Prelab2

1. - 200 OK: The request is processed successfully.
   - 201 Created: The request has been completed and a new resource has been created.
   - 301 Moved Permanently: The requested resource has been permanently moved to a new URL.
   - 404 Not found: The server cannot find the requested resource.
   - 500 Internal Server Error: A general error message, given when an unexpected condition is encountered and no more specific message applies.
2. - GET - retrieve information from the server using the given URI
   - HEAD - Retrieves only the headers of the HTTP request/response
   - POST - Submits an entity to be processed by the resource identified by the URI
   - PUT - replaces all current representations of the target resource with the uploaded content
   - DELETE - deletes the specified resource
   - CONNECT - Establishes a network connection to the web server and returns the response in a way that can be used as a tunnel
   - OPTIONS - describes the communication options for the target resource
   - TRACE - Performs a message loopback test along the path to the target resource
3. (Example) If we want to get the last modification date of www.example.com, we can enter "wget --server-response --spider http://example.com 2>&1 | grep -i Last-Modified" to achieve this purpose.
4. When all the commands are typed in, it starts playing the Star Wars clip that gives the ASCII pretensions.
5. A DNS resource record (RR) is a database record that maps a domain name to an IP address or other information about the domain. It contains information about various aspects of a domain such as its name servers, mail servers, and IP addresses. After I entered the corresponding command, I saw

Server: 10.211.55.1
Address: 10.211.55.1#53

ucsc.edu mail exchanger = 5 alt2.aspmx.l.google.com
ucsc.edu mail exchanger = 5 alt1.aspmx.l.google.com
ucsc.edu mail exchanger = 1 aspmx.l.google.com
ucsc.edu mail exchanger = 10 alt3.aspmx.l.google.com
ucsc.edu mail exchanger = 10 alt4.aspmx.l.google.com

According to the above two lines, the IP address of the DNS server used for this lookup is 10.211.55.1. Shown below are five mail exchange records. Mail will be sent to the server with the highest priority (1) first, if not available, it will be sent to the server with the second

highest priority (2), and so on up to 5.

6. The output is showed like that:
Server: 10.211.55.1
Address: 10.211.55.1#53

Non-authoritative answer:
.nameserver = m.root-servers.net.
.nameserver = j.root-servers.net.
.nameserver = g.root-servers.net.
.nameserver = h.root-servers.net.
.nameserver = i.root-servers.net.
.nameserver = a.root-servers.net.
.nameserver = d.root-servers.net.
.nameserver = f.root-servers.net.
.nameserver = c.root-servers.net.
.nameserver = l.root-servers.net.
.nameserver = e.root-servers.net.
.nameserver = k.root-servers.net.
.nameserver = b.root-servers.net.

Anthoritative answers can be found from:

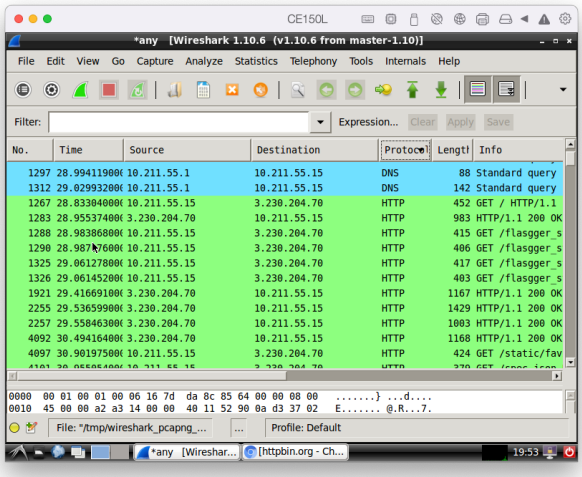
Command ″nslookup -type=ns″. Performs a DNS lookup to the authoritative name server (NS) for the root domain of the DNS hierarchy (indicated by a dot ″.″ in the command). The output of this command shows the root domain′s nameservers, which are listed as non-authoritative answers. These name servers are operated by various organizations, maintain information about top-level domains (such as .com, .org, .net, etc.), and delegate DNS resolution to the respective authoritative name servers. Each non-authoritative answer line shows the name of the root nameserver, preceded by a dot (″.″) to indicate that it is a fully qualified domain name. The order in which the nameservers are listed is not important. The line ″Authoritative answers can be found from:″ indicates that if the command is run with a domain name other than ″.″, the output will include any authoritative nameservers for that domain.

7. A host′s IP address is unique, but it also has many ports. The number is different for each port running different content. This can be used for identification.

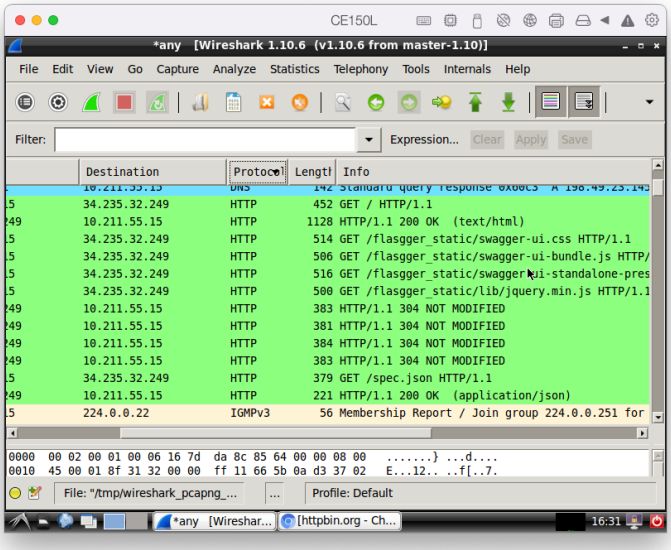
8. The purpose of the windowing mechanism in TCP is to manage the flow of packets between two computers or network hosts. It uses a sliding window protocol to alleviate the problem of clients and servers trying to share data segments that are either too large or too small to transmit efficiently.

9. MTU stands for Maximum Transmission Unit and it is a measurement representing the largest data packet that a network-connected device will accept1. When a packet is larger than the MTU, a device will break the packet into smaller fragments.

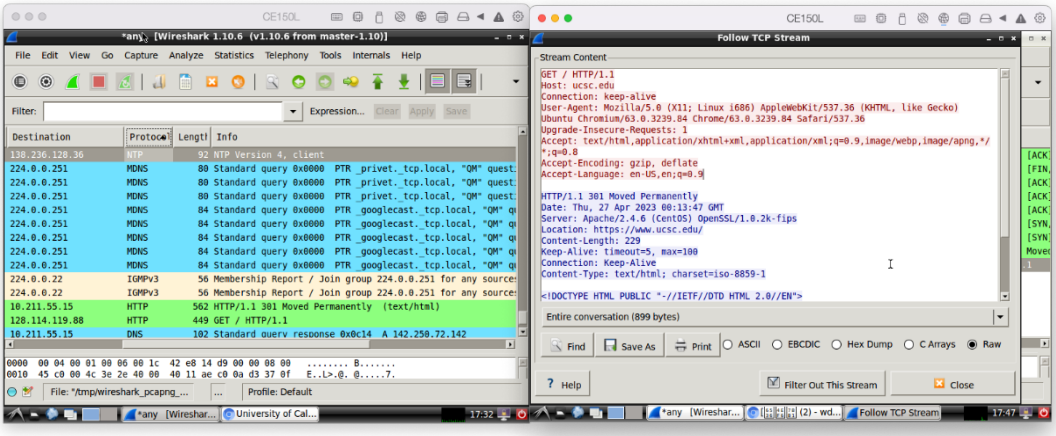
Lab2



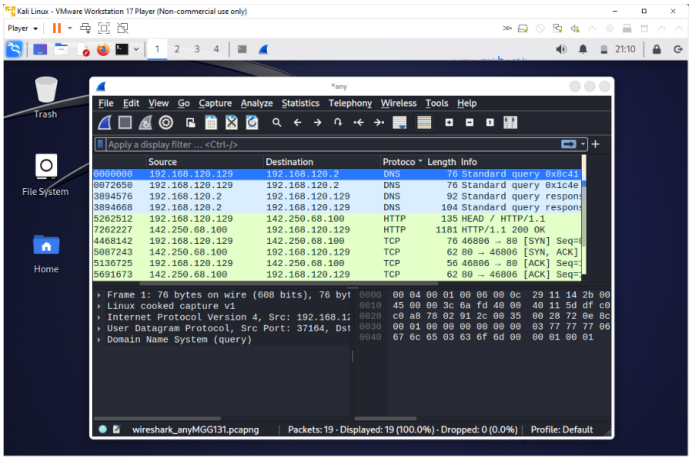
1. The request used by my computer is GET. (The above is the screenshot corresponding to the first question).



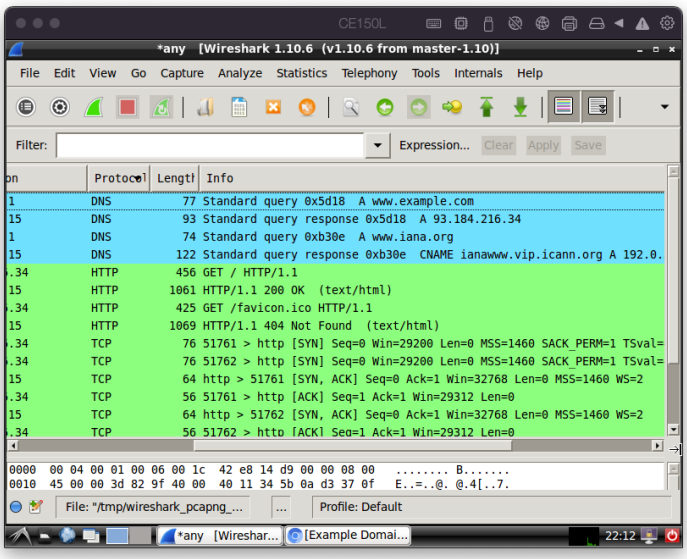
2. According to the picture I cut above, the corresponding HTTP code is 200. The content is of type (text/html).



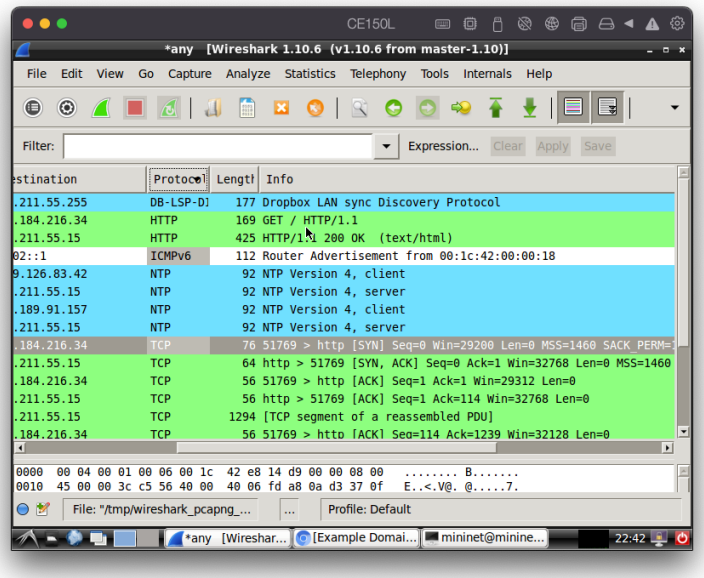
3. After I followed the TCP stream, I found that the URL and location of the two HTTP packets are not the same. Since the content to be accessed has been transferred to a new URL, the server returns 301 as the HTTP code. At the same time, the request was transferred to the new URL (that is, http://www.ucsc.edu).



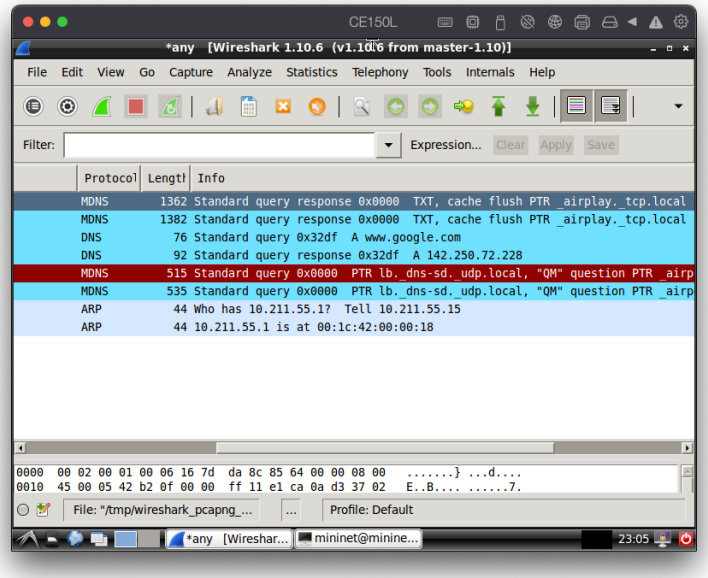
4. Since I couldn't install the curl command on the virtual machine suggested by CSE 150, I did this on Kali Linux. I typed "curl -I https://www.google.com" in the terminal to send the HEAD command to Google's server. Meanwhile, I've been using wireshark for packet capture. According to the screenshot, there are two HTTP entries (request and reply). The requested method is HEAD.



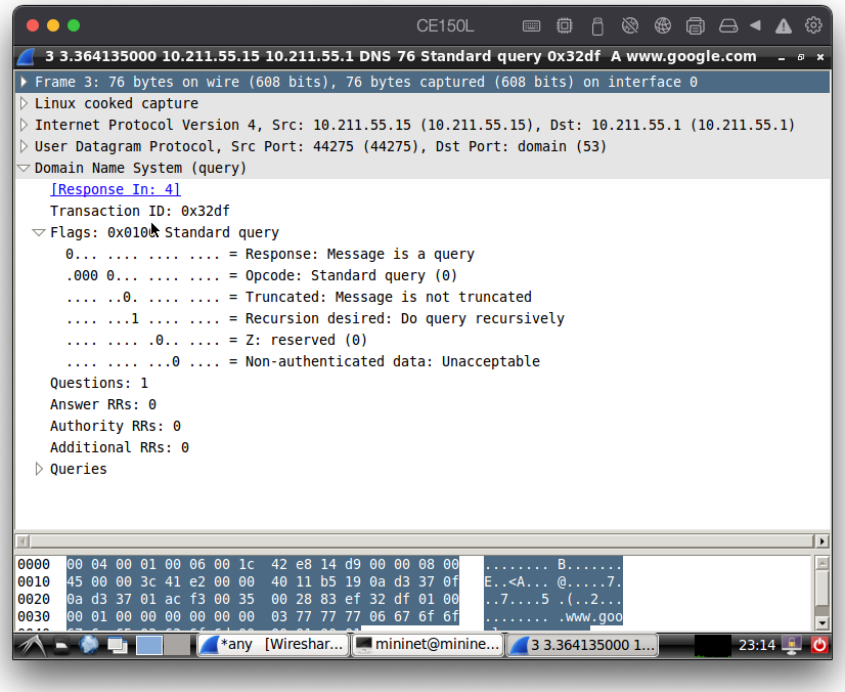
5. Before loading a web page, my computer performs a DNS query to resolve domain names to IP addresses. The DNS packets that help load www.example.com are the first and second in the screenshot. The first is a DNS request sent by my computer to resolve a website's IP address. The second is a DNS reply to my request. According to the above screenshot, the IP address of
www.example.com is 93.184.216.34.



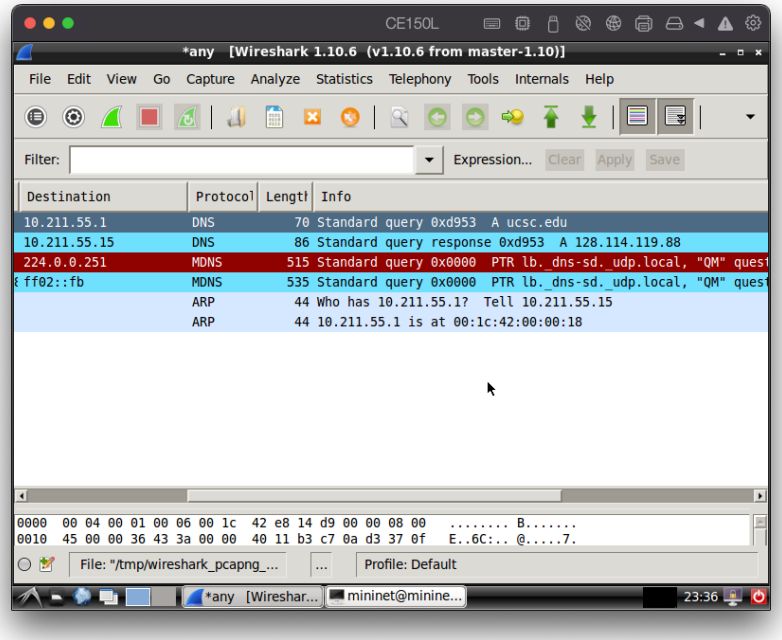
6. The command I use is "wget --header="Host: www.example.com" http://93.184.216.34". The screenshot includes two HTTP packets related to this. The reason I think they are related is because one of their destination or source is 93.184.216.34 (although it is not shown in the screenshot).



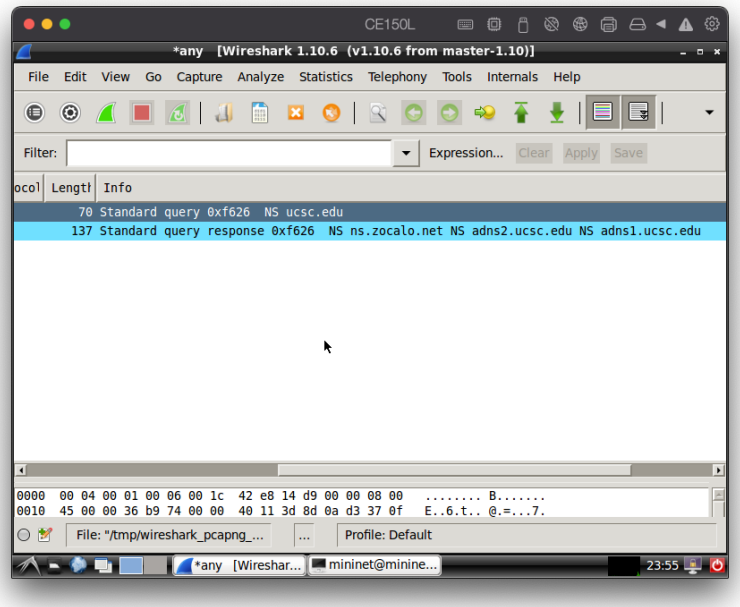
7. The screenshot required for the first sub-question is above. The IP address given for www.google.com is 142.250.72.228.



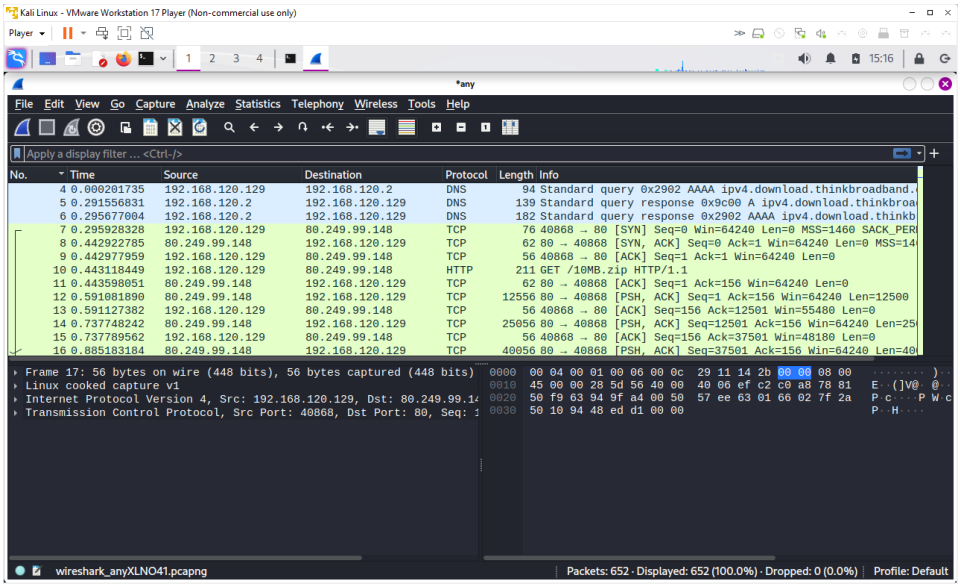
8. Yes, my computer wants to fulfill the request recursively. I know this is because the "Recursion Desired" flag is set to 1 in the DNS query packet.



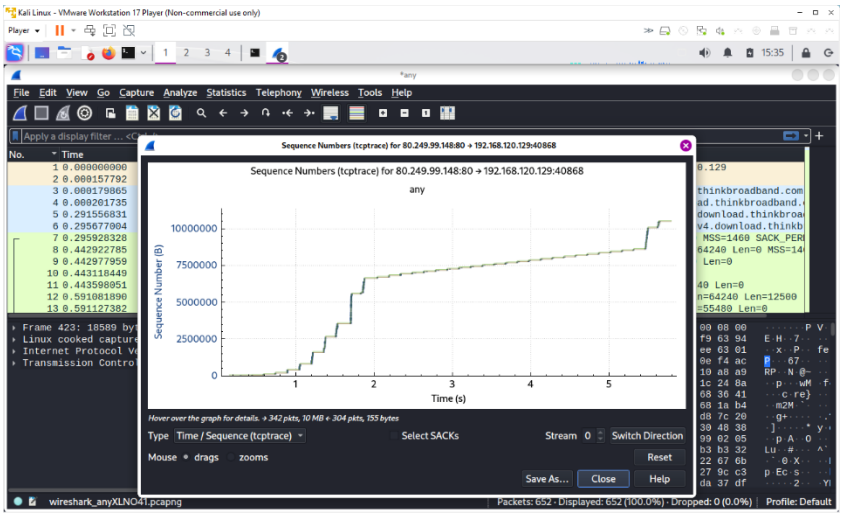
9. The screenshot is above. The IP address you were given for ucsc.edu is 128.114.119.88.



10. The authoritative name servers for the ucsc.edu domain are ns.zocalo.net, adns2.ucsc.edu, and adns1.ucsc.edu. I know this because I found this information in the DNS response packet in Wireshark when I ran the “nslookup -type=NS ucsc.edu” command.

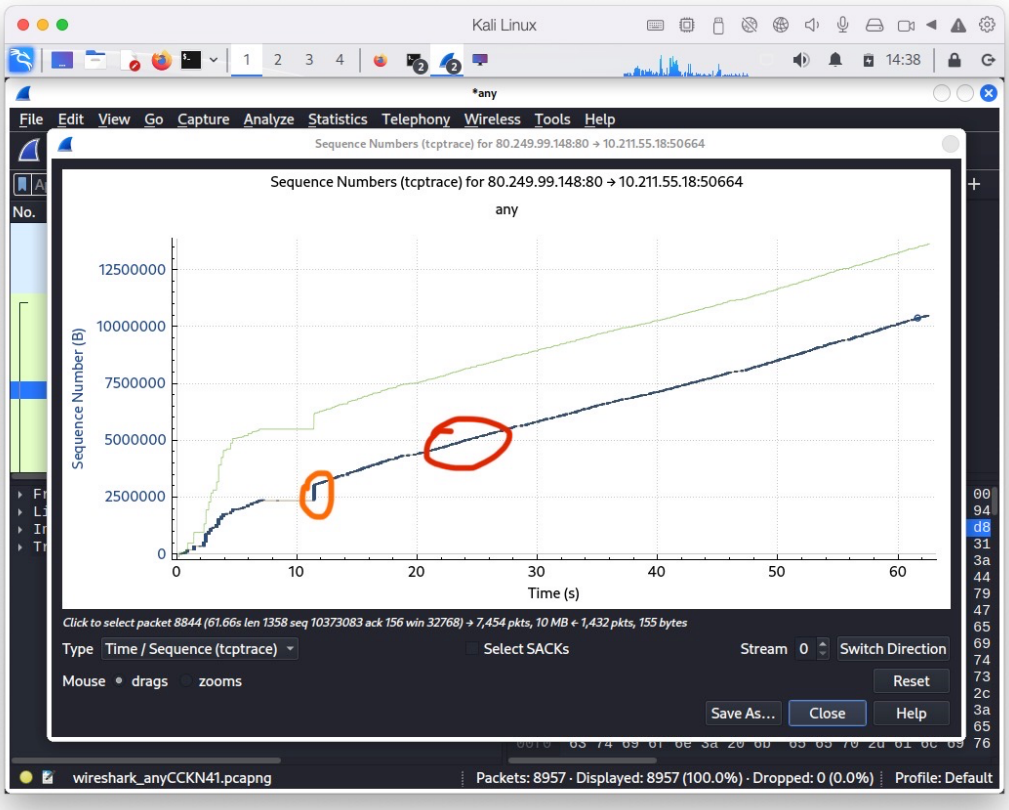


11. The entries have 7-9 labels are the three which initiated the TCP connection for this file transfer. According to package 7’s info, my initial windows size is 64240. According to the info of package 8, the server’s advertised window size is 64240.



12. The package I picked is number 12 (it is showed in the screenshot). This graph shows the behavior of a TCP connection over time. It uses some other packages including package

12. It is a visualization of the rate at which data is sent and acknowledged. It should be able to be used to determine the performance of TCP connections



13. This diagram basically introduces a TCP workflow. Under normal circumstances, there will be no intermediate level (this section is caused by manually increasing the packet loss rate). The orange part is the ″show 0%″ part (vertical). The red part is the ″slow start and congestion avoidance″ part (the slope is relatively stable).