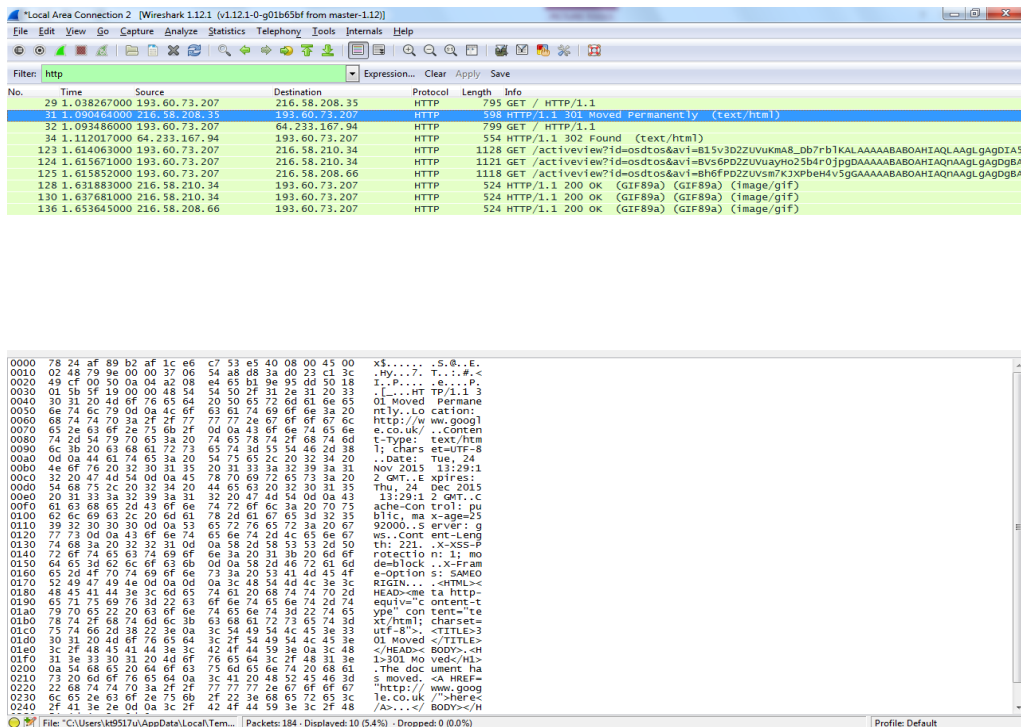
HTTP – TCP starting the 3-way handshake (SYN bit =1) – note sequence numbers



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



HTTP 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

No.	Time	Source	Destination	Protocol	Length	Info
249	24.9019370	10.0.1.35	10.0.0.253	XMPP/XML	189	MESSAGE > kw116-049@ubuntu-server
250	24.9021680	10.0.0.253	10.0.1.35	TCP	60	5222->49158 [ACK] Seq=668 Ack=3778 win=40595 Len=0
251	24.9472520	10.0.1.76	10.255.255.255	NBNS	92	Name query nb WPAD<0>
252	25.3442850	10.0.1.4	10.255.255.255	NBNS	92	Name query nb WPAD<0>
253	25.4583580	10.0.1.35	10.0.0.253	XMPP/XML	192	MESSAGE > kw116-049@ubuntu-server
254	25.4585940	10.0.0.253	10.0.1.35	TCP	60	5222->49158 [ACK] Seq=668 Ack=3916 win=40595 Len=0
255	25.5534410	84:b5:17:7b:af:ad	Spanning-tree-(For-STP			
256	25.7332050	10.0.1.76	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x43c62965
257	25.7334900	10.0.0.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x43c62965
258	25.7357700	10.0.1.76	10.255.255.255	NBNS	92	Name query nb WPAD<0>
259	26.0904090	10.0.1.35	10.0.0.253	XMPP/XML	206	MESSAGE > kw116-049@ubuntu-server
260	26.0906990	10.0.0.253	10.0.1.35	TCP	60	5222->49158 [ACK] Seq=668 Ack=4068 win=40595 Len=0
261	26.0973220	10.0.1.4	10.255.255.255	NBNS	92	Name query nb WPAD<0>
262	26.1078140	10.0.1.35	10.0.0.253	XMPP/XML	189	MESSAGE > kw116-049@ubuntu-server
263	26.1080360	10.0.0.253	10.0.1.35	TCP	60	5222->49158 [ACK] Seq=668 Ack=4203 win=40595 Len=0
264	26.4917060	10.0.1.76	10.255.255.255	NBNS	92	Name query nb WPAD<0>
265	26.7274620	10.0.1.35	10.0.0.2	DNS	77	Standard query 0xb417 A crl.microsoft.com
266	26.8481400	10.0.1.4	10.255.255.255	NBNS	92	Name query nb WPAD<0>
267	26.9168440	10.0.1.14	255.255.255.255	UDP	82	Source port: 52167 Destination port: 1947
268	26.9838740	10.0.1.93	255.255.255.255	UDP	82	Source port: 62796 Destination port: 1947
269	27.1383950	10.0.1.35	10.0.0.253	XMPP/XML	192	MESSAGE > kw116-049@ubuntu-server
270	27.1386640	10.0.0.253	10.0.1.35	TCP	60	5222->49158 [ACK] Seq=668 Ack=4341 win=40595 Len=0
271	27.2560330	10.0.1.76	10.255.255.255	NBNS	92	Name query nb WPAD<0>
272	27.5400650	84:b5:17:7b:af:ad	Spanning-tree-(For-STP			
273	27.5703650	10.0.1.35	10.0.0.253	XMPP/XML	205	MESSAGE > kw116-049@ubuntu-server
274	27.5706200	10.0.0.253	10.0.1.35	TCP	60	5222->49158 [ACK] Seq=668 Ack=4492 win=40595 Len=0
275	27.6021720	10.0.1.35	10.0.0.253	XMPP/XML	189	MESSAGE > kw116-049@ubuntu-server
276	27.6024110	10.0.0.253	10.0.1.35	TCP	60	5222->49158 [ACK] Seq=668 Ack=4627 win=40595 Len=0
277	27.6458810	10.0.1.4	10.255.255.255	NBNS	92	Name query nb WPAD<0>
278	28.0315530	IntelCor_0b:d3:9d	Broadcast	ARP	60	Who has 10.0.0.27 Tell 10.0.1.49
279	28.0592910	fe80::702b:1865:c83ff02:16	ICMPv6	90	Multicast Listener Report Message v2	
280	28.0728570	fe80::702b:1865:c83ff02:16	ICMPv6	90	Multicast Listener Report Message v2	
281	28.0743660	fe80::702b:1865:c83ff02:16	ICMPv6	90	Multicast Listener Report Message v2	
282	28.0826890	fe80::702b:1865:c83ff02:16	ICMPv6	90	Multicast Listener Report Message v2	
283	28.0836810	fe80::702b:1865:c83ff02:113	LLMNR	89	Standard query 0xf907 ANY Comms-001	
284	28.0837710	10.0.1.49	224.0.0.252	LLMNR	69	Standard query 0xf907 ANY Comms-001

Frame 245: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0

Interface id: 0 (Device\NPF{C7092455-6D9E-4124-A938-902E52B4439E})

Encapsulation type: Ethernet (1)

Arrival Time: Nov 24, 2015 13:47:19.967741000 GMT Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1448372839.967741000 seconds

[Time delta from previous captured frame: 0.022412000 seconds]

[Time delta from previous displayed frame: 0.022412000 seconds]

[Time since reference or first frame: 24.205402000 seconds]

Frame Number: 245

Frame Length: 82 bytes (656 bits)

0000 ff ff ff ff ff ff 40 16 7e a4 9a ae 08 00 45 00@.....E.
0010 00 44 6c f7 00 00 80 11 b7 6a 0a 00 01 49 0a ff .Dl.....j...i..
0020 ff ff c2 02 07 9b 00 30 64 c8 58 64 56 56 4f 4b0 d.xdvvok
0030 74 59 2f 4d 70 6f 60 73 63 2b 32 34 50 13 31 56 ty/tpoks t+24PC1V
0040 33 4e 72 48 42 53 74 37 6c 41 64 48 68 38 59 33 3NHBSE7 TAdHh8Y3

File: C:\Users\Student\AppData\Local\Temp... Packets: 319 | Displayed: 319 (100.0%) | Dropped: 0 (0.0%)

Profile Default

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

Frame 253: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface 0
Ethernet II, Src: IntelCor_6e:58:5d (00:1b:21:6e:58:5d), Dst: Vmware_89:bc:3d (00:0c:29:89:bc:3d)
Internet Protocol Version 4, Src: 10.0.1.35 (10.0.1.35), Dst: 10.0.0.253 (10.0.0.253)
Transmission Control Protocol, Src Port: 49158 (49158), Dst Port: 5222 (5222), Seq: 3778, Ack: 668, Len: 138
Source Port: 49158 (49158)
Destination Port: 5222 (5222)
[Stream index: 0]
[TCP Segment Len: 138]
Sequence number: 3778 (relative sequence number)
[Next sequence number: 3916 (relative sequence number)]
Acknowledgment number: 668 (relative ack number)
Header Length: 20 bytes
.... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
window size value: 256
[Calculated window size: 256]
[window size scaling factor: -1 (unknown)]
Checksum: 0x16c4 [validation disabled]
urgent pointer: 0
[SEQ/ACK analysis]

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

The screenshot shows the Wireshark interface with a packet capture from the Local Area Connection. The packet list on the left shows various protocols including NBNS, DHCP, ARP, LLMNR, and XMPP. Packet 690 is selected, which is an XMPP message. The packet details pane on the right shows the structure of the XMPP message, including the envelope, body, and chatstate. The packet bytes pane at the bottom shows the raw data of the selected packet.

Packet 690 details:

- Envelope: {id: "purple3cad42c5", type: "chat", chatstate: "composing"}
- Body: I'm not here right now
- Chatstate: composing

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-ftp)
132	12.1527690	10.0.1.2	10.0.0.253	FTP	70	Request: USER kw116-047
134	12.1537130	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 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..i(3P.
0030  00 e5 61 ec 00 00 32 33 20 55 73 65 72 20 6b    ..a...23 0 User k
0040  77 31 31 36 2d 30 34 37 20 6f 67 67 65 64 20  w116-047 logged
0050  6b 77 31 31 36 2d 30 34 37 2e 0d 0a            in

```

Packets: 2075 · Displayed: 11 (0.5%) · Dropped: 0 (0.0%)

Profile: Default

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-ftp)
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 6.4/openBSD/Linux-ftp)
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 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..i(3P.
0030  00 e5 61 ec 00 00 32 33 20 55 73 65 72 20 6b    ..a...23 0 User k
0040  77 31 31 36 2d 30 34 37 20 6f 67 67 65 64 20  w116-047 logged
0050  6b 77 31 31 36 2d 30 34 37 2e 0d 0a            in

```

Local Area Connection: <live capture in prog...> Packets: 1687 · Displayed: 11 (0.7%)

Profile: Default

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-DA1	109	FTP Data: 43 bytes

NO-Operation (NOP)
No-Operation (NOP)
Timestamps: TSVa1 3740125791, TSecr 75515
[SEQ/ACK analysis]
[RTT: 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	...l..4.. }..m..E..
0010	00 5f e0 65 40 00 00 06	44 2d 0a 00 00 fd 0a 00	...e@.0. 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 6f 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-DA1	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-A938-9D2E52B4439E})
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	...l..4.. }..m..E..
0010	00 5f e0 65 40 00 00 06	44 2d 0a 00 00 fd 0a 00	...e@.0. 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 6f 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

*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 261: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

Ethernet II, Src: IntelCor_a6:06:34 (00:1b:21:a6:06:34), Dst: Vmware_89:bc:3d (00:0c:29:89:bc:3d)

Internet Protocol Version 4, Src: 10.0.1.2 (10.0.1.2), Dst: 10.0.0.253 (10.0.0.253)

Version: 4

Header Length: 20 bytes

Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))

Total Length: 56

Identification: 0x02a7 (679)

Flags: 0x02 (Don't Fragment)

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0x0000 [validation disabled]

[good: False]

[bad: False]

Source: 10.0.1.2 (10.0.1.2)

Destination: 10.0.0.253 (10.0.0.253)

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

```

0000  00 0c 29 89 bc 3d 00 1b 21 a6 06 34 08 00 45 00  ..)..!.4..E.
0010  00 38 02 a7 40 00 80 06 00 00 0a 00 01 00 0a 00  .8..@... ..A...
0020  00 fd c0 0e 00 15 99 31 28 23 1b 44 55 c9 50 18  .....1 (#.DU.P.
0030  1f 7b 16 29 00 00 50 41 53 53 20 6b 77 31 31 36  .{)..PA SS kw116
0040  2d 30 34 37 0d 0a                                -047..

```

Source (ip.src), 4 bytes

Packets: 2075 - Displayed: 11 (0.5%) - Dropped: 0 (0.0%)

Profile: Default

14:20 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