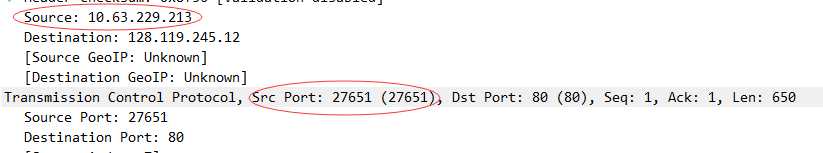
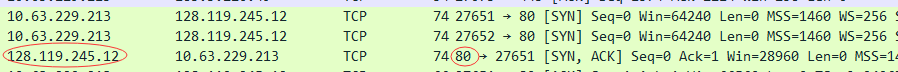
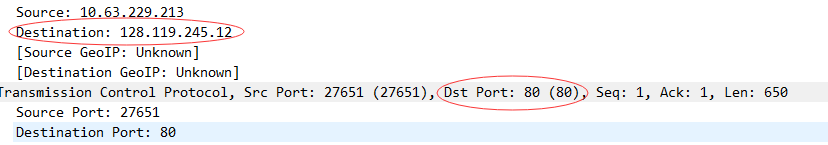
1. TCP
2. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to gaia.cs.umass.edu? To answer this question, it’s probably easiest to select an HTTP message and explore the details of the TCP packet used to carry this HTTP message, using the “details of the selected packet header window” (refer to Figure 2 in the “Getting Started with Wireshark” Lab if you’re uncertain about the Wireshark windows.

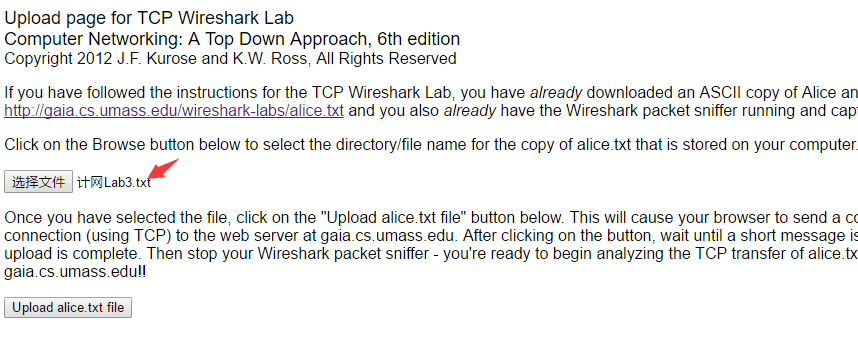


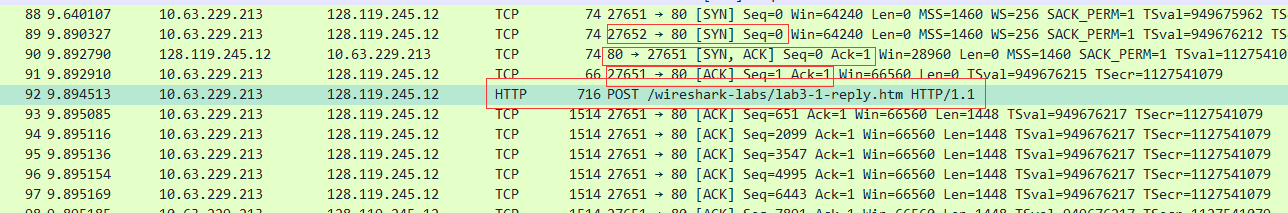


1. What is the IP address of gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection

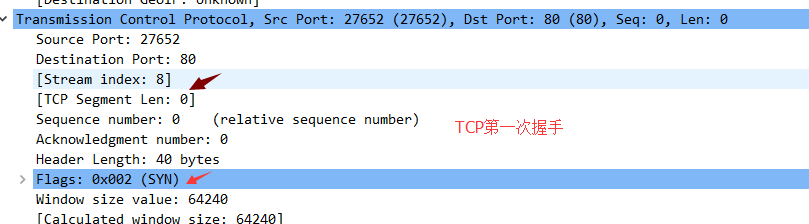




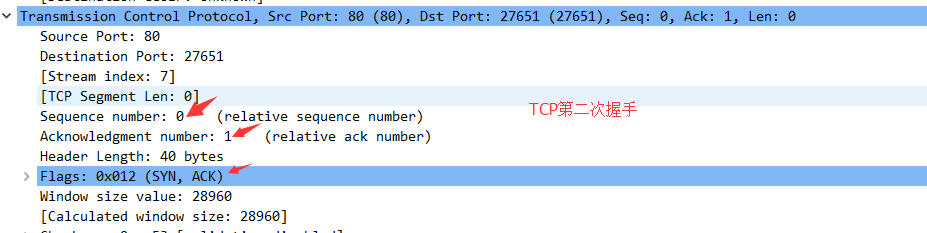


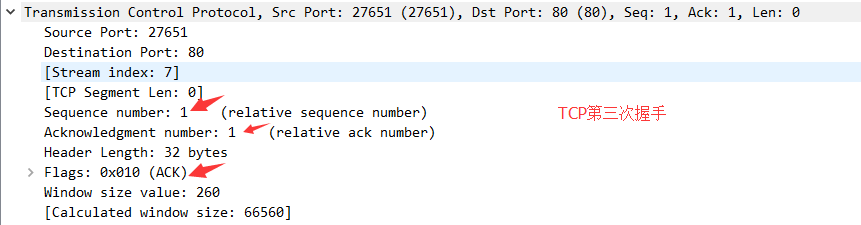


4. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu? What is it in the segment that identifies the segment as a SYN segment?

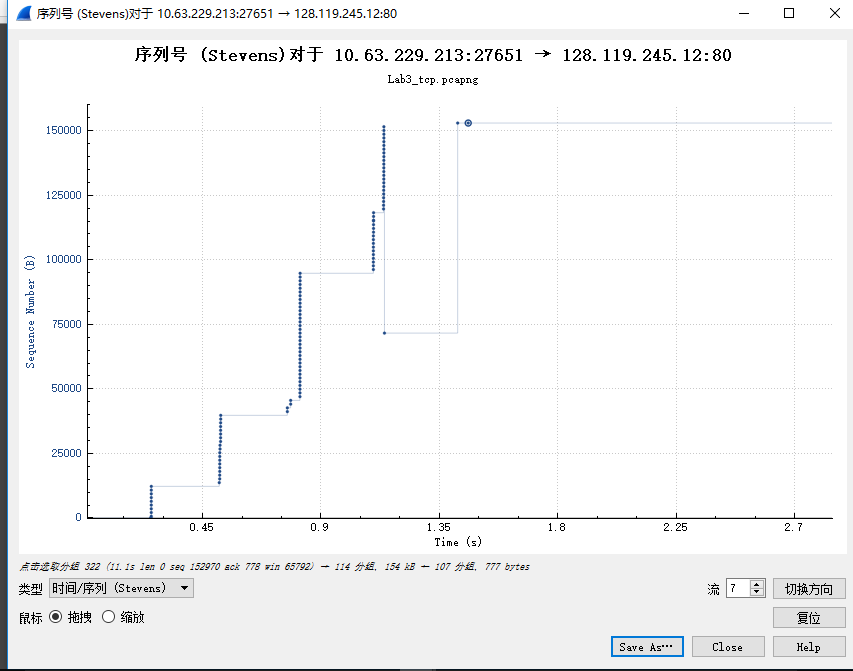


5.What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?





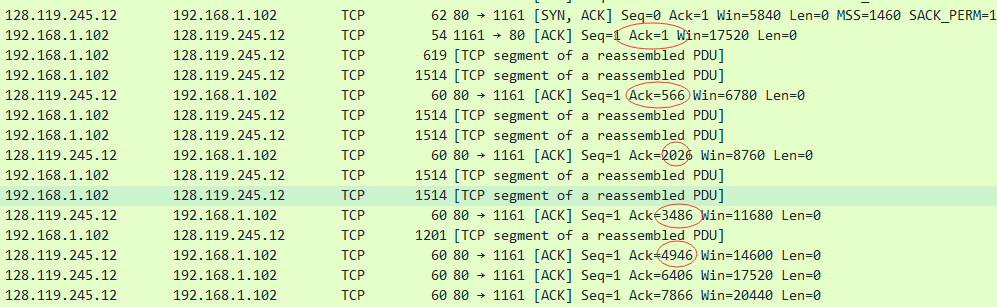
TCP控制

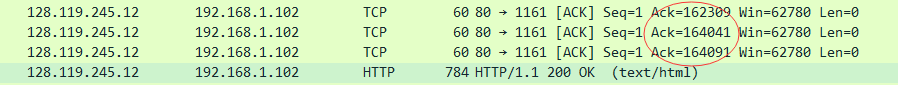


8. What is the length of each of the first six TCP segments?4

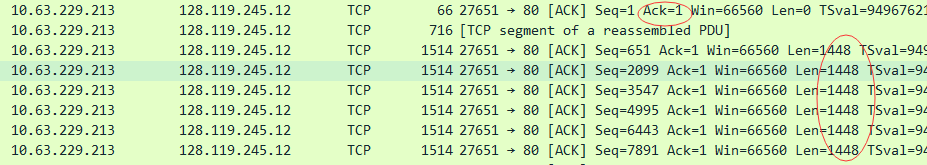
9. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

13. Use the Time-Sequence-Graph(Stevens) plotting tool to view the sequence number versus time plot of segments being sent from the client to the gaia.cs.umass.edu server. Can you identify where TCP’s slowstart phase begins and ends, and where congestion avoidance takes over? Comment on ways in which the measured data differs from the idealized behavior of TCP that we’ve studied in the text.

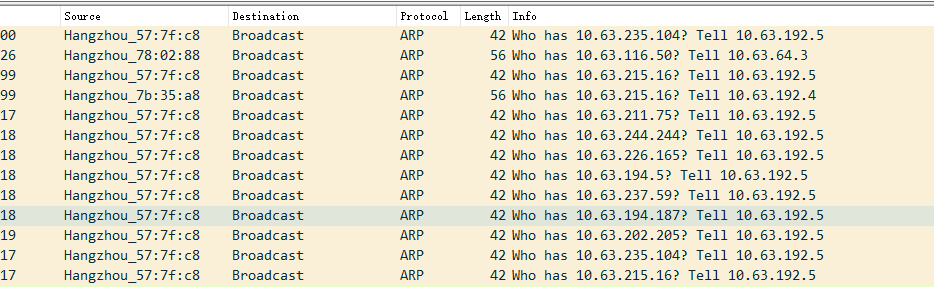


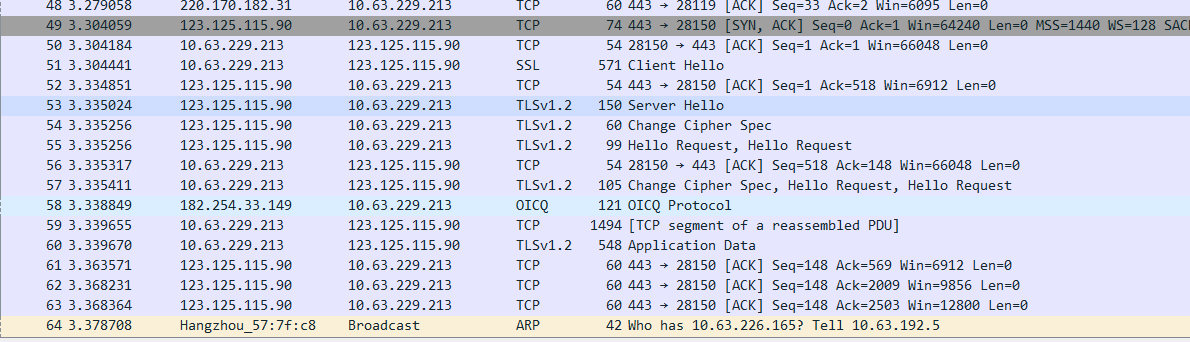


我所捕获的分组



ARP：



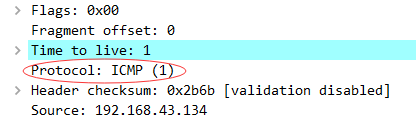


IP

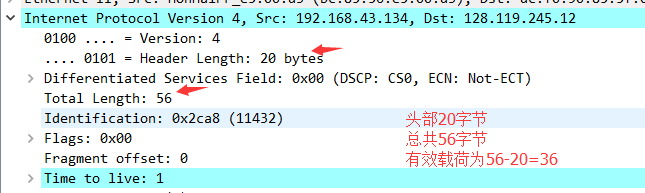
1. What is the IP address of your computer?



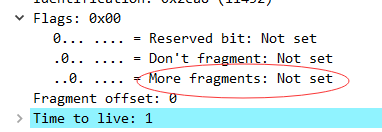
1. Within the IP packet header, what is the value in the upper layer protocol field?



1. 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



1. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented



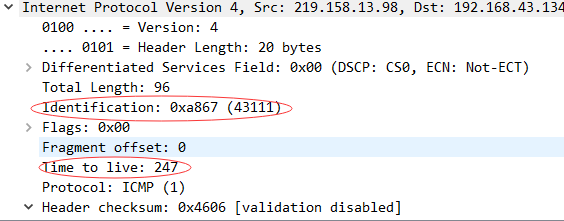
1. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
2. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

必须改变的：Identification(标识)、Header checksum(头部检验和)

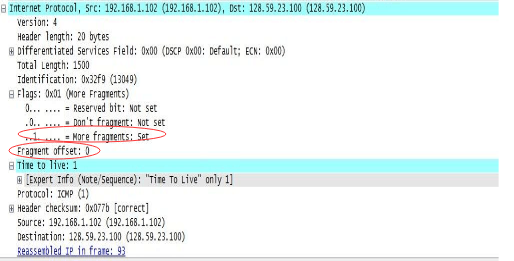
标识是源主机赋予IP数据报的标识符、头部校验和用于保证IP数据报报头的完整性。

必须保持不变的：Version(版本)、Header length(头部长度)、Differentiated Services  Field(区分服务)、Flags(标记)、Fragment offset(片偏移)、Protocol(协议)、 Destination(目地地址)

8.What is the value in the Identification field and the TTL field?



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?



该消息传送多于一个IP数据包的分段，More fragment被置为1；Fragment offset：0，说明为第一个片段；Total length:1500。第二个片段Total length:548, 两个片段总长度相加为2048 bytes，减去IP头部20 bytes，等于2028 bytes

13. What fields change in the IP header between the first and second fragment

Total length、Flags中的More fragment、Fragment offset、Header checksum改变

14. How many fragments were created from the original datagram?

15. What fields change in the IP header among the fragments?

ARP

Write down the contents of your computer’s ARP cache. What is the meaning of each column value?

