

Packet Sniffing:

Thomas Joseph Nairn: 000744320

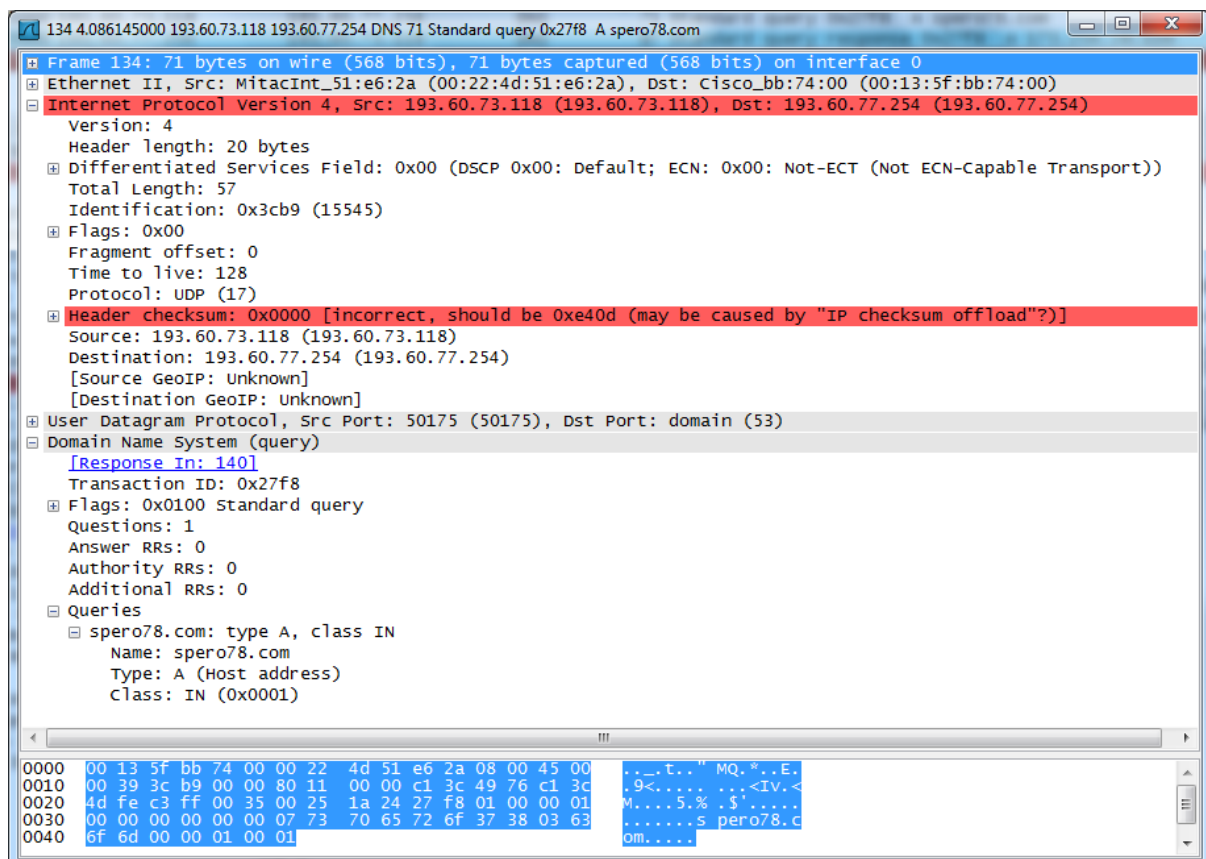
PT McDonnell: 000732831

Ashley Bennett: 000725945

Milena Krecisz: 000724968

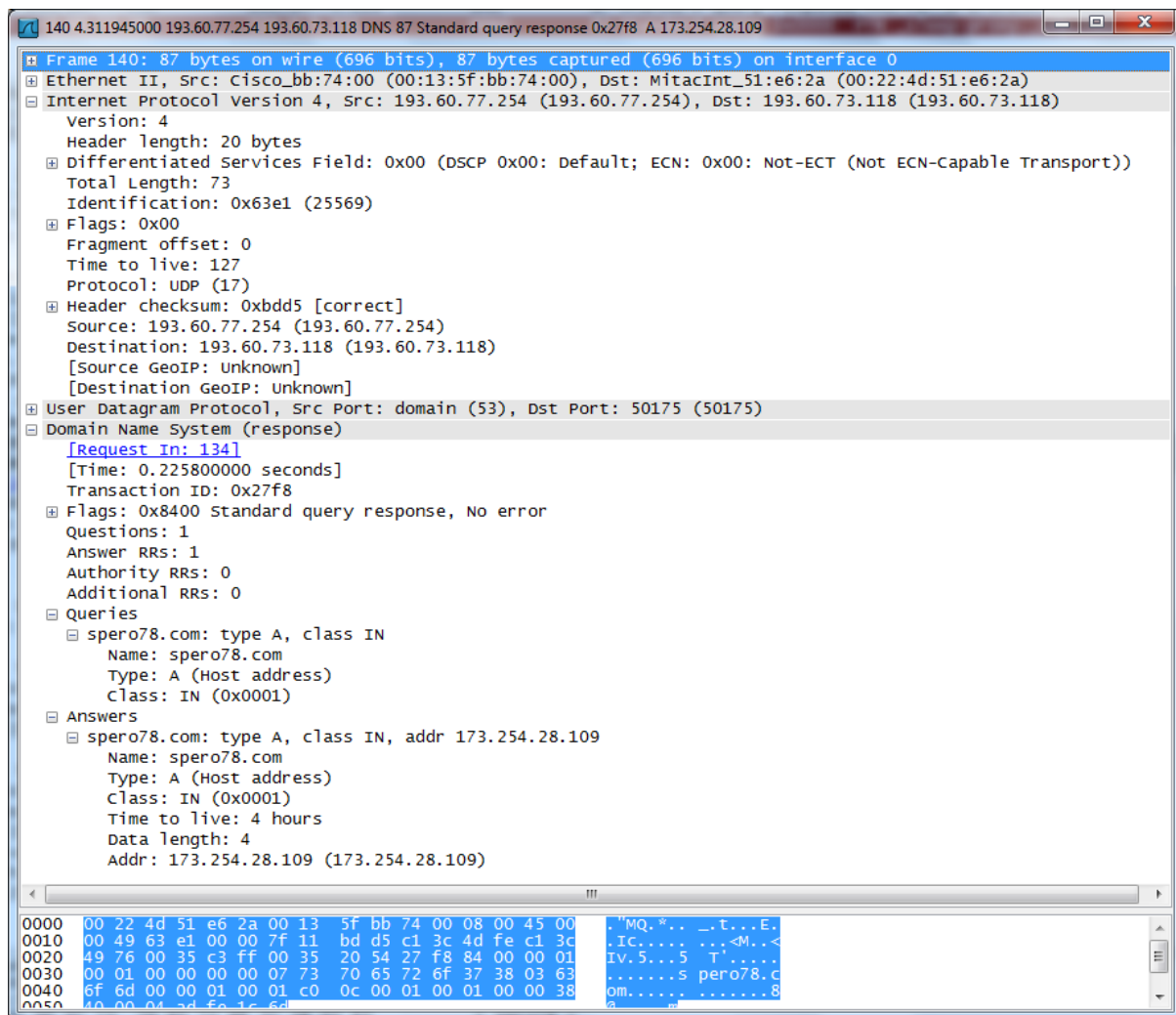
Task 1: Capture a HTTP Request sequence

Domain Name System (DNS) request for the IP address that corresponds to the Uniform Resource Locator (URL):



DNS request is sent.

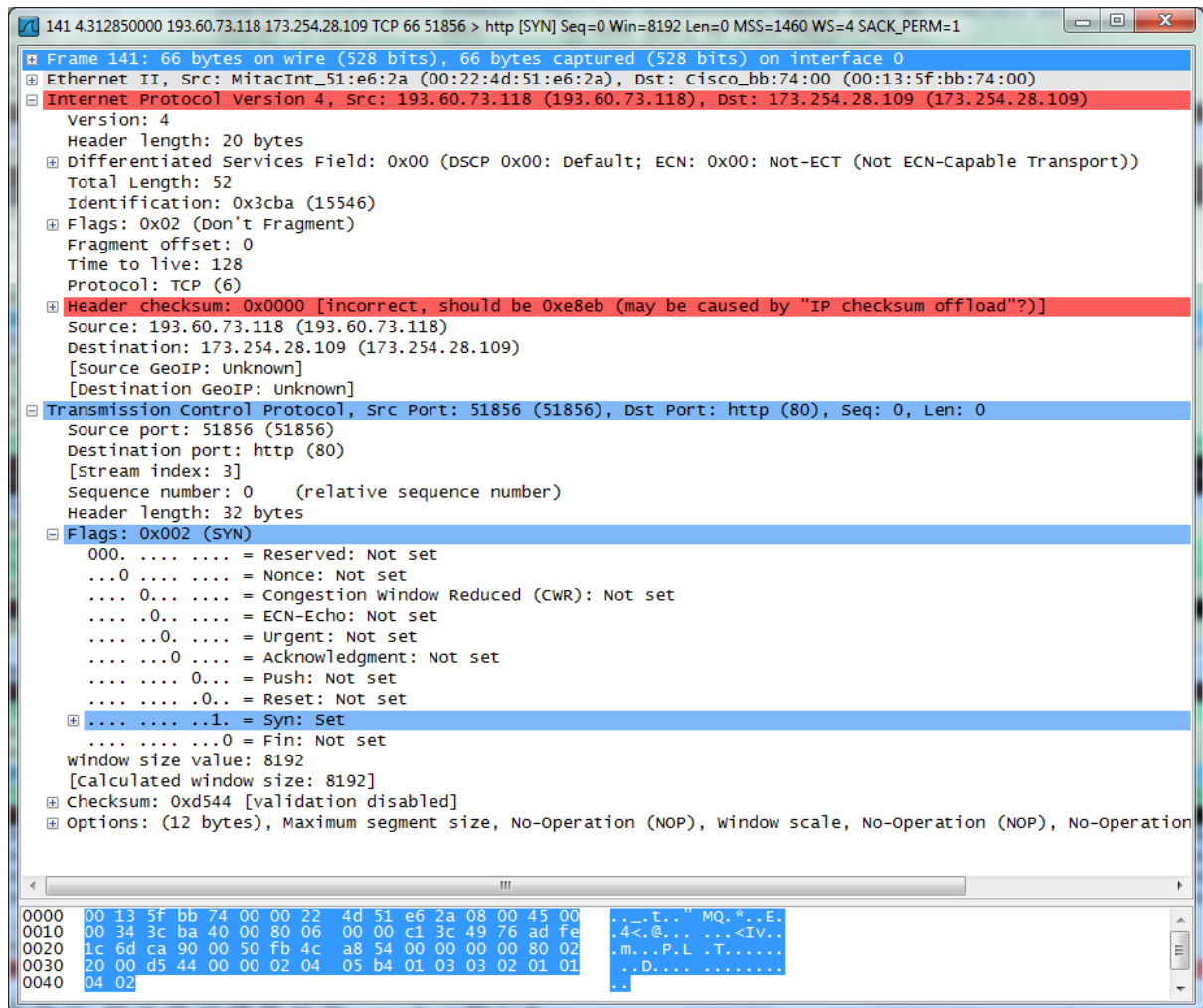
DNS response returned with the IP address clearly seen:



DNS Response.

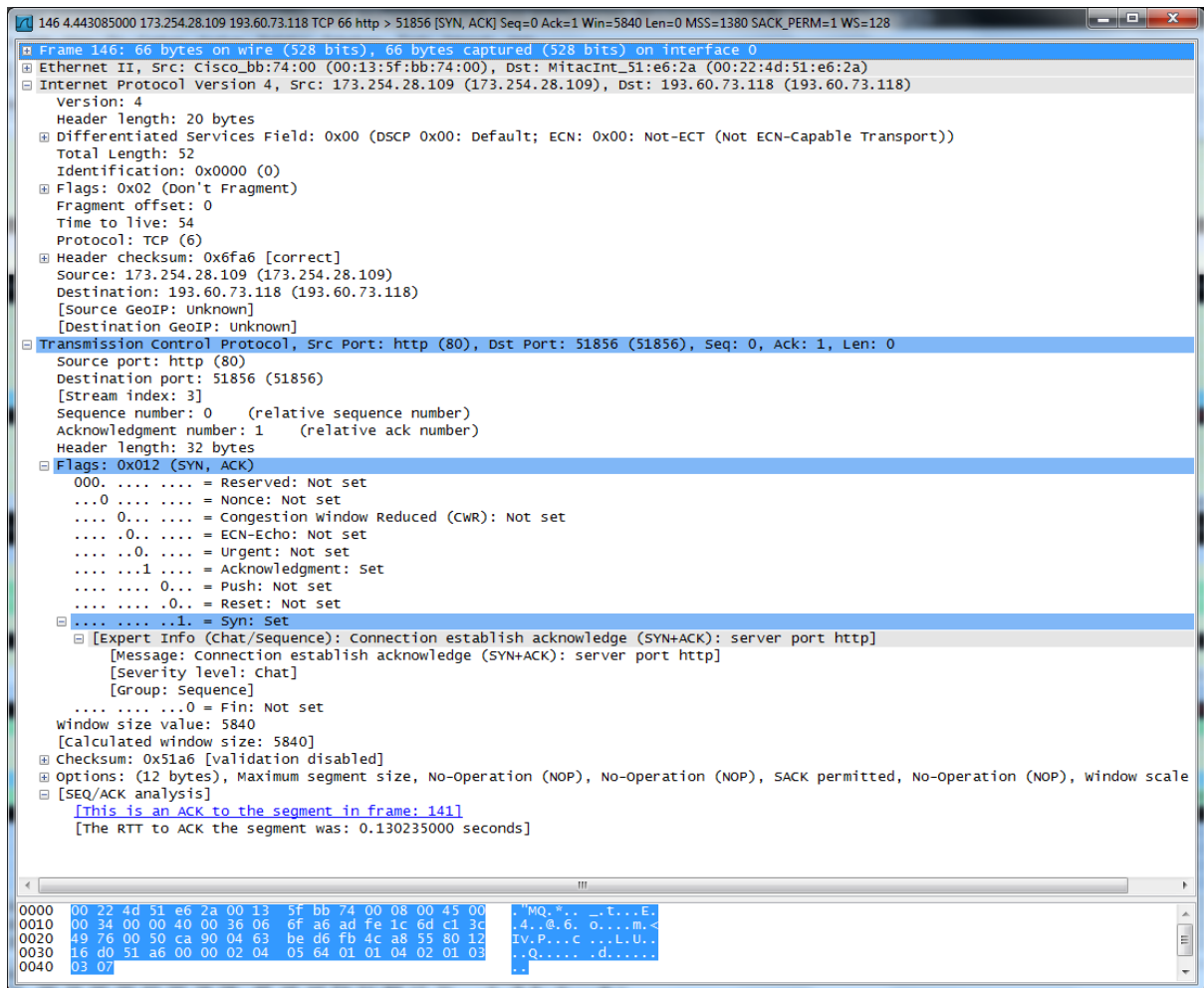
Address Line: spero78.com: type 173.254.28.109 A, class IN, addr

Hyper Text Transfer Protocol (HTTP) - actually TCP starting the 3 way handshake (SYN bit = 1) - note sequence numbers:



TCP Syn flag set.

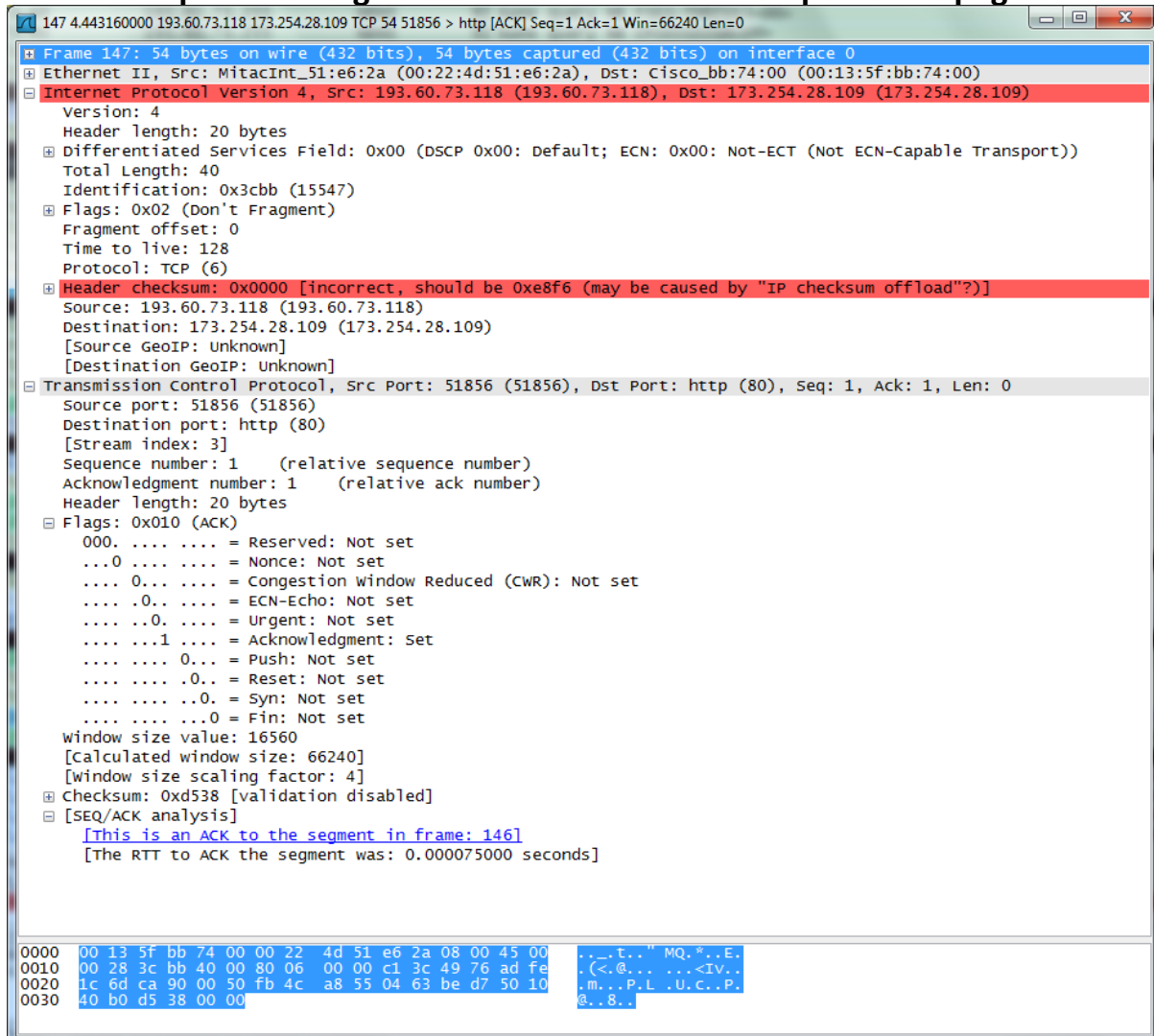
Start of 3 way handshake. (Sequence number: 0 (relative sequence number))



Syn + Ack, sent from server.

3 way handshake part 2. (Sequence number: 0 (relative sequence number))

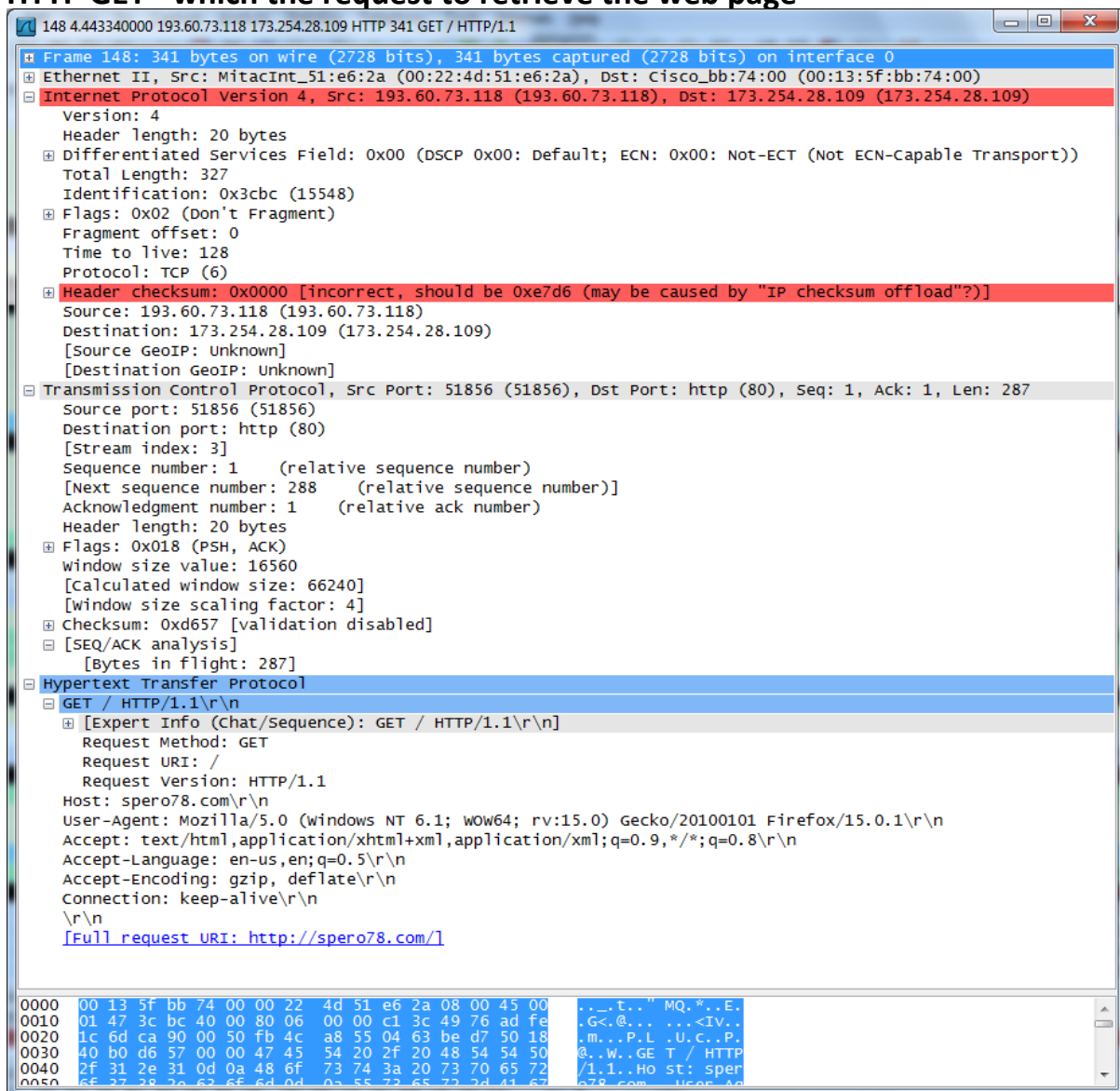
HTTP - TCP Acknowledgement to server (port 80) (SYN bit = 1, ACK bit = 1) - look at seq numbers again now browser starts to request web pages.



Ack sent from client to server.

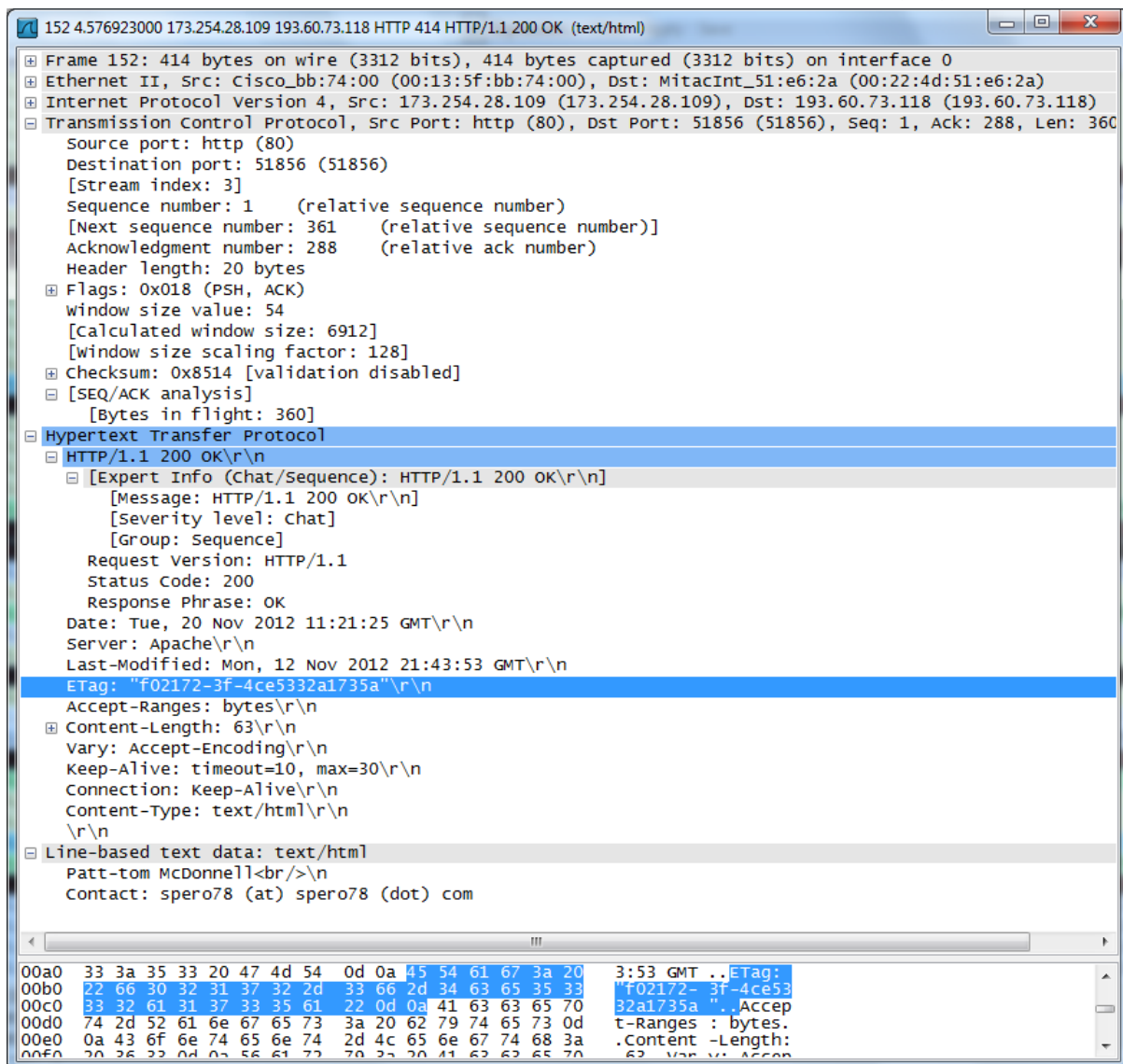
3rd part of 3 way handshake. (Sequence number: 1 (relative sequence number))

HTTP GET - which the request to retrieve the web page



GET request to server.

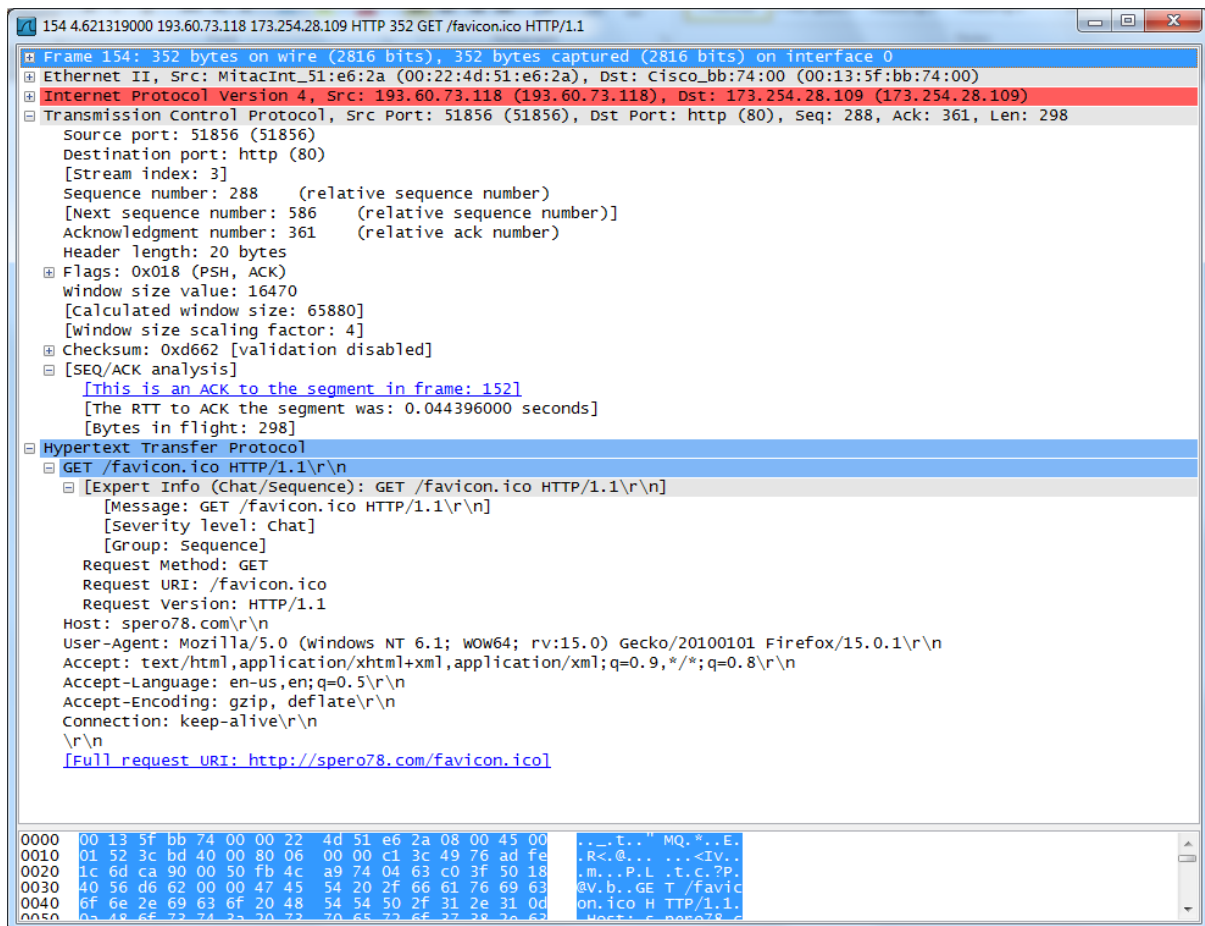
HTTP returned with data - this will be the header for the web page



HTTP 200, OK. Header received

Begin receiving web page data.

Many HTTP data packets each with Hyper Text Markup Language(HTML) code in it - the data to display the Web page



Additional request for other part of webpage.

TASK 2: Capture a Chat Session:

List the different protocols captured:

XMPP/XML

TCP

What is the protocol that delivers the chat packets?

XMPP/XML

What ports are involved in the Chat messaging?

Chat is sent from: 49178

Chat is received and listens on :5222

What else can you find out about the protocol?

When you begin to start typing, it sends a packet to the other user to say that you are typing. Then after every packet, the other user send an ACK using TCP .

All Jabber Packets sent and received:

4 interfaces [Wireshark 1.8.0 (SVN Rev 43431) from /trunk-1.8]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: xmpp Expression: Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
14	1.259081000	10.0.0.253	10.0.1.28	XMPP/XML	193	IQ(get) QUERY(jabber:iq:version) < manager.ubuntu-server
15	1.259368000	10.0.1.28	10.0.0.253	XMPP/XML	221	IQ(result) QUERY(jabber:iq:version) > manager.ubuntu-server
67	6.305430000	10.0.1.28	10.0.0.253	XMPP/XML	191	MESSAGE > kw116-046@ubuntu-server
78	7.192114000	10.0.1.28	10.0.0.253	XMPP/XML	206	MESSAGE > kw116-046@ubuntu-server
80	7.212597000	10.0.1.28	10.0.0.253	XMPP/XML	188	MESSAGE > kw116-046@ubuntu-server
95	9.162559000	10.0.0.253	10.0.1.28	XMPP/XML	251	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
102	9.819023000	10.0.0.253	10.0.1.28	XMPP/XML	264	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
104	10.022515000	10.0.0.253	10.0.1.28	XMPP/XML	248	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
111	10.695895000	10.0.1.28	10.0.0.253	XMPP/XML	205	MESSAGE > kw116-046@ubuntu-server/ubuntu-server
123	12.023942000	10.0.1.28	10.0.0.253	XMPP/XML	227	MESSAGE > kw116-046@ubuntu-server/ubuntu-server
129	12.058116000	10.0.1.28	10.0.0.253	XMPP/XML	202	MESSAGE > kw116-046@ubuntu-server/ubuntu-server
138	13.274181000	10.0.0.253	10.0.1.28	XMPP/XML	251	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
143	13.626120000	10.0.0.253	10.0.1.28	XMPP/XML	264	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
148	13.832413000	10.0.0.253	10.0.1.28	XMPP/XML	248	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
170	16.546146000	10.0.0.253	10.0.1.28	XMPP/XML	251	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
178	16.939774000	10.0.1.28	10.0.0.253	XMPP/XML	205	MESSAGE > kw116-046@ubuntu-server/ubuntu-server
180	17.258130000	10.0.0.253	10.0.1.28	XMPP/XML	266	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
183	17.463955000	10.0.0.253	10.0.1.28	XMPP/XML	248	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
188	17.935803000	10.0.1.28	10.0.0.253	XMPP/XML	218	MESSAGE > kw116-046@ubuntu-server/ubuntu-server
190	17.955276000	10.0.1.28	10.0.0.253	XMPP/XML	202	MESSAGE > kw116-046@ubuntu-server/ubuntu-server
200	19.610034000	10.0.0.253	10.0.1.28	XMPP/XML	251	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
205	20.050041000	10.0.0.253	10.0.1.28	XMPP/XML	264	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
209	20.264381000	10.0.0.253	10.0.1.28	XMPP/XML	248	MESSAGE < kw116-046@ubuntu-server/ubuntu-server
219	21.415743000	10.0.1.28	10.0.0.253	XMPP/XML	202	MESSAGE > kw116-046@ubuntu-server/ubuntu-server
231	23.141126000	10.0.0.253	10.0.1.28	XMPP/XML	158	PRESENCE < kw116-047@ubuntu-server/ubuntu-server

Frame 14: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface 1

Interface id: 1

WTAP_ENCAP: 1

Arrival Time: Nov 20, 2012 12:35:02.828366000 GMT Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1353414902.828366000 seconds

[Time delta from previous captured frame: 0.166393000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 1.259081000 seconds]

Frame Number: 14

Frame Length: 193 bytes (1544 bits)

Capture Length: 193 bytes (1544 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ip:tcp:xmpp:xml]

[Coloring Rule Name: TCP]

[Coloring Rule String: tcp]

Ethernet II, Src: Vmware_89:bc:3d (00:0c:29:89:bc:3d), Dst: IntelCor_6e:58:68 (00:1b:21:6e:58:68)

Internet Protocol Version 4, Src: 10.0.0.253 (10.0.0.253), Dst: 10.0.1.28 (10.0.1.28)

Version: 4

Header length: 20 bytes

0000 00 1b 21 6e 58 68 00 0c 29 89 bc 3d 08 00 45 00 ...!rxh...}...E.

0010 00 b3 d1 18 40 00 40 06 53 14 0a 00 00 fd 0a 00S.....

0020 01 1c 14 66 c0 3b 86 23 44 08 e7 b4 02 7b 50 18 ...f.i.#....{P.

0030 29 14 44 af 00 00 3c 69 71 20 74 79 70 65 3d 22 }..O..<g type=

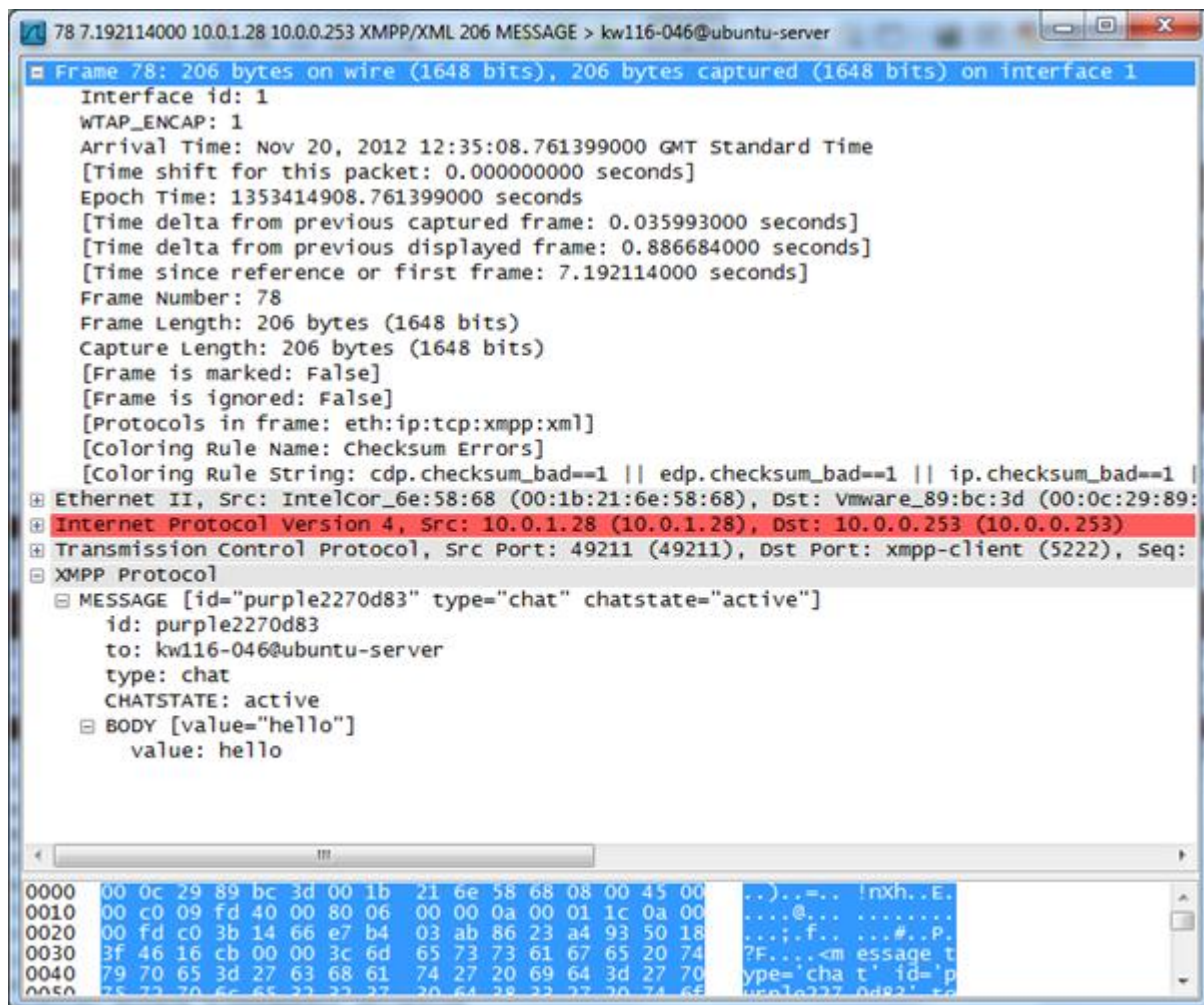
0040 67 65 74 22 20 69 64 3d 22 34 35 32 2d 31 31 37 get" id= 452-117

0050 33 70 74 64 2d 7d 7d 6b 77 21 24 26 7d 20 24 26 40 #...=...452-117

File: C:\Users\Student\AppData\Local\Temp\... Packets: 262 Displayed: 25 Marked: 0 Dropped: 0

Profile: Default

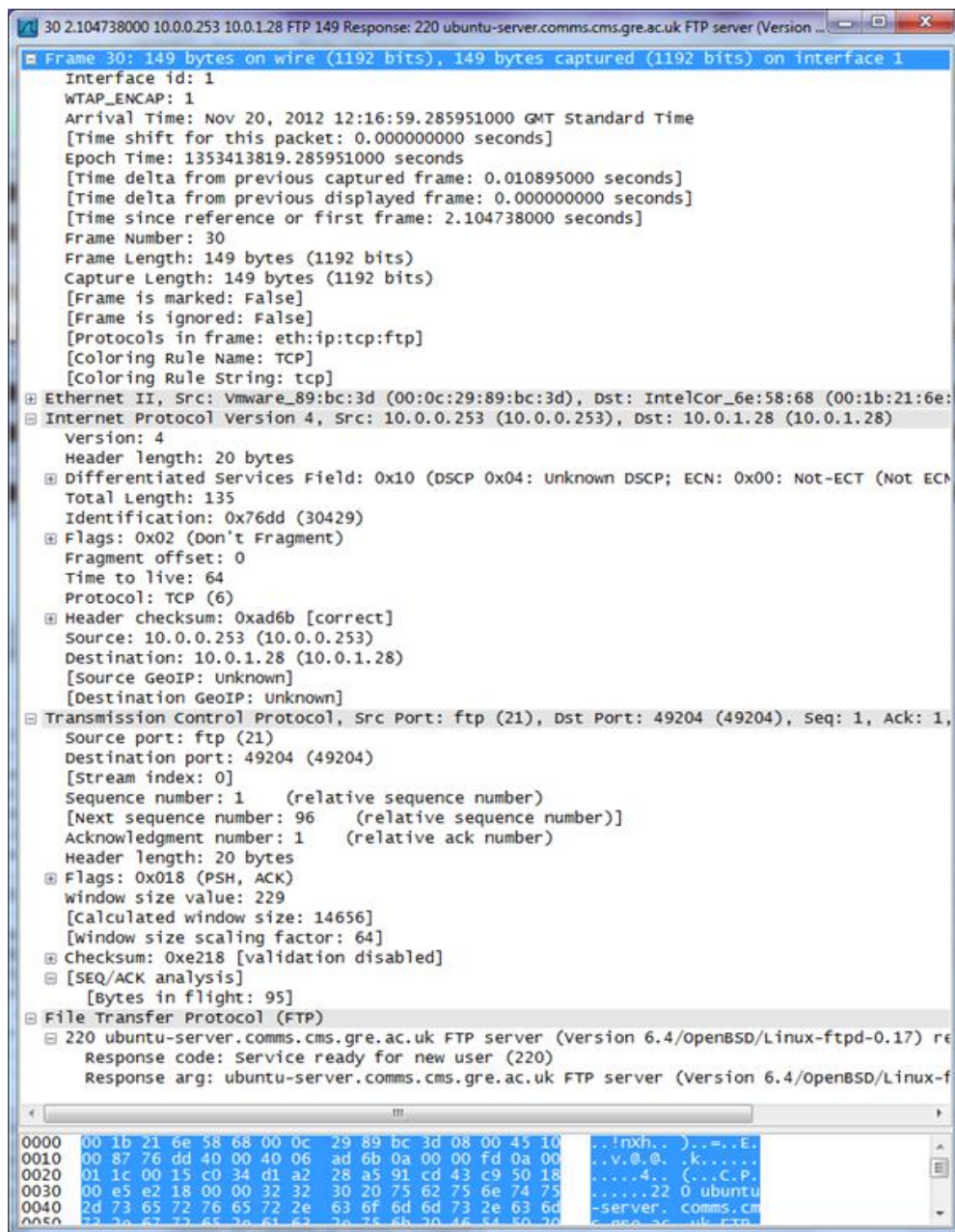
Here you can see the message that was sent in the packet.



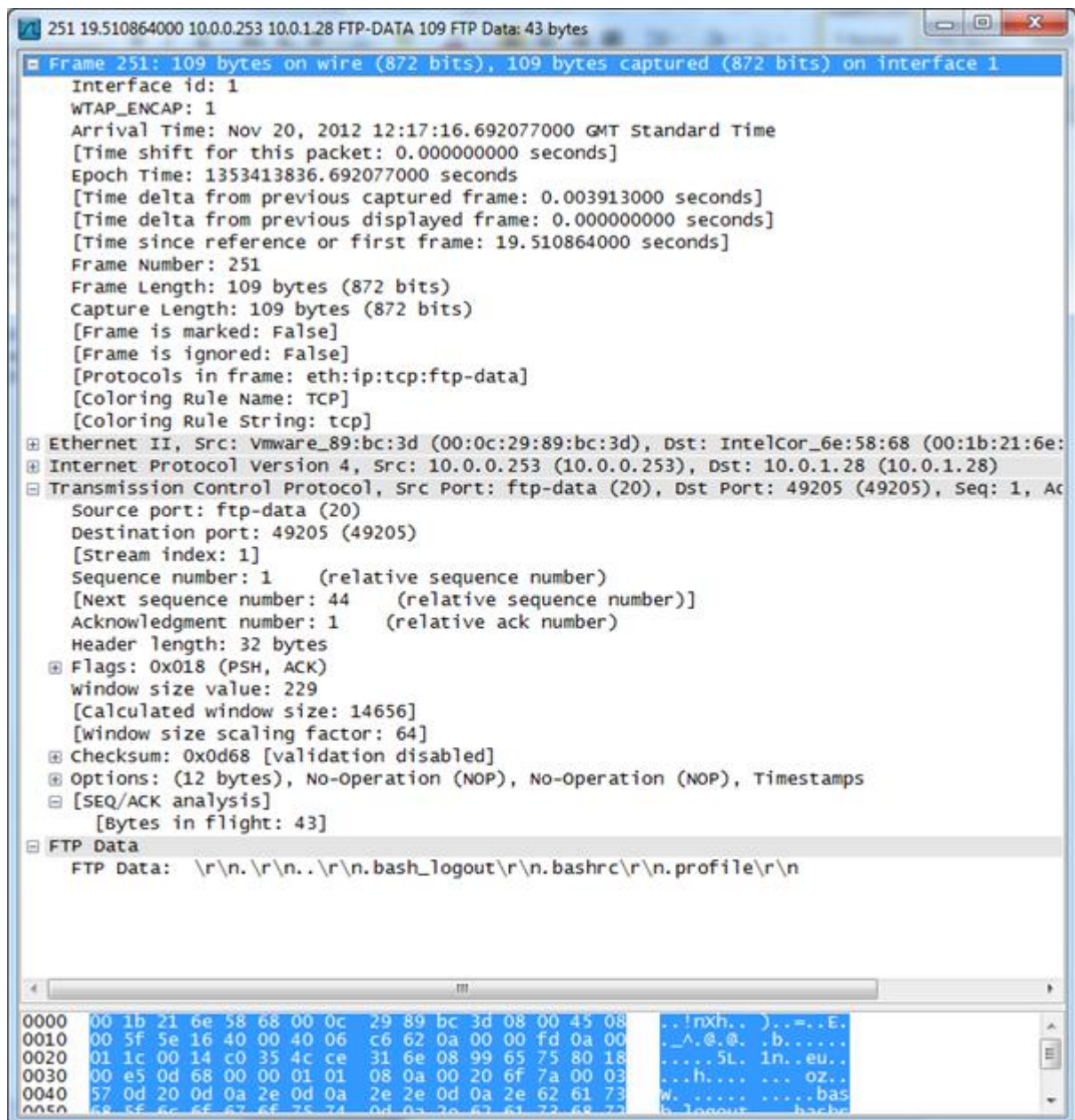
TASK 3: Capture an FTP Session

What messages did you receive?

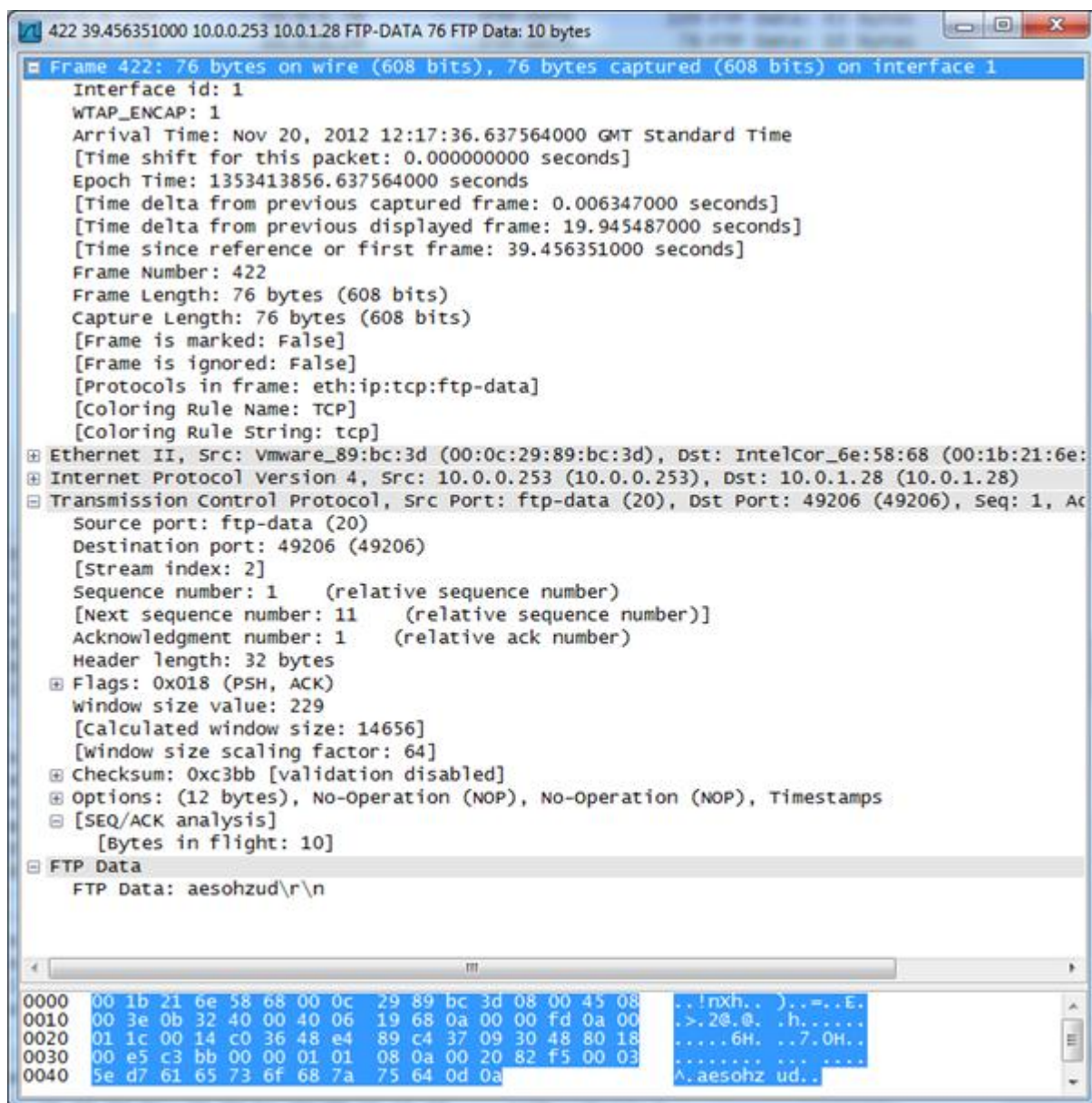
- Server identification
- A password request
- Welcome message
- File message



Server Identification.



Time and date, with IP Address in the image above.



File transfer response, ASCII Data transferred clearly visible.

4 interfaces [Wireshark 1.8.0 (SVN Rev 43431) from trunk-1.8]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **ftp** Expression: Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
142	1.615077000	10.0.0.253	10.0.1.28	FTP	149	Response: 220 ubuntu-server.comms.com.ac.uk FTP server (Version 6.4.0pre601)
143	0.721999000	10.0.1.28	10.0.0.253	FTP	20	Request: USER kw16-043
144	0.725699000	10.0.0.253	10.0.1.28	FTP	92	Response: 331 Password required for kw16-043.
145	0.728249000	10.0.1.28	10.0.0.253	FTP	20	Request: PASS kw16-043
146	0.842478000	10.0.0.253	10.0.1.28	FTP	123	Response: 230 Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-13-generic-pae 1686)
147	11.054600000	10.0.0.253	10.0.1.28	FTP	535	Response: 230-
148	13.146421000	10.0.1.28	10.0.0.253	FTP	77	Request: PORT 10.0.1.28,192,64
149	13.147024000	10.0.0.253	10.0.1.28	FTP	84	Response: 200 PORT command successful.
150	13.150317000	10.0.0.253	10.0.0.253	FTP	63	Request: NLST -a
151	13.155819000	10.0.0.253	10.0.1.28	FTP	109	Response: 150 Opening ASCII mode data connection for "/bin/ls".
152	13.363275000	10.0.0.253	10.0.1.28	FTP	78	Response: 226 Transfer complete.
153	20.761616000	10.0.1.28	10.0.0.253	FTP	77	Request: PORT 10.0.1.28,192,64
154	20.762317000	10.0.0.253	10.0.1.28	FTP	84	Response: 200 PORT command successful.
155	20.766499000	10.0.1.28	10.0.0.253	FTP	62	Request: RETR
156	20.767384000	10.0.0.253	10.0.1.28	FTP	113	Response: 150 Opening ASCII mode data connection for " " (9 bytes).
157	20.975910000	10.0.0.253	10.0.1.28	FTP	78	Response: 226 Transfer complete.
158	22.121918000	10.0.1.28	10.0.0.253	FTP	60	Request: QUIT
159	22.522340000	10.0.0.253	10.0.1.28	FTP	68	Response: 221 Goodbye.

Frame 16: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 1

Interface id: 1

WTAP_ENCAP: 1

Arrival Time: Nov 20, 2012 12:43:05.717266000 GMT Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1353413385.717266000 seconds

[Time delta from previous captured frame: 0.011017000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 1.615077000 seconds]

Frame Number: 16

Frame Length: 149 bytes (1192 bits)

Capture Length: 149 bytes (1192 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ip:tcp:ftp]

[Coloring Rule Name: TCP]

0000 00 1b 21 6e 58 68 00 0c 29 89 bc 3d 08 00 45 10 ..!mXh.. }...E.

0010 00 87 15 47 40 00 04 0f 02 0a 00 00 fd 0a 00 ...GB@.....

0020 01 3c 00 15 c0 3f 8c 25 43 2f 9b de c2 d4 50 187.%C/...P.

0030 00 e5 83 e4 00 00 32 32 30 20 75 62 75 6e 74 7522 0 ubuntu

0040 2d 73 65 72 76 65 72 2e 63 6f 6d 6d 73 2e 63 6d -server.comms.com

0050 12 3a 67 75 65 7a 64 43 7a 75 6b 7b 66 6a 60 7b:..z..b..r..

File: C:\Users\Student\AppData\Local\Temp\... Packets: 294 Displayed: 18 Marked: 0 Dropped: 0

Profile: Default

FTP Messages