Anarchy-R-Us, Inc. suspects that one of their employees, Ann Dercover, is really a secret agent working for their competitor. Ann has access to the company’s prize asset, the secret recipe. Security staff are worried that Ann may try to leak the company’s secret recipe.

Security staff have been monitoring Ann’s activity for some time, but haven’t found anything suspicious– until now. Today an unexpected laptop briefly appeared on the company wireless network. Staff hypothesize it may have been someone in the parking lot, because no strangers were seen in the building. Ann’s computer, (**192.168.1.158**) sent IMs over the wireless network to this computer. The rogue laptop disappeared shortly thereafter.

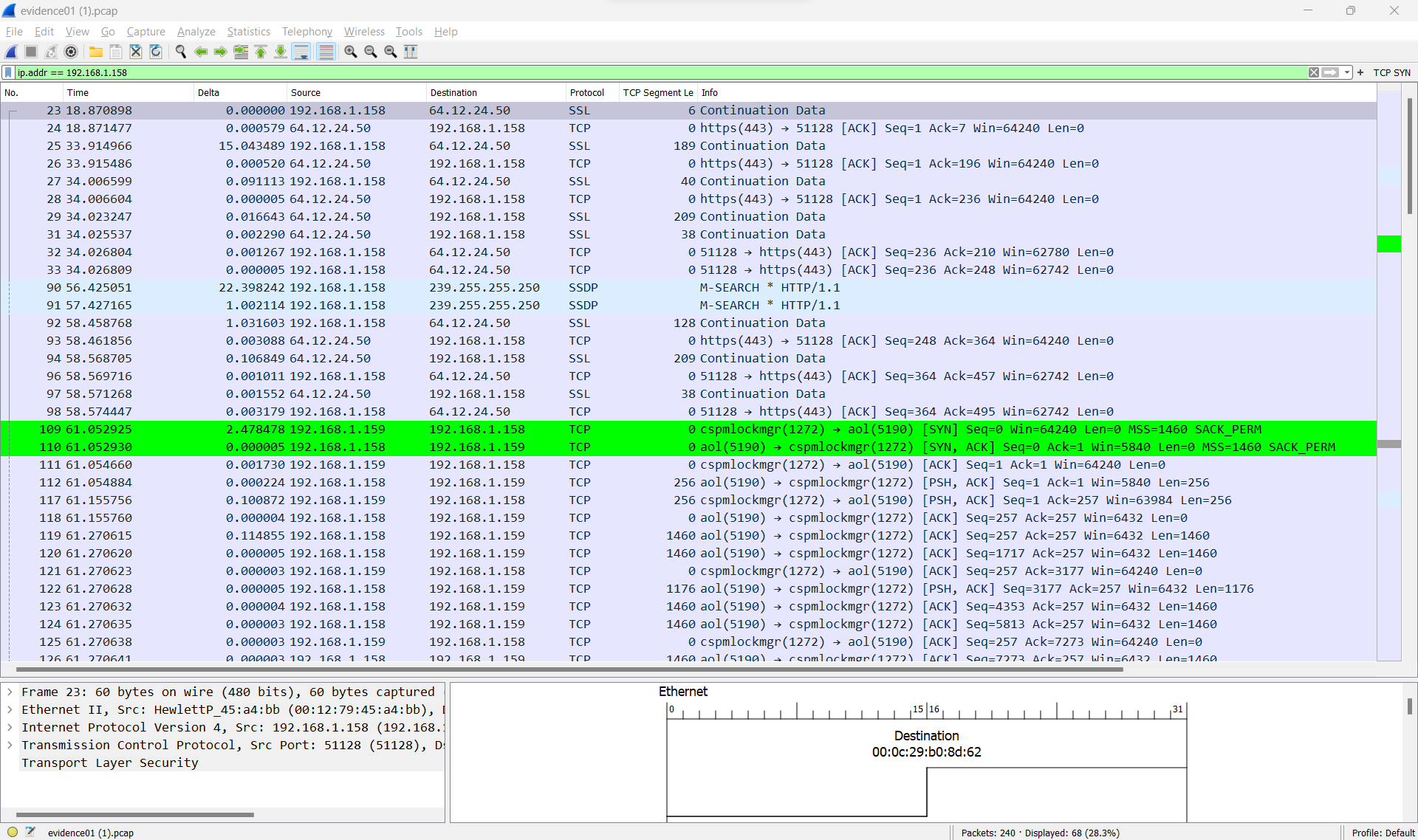
“We have a [packet capture](https://forensicscontest.com/contest01/evidence01.pcap) of the activity,” said security staff, “but we can’t figure out what’s going on. Can you help?”

You are the forensic investigator. Your mission is to figure out who Ann was IM-ing, what she sent, and recover evidence including:

1. What is the name of Ann’s IM buddy?  
2. What was the first comment in the captured IM conversation?  
3. What is the name of the file Ann transferred?  
4. What is the magic number of the file you want to extract (first four bytes)?  
5. What was the MD5sum of the file?  
6. What is the secret recipe?

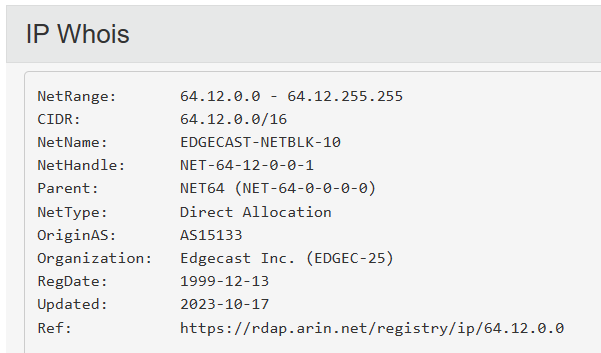
Step1) Filter out the IP address 192.168.1.158 using the following

ip.addr == 192.168.1.158



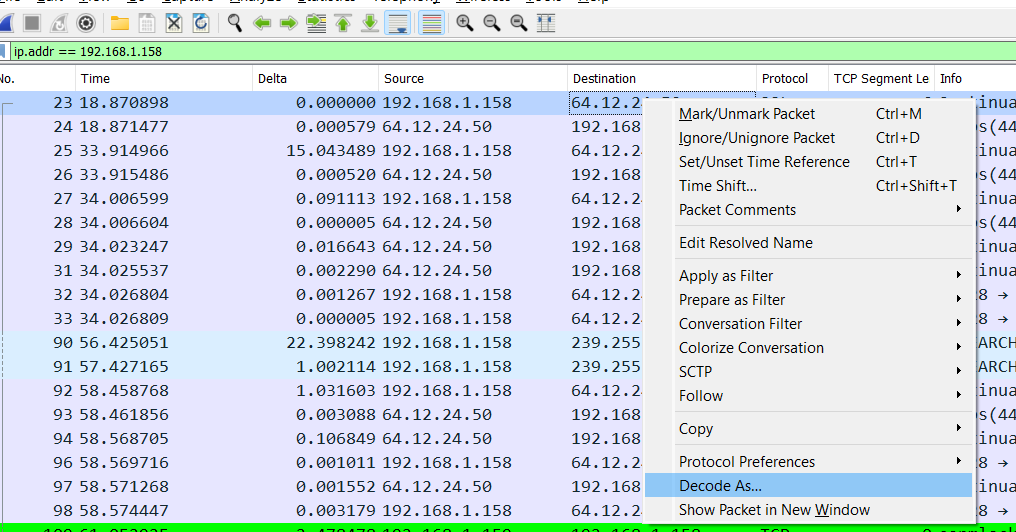
Step2) From the filter, I can see that the first ip address that interacted with 192.168.1.158 is 64.12.24.50 , it is public ip address

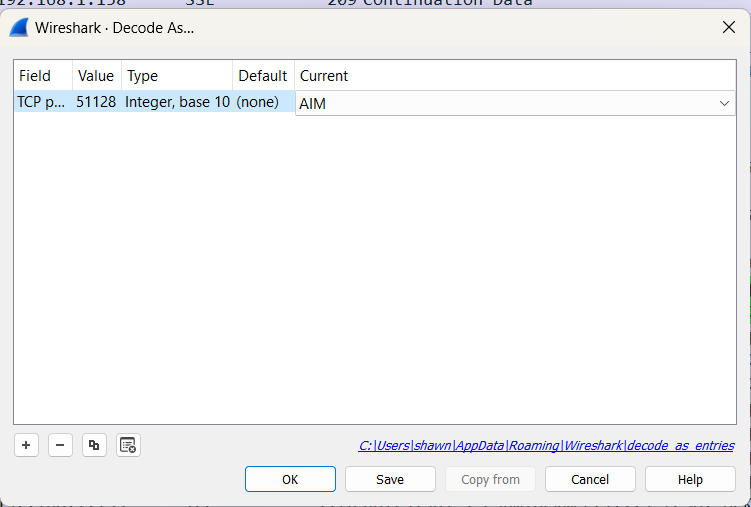
I will use who.is website to find out where does this ip address leads to.



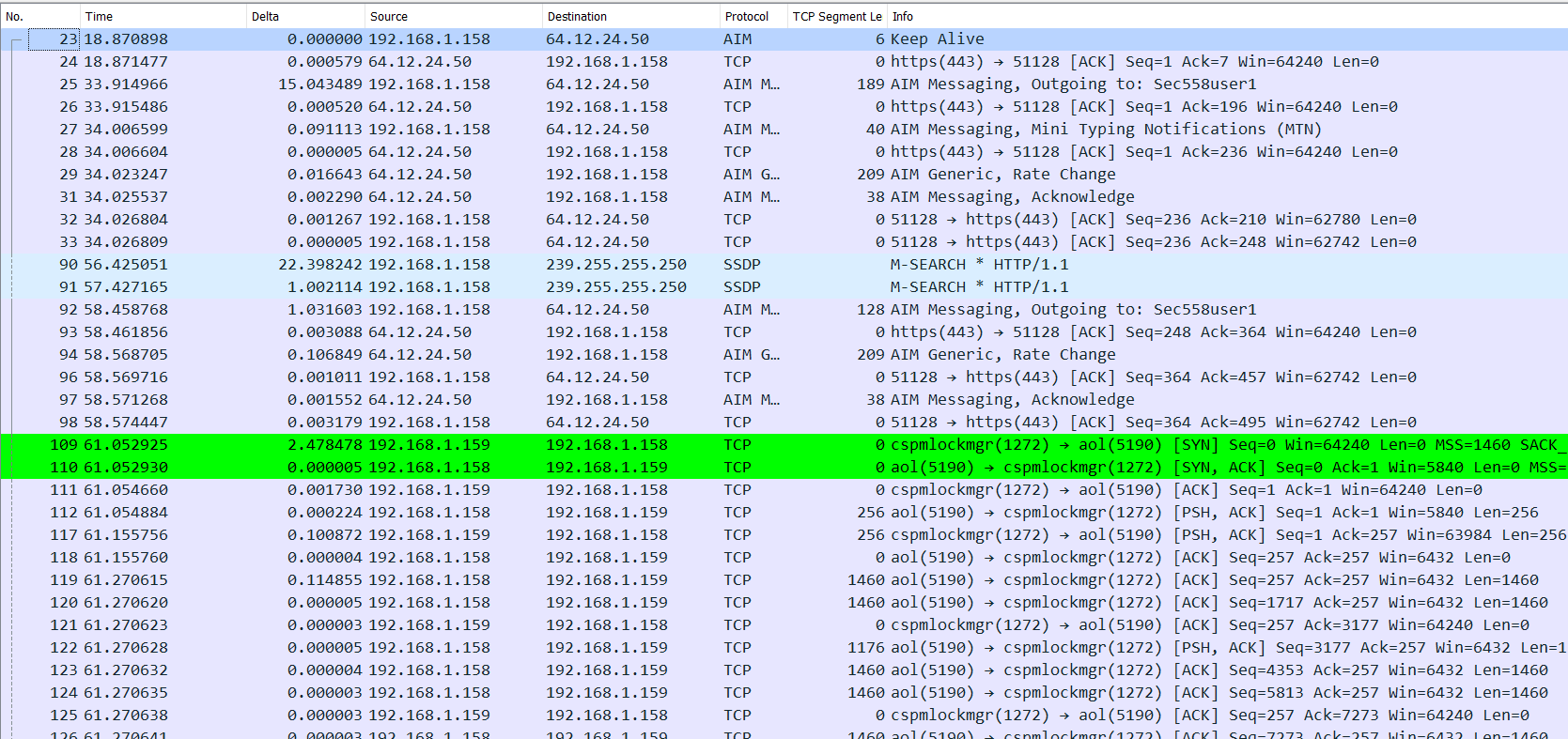
By right it should be AOL, but now is edgecast

Step 4) The protocol used to connect to 64.12.24.50 is using SSL. SSL used port 443 for communications. In order to make it readable format, I will need to decode it



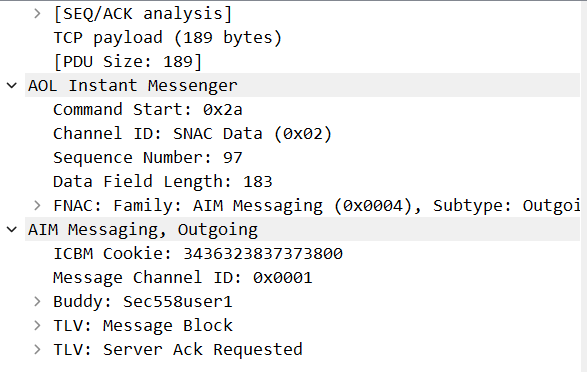


Now the captured packets will look like this



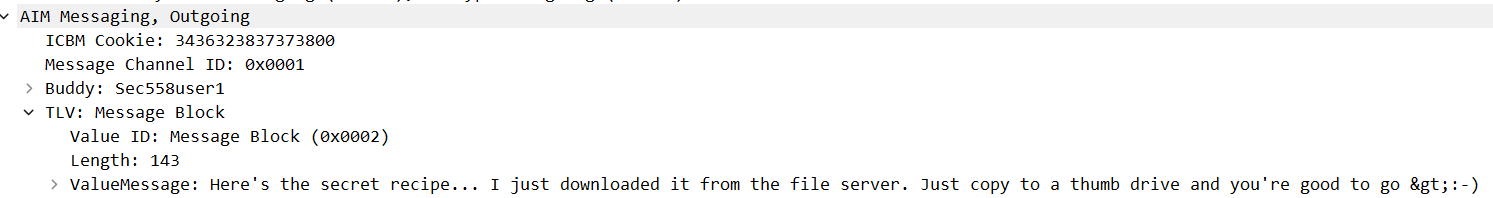
From the 25th line, I can find out who was Ann’s IM buddy





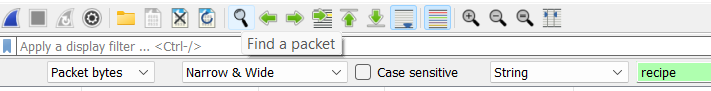
1. What is the name of Ann’s IM buddy? Sec558user1

From the 25th line I can find out the first comment captured in the IM message



2. What was the first comment in the captured IM conversation? Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go &gt;:-)

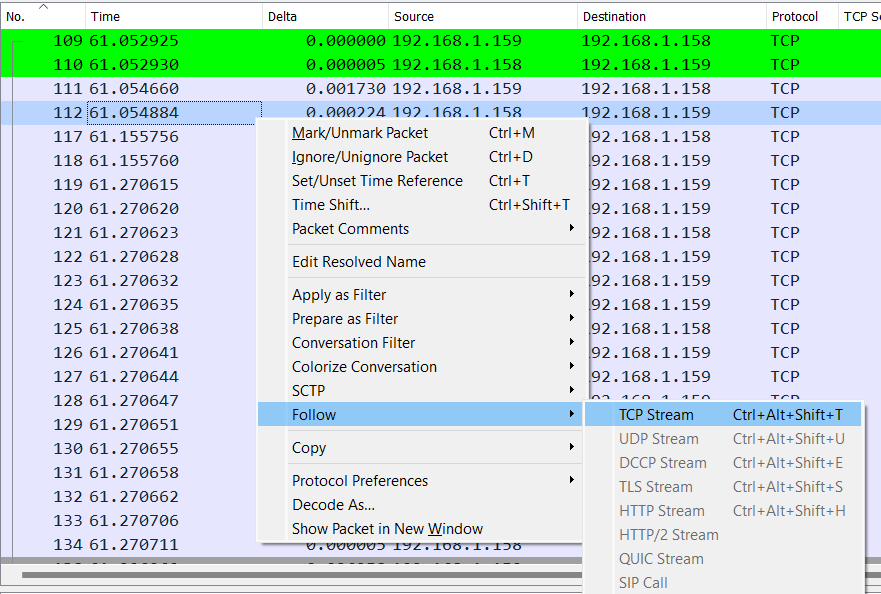
To find out the file that was been transferred, I will use Wireshark find a packet function and key recipe as the keyword to search



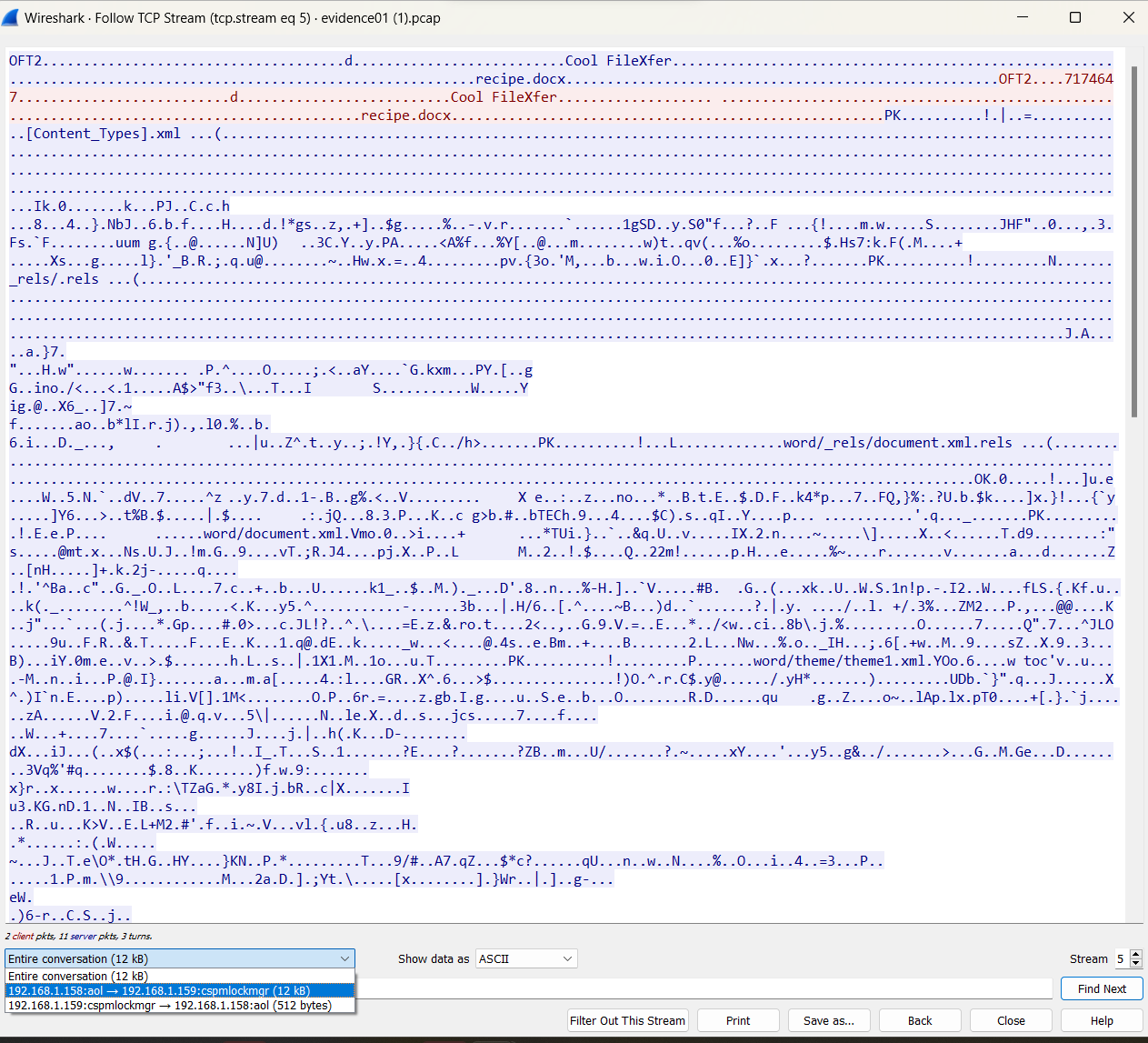
From the search results I can find recipe.docx in the packets

3. What is the name of the file Ann transferred? Recipe.docx

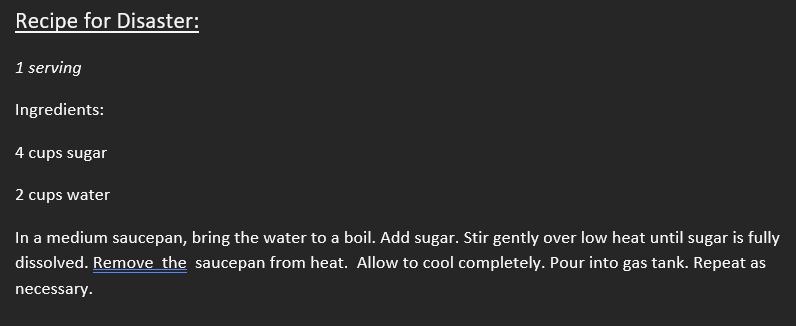
To extract the file. I will use follow TCP stream on the first instance of the results from find a packet function using recipe as the keyword

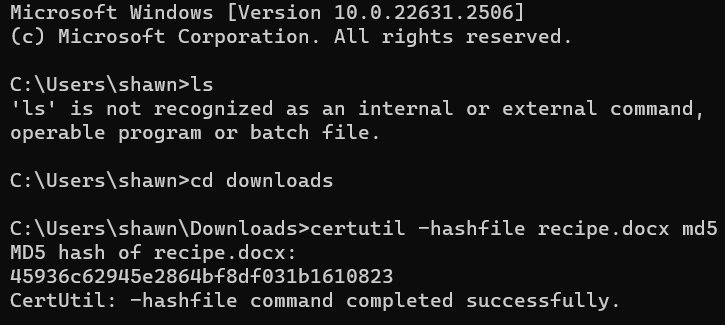


Next I am only interested in the outgoing conversation from Ann’s computer, so I select the outgoing conversation from IP 192.168.1.158



After extraction, the file contents are shown below





The md5 of the file is

45936c62945e2864bf8df031b1610823