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?

Answer: The name of Ann's IM buddy is "**Sec558user1**".

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

Answer: The first comment captured in the conversation is "**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?

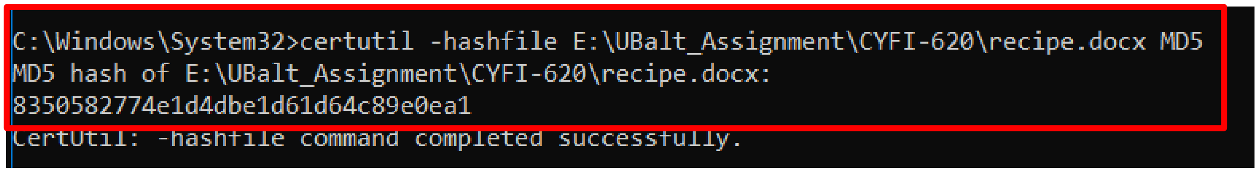
Answer: The name of the file transferred by Ann is "**recipe.docx".**

4. What is the magic number of the file you want to extract (first four bytes)?

Answer: The magic number of the word file that is to be extracted is “**50 4B 03 04**”.

5. What was the MD5sum of the file?

Answer: The MD5 sum of the file named “recipe.docx” is “**8350582774e1d4dbe1d61d64c89e0ea1**”.



```
C:\Windows\System32>certutil -hashfile E:\UBalt_Assignment\CYFI-620\recipe.docx MD5
MD5 hash of E:\UBalt_Assignment\CYFI-620\recipe.docx:
8350582774e1d4dbe1d61d64c89e0ea1
CertUtil: -hashfile command completed successfully.
```

6. What is the secret recipe?

Answer: The secret recipe acquired from the Wireshark packet is:

“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 heat. Allow to cool completely. Pour into gas tank. Repeat as necessary. “

MD5 (evidence.pcap) = d187d77e18c84f6d72f5845edca833f5

- By Mohit Dhabuwala

mohit.dhabuwala@ubalt.edu