LAB 4 – Ann’s Secret Recipe

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 Instant Messages 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 Instant Messaging, what she sent, and recover evidence including:

- What is the name of Ann’s IM buddy?
- What was the first comment in the captured IM conversation?
- What is the name of the file Ann transferred?
- What is the magic number of the file you want to extract (first four bytes)?
- What was the MD5sum of the file?
- What is the secret recipe?