# DIGITAL FORENSICS LAB SERIES

# Lab 12: Communication Artifacts

## Objective - User Communications Analysis

**Document Version: 2014-02-07 (Beta)**

**Organization:** Moraine Valley Community College
Author: Jesse Varsalone



The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah. 

## Contents



## Introduction

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

This lab includes the following tasks:

1. Email Messages and Programs
2. Examining Emails in Network Traffic
3. Internet Relay Chat

Performing this lab will provide the student with a hands-on lab experience meeting the Evidence Acquisition, Preparation and Preservation Objective:

*The candidate will demonstrate an understanding of forensic examination of user communication applications and methods, including host-based and mobile email applications, Instant Messaging, and other software and Internet-based user communication applications.*

Email messages can play a critical role in criminal investigations, the e-discovery process, and just litigation in general. Forensic Software like EnCase and FTK will allow you to view the email messages from programs like Outlook and Outlook Express.

**IRC–** Internet Relay Chat is used to communicate with other Internet users. IRC is an older technology and is not considered as mainstream today.

**POP3** – Post Office Protocol Version 3. Uses Port 100 by default to deliver mail.

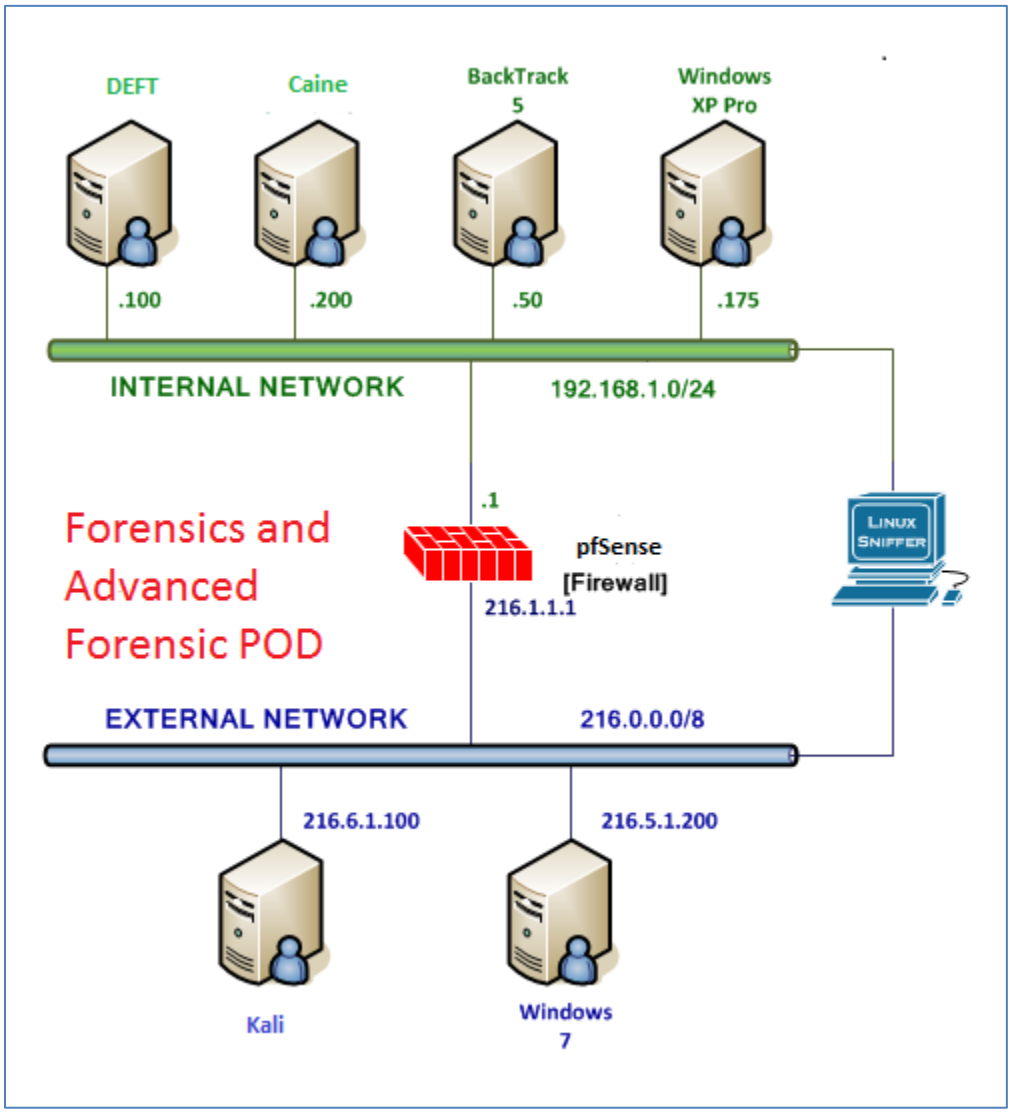
**SMTP** – Simple Mail Transfer Protocol. Uses Port 25 by default to send mail.

**Wireshark®** – A protocol analyzer that can also be used as a sniffer tool. Wireshark is free and can be downloaded from the following link: www.wireshark.org/download.html.

**Network Miner** – An NFAT, Network Forensic Analysis Tool. The free version can be downloaded at http://sourceforge.net/projects/networkminer/files/latest/download.

## Lab Topology



## Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

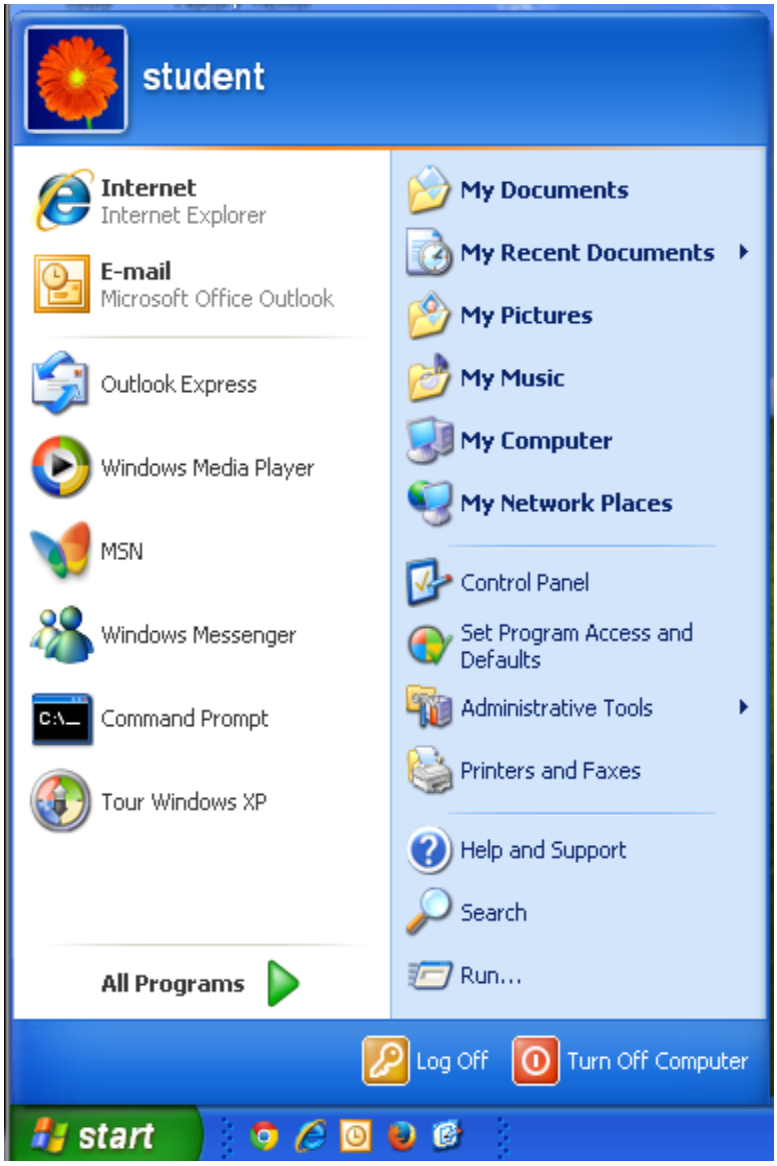
| **Virtual Machine** | **IP Address** | **Account** (if needed) | **Password** (if needed) |
|---|---|---|---|
| Windows XP Pro Internal Machine | 192.168.1.175 | | |
| Windows 7 External Machine | 216.5.1.200 | student | password |
| Linux Sniffer | No IP address | root | toor |

# 1 Email Messages and Programs

Email messages can play a critical role in criminal investigations, the e-discovery process, and litigation in general. Forensic software like EnCase and FTK will allow you to view the email messages from programs like Outlook and Outlook Express. Outlook comes with Microsoft Office, and Outlook Express is a free program that was included with almost all versions of Microsoft Windows prior to Windows Vista. EnCase and FTK are commercial software packages that require a hardware dongle. The free products, like Autopsy, will not parse PST files or DBX files from a forensic image. If you do not have the commercial software, you can use the applications to view messages.

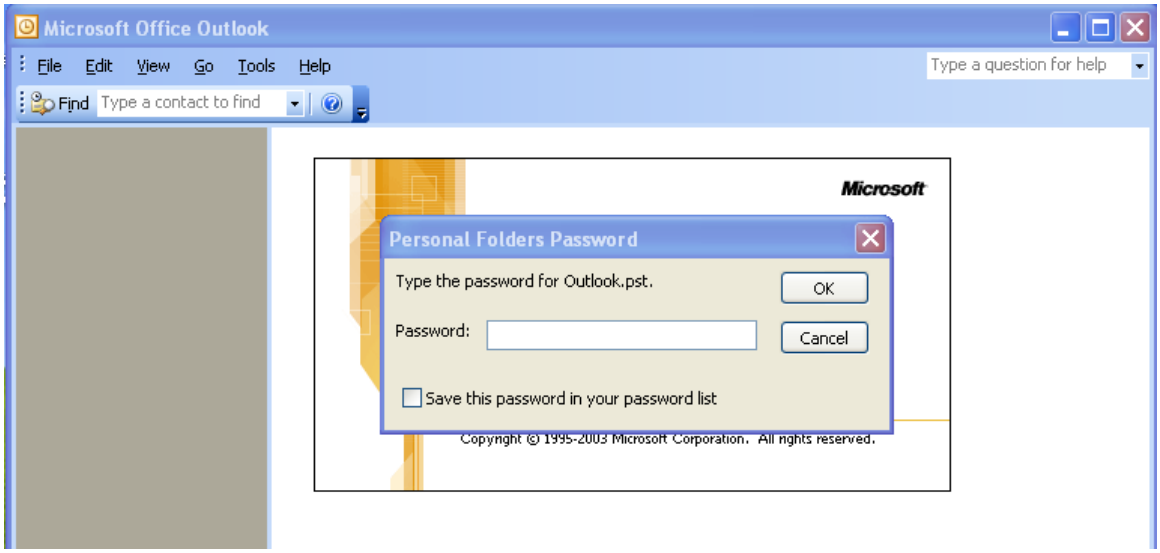
## 1.1 Viewing Workstation Email

1. On the Windows XP Pro Internal Machine, click on the Start button and select E-mail.



2. You are prompted for a Personal Folders Password. You do not know this password. Close the window.




3. On the Windows XP Pro Internal Machine, click on the Start button and select Computer.

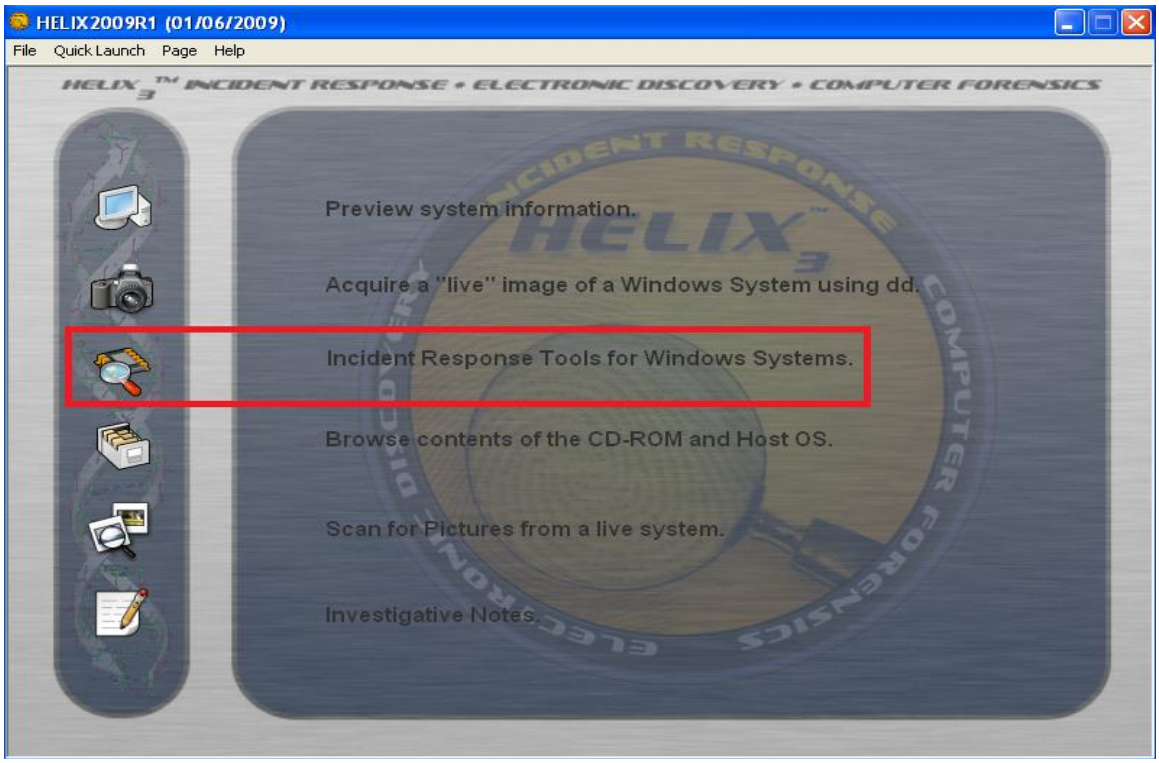

  

4. Double-click on the link to **HELIX** (the name may contain additional characters).

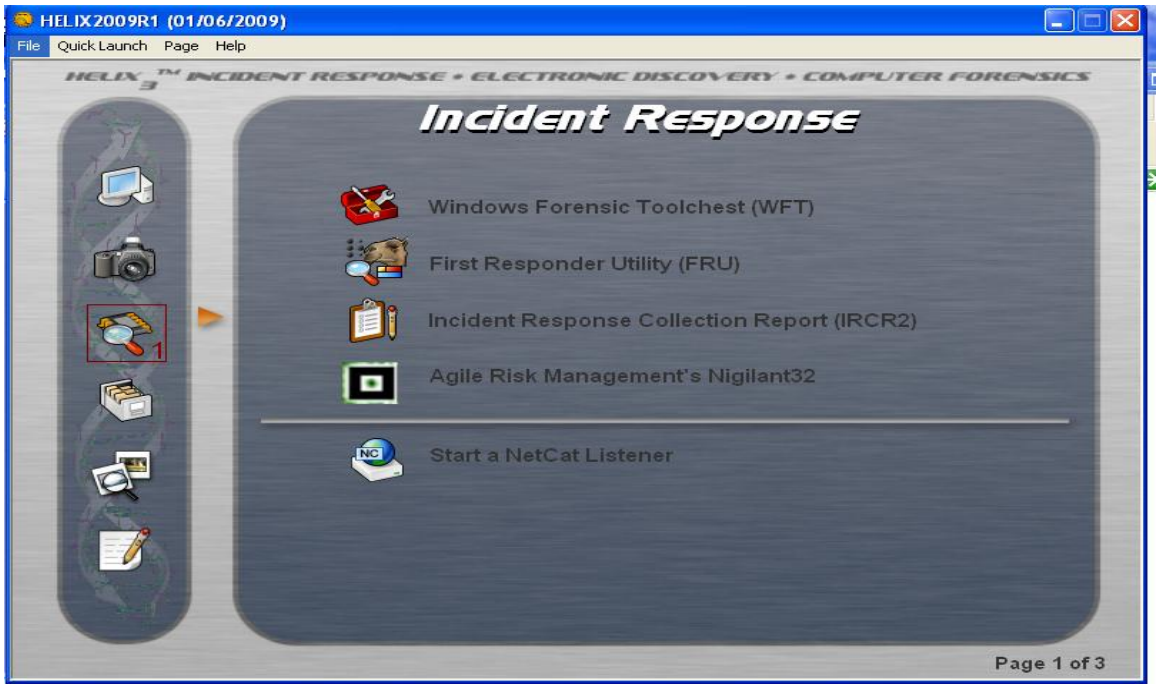

5. Click **Accept** to Accept the HELIX warning.

6. Click on the icon to select the **Incident Response Tools for Windows Systems**.

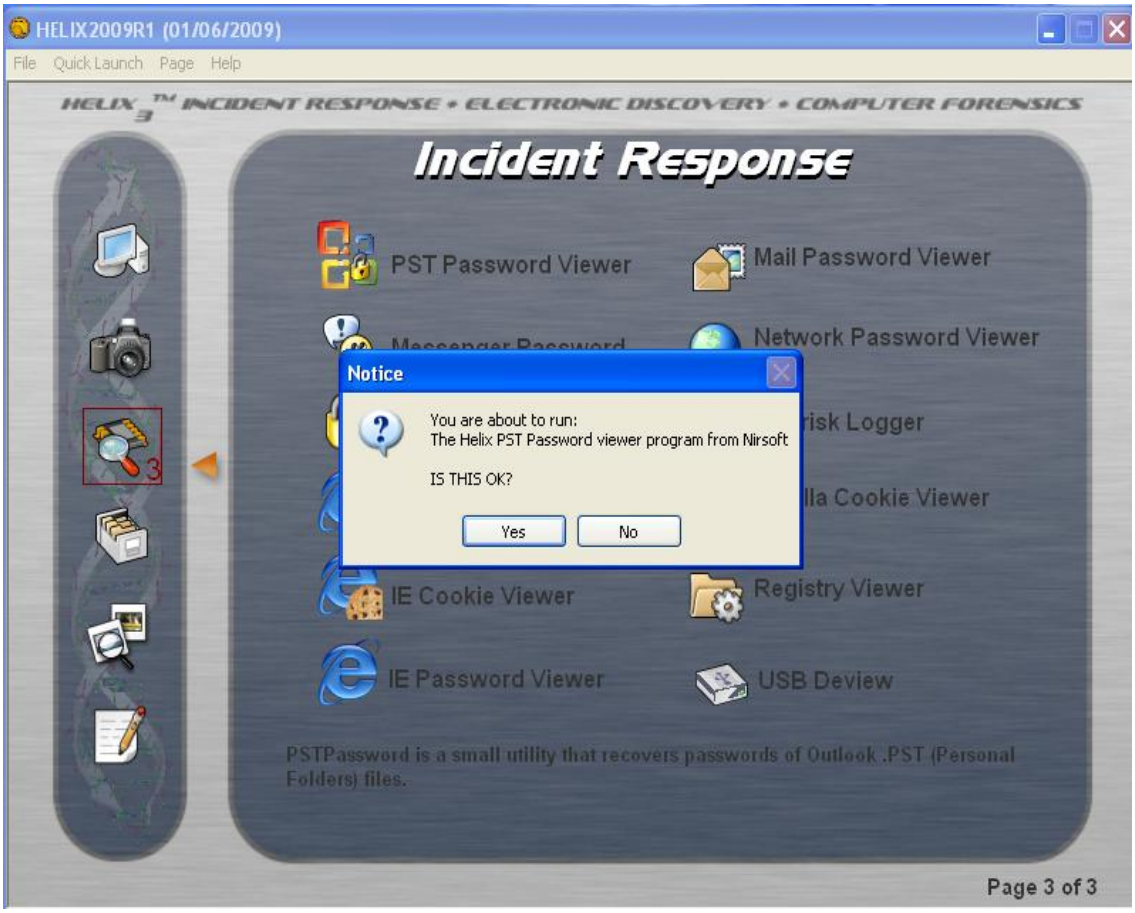



7. Click the arrow to page down to Page 3 of the Incident Response Tools for Windows Systems.



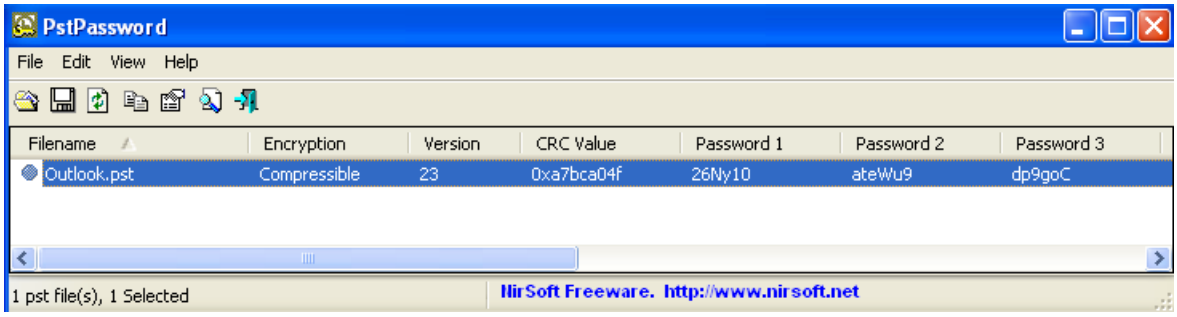

  

8. Click the icon in front of the **PST Password Viewer**. Click **Yes** in response to, IS THIS OK?




9. View the three passwords that the PSTPassword program has given you.

Make note of these passwords for later use.

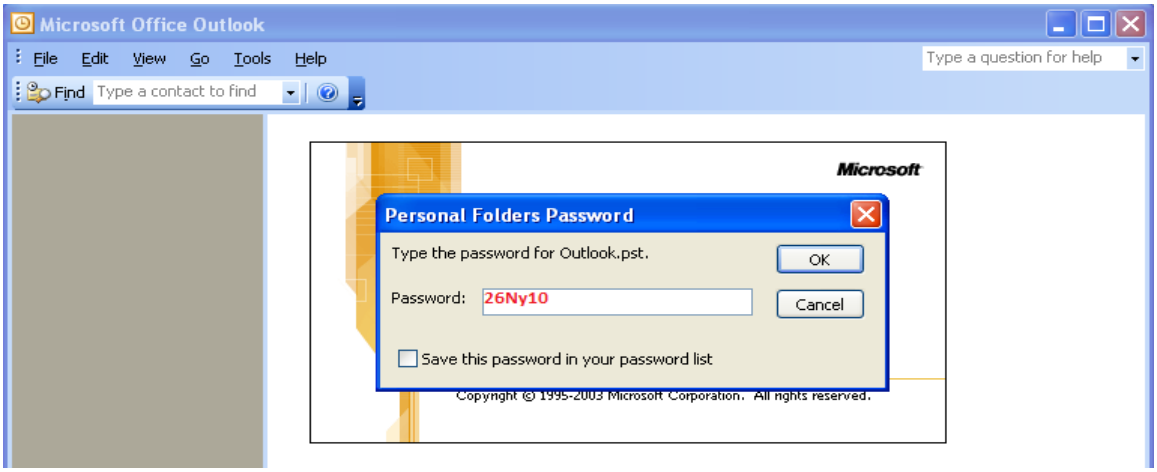


10. Once again, on the Windows XP Pro Internal Machine, click on the Start button and select E-mail.

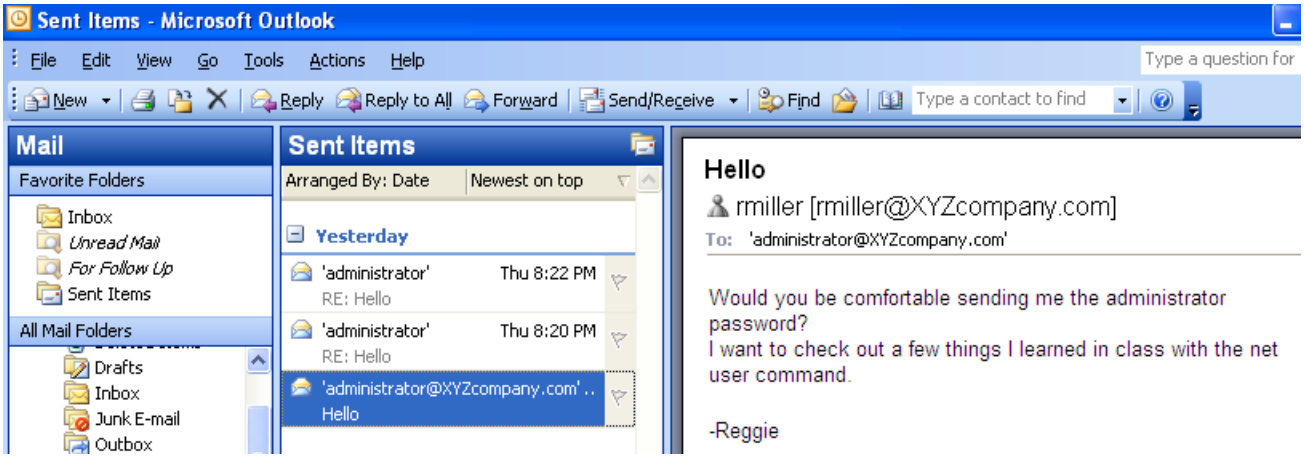

11. You are prompted for a Personal Folders Password. Enter one of the three passwords that PSTPassword provided (in the example below, we use the password **26Ny10,** see Step 9) and click OK.

Be aware that passwords are case sensitive.

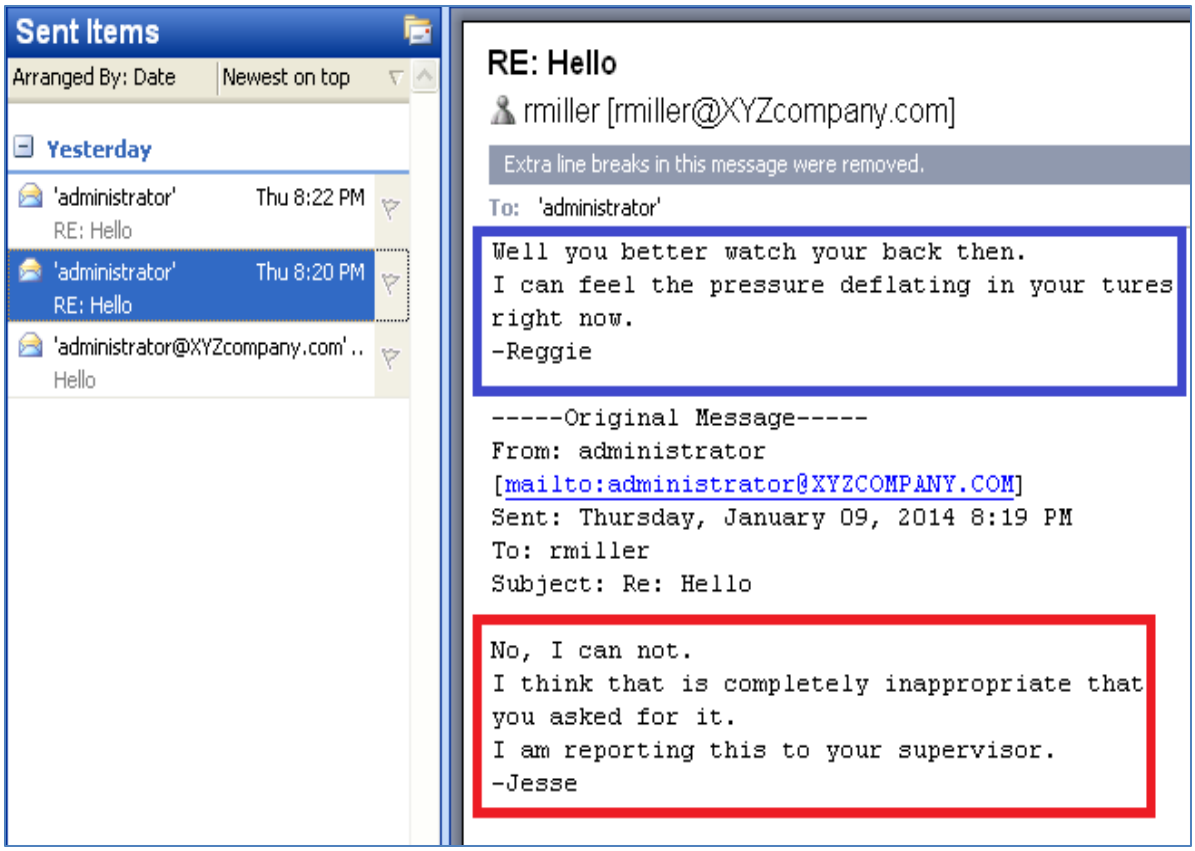


12. Click on the Sent Items folder. Select the email at the bottom of the list and read it.

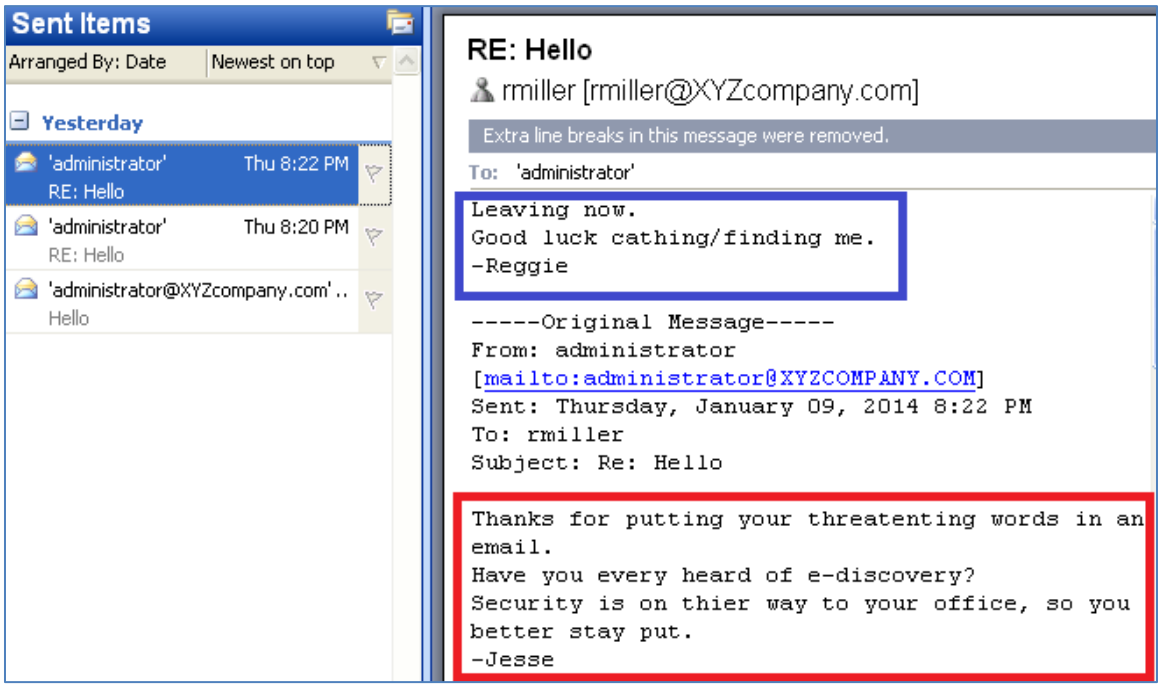



13. In the Sent Items folder, select the middle email in the list and read it.



14. In the Sent Items folder, select the email at the top of the list and read it.

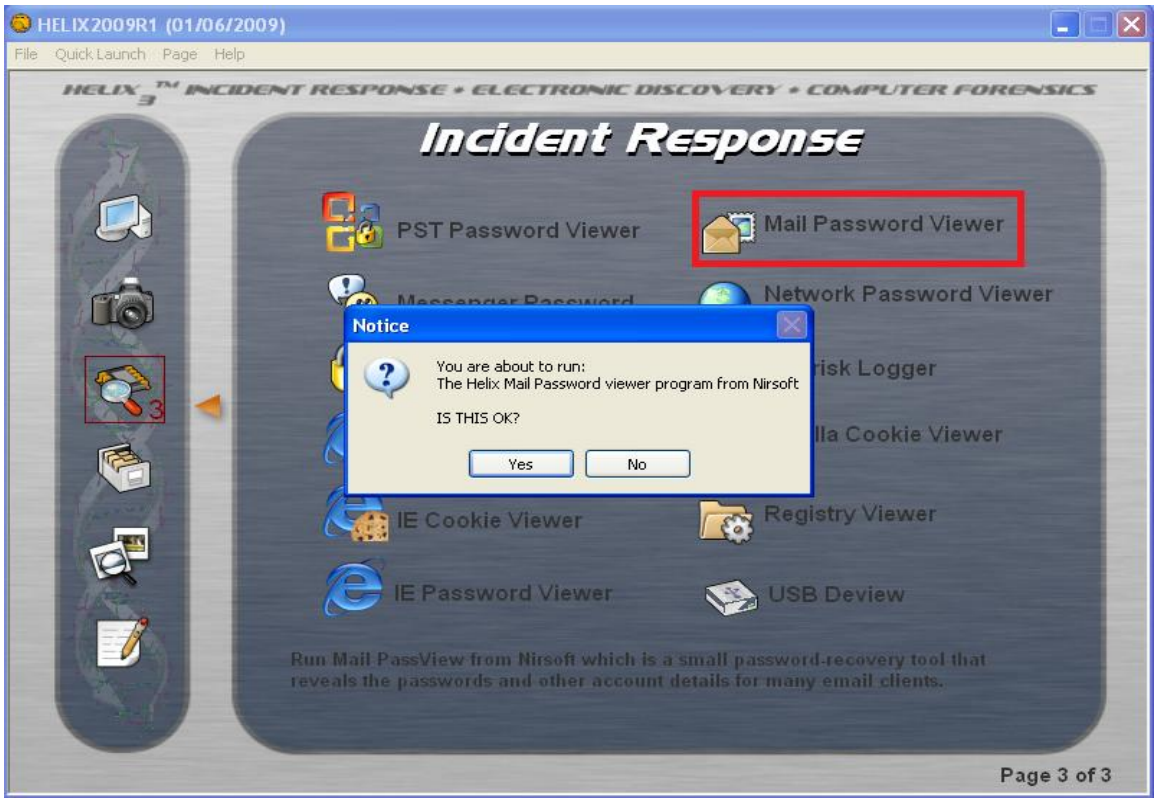



15. Close Outlook when you are finished viewing the email correspondence.
16. On the Windows XP Pro Internal Machine, click on the Start button and select Outlook Express.

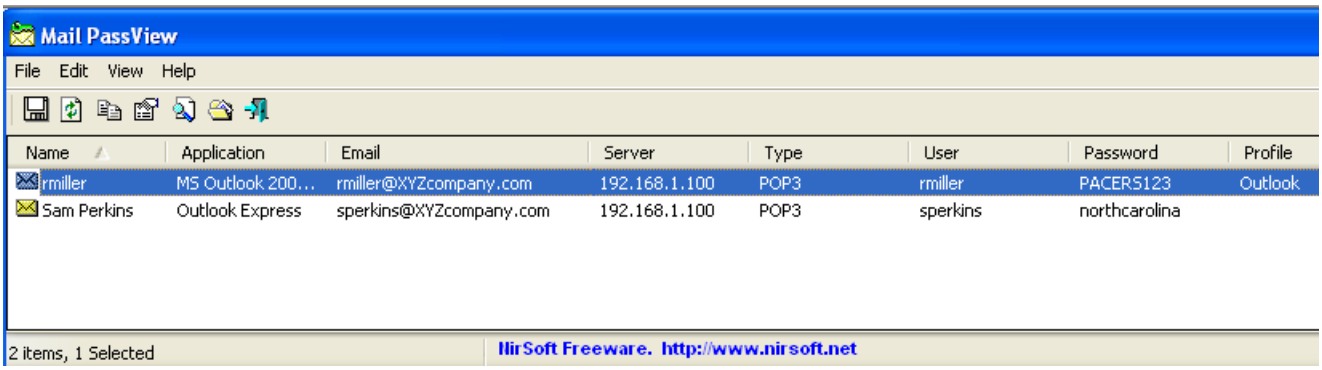
17. Click Main Identity. We do not know the password.


18. Go back to HELIX and run the **Mail Password Viewer** from Page 3 of the Incident Response Tools for Windows. Click **Yes** in response to, IS THIS OK?



19. View the extracted passwords for Outlook and Outlook Express.

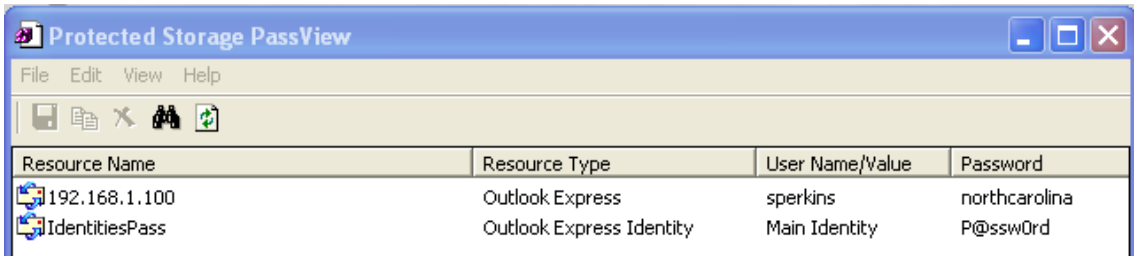



While those passwords we extracted are the passwords for the email accounts, they will not work if the user has selected a different Personal Folder password in Outlook or a Login Identity password in Outlook Express. HELIX provided the PST password, but that will not work for Outlook Express. We can obtain it from the Protected Storage Viewer.

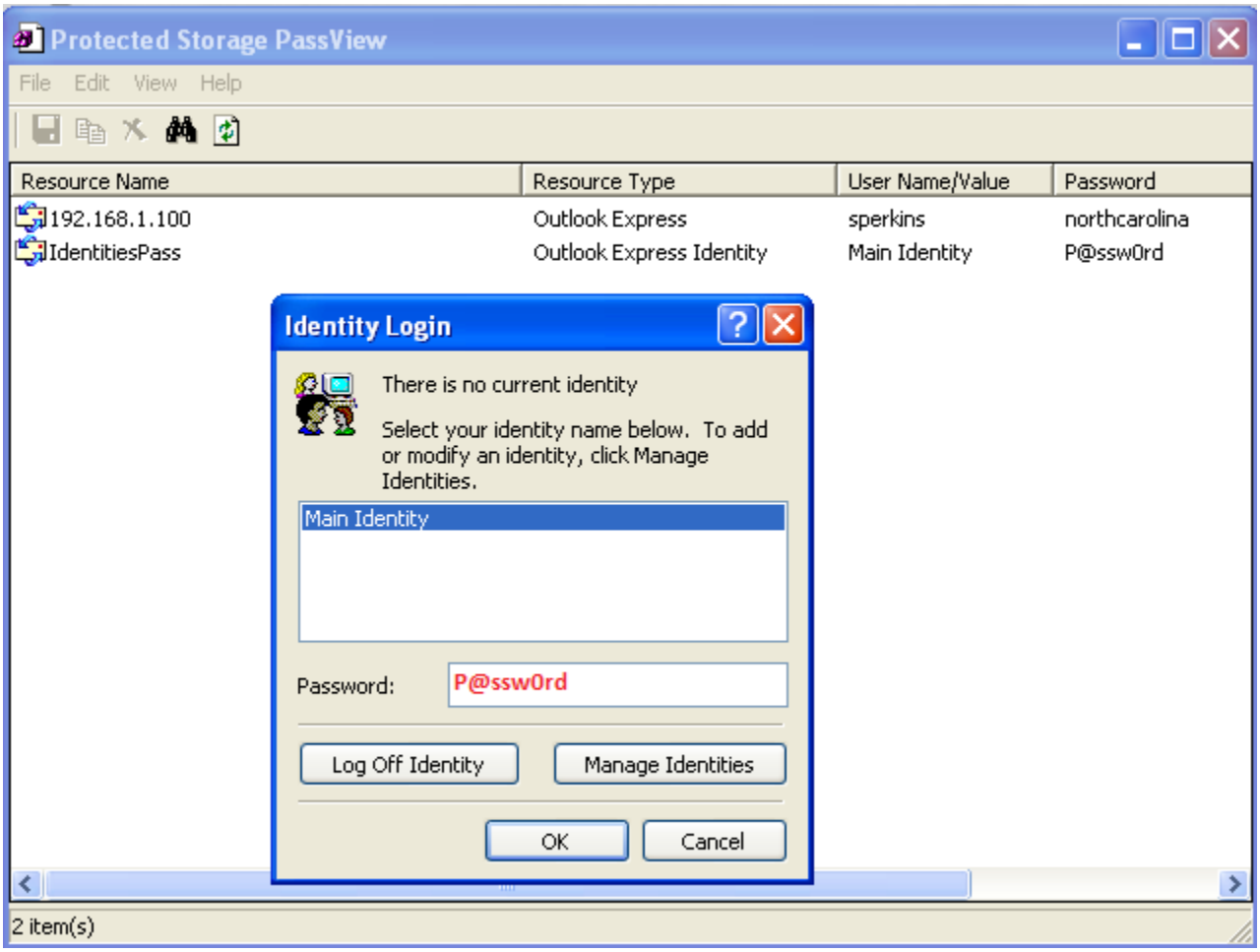
20. Go back to HELIX and run the **Protected Storage Viewer** from Page 3 of the Incident Response Tools for Windows. Click Yes in response to, IS THIS OK?

21. View the password for the Main identity in the Protected Storage PassView.

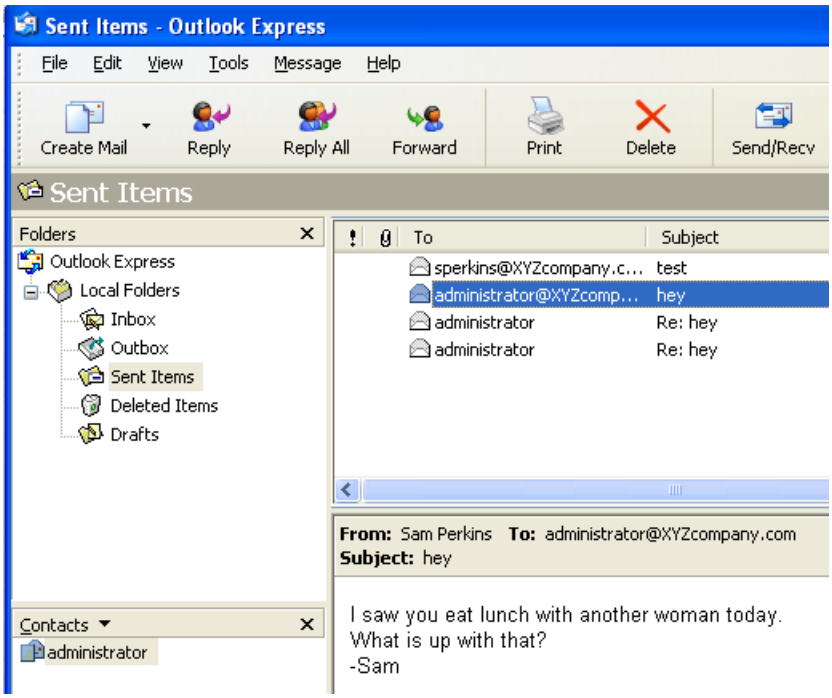



22. Return to the Outlook Express Identity Login window. Click Main Identity and type **P@ssw0rd**.

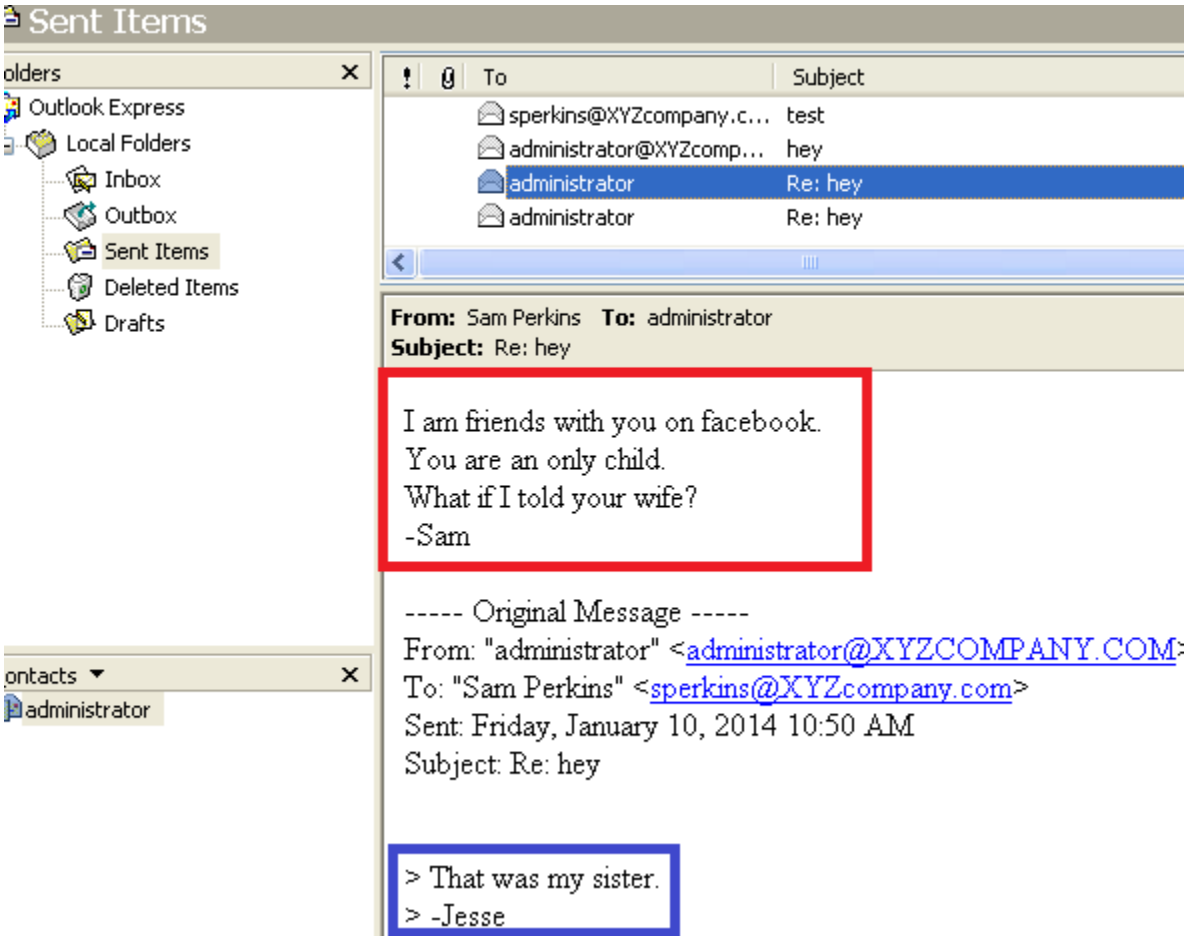


23. Click the Sent Items folder. Read the second email (from the top).

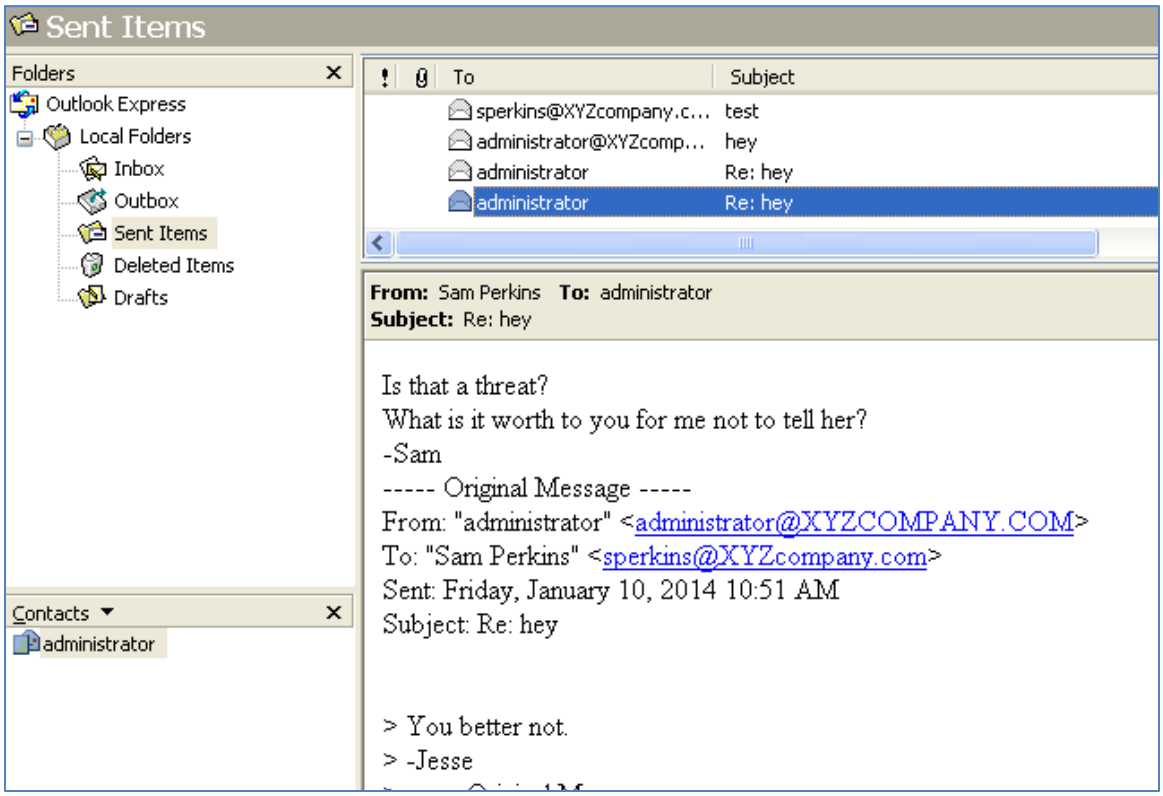



24. Click the Sent Items folder. Read the second email (from the top).



25. Click the Sent Items folder. Read the second email (from the top).




26. Close Outlook Express when you are finished viewing the messages.
27. Close HELIX.

## 1.2 Conclusion

Email messages can provide valuable information for criminal and civil cases. It helps to have a commercial forensic tool like EnCase or FTK to parse PST and DBX files. However, if you do not have the commercial tools, you can boot the image up with Live View and get the email messages off the system. If the user has a Personal Folder password for Outlook or a Login Identity password in Outlook Express, HELIX can extract these passwords.

## 1.3 Discussion Questions

1. Which application uses a PST file?
2. How can you get the password for a Personal Folder for Outlook?
3. How can you get the password for Login Identity for Outlook Express?
4. Where can you get passwords for Email accounts using HELIX?

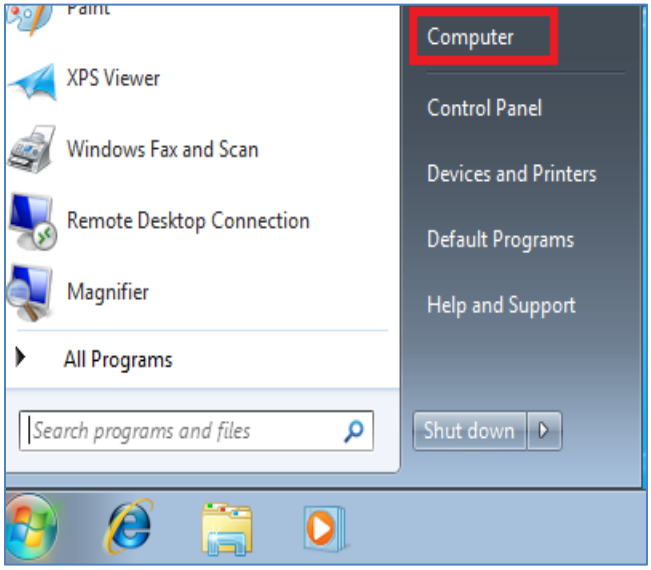
# 2 Examining Emails in Network Traffic

In the first task, we looked at email messages on the system. In this task, we will examine email messages in network traffic. You can get information about sent messages as well as view email passwords if the communication is not encrypted. Tools like Wireshark and Network Miner will allow you to view plain text information in network captures.

## 2.1 Viewing File Systems

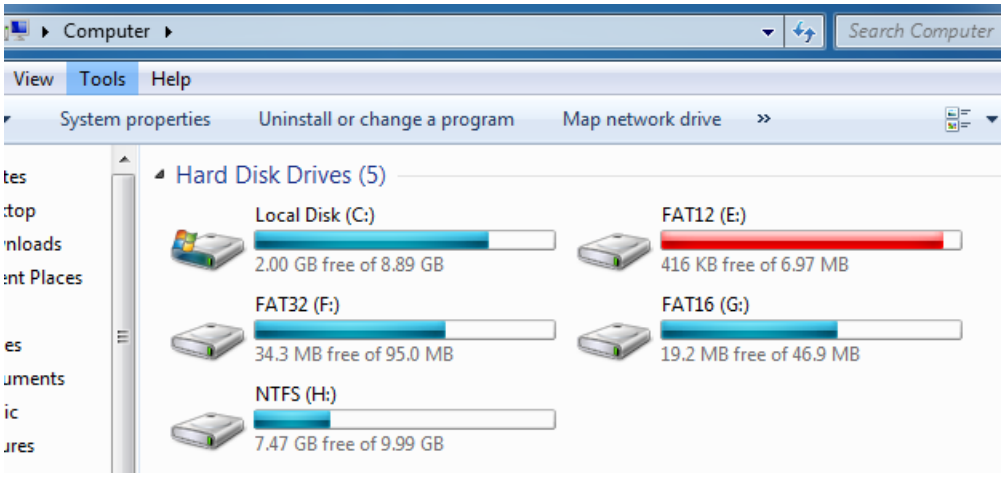
1. To log into the **Windows 7 External Machine**, click on the **Windows 7** icon on the topology.
2. If required, enter the username, **student**.
3. Type in the password, **password,** and press **Enter** to log in.


4. Click on the Start button and click on the link to **Computer**.

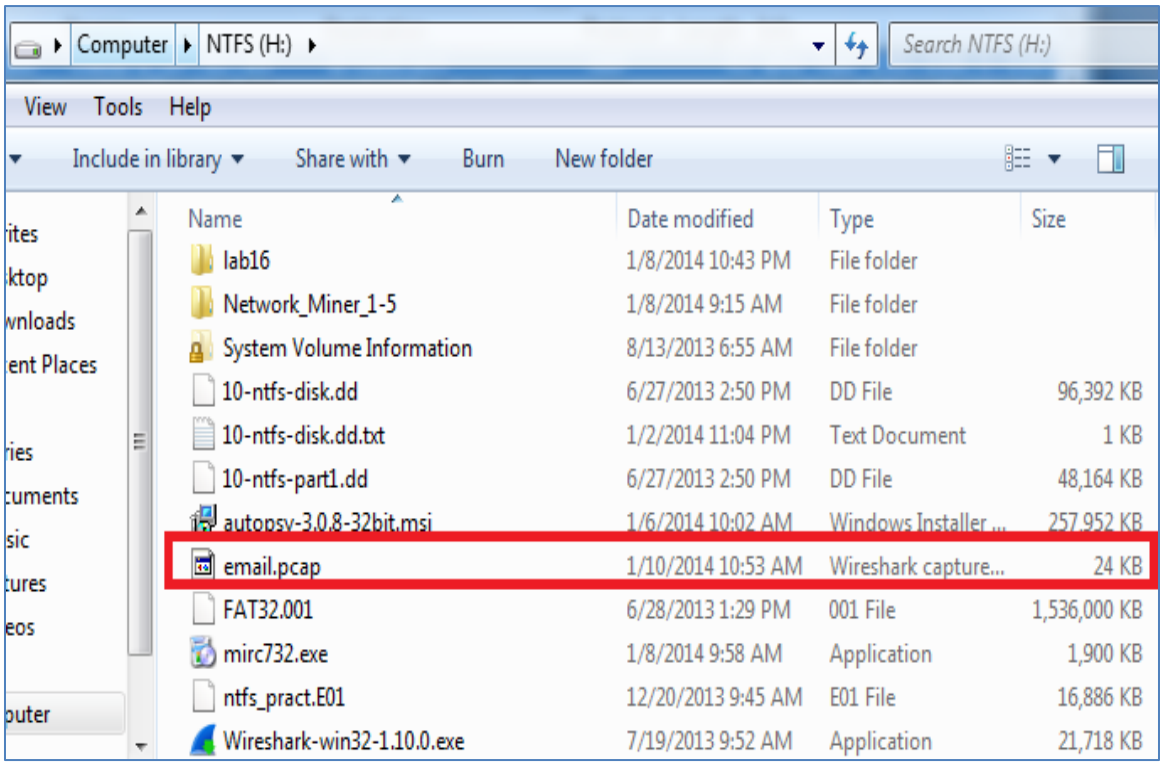



5. Double-click on the NTFS (H:) Drive to access the email capture file.

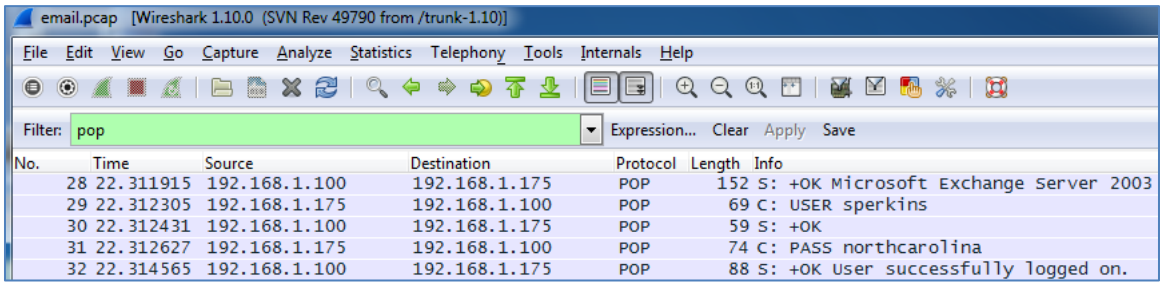



6. Double-click **email.pcap** to open the file in Wireshark.

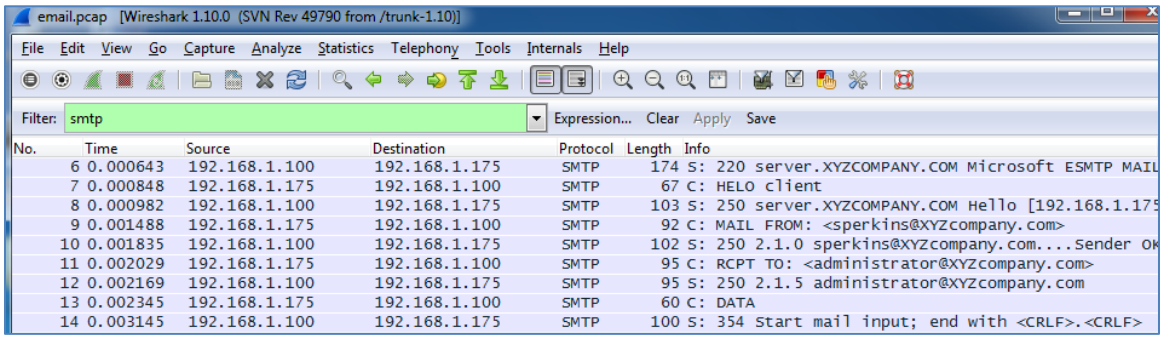


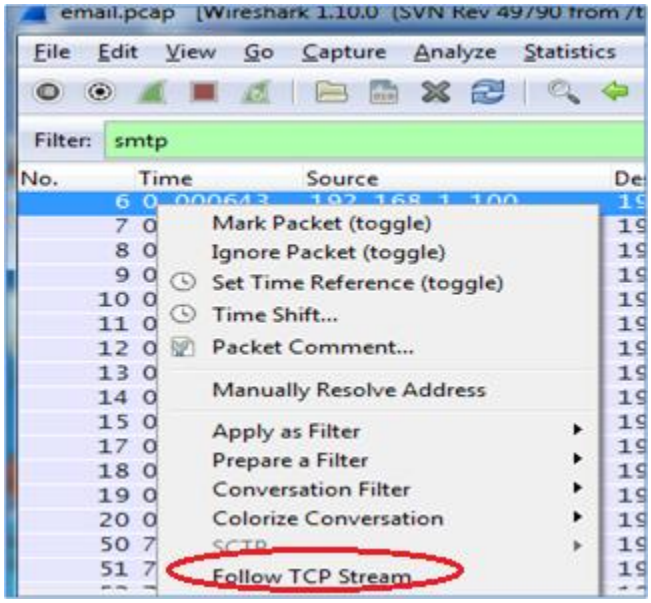
7. Type **pop** in the Wireshark Filter Pane and click Apply. View the POP3 password.




8. Click the Clear button. Type **smtp** in the Wireshark filter pane and click Apply.

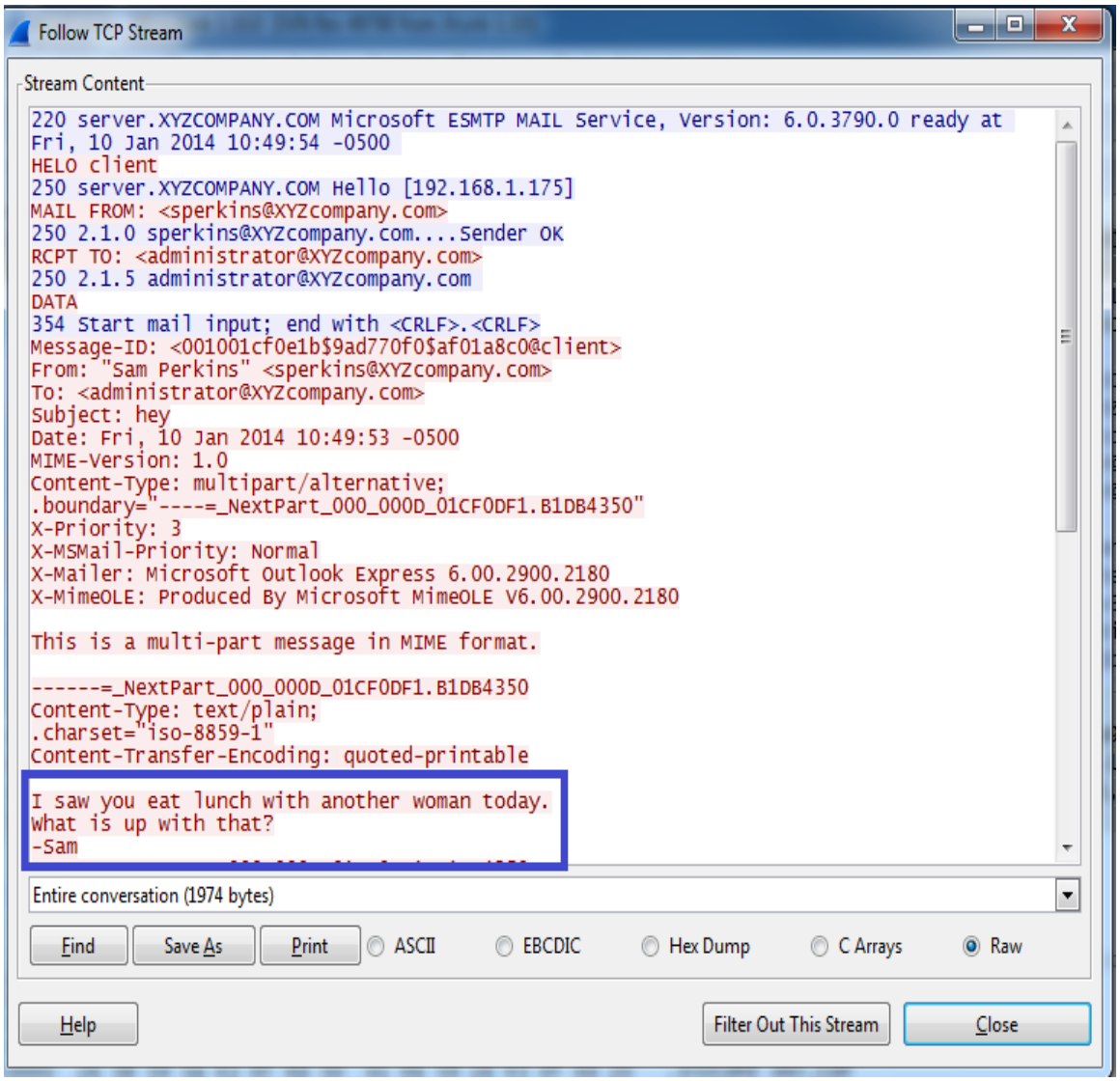



9. Right-click on the first packet (No. 6) and select **Follow TCP Stream**.



10. View the email message contained with the TCP Stream.

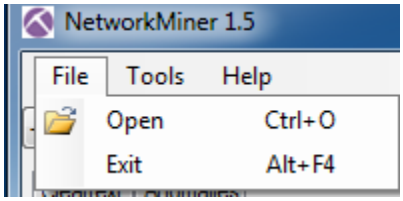



11. Close the TCP Stream and close Wireshark by clicking the red X in the upper-right corner.

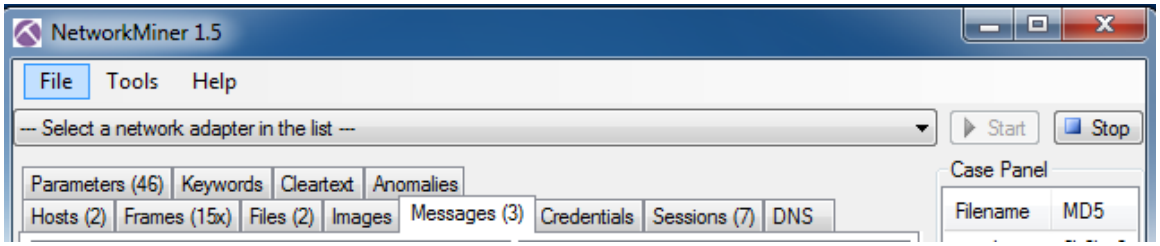
  

12. Click the shortcut to Network Miner on the Windows 7 External Machine desktop.

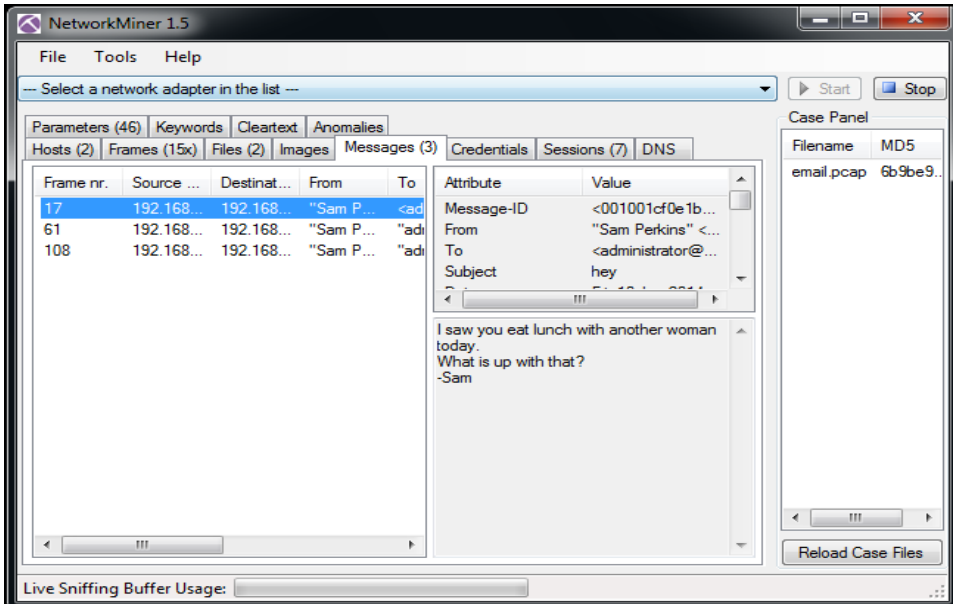

13. Select File from the Menu bar and then select Open.




14. Click on the Messages tab within Network Miner.

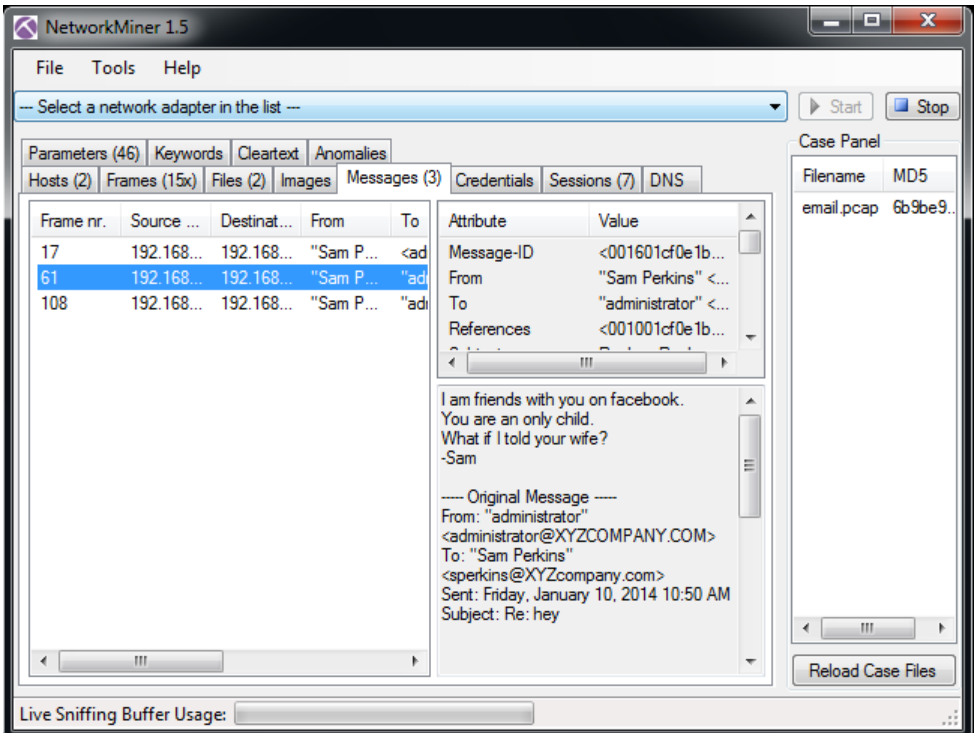



15. Click on the first email message (top) in the list. Read the email.

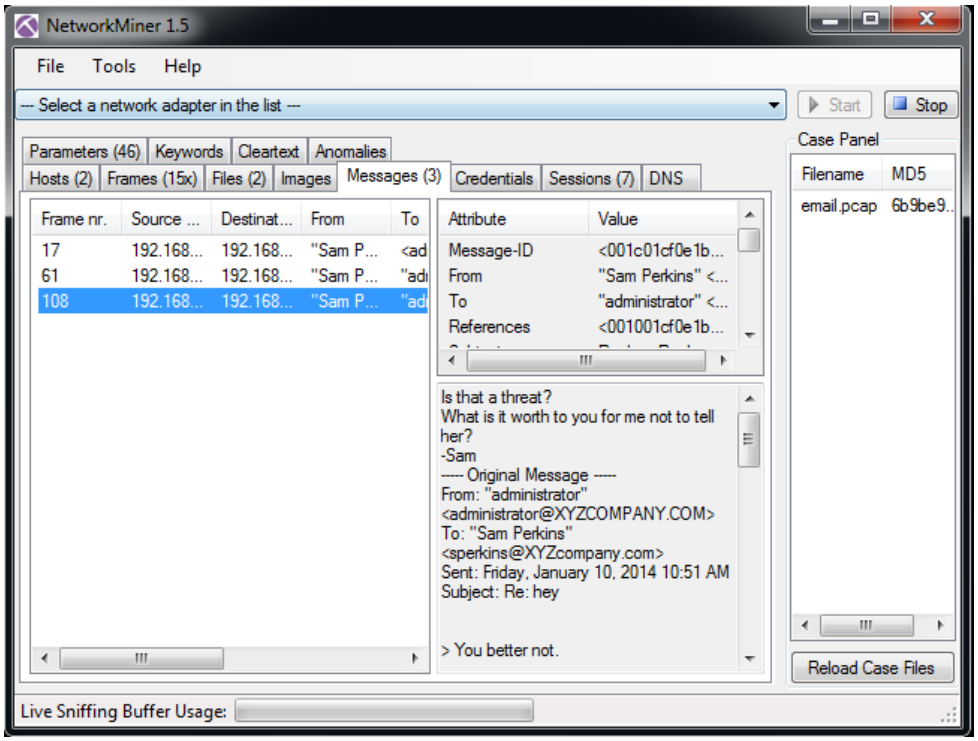


16. Click on the second email message (middle) in the list. Read the email.




17. Click on the third email message (bottom) in the list. Read the email.




18. Close Network Miner when you are finished viewing the emails.

## 2.2 Conclusion

Network forensics tools allow you to look through capture files and find forensic evidence, such as email messages. Commonly used network forensics tools include Wireshark and Network Miner, which will allow you to view plain text information in network captures.

## 2.3 Discussion Questions

1. What filter in Wireshark might provide you with plain text email passwords?
2. Where do you go within Network Miner to view email messages in plain text?
3. What filter in Wireshark will allow you to view plain text sent mail?
4. How do you get more information about a TCP Stream in Wireshark?

# 3 Internet Relay Chat

Internet Relay Chat is used to communicate with other Internet users. IRC is an older technology and is not considered mainstream today.

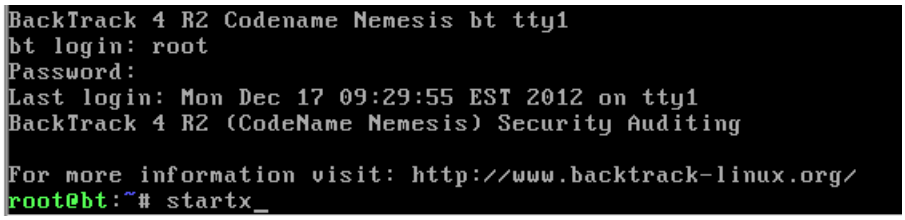
Keep in mind that **Linux commands are case sensitive**. The commands below must be entered exactly as shown.

## 3.1 Extracting Files from PTK

1. Log into the Linux Sniffer with the username of **root** and the password of **toor**.

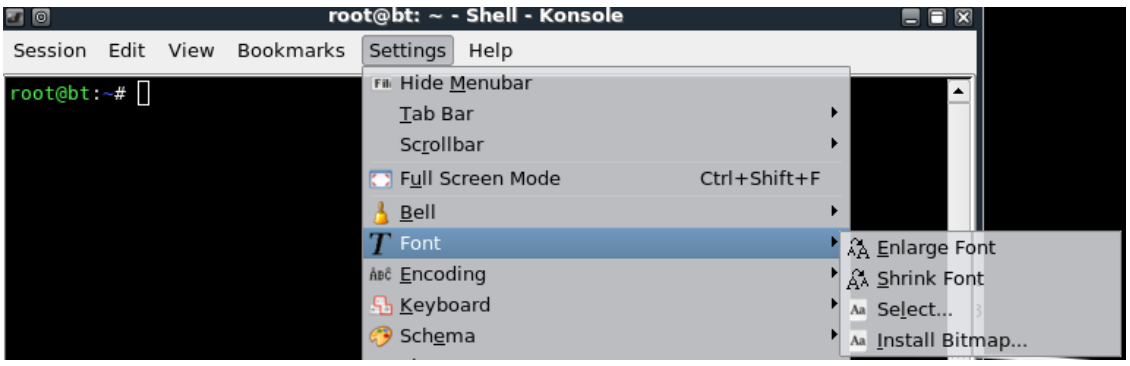
For security purposes, the password will not be displayed.

2. Type the following command to initialize the GUI, Graphical User Environment:
   root@bt:~**#startx**




3. Open a terminal on the Linux system by clicking the picture to the right of Firefox in the task bar in the bottom of the screen in BackTrack.

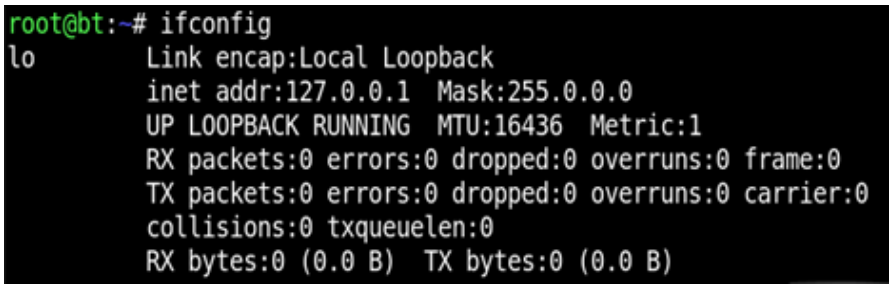
4. After opening the terminal, you may want to consider adjusting the size of the font. To increase the font size within the terminal, click **Settings** from the Terminal menu bar, select font, then select enlarge font.



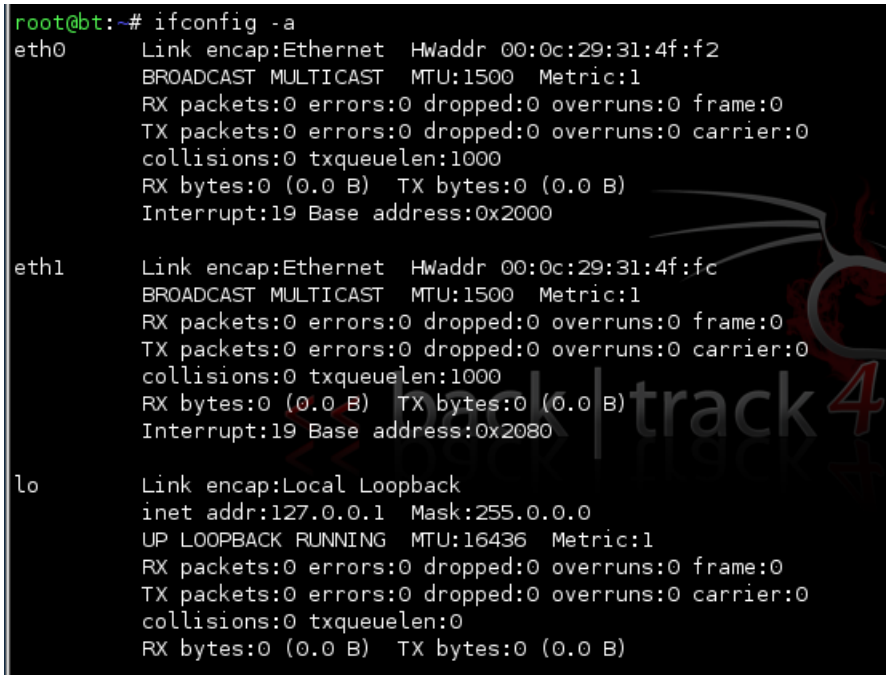

  

One of the nice features off some versions of BackTrack is that they are not automatically assigned IP addresses through the use of Dynamic Host Configuration Protocol (DHCP). The idea is to come on the network quietly, without being detected.

5. Only the loopback address, 127.0.0.1, is displayed when you type:
   root@bt:~**#ifconfig**




6. Type the following command to view all available interfaces on the system:
   root@bt:~**#ifconfig -a**




7. To activate the second interface, type the following command:
   root@bt:~**#ifconfig eth1 up**

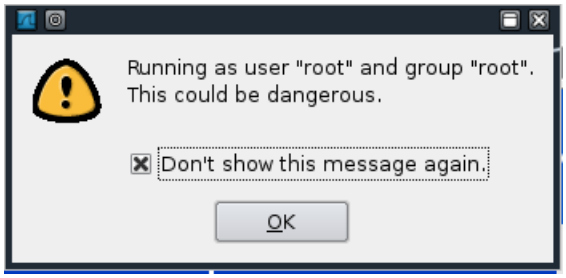
8. To verify the first interface, type the following command:
   root@bt:~**#ifconfig eth1**

```
root@bt:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:0c:29:64:0f:a2
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:82 (82.0 B)  TX bytes:0 (0.0 B)
          Interrupt:16 Base address:0x20a4
```

9. On the sniffer machine, type the following command to launch Wireshark:
   root@bt:~# **wireshark**

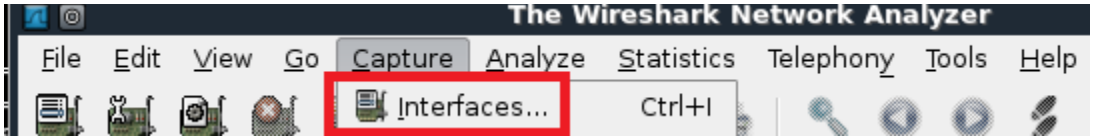
```
root@bt:~# wireshark
```

10. Check the *Don't show the message again* box and click the OK button.

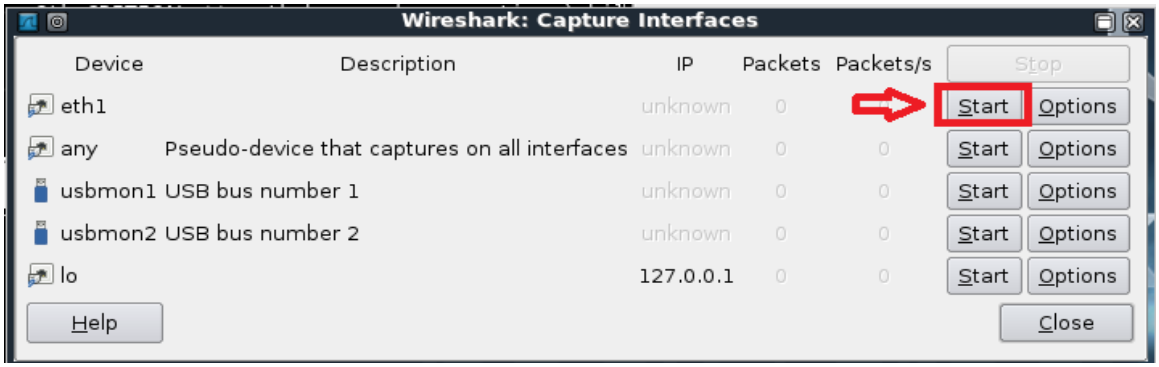



Before sniffing network traffic, we want to designate the External interface.

11. Select Capture from the Wireshark menu bar and choose **Interfaces**.



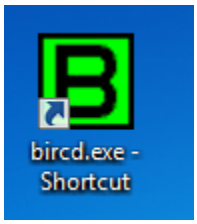

12. Locate eth1 on the left side. Click the Start button to the right of it.




13.

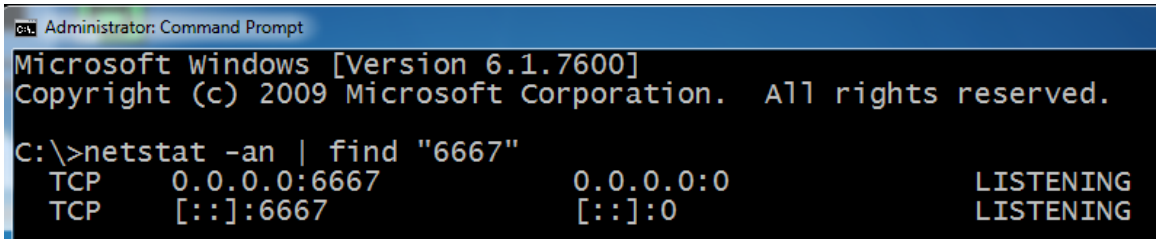
  

14. On the Windows 7 External Machine, double-click on the shortcut to **bircd.exe**.




15. On the Windows 7 External Machine, double-click on the shortcut to the command prompt.

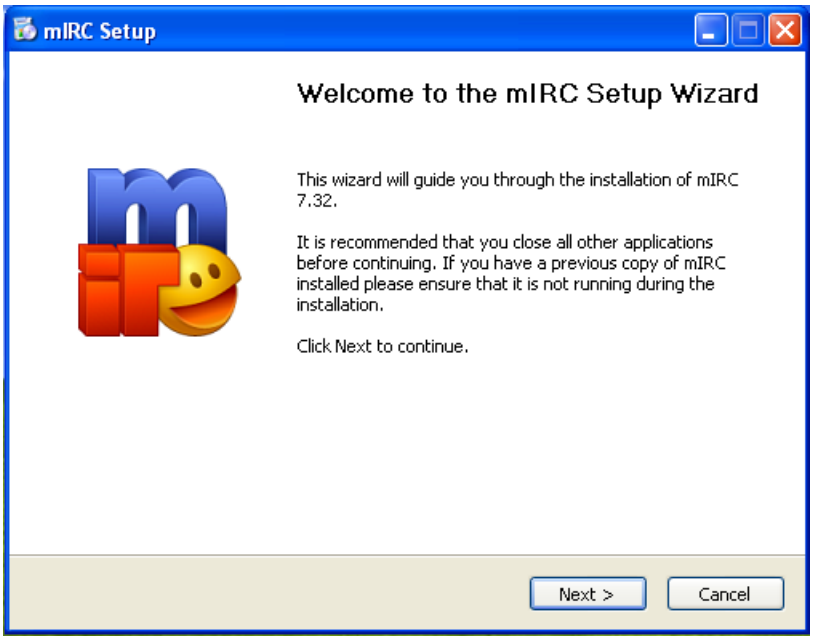

16. Type the following to verify that Windows 7 is listening on the IRC port:
C:\>**netstat -an | find "6667"**



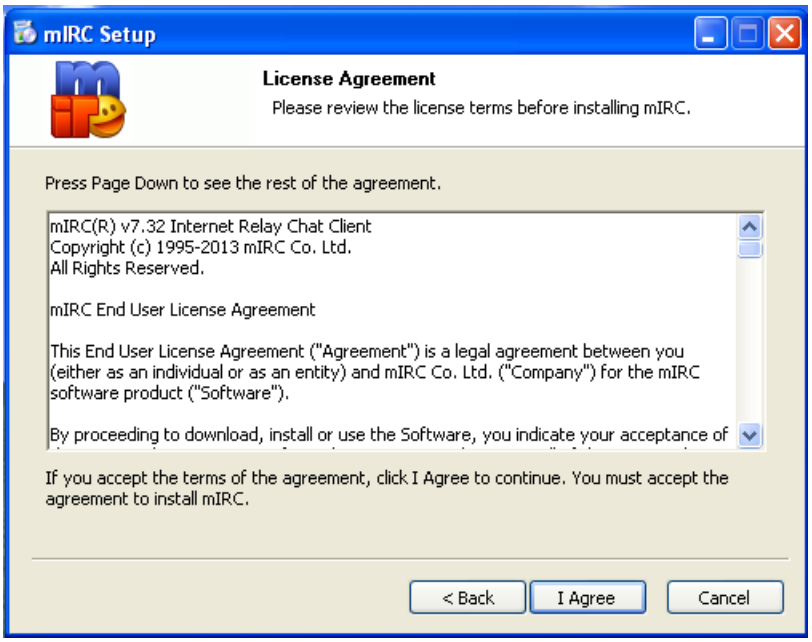

17. On the Windows XP Pro Internal Machine, double-click **mirc732.exe** on the desktop.

18. Click next at the Welcome to the mIRC setup Wizard.

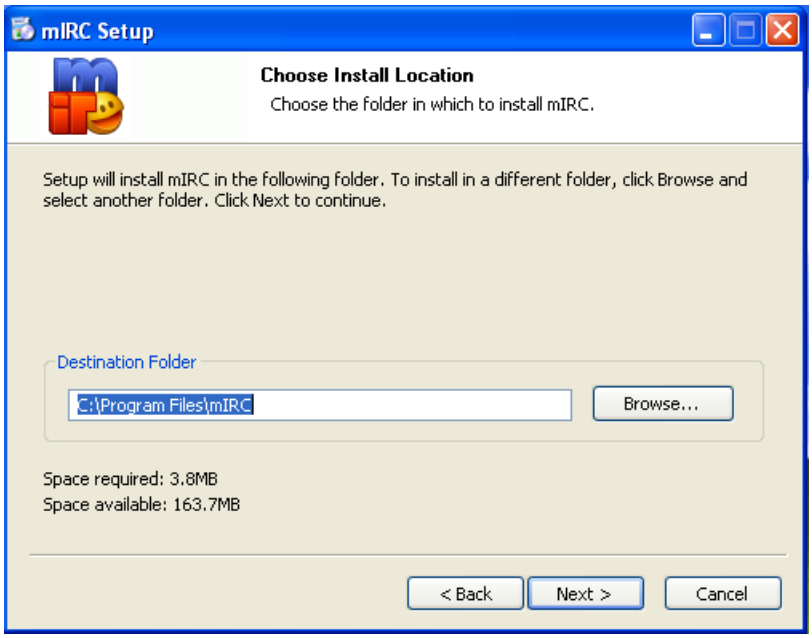



19. Read over the license agreement and click Agree if you agree to the terms.

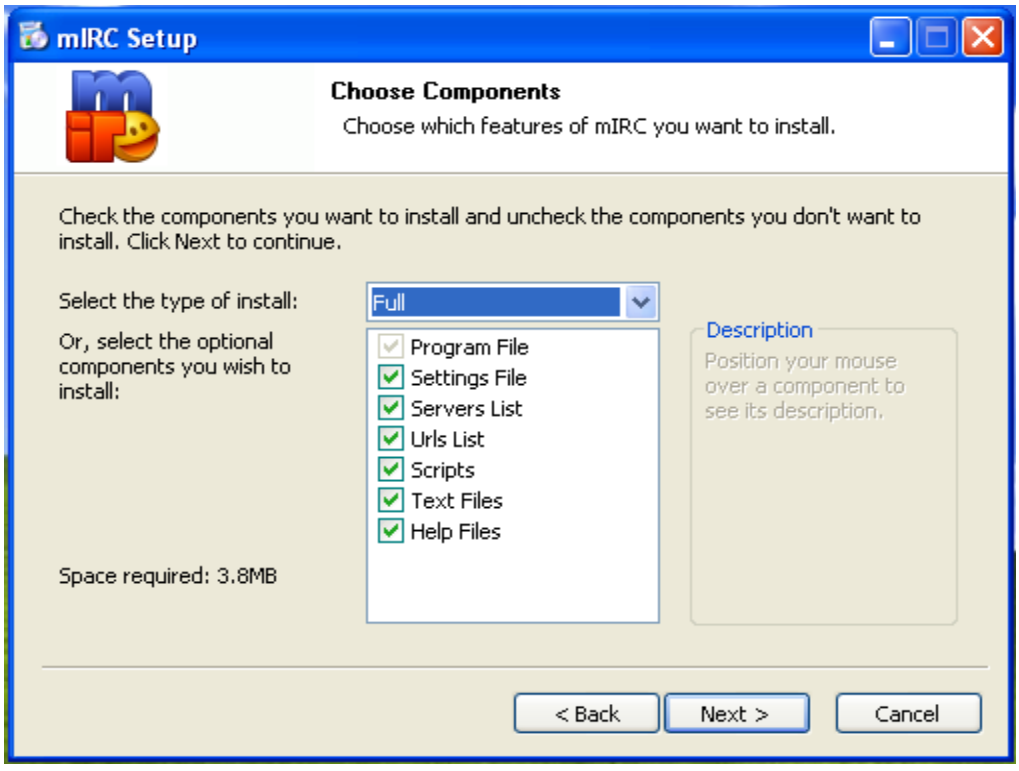


20. Click Next at the Choose Install Location (to accept the default).

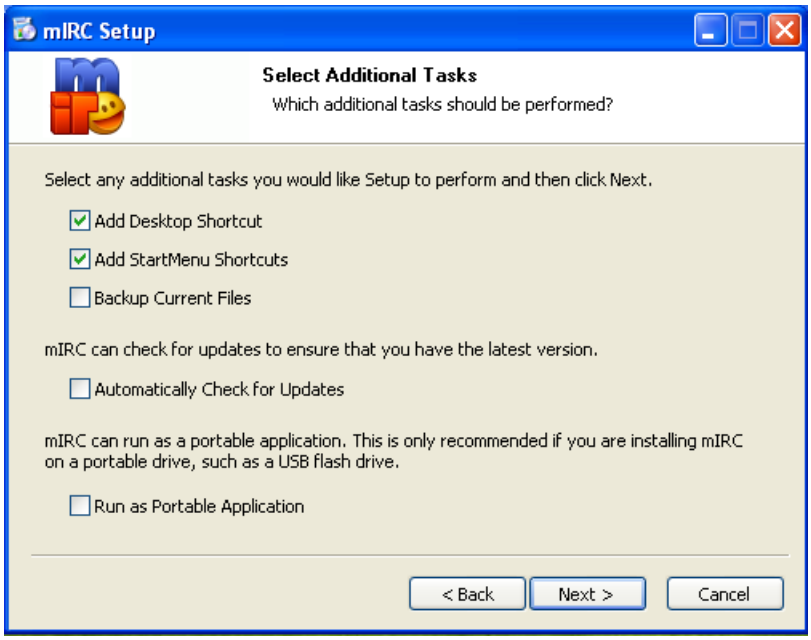



21. Click Next at the Choose Components Screen of mIRC.

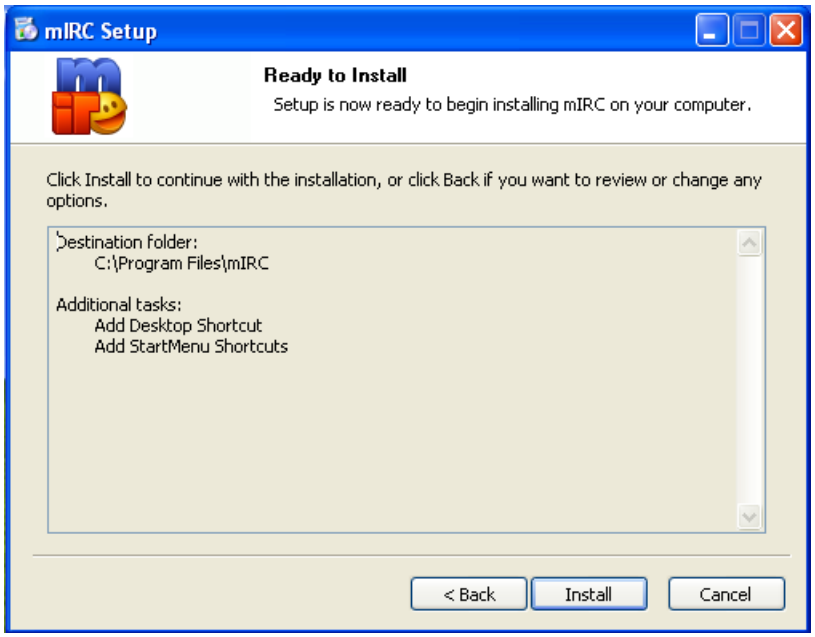


22. Uncheck **Backup Current Files** and **Automatically Check for Updates**. Click Next.




23. Click Install at the Ready to Install screen.



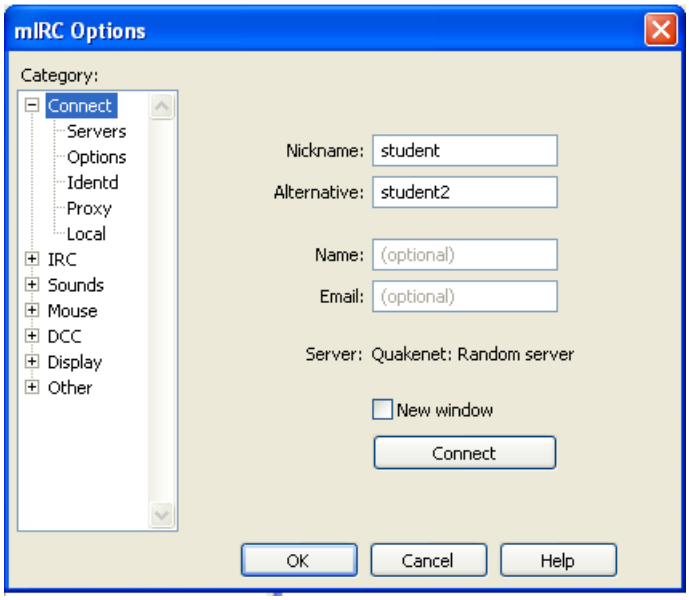

  

24. At the Completing the mIRC Setup Wizard screen, check Run mIRC.

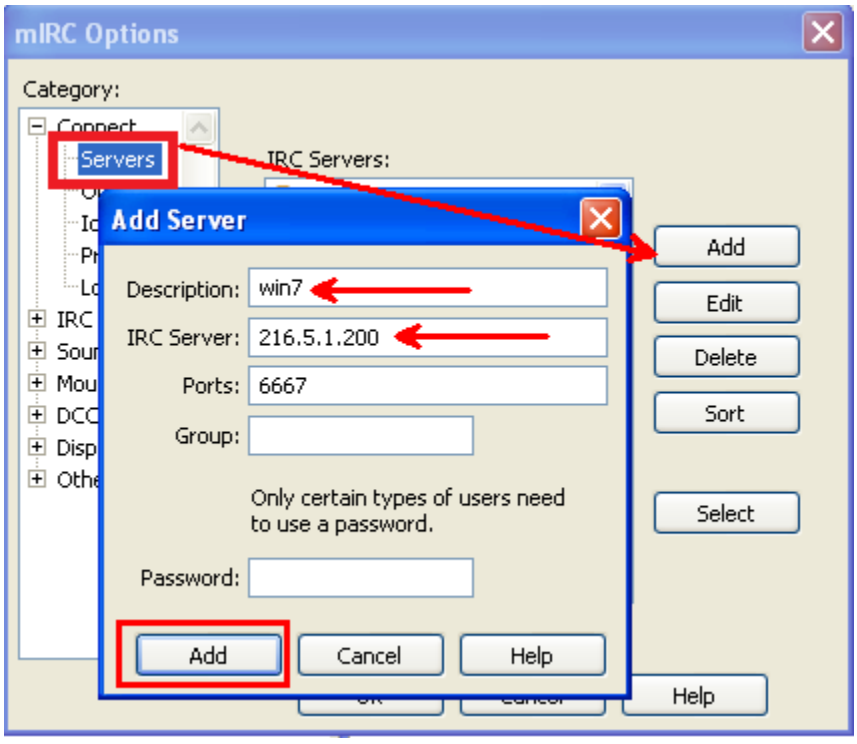

25. Click Continue at the About mIRC screen. You will be using an evaluation copy that will function for 30 days.

26. For nickname, enter **student**. For alternate, enter **student2**.

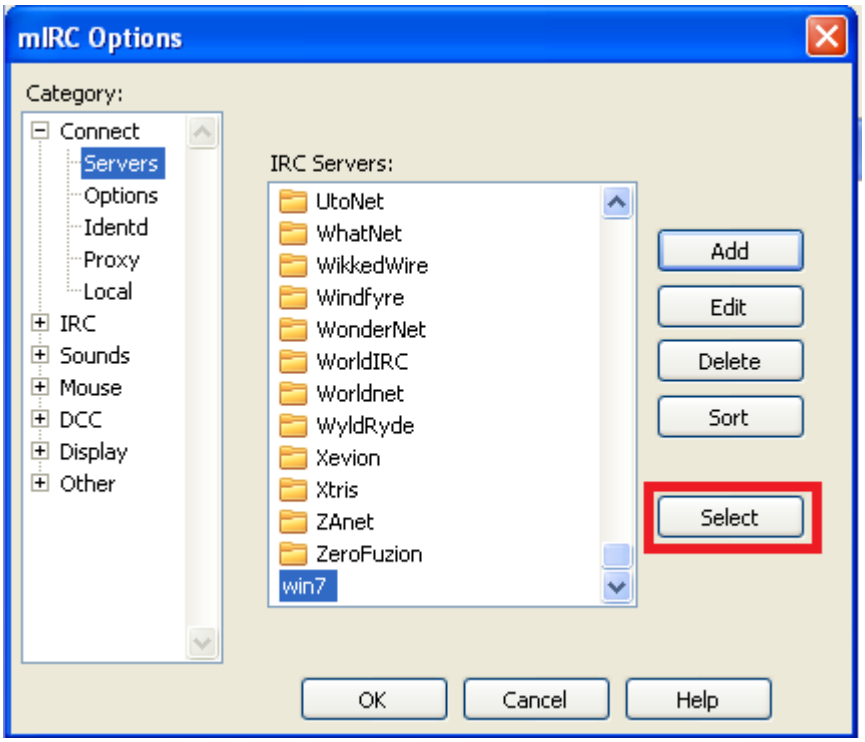



27. Click **Servers**. Click **Add**. For the description, put **Win7**. Enter **216.5.1.200** for the Internet Protocol (IP) address of the Internet Relay Chat (IRC) Server.

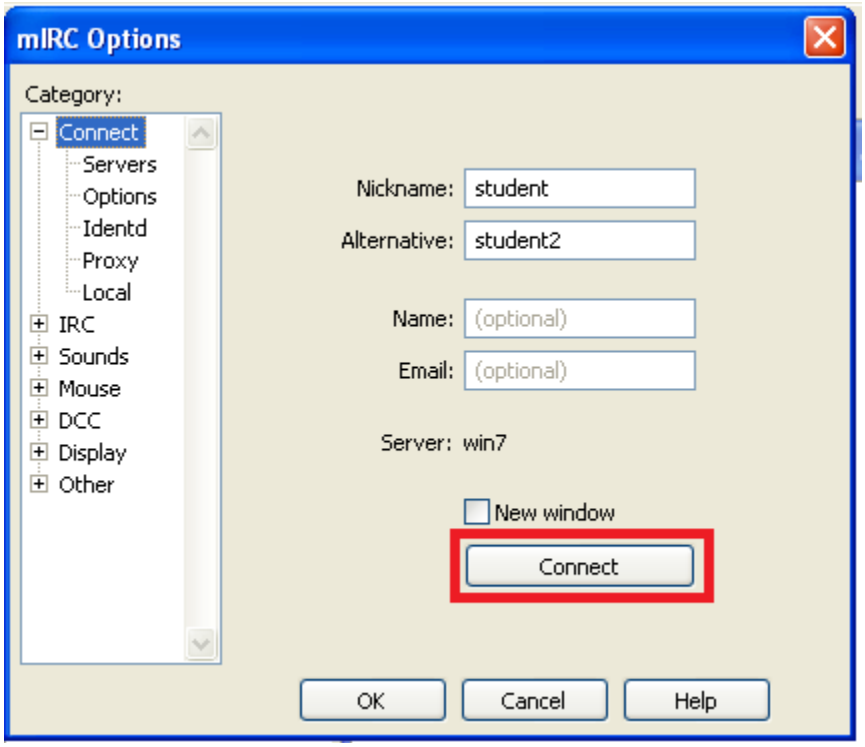


28. Click the **Select** button and click OK.

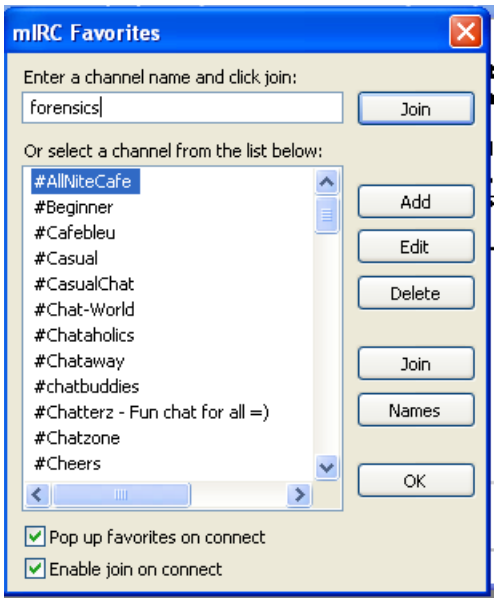



29. Click **Connect** to connect to the IRC server with the nickname student.

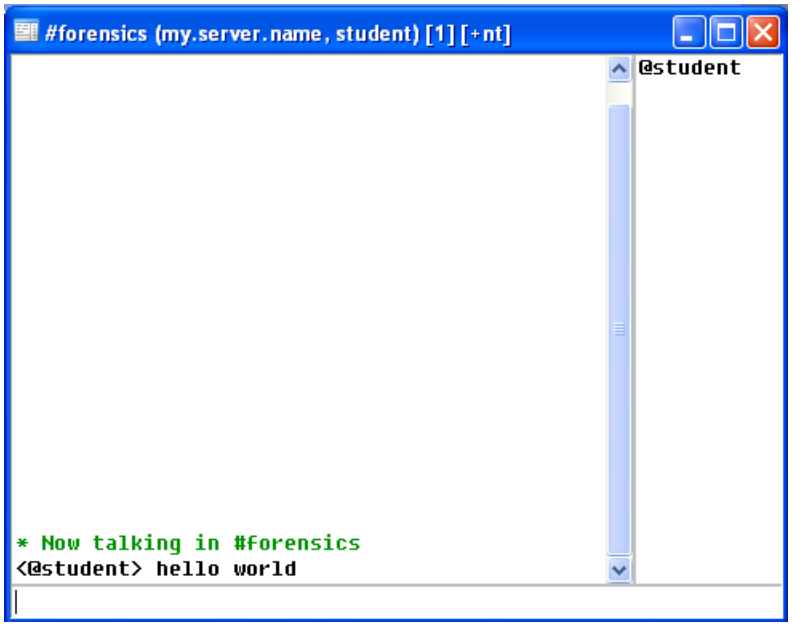


30. After the connections, type forensics for the channel name and click Join.

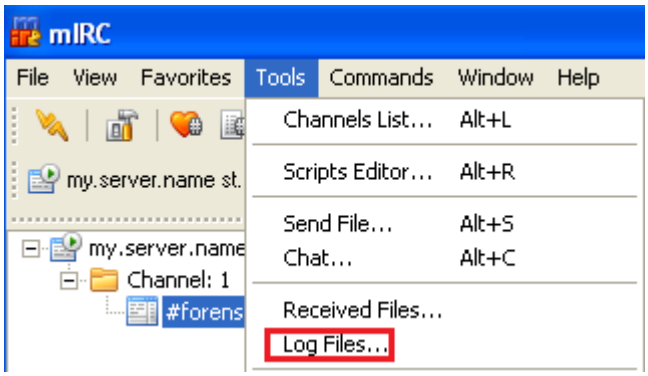



31. In the forensics room, type **hello world** and press Enter.

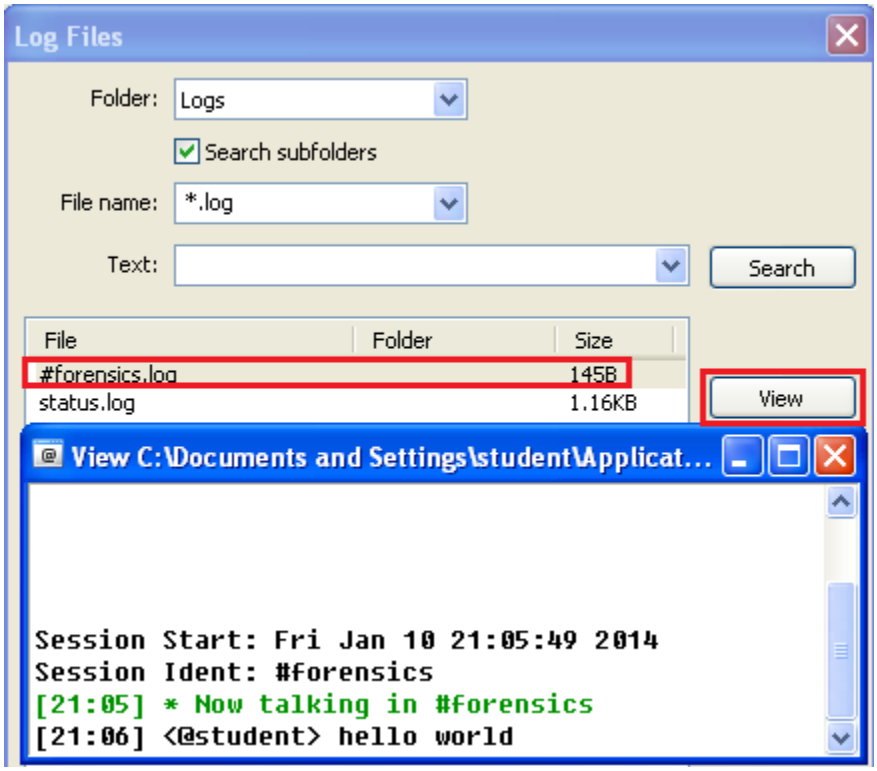


32. To access the chat logs on the system, select Tools, then **Log Files**.

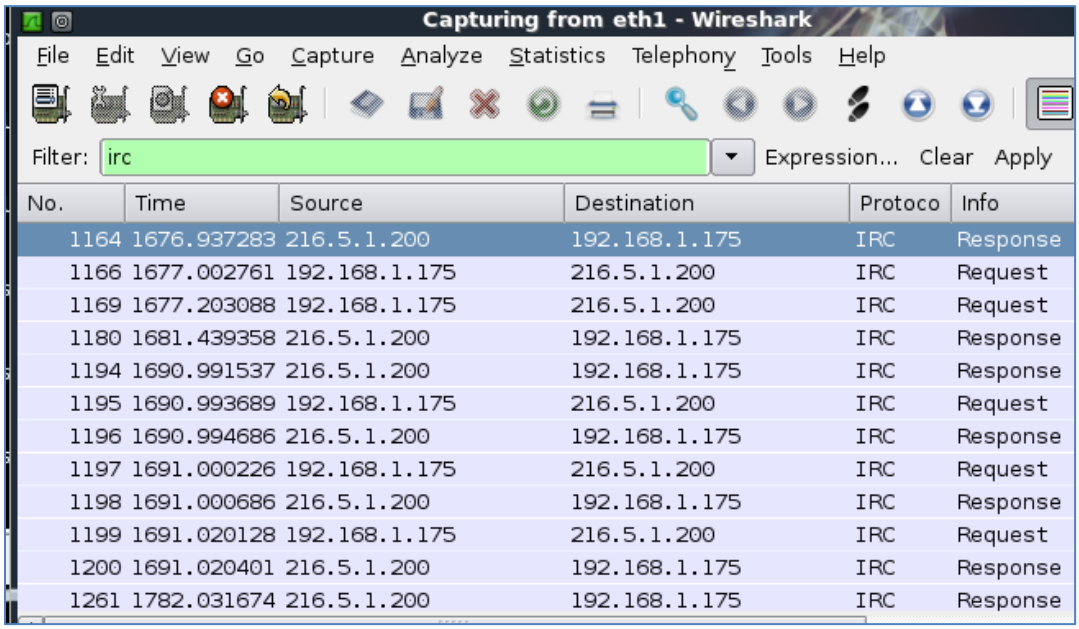



33. To view the chat logs on the system, select the forensics log and click **View**.

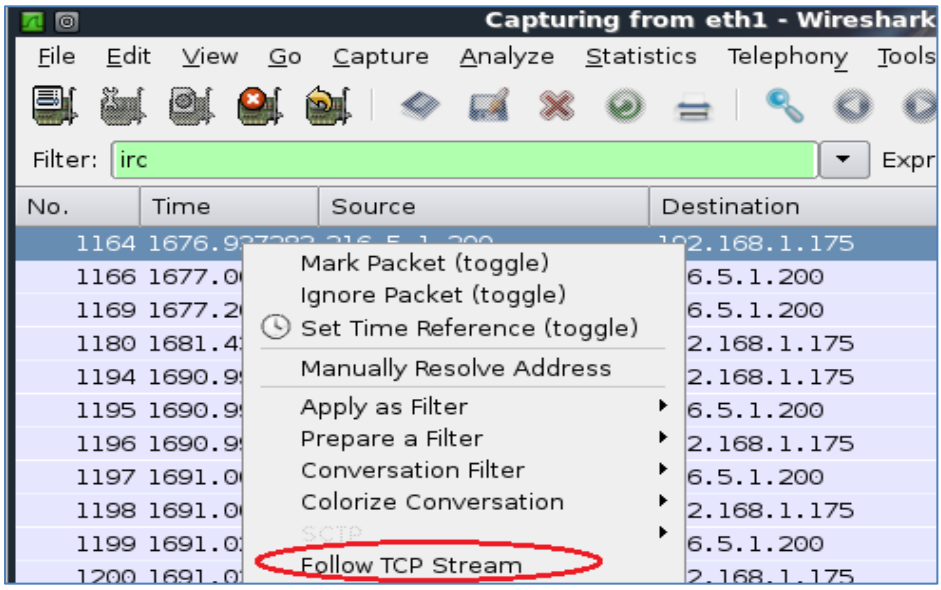


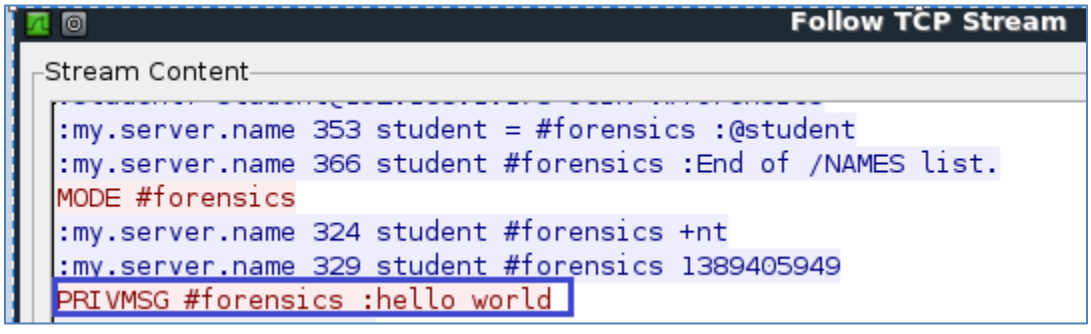
34. On the Linux Sniffer, type irc in the filter pane and click Apply.




35. Right-click on the first displayed packet and select **Follow TCP Stream**.




36. View the Transmission Control Protocol (TCP) Stream.



## 3.2 Conclusion

Internet Relay Chat is used to communicate with other Internet users. IRC is an older technology, which is not always encrypted, and typically uses port 6666-6669.

## 3.3 Discussion Questions

1. What ports does IRC typically use?
2. What does IRC stand for?
3. Name an application that can be used as an IRC client.
4. What command can be used to verify an IRC server is listening on a port?

## References


1. Outlook Express:
   http://en.wikipedia.org/wiki/Outlook_Express

2. Microsoft Outlook:
   http://office.microsoft.com/en-us/outlook/

3. Internet Replay Chat:
   http://en.wikipedia.org/wiki/Internet_Relay_Chat

4. Simple Mail Transfer Protocol:
   http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

5. Post Office Protocol (Version 3):
   http://en.wikipedia.org/wiki/Post_Office_Protocol