NYU Forensics Challenge

Bob’s Burritos has a super top secret recipe for their special burrito. Three days ago an employee was fired for suspected theft and was allowed back into the restaurant to gather a few things. The manager was dealing with a customer and looked back and saw that the fired employee was on the computer. Anticipating this, the manager called the employee that handles IT who had recently started logging all traffic on the network for another compliance project. The IT employee was able to pull a packet capture of the network during the time the fired employee was using the computer. Given the PCAP file can you answer;

1. What was the employee doing on the machine.
2. What was IP address of the FTP server that the employee sent data to?
3. What was the username/password of the FTP server the employee sent data to?
4. What was the filename of the file the employee attempted to send?
5. What is in the contents of the file?