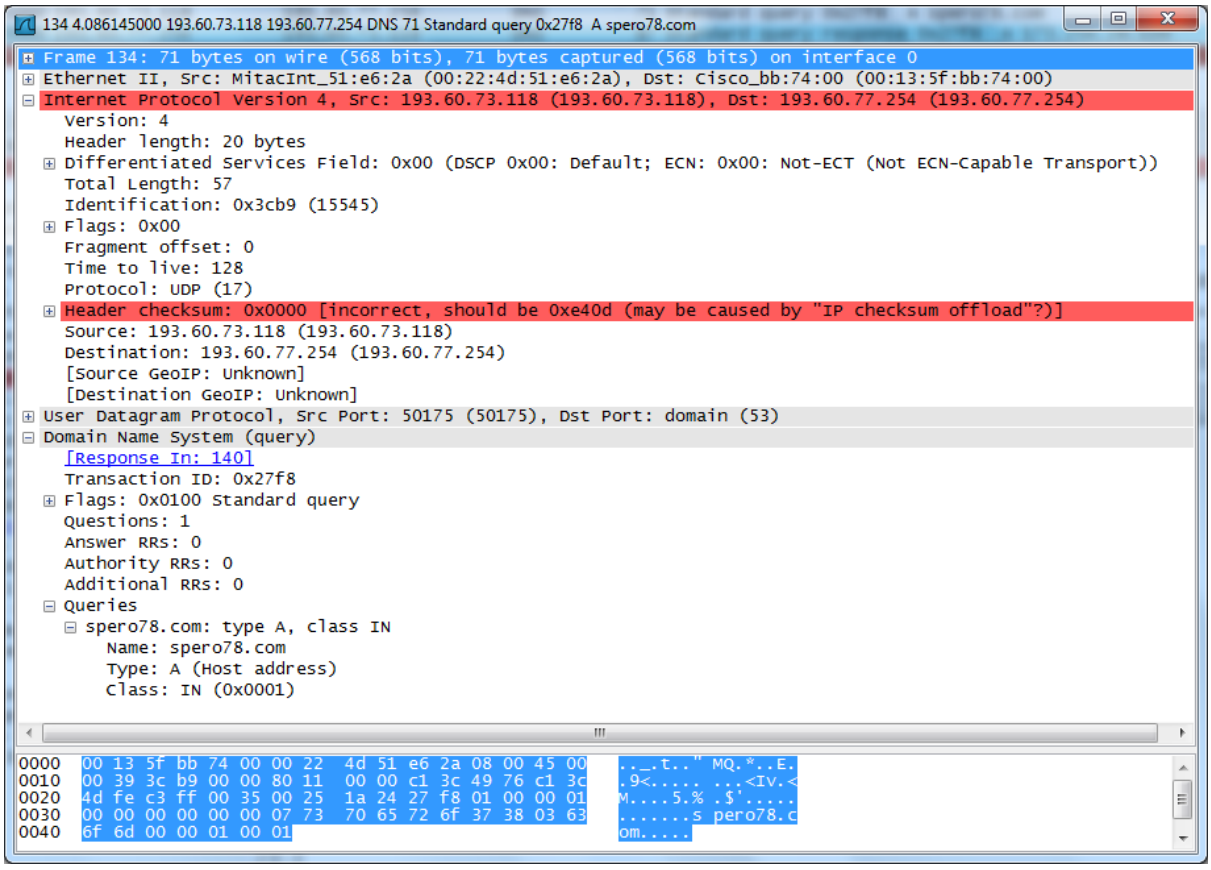
Packet Sniffing:

Thomas Joseph Nairn: 000744320
PT McDonnell: 000732831
Ashley Bennett: 000725945
Milena Krecisz: 000724968

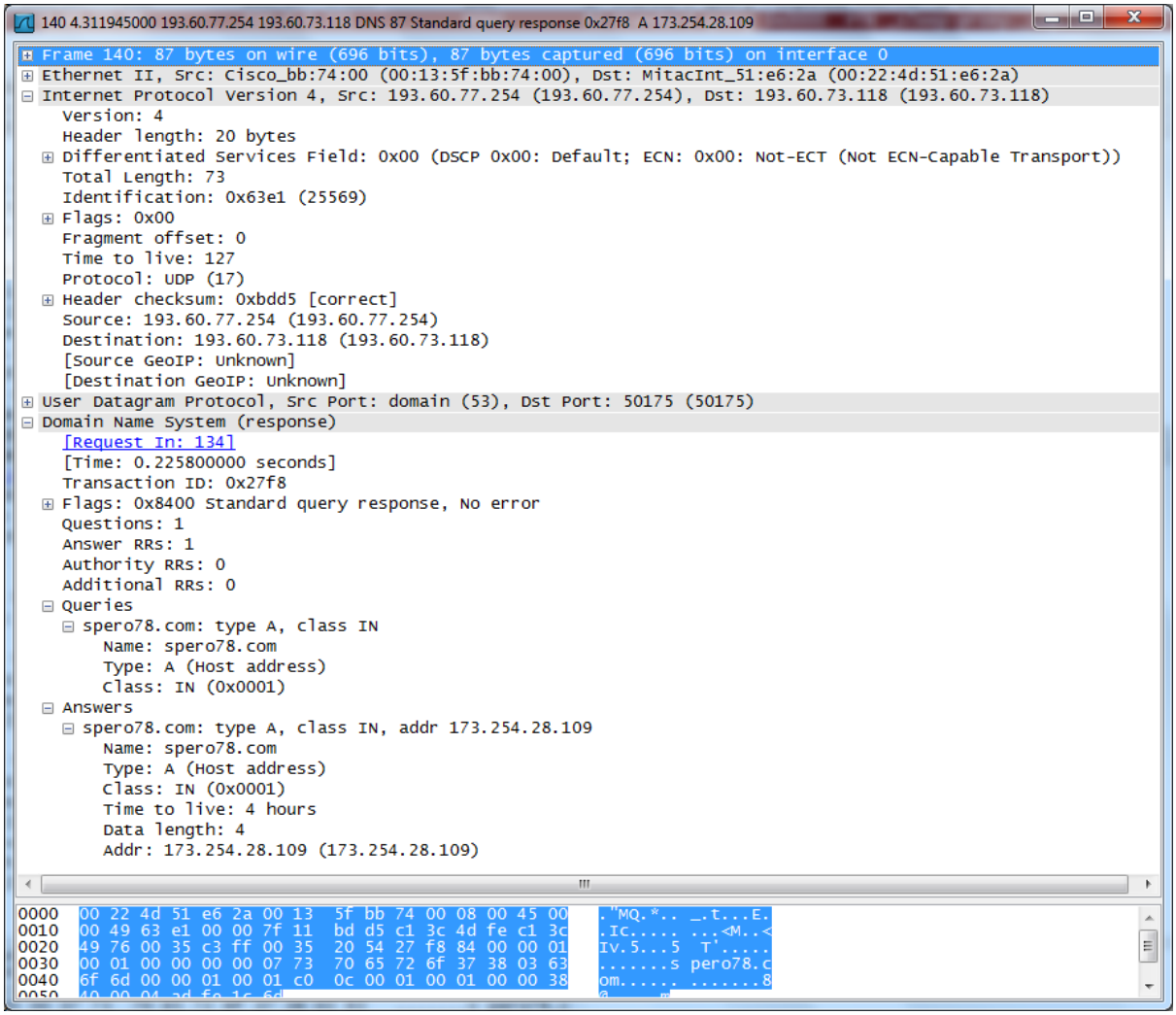
Task 1: Capture a HTTP Request sequence

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



DNS request is sent.

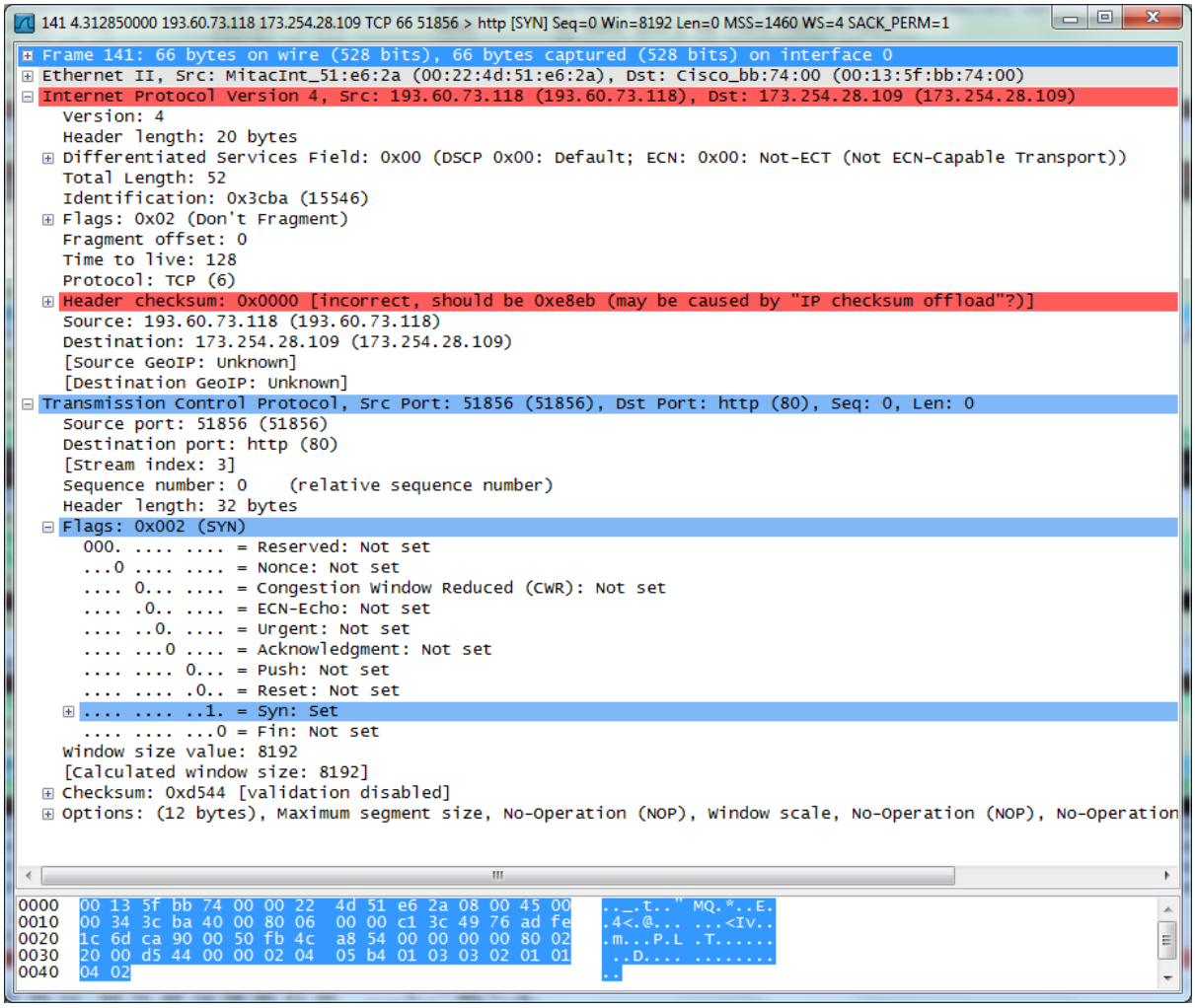
DNS response returned with the IP address clearly seen:



DNS Response.

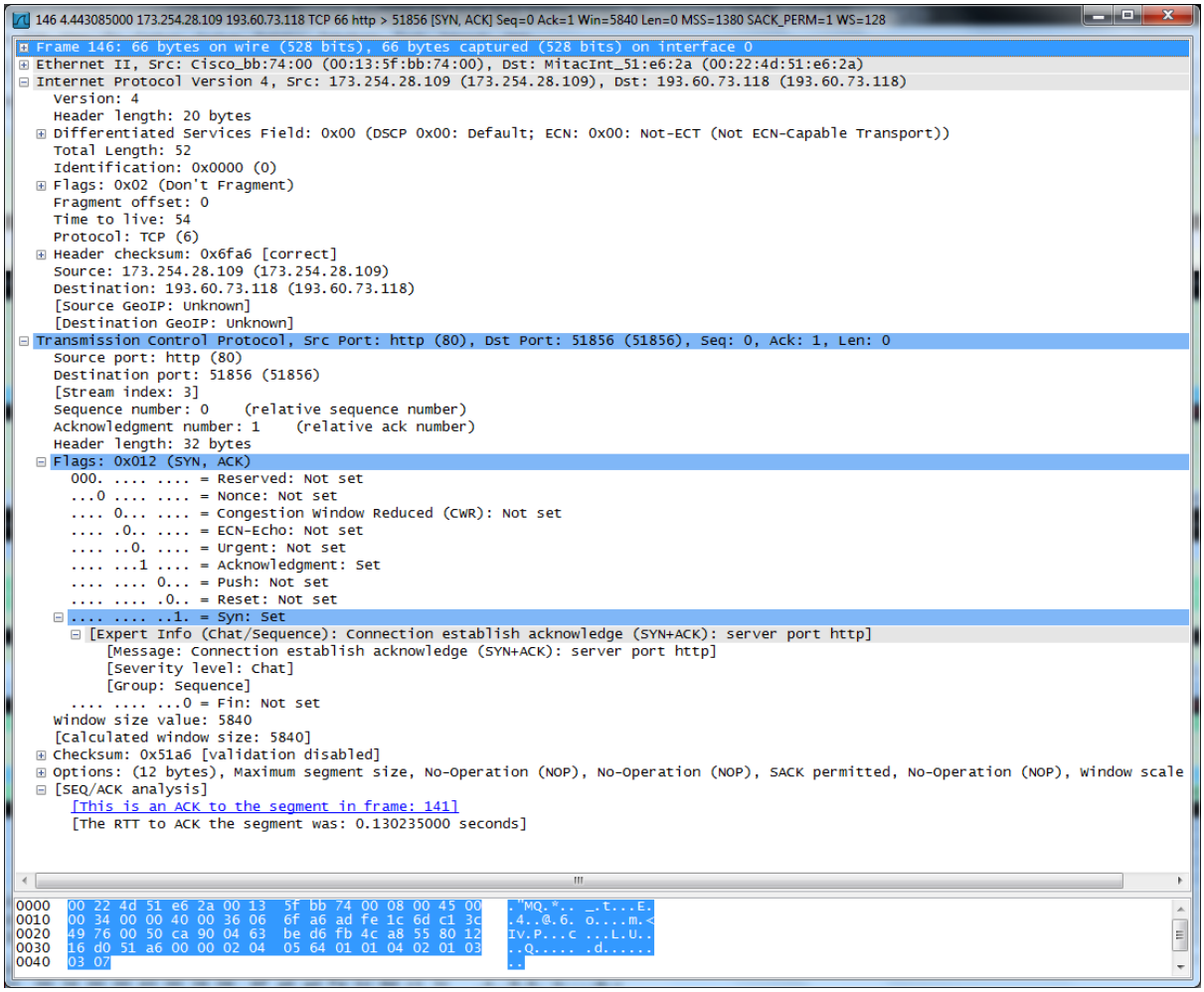
Address Line: spero78.com: type173.254.28.109 A, class IN, addr

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



TCP Syn flag set.

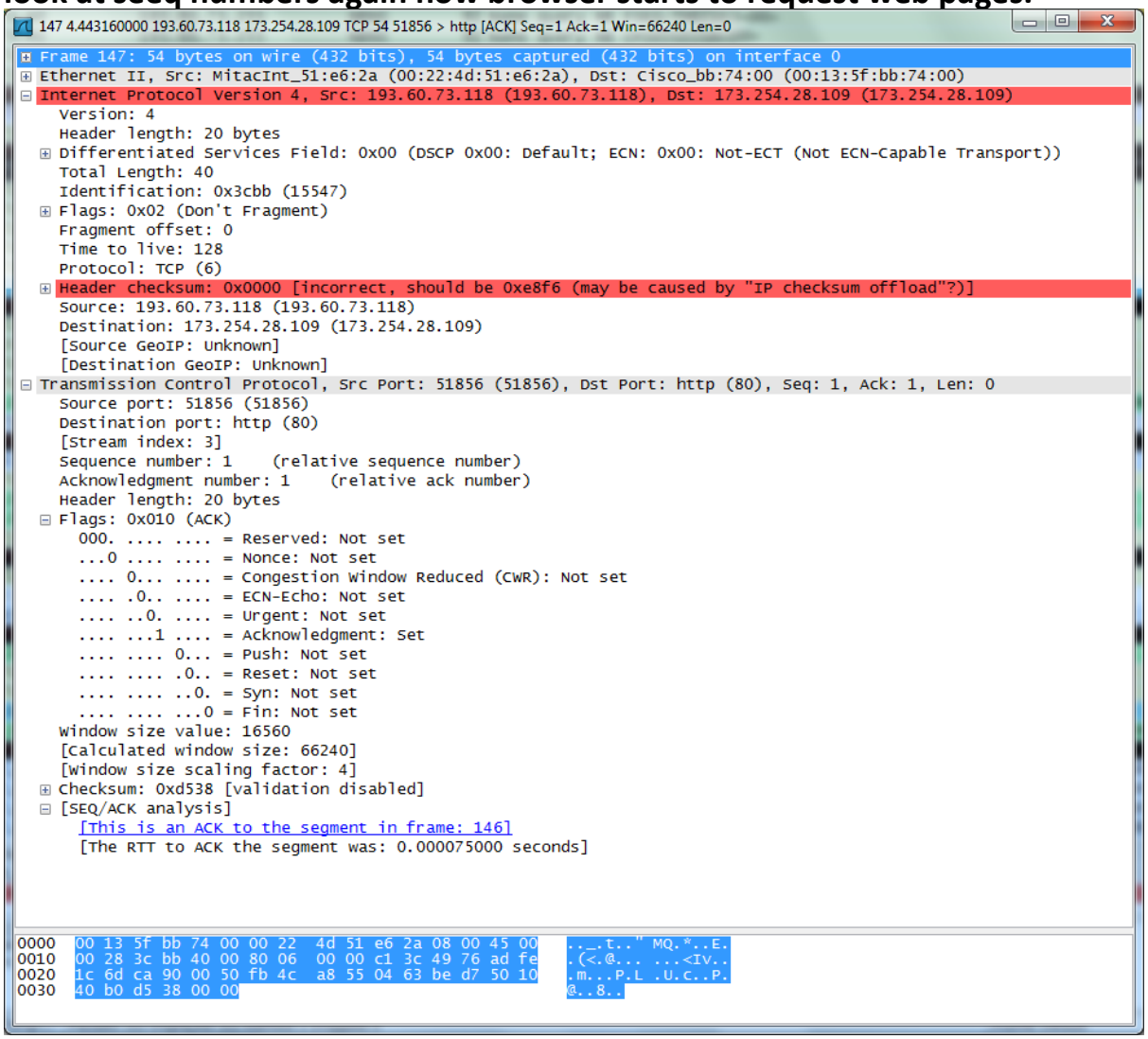
Start of 3 way handshake. (Sequence number: 0 (relative sequence number))



Syn + Ack, sent from server.

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

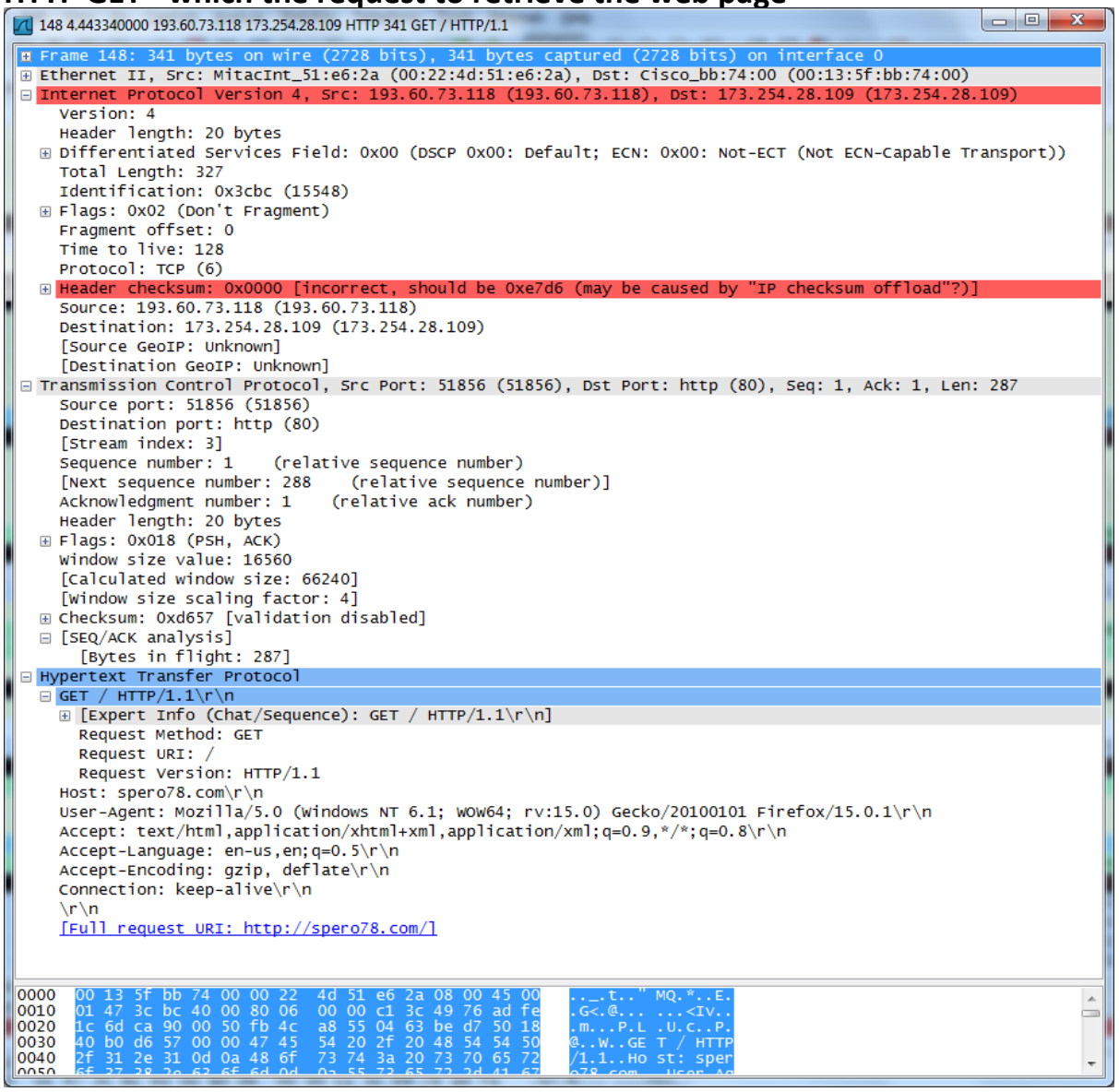
HTTP - TCP Acknowledgement to server (port 80) (SYN bit = 1, ACK bit = 1) - look at seeq numbers again now browser starts to request web pages.



Ack sent from client to server.

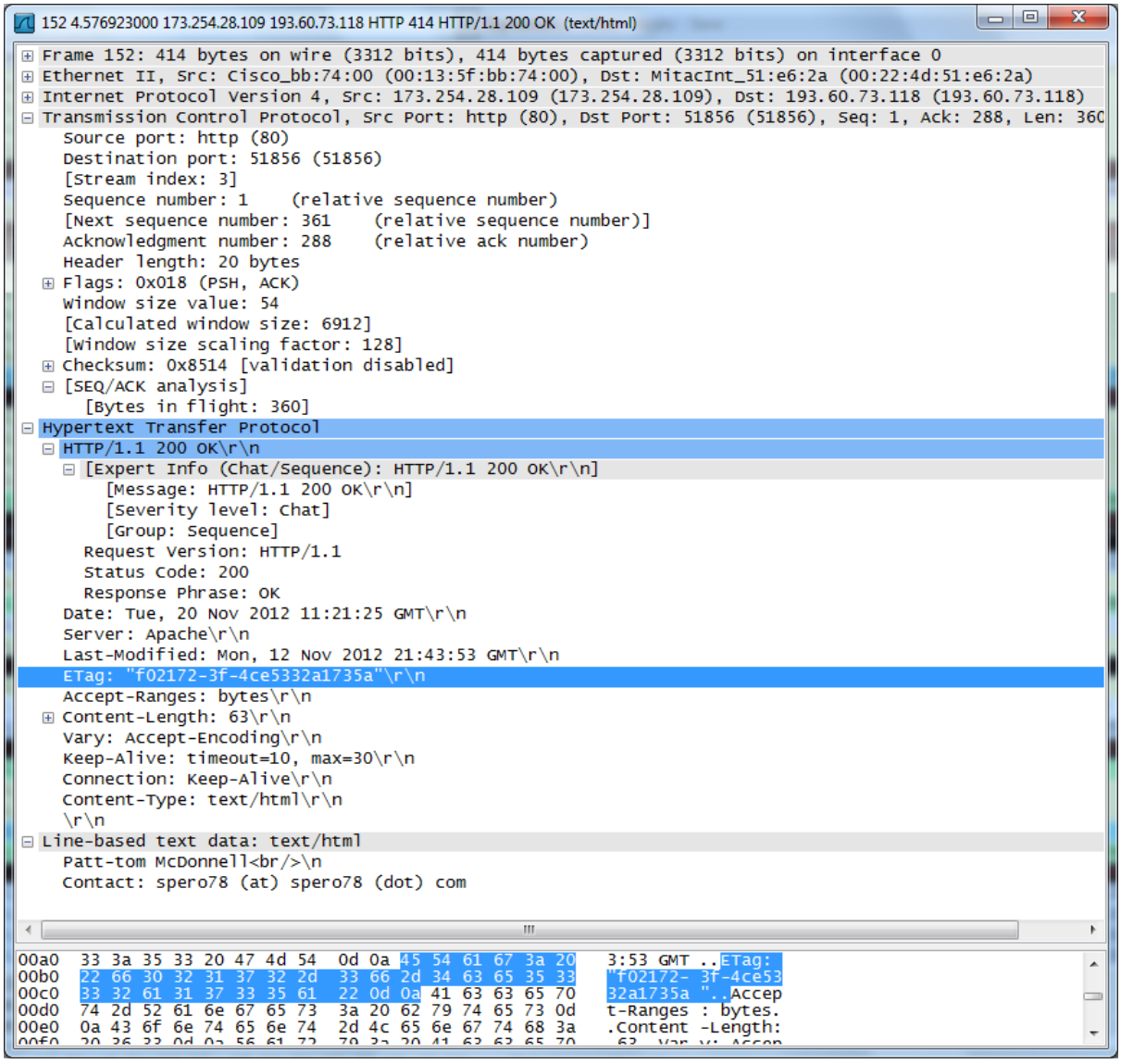
3rd part of 3 way handshake. (Sequence number: 1 (relative sequence number))

HTTP GET - which the request to retrieve the web page



GET request to server.

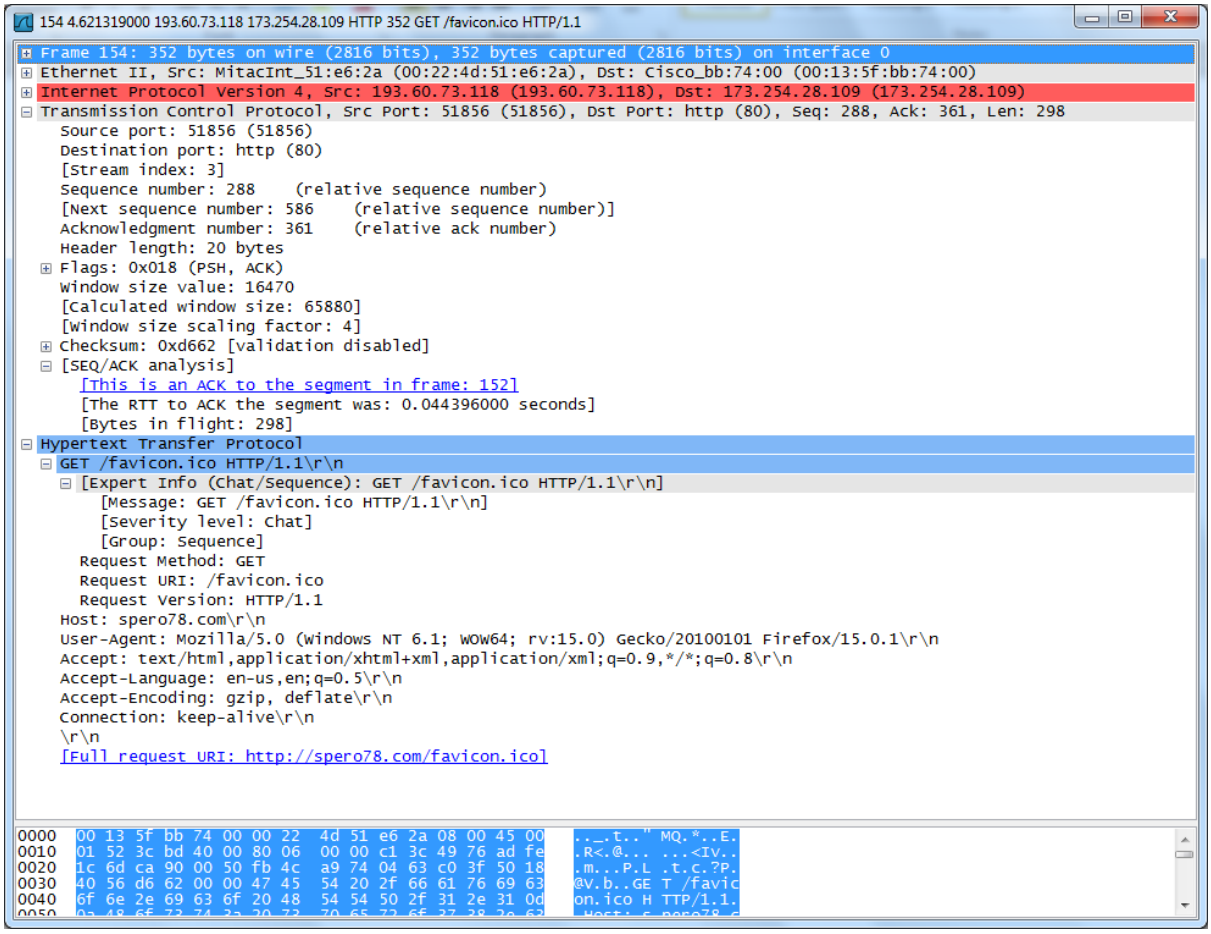
HTTP returned with data - this will be the header for the web page



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

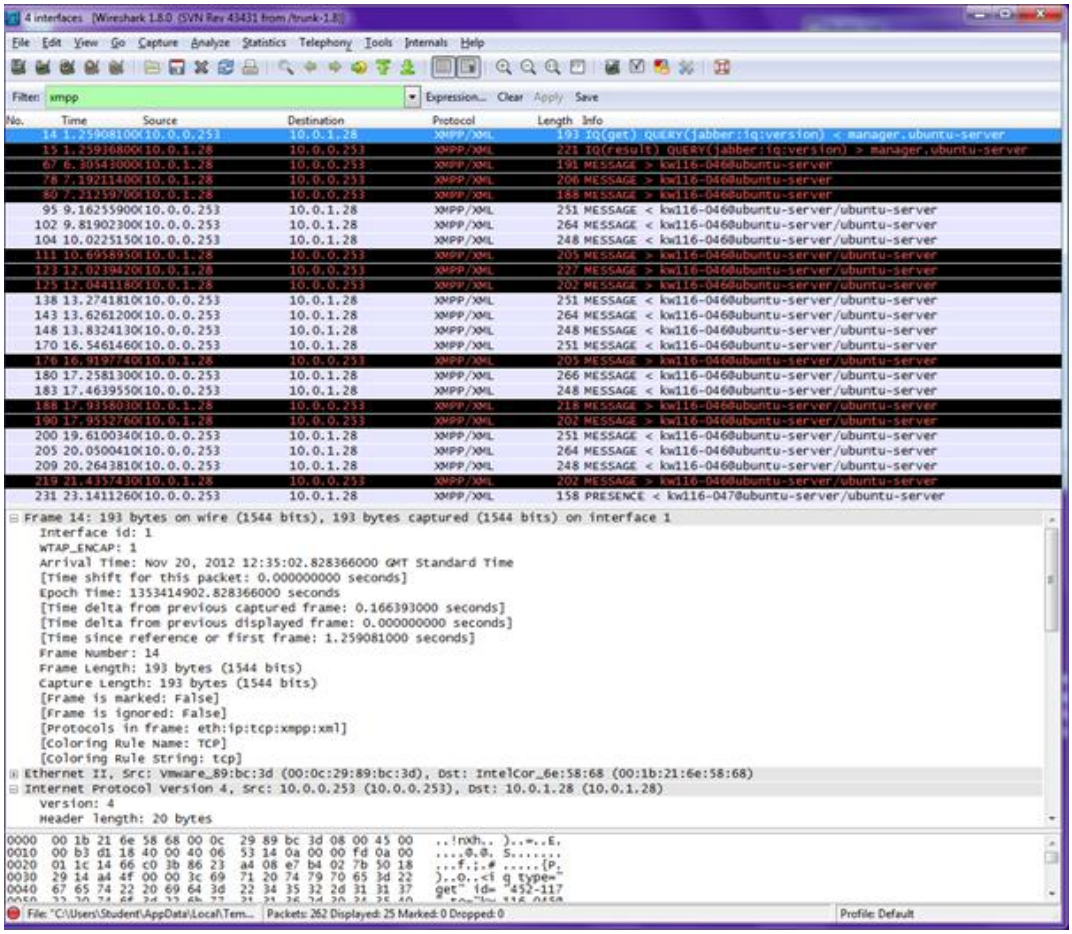
What ports are involved in the Chat messaging?

Chat is sent from: 49178
Chat is received and listens on :5222

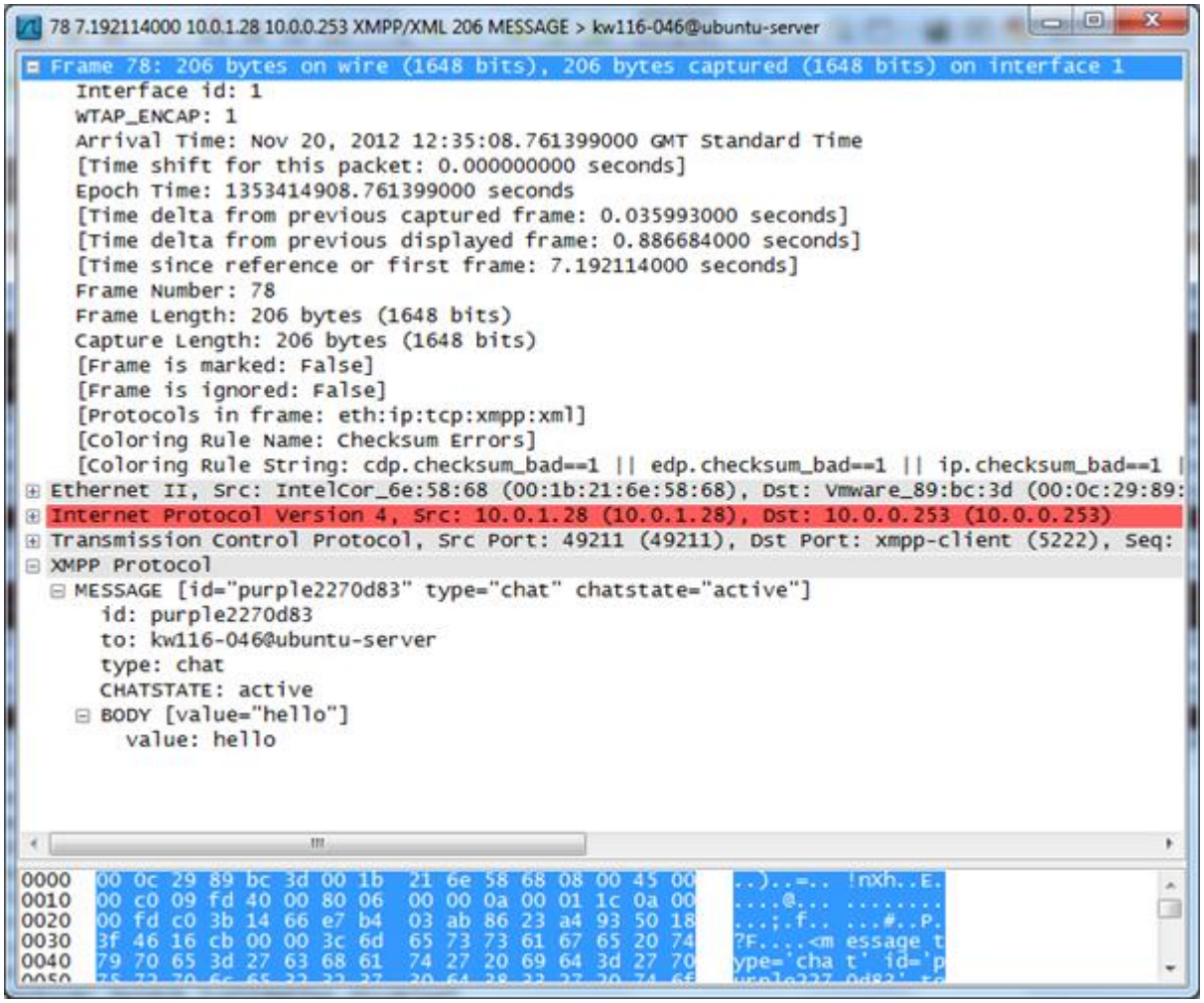
What else can you find out about the protocol?

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:



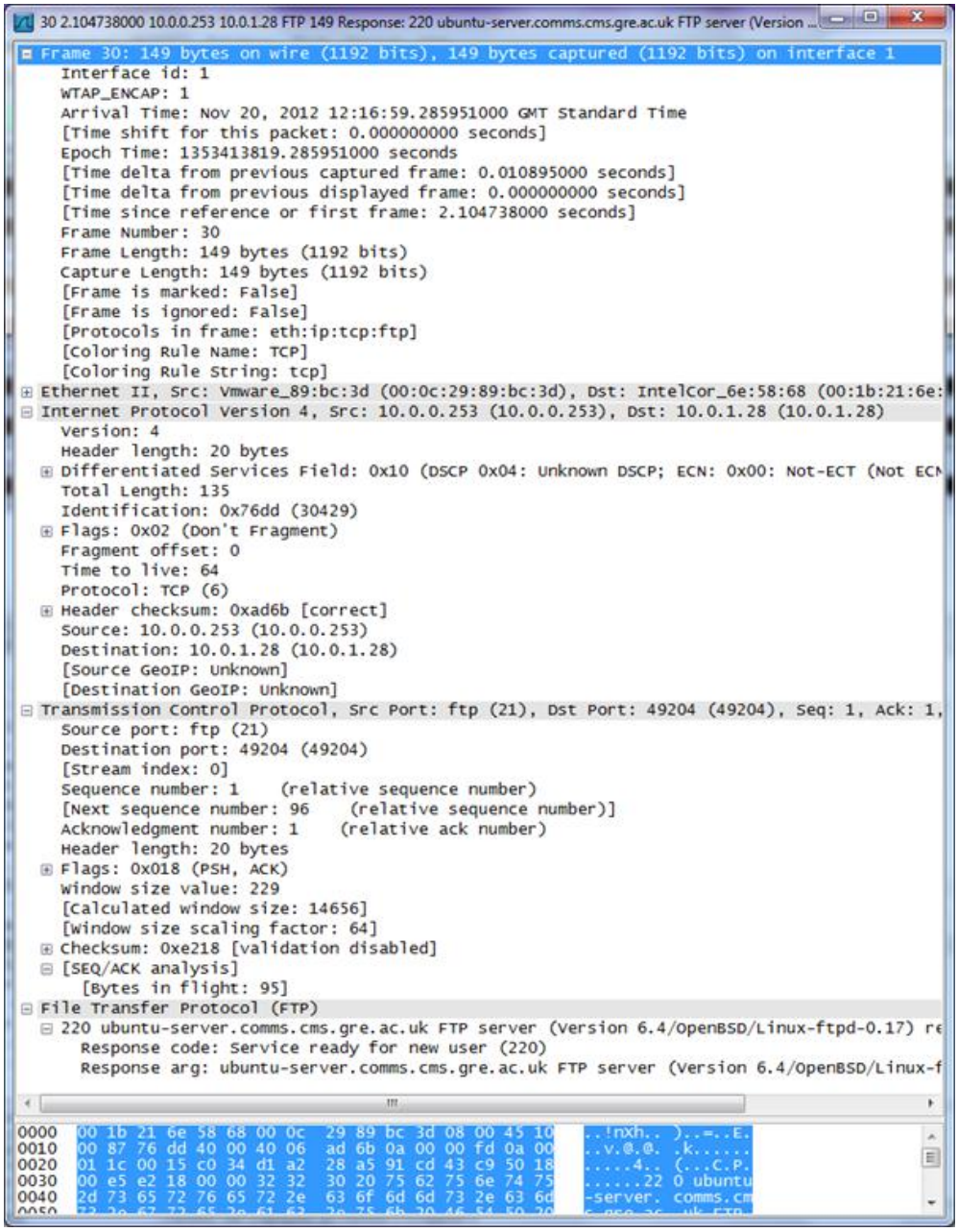
Here you can see the message that was sent in the packet.



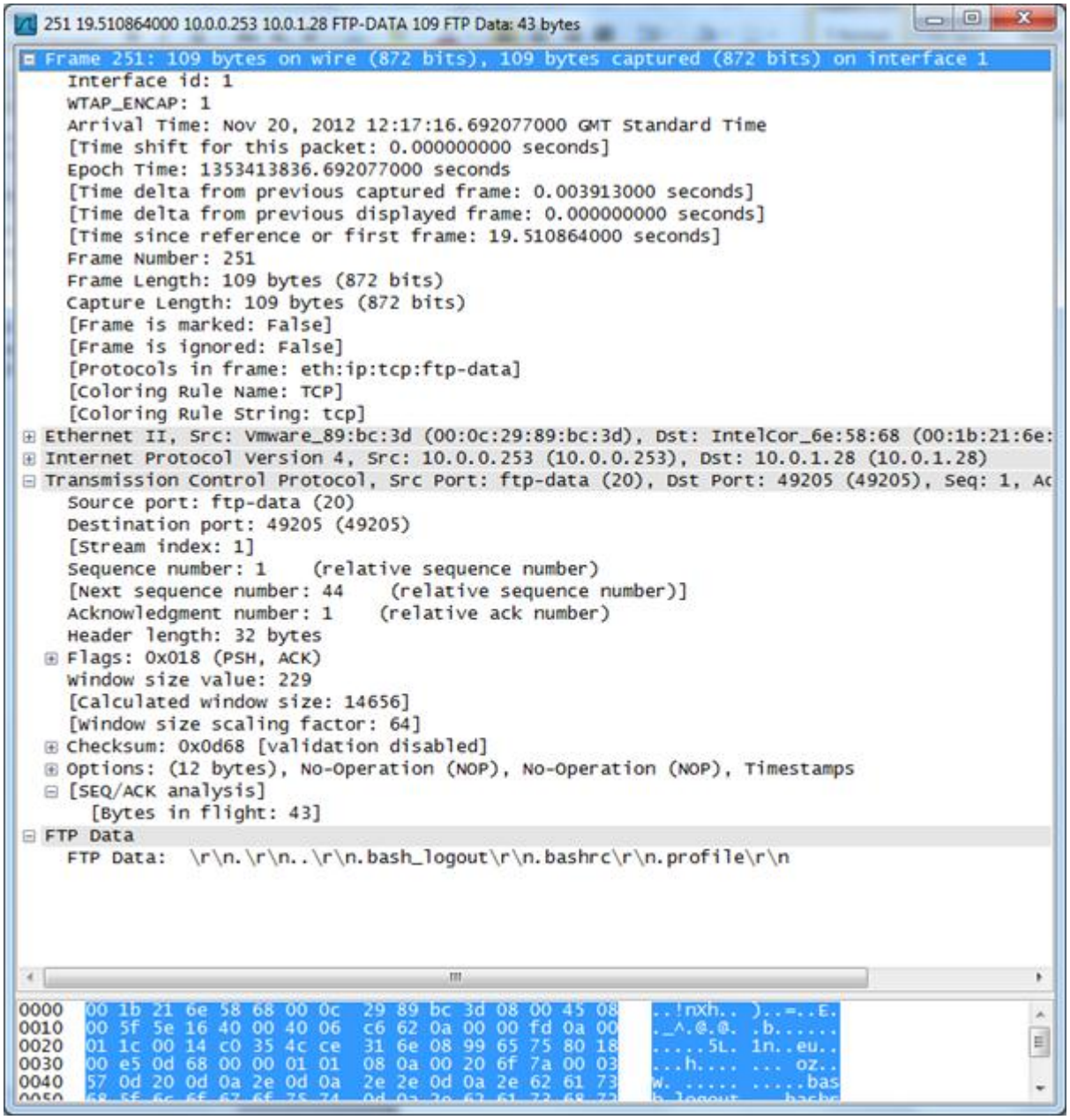
TASK 3: Capture an FTP Session

What messages did you receive?

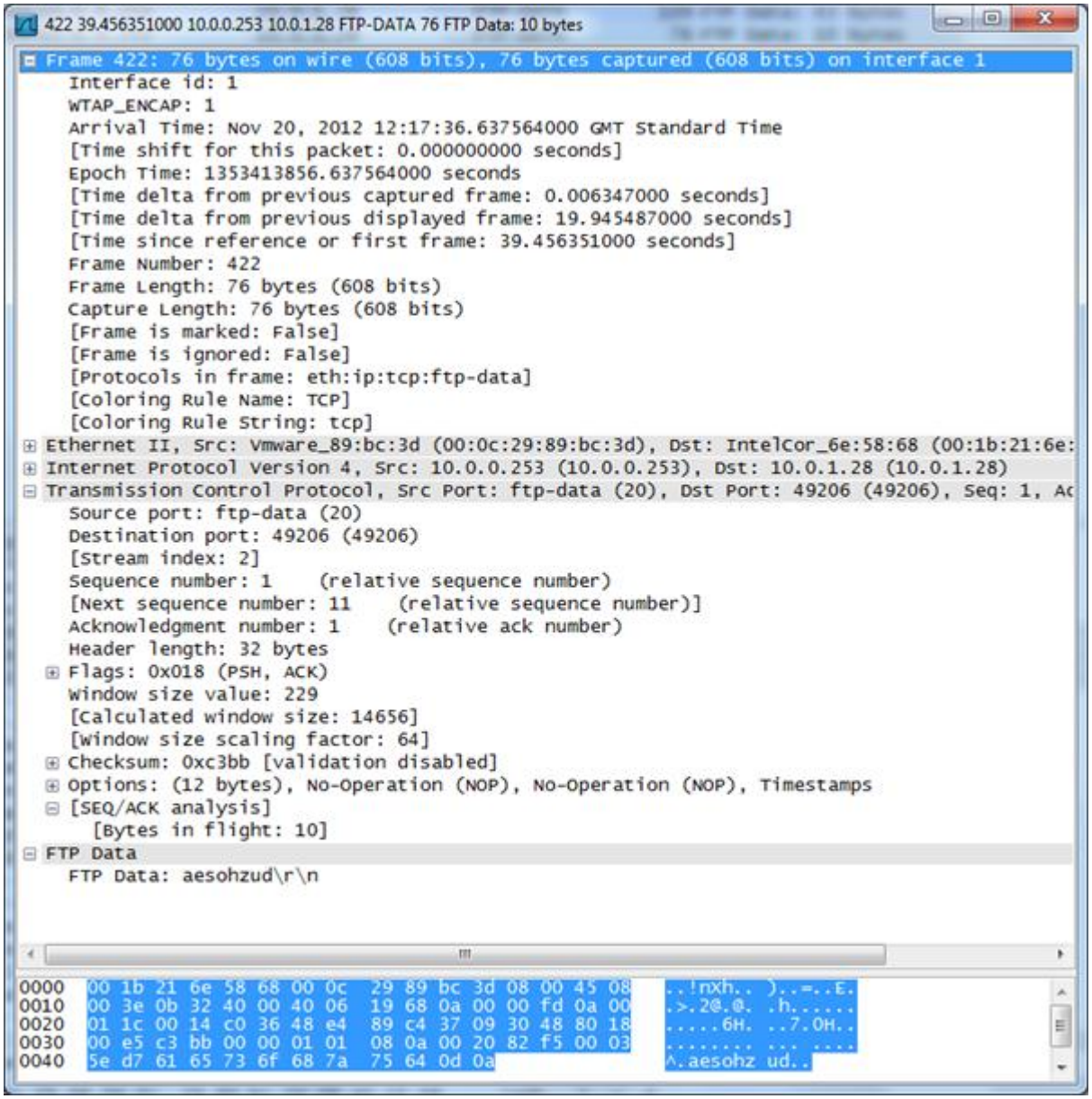
Server identification
A password request
Welcome message
File message



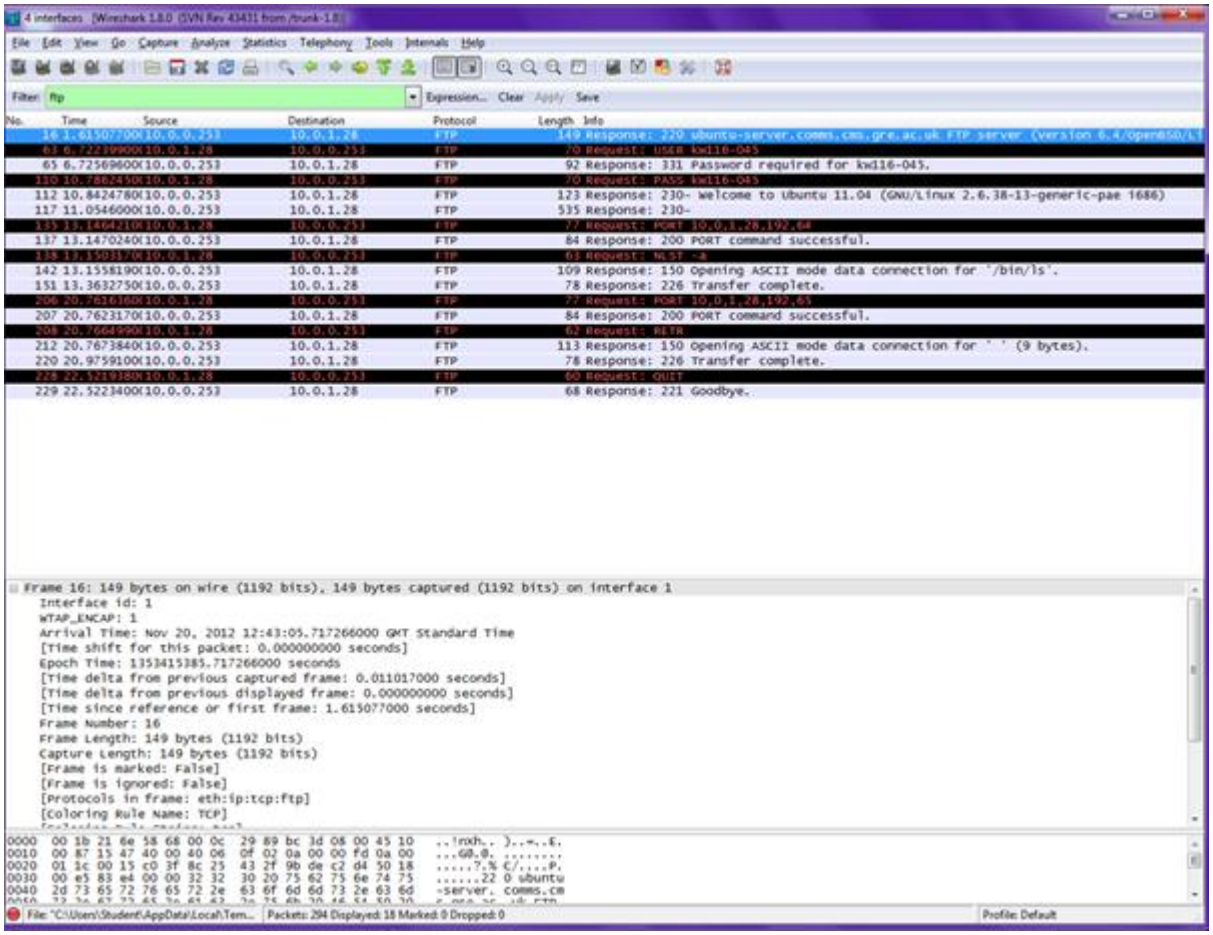
Server Identification.



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



File transfer response, ASCII Data transferred clearly visible.



FTP Messages