School of Computer Science and Cybersecurity

CUC

Lab Report #

|  |  |
| --- | --- |
| Lab Name | Wireshark Lab4:IP |
| Course Name | Computer Networks |

|  |  |  |  |
| --- | --- | --- | --- |
| Name | 赵婧宇 | Student ID | 201711123028 |

|  |  |
| --- | --- |
| Partners |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Date | 2019.06.12 | Lab Location | #48 |

|  |
| --- |
| Notes： |

**Section I Introduction**

Prepares the reader to understand the whole experiment.

|  |  |
| --- | --- |
| **Must Have:**  1. Clearly stated purpose of the experiment  2. Important background and/or theory | **May include:**  1. Description of specialized equipment  2. Justification of experiment's importance |

In this lab, we’ll investigate the IP protocol, focusing on the IP datagram. We’ll do so by analyzing a trace of IP datagrams sent and received by an execution of the traceroute program (the traceroute program itself is explored in more detail in the Wireshark ICMP lab). We’ll investigate the various fields in the IP datagram, and study IP fragmentation in detail.

**Section II Methods & Materials**

Can be lists or even "refer to lab manual" where appropriate.

**Section III Procedure & Results**

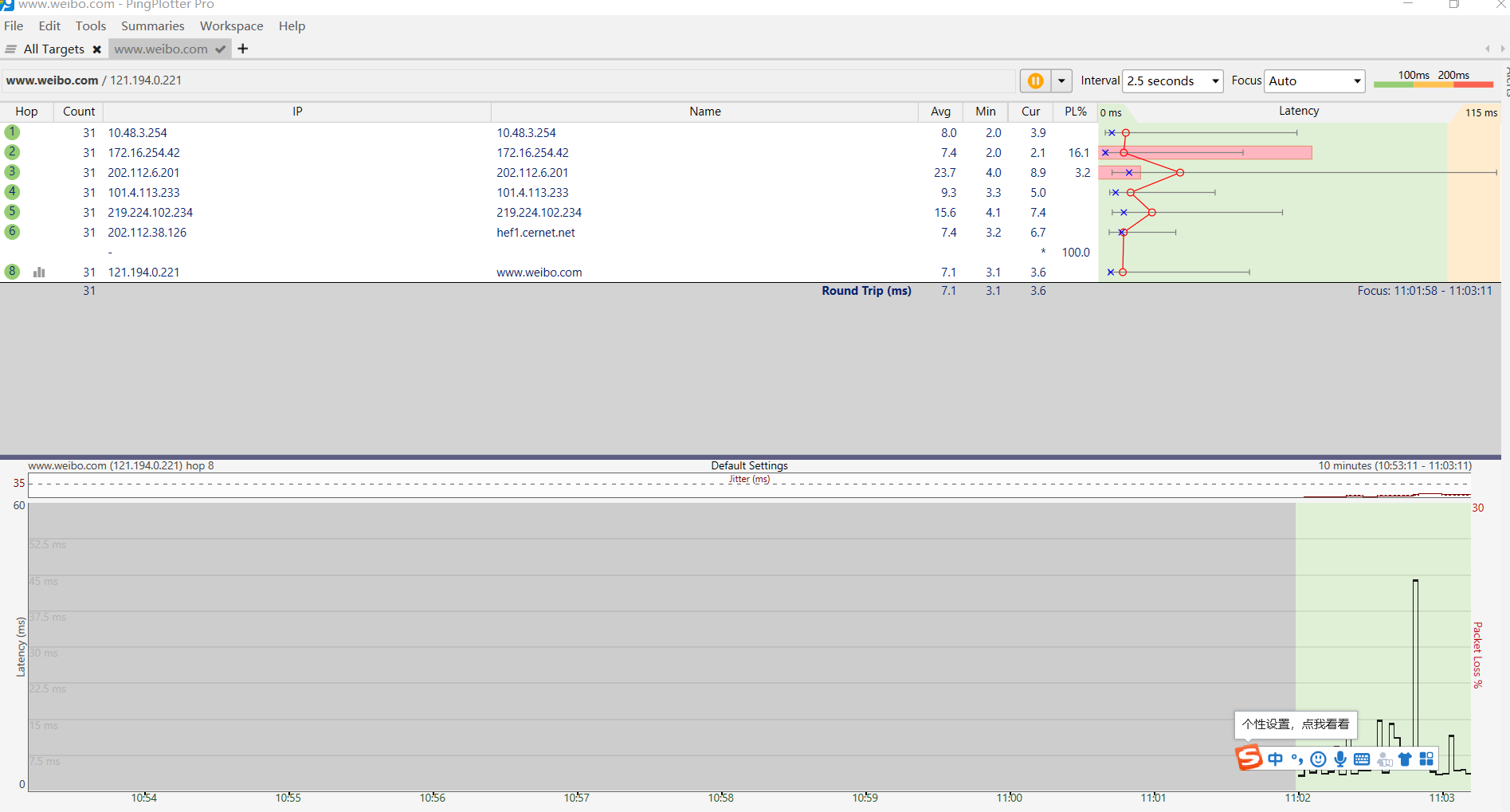
Describes ACTUAL process, especially changes from planned method.

|  |
| --- |
| * **number** and **title** tables and graphs correctly and clearly * draw attention to key points in tables or graphs with a sentence * provide sample calculation only * state key result in sentence form |

1. Capturing packets from an execution of traceroute

Start up Wireshark and begin packet capture (Capture->Start) and then press OK on the Wireshark Packet Capture Options screen (we’ll not need to select any options here).

If you are using a Windows platform, start up pingplotter and enter the name of a target destination in the “Address to Trace Window.” Enter 3 in the “# of times to Trace” field, so you don’t gather too much data. Select the menu item Edit >Advanced Options->Packet Options and enter a value of 56 in the Packet Size field and then press OK. Then press the Trace button. You should see a pingplotter window that looks something like this:

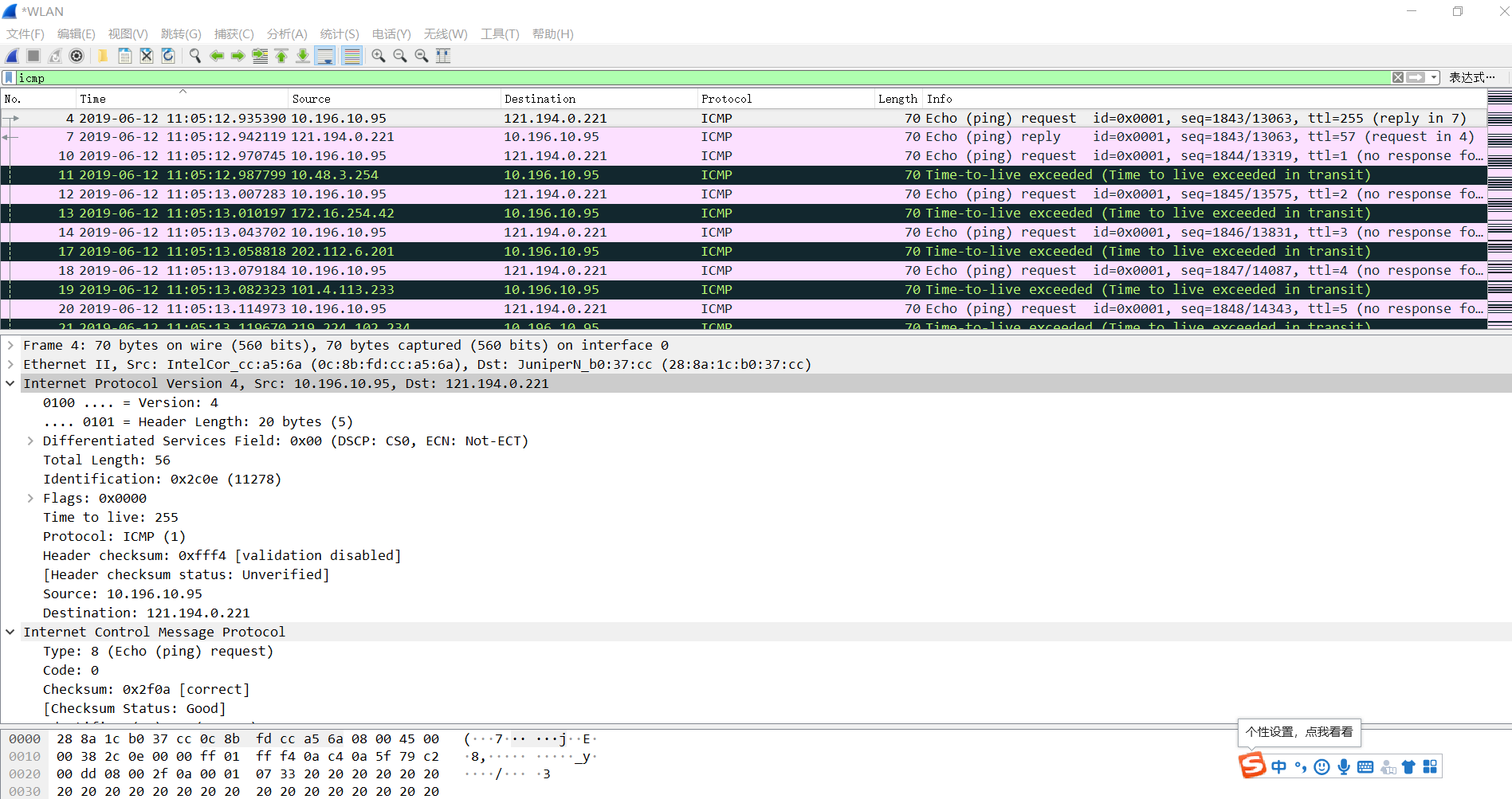


Finally, send a set of datagrams with a longer length, by selecting Edit>Advanced Options->Packet Options and enter a value of 3500 in the Packet Size field and then press OK. Then press the Resume button.

Stop Wireshark tracing.

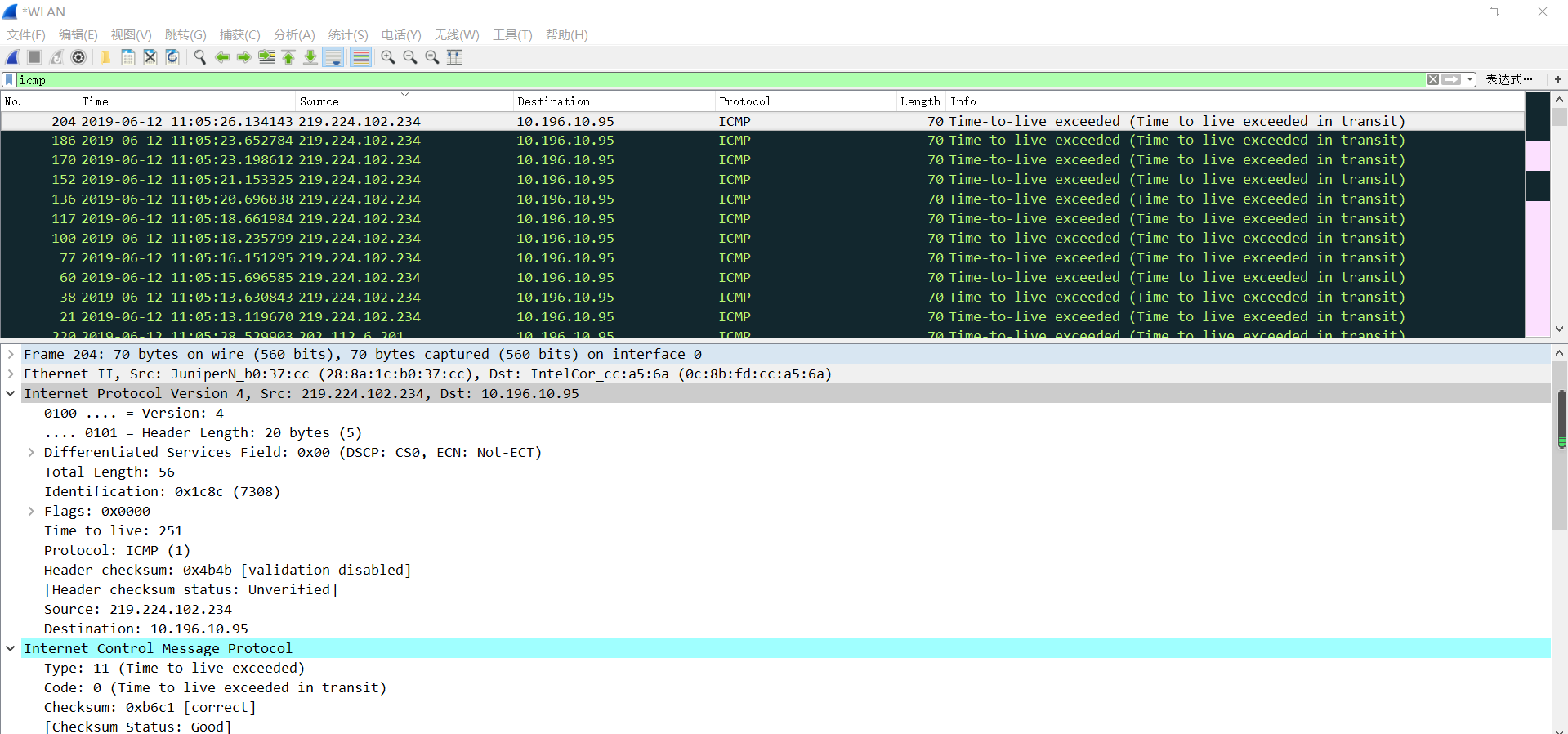
1. A look at the captured trace

Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.



Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again.

Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by your computer.



Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

Sort the packet listing according to time again by clicking on the Time column.

Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

**Section IV Discussion**

Answer the questions in the section [what to hand in] of the lab guide, includes two aspects:

|  |
| --- |
| 1. What is the IP address of your computer?  10.196.10.95  2. Within the IP packet header, what is the value in the upper layer protocol field?    3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.  IP header: 20 bytes  The payload of the IP datagram: 56-20=36bytes  Total length-Header length= the number of payload bytes  4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.  No, it hasn’t. Both Flags and Fragment offset are 0  5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?  Answer: TTL, head checksum, identity and so on are constantly changing  6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?  Answer: stay constant: Version number, header length, service type, Identification, offset, upper layer protocol, destination and source IP address.  Must stay constant: Version number, source and destination IP address  Must change: Identification, header checksum  7. Describe the pattern you see in the values in the Identification field of the IP datagram.  Answer: Each IP datagram header has a different identifier field, one at a time  8. What is the value in the Identification field and the TTL field?  Answer: The Identification field: 11278  The TTL field:255  9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why? |
| 10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? [If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.1]  Answer: Yes  11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?  Answer:  10. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?  Answer: 520-20=500 bytes  11. What fields change in the IP header between the first and second fragment?  Answer: Total length, Flags, Fragment offset, Head checksum and so on.  12. How many fragments were created from the original datagram?  Answer:3  13. What fields change in the IP header among the fragments?  Answer: Total length, Flags, Fragment offset, Head checksum and so on. |

**Section V Conclusion**

States what is known as a result of the experiment.

|  |  |
| --- | --- |
| **Must do:**  1. State what's known  2. Justify that statement | **May do:**  1. State significance of findings  2. Suggest further research |

Through experiments, IP datagram is analyzed in detail