Assignment 2

IERG5320, Fall 2021

General Instructions:

(1) you need to complete all problems in this assignment

(2) you need to submit a report which contains not only the information to be recovered, but also the steps and commands (if any) to recover that information.

(3) You can use the Wiresharp/Tshark (https://www.wireshark.org/) or other open source tools to complete this assignment. Commercial tools are not allowed.

(4) **Deadline: 11:59pm, Dec 19 (Sun), 2021**. Please submit it through blackboard system.

Problem 1: One morning, one staff working at IT department of a company noticed a strange laptop which connected from a Wi-Fi Access Point at parking lot instead of regular office area, so he started to capture the network traffic immediately (the captured packets are saved in file "problem_1.pcap"). However, the strange laptop got offline and disappeared very quickly. No strange things had happened (no network scanning, no denial-of-service attack, no brute-force attack on SSH servers, etc.), except a computer (with IP address 192.168.1.158) sent some IMs over the wireless network to that laptop. Through the log files of DHCP server, he know that the computer belongs to an employee named Ann.

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?

Problem 2: A company has come and asked for your help on a recent security incident, in which an important file was stolen. Since employees could not use any USB sticks or similar, the file must been stolen through network. Fortunately, they have got a copy of network traffic file for that day (i.e., problem_2.pcap) . As a network forensic expert, could you help them get following information?

(1) Attacker's IP address

(2) The MD5 hash value of the stolen file

(3) The time when the file was stolen

Please write a report recording your analysis process and attach the file you extracted.