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 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?

Here, I immediately went to the first packet found of Anns computer IP, packet 23. Following this TCP stream, we find the following, revealing she did send their secret recipe to someone:

after only finding the definitive name sec558user1, I decided to follow a few other streams in the capture, since the capture is relitively short. I did find, towards the end, some http requests from another company IP, 192.168.1.159, to the same server. And it redirecting a few times. It appears it was sent to "user1" at a "sec558" server.

2. What was the first comment in the captured IM conversation?

In the same sc as above, we can see the first comment to be "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 (first four bytes)?

This took quite a bit of time for me, and much digging. I glossed over a few stray streams and finally found a second stream that had recipe.docx in it, stream 5. I concluded 4F 46 54 32 is the magic number, the OFT filetype header. After doing some digging and reading through a presentation of packet flow and OFT2 header dissection, I concluded the PK lettering, and 504b, are indeed the magic

numbers, for a docx file header.

5. What was the MD5sum of the file?

I got a few different answers here, mainly because I had some trouble getting the docx file right. After my reading, I tried a few different scalping for the document in vi, and could not get it to open(MacOS and windows). After an hour or two of trying, I bowed and went to walkthroughs of this challenge, who used different techniques/apps to scalp the same parts, and were able to open the document. I tried different combinations but ultimately could not get the correct hash or the file to open, after trying to scrape the OFT header down to 504b as the starting bytes, and taking off 2 bytes on the end and trying md5 hashes again and again. I need some help when it comes to exporting and hashing from Wireshark it appears, but this could possibly be an issue when working on Mac OS, which I have been for this challenge.

6. What is the secret recipe?

As I could not get the docx to open even when following walkthroughs, I was unable to answer this, but will come back to it hopefully.