Lab 11: Communication Artifacts

Lab 11 report Name: Kevin Ubilla

This Lab is required for Unit 6. It is worth 15 points. The Challenge Flags are worth 2.5 Extra Credit points.

1. **Email Messages and Programs, Step 9.** In your own words, please describe the scope of Helix’s capabilities and the way in which Helix is being executed here.

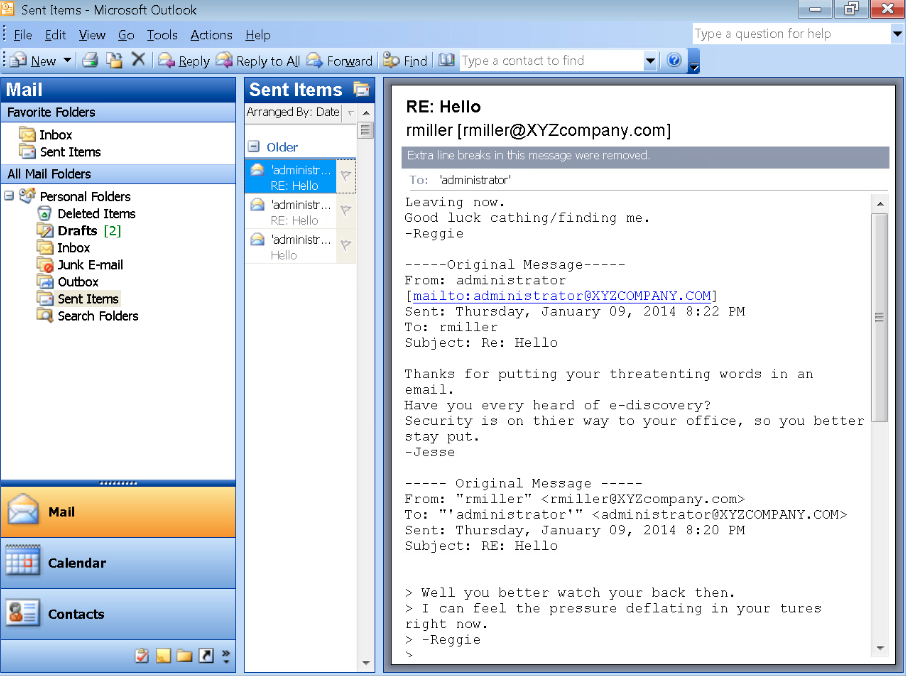
**→**We are using Helix to analyze Outlook PST files. Helix provides system information, acquisition, browsing, and scanning of files, as well as incident response←

1. **Email Messages and Programs, Step 15.** You have just used Helix to launch the PST Password Viewer. Please capture the **PstPassword** screen that shows the three passwords and paste it below.

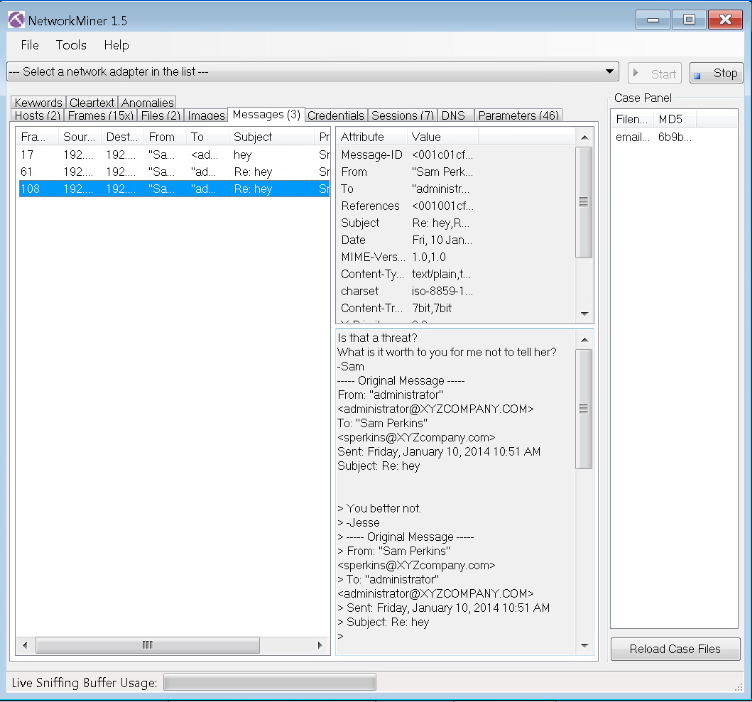
**→ Graphical user interface, text, application, Word

Description automatically generated ←**

1. **Email Messages and Programs, Step 20.** You are in Microsoft Outlook in the Sent Items folder looking at the top email (the most recent at 8:22 PM). Please capture the email in Outlook, including the “Sent Items” pane at the left and the full email at the right, and paste it below.

**→ ←**

1. **Examining Emails in Network Traffic, Step 26.** You have followed the stream of communications through to the third email from Sam Perkins. Please capture the email inside the Network Miner window and include the Network Miner heading and the full content of the third message, including “from: , “to:” and “sent:” and paste it below.

**→ ←**

1. **Internet Relay Chat, Step 36.** You have carried out many steps thus far, all of which were designed to begin monitoring network traffic and to set an IRC chat. How does the command **wireshark badtraffic.cap** fit into this bigger picture? Please tell it in three sentences or less below.

**→**Well IRC is an older technology that is not common today. However, the command wireshark badtraffic.cap is a command that allows us to intercept this network in order to sniff the messages. We can then examine them for details. **←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**