###

Class Work

(16SN602 Cyber Forensic and Incident Response Course - Network Forensics)

By:- Pratyush and Sreelakshmi
Department Of Cyber Security Systems and Networks

###

MD5sum(File - 1) - d187d77e18c84f6d72f5845edca833f5
MD5sum(File - 2) - cfac149a49175ac8e89d5b5b5d69bad3

Q. 1) 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?

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?

****

**

Q.2) After being released on bail, “Ann Dercover” disappears! Fortunately, investigators were carefully monitoring her network activity before she skipped town.

“We believe Ann may have communicated with her secret lover, Mr. X, before she left,” says the police chief. “The packet capture may contain clues to her whereabouts.”

<u>You are the forensic investigator</u>. Your mission is to figure out what Ann emailed, where she went, and recover evidence including:

1. What is Ann’s email address?
2. What is Ann’s email password?
3. What is Ann’s secret lover’s email address?
4. What two items did Ann tell her secret lover to bring?
5. What is the NAME of the attachment Ann sent to her secret lover?
6. What is the MD5sum of the attachment Ann sent to her secret lover?
7. In what CITY and COUNTRY is their rendez-vous point?
8. What is the MD5sum of the image embedded in the document?

##Write a small write-up answering each questions.