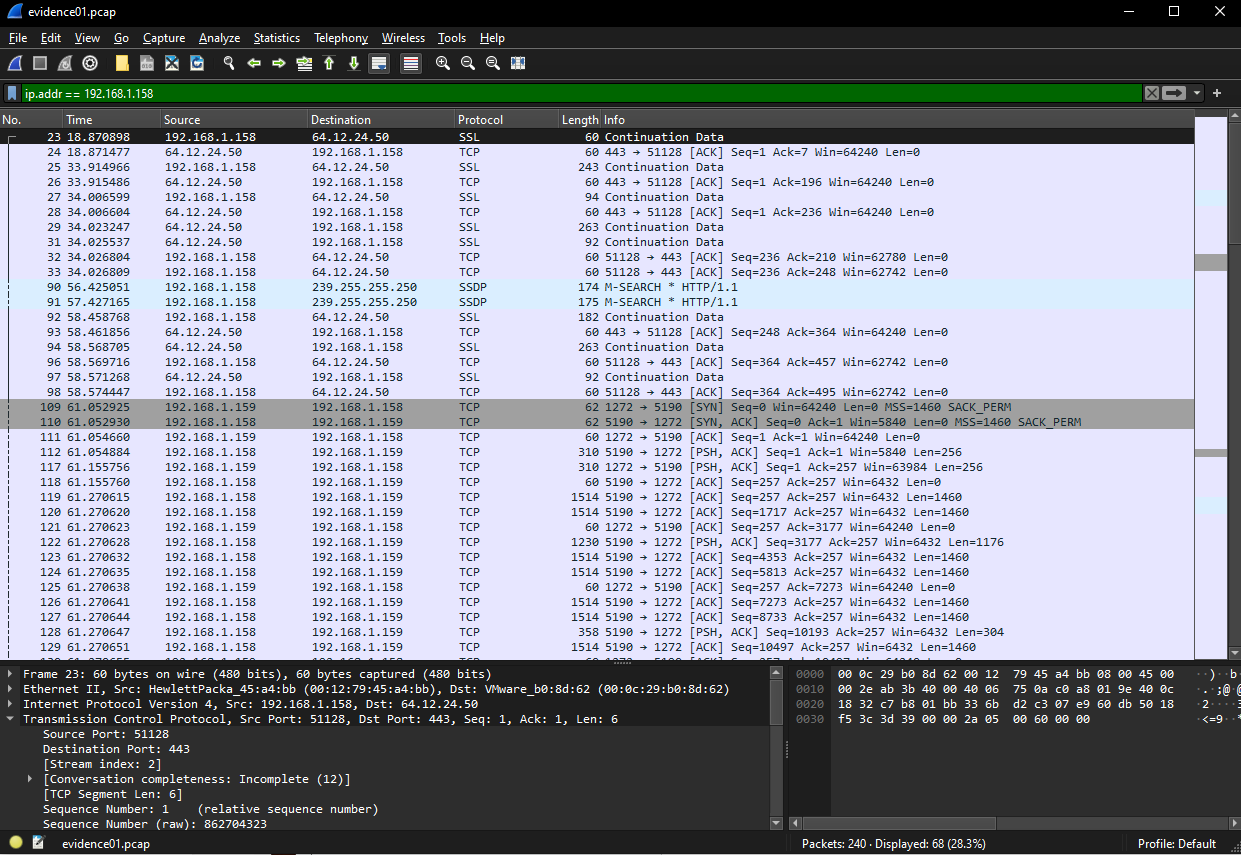
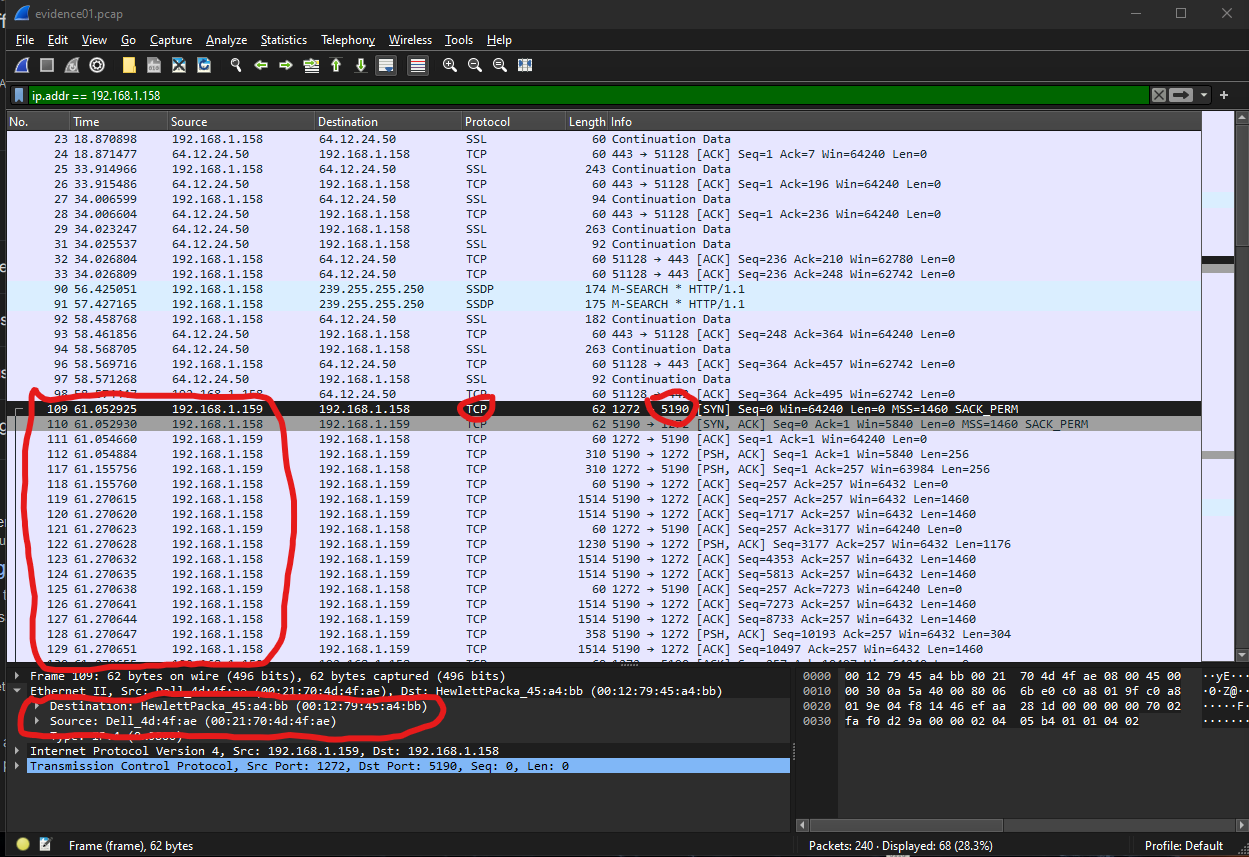
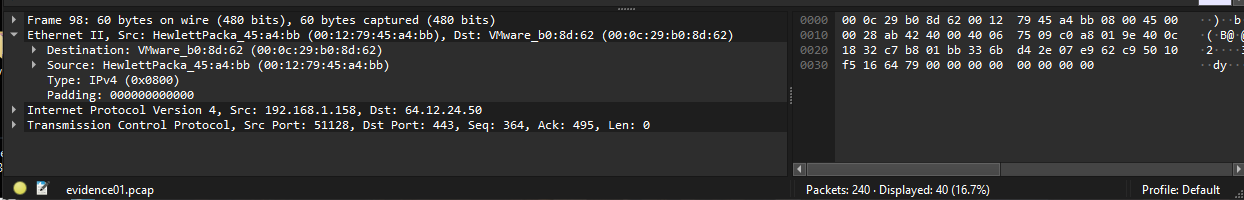
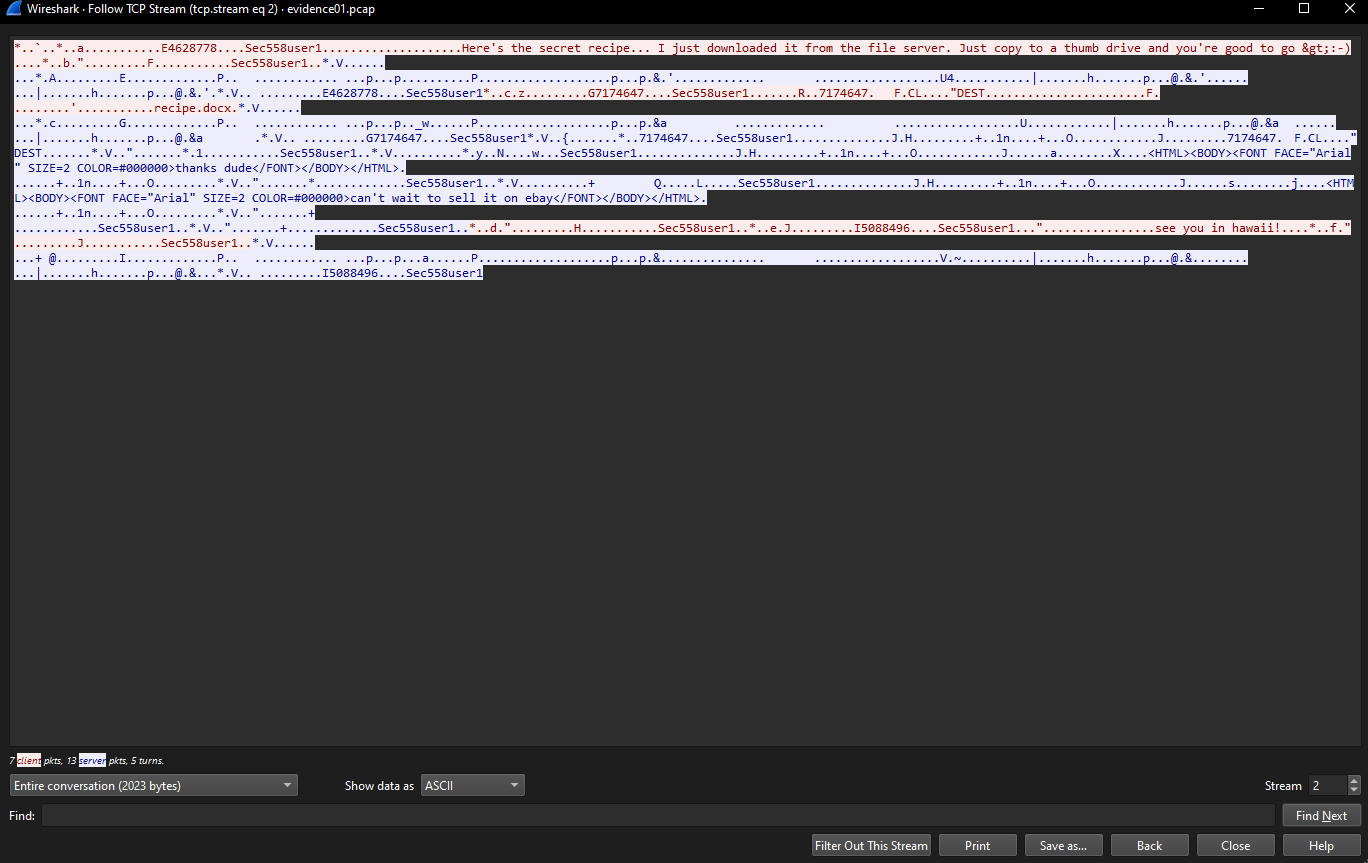
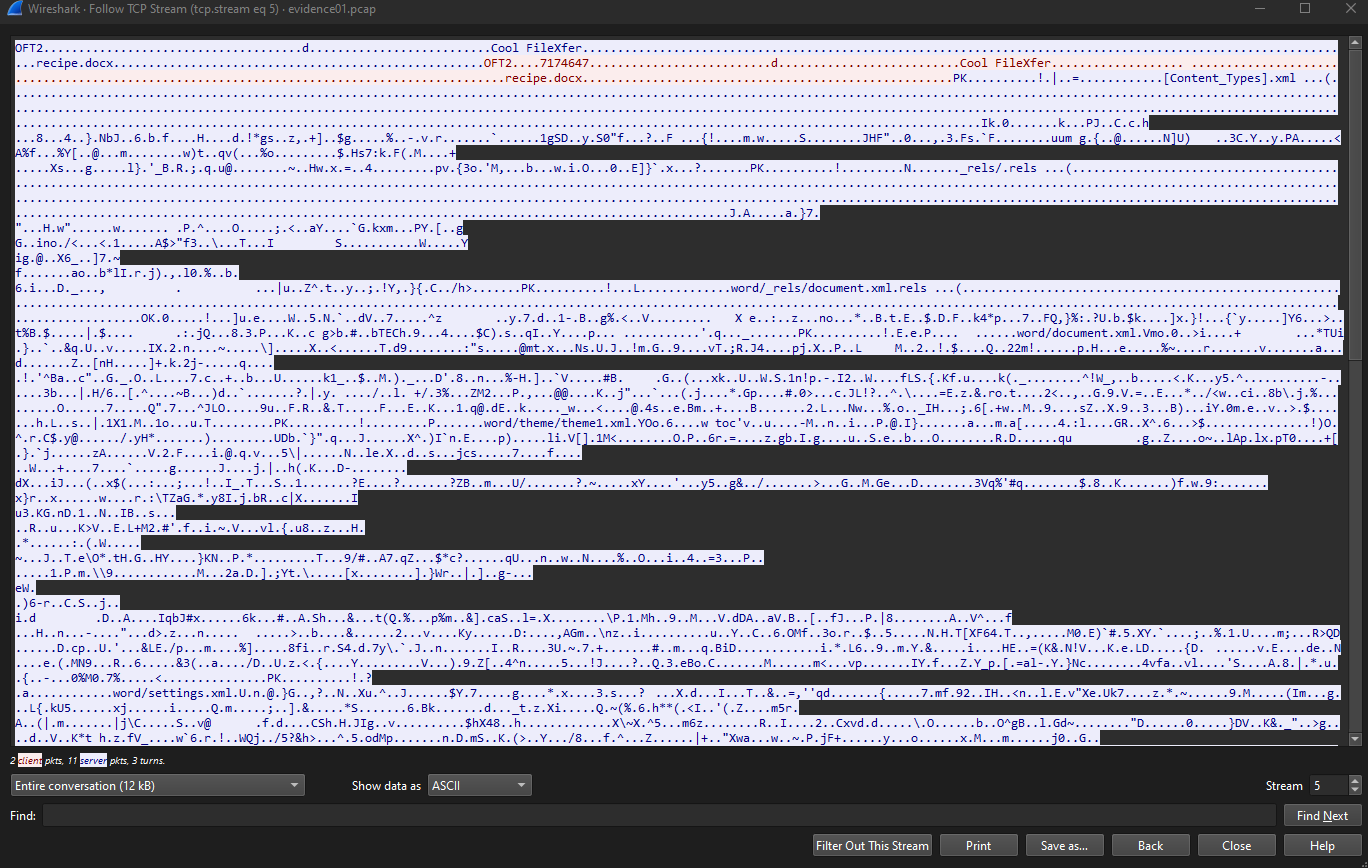
Hello, and today we will be going over my process of analyzing the evidence provided in regards to Ann's computer.

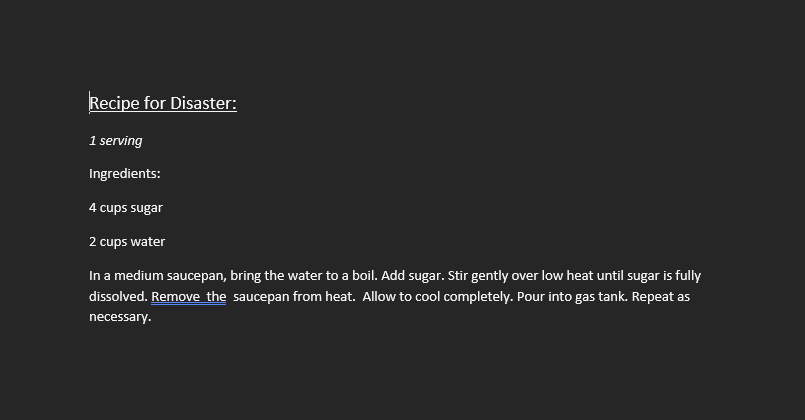
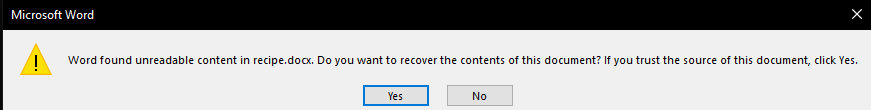
First I started by filtering out all traffic with Ann’s computer at the IP address provided (192.168.1.158). 

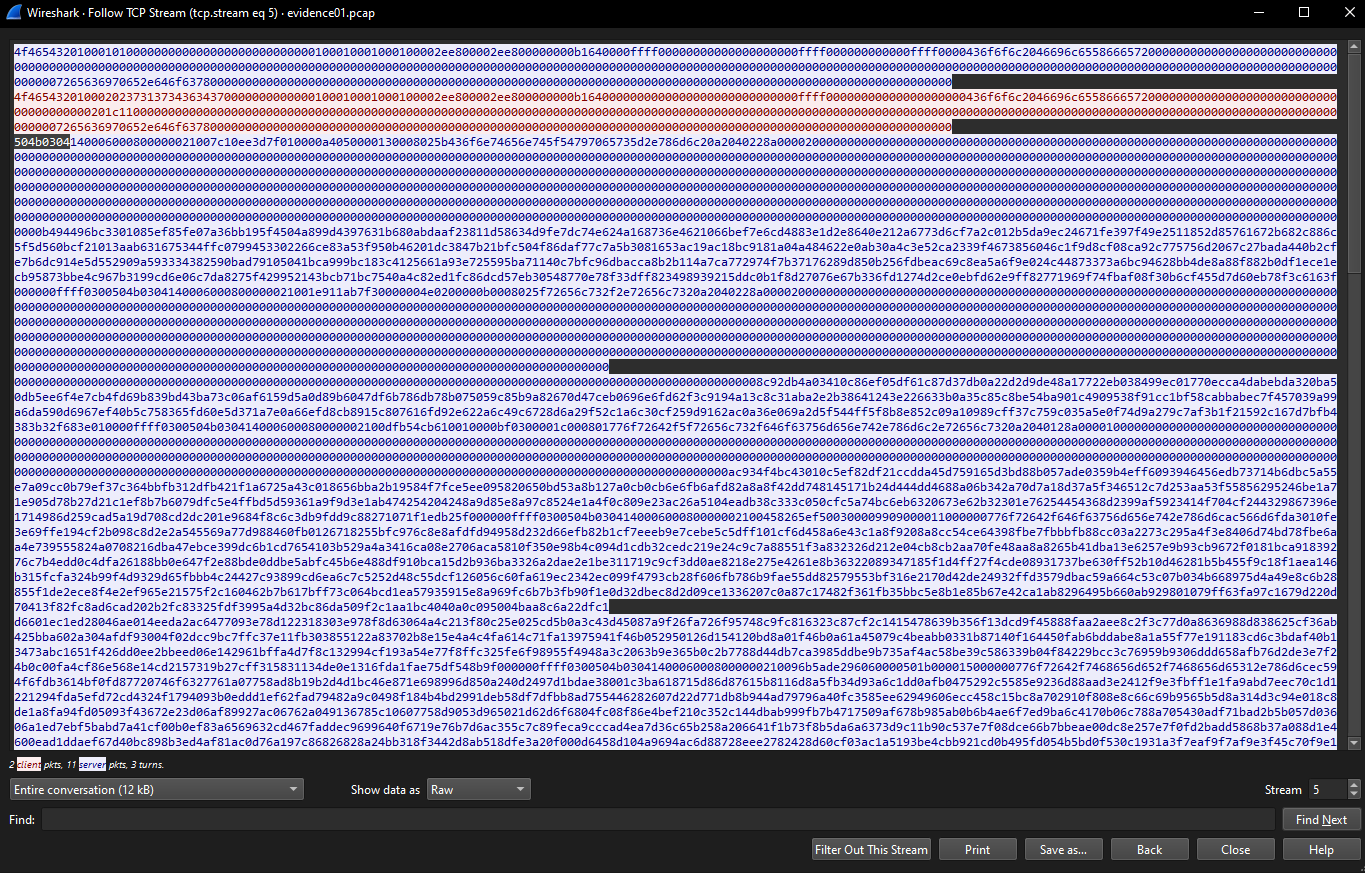
From here I looked for things that stuck out and indicators of the use of AIM. AIM typically uses the TCP transport protocol. I then used the information that the TCP port for AIM traffic typically operates on port 5190. From there I was able to look at all the IP addresses Ann’s computer was speaking with and find which ones were operating on both TCP and port 5190 as we can see from the screenshot below a Dell device was speaking with Ann’s HP device.

What is very interesting is that Anne actually sent the file recipe.docx over to a different IP which leads me to believe the attacker was operating using a VM. If we follow the TCP stream between 192.168.1.158 we can see that Anne is talking to 64.12.24.50 which if we inspect that we can see in the details that the destination is in fact a VMware machine. Here is both the conversation and the inspection proof. 



In the above screenshot, we can also see who Anne was talking to as well as the message that was sent. Now if we follow the TCP trail of the conversation between Anne's computer and the main host of that VM we can see the following data that would show Anne shared recipe.docx. 

Now how are we going to find what is in the file what we can do is inspect the stream that has the file in it from here we are going to filter out the whole conversation only to show what Anne sent over. Then from here, we are going to show the data as RAW and save to our machine but we are going to save it as recipe.docx. Then we will open it and Word will restore this for us and voila we have the secret recipe. 

We can also see from the raw data capture the secret number or binary header highlighted 

So we will now answer the following questions

1. What is the name of Ann’s IM buddy?  
 sec558user1

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 >:-)

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

4. What is the magic number of the file you want to extract?  
 0x504B0304

6. What is the secret recipe?  
 Recipe for Disaster:  
 1 serving  
 Ingredients:  
 4 cups sugar  
 2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from the heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.