Case Study 2

Making life easy by using tools

Case Study from Forensic Contest

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.”

You are the forensic investigator. 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?

Using Network Miner

- Make life easy by using tools
  - http://www.netresec.com/?page=NetworkMiner
- Demo of the tool