



## DIGITAL FORENSICS LAB SERIES

### Lab 12: Communication Artifacts

**Objective: User Communications Analysis**

**Document Version: 2015-09-28**



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

Development was 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.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.

## Contents

Introduction .....	3
Objective: User Communications Analysis .....	3
Lab Topology .....	4
Lab Settings .....	5
1 Email Messages and Programs .....	6
1.1 Viewing Workstation Email .....	6
1.2 Conclusion .....	18
1.3 Discussion Questions.....	18
2 Examining Emails in Network Traffic .....	19
2.1 Viewing File Systems .....	19
2.2 Conclusion .....	26
2.3 Discussion Questions.....	26
References .....	27



## Introduction

This lab includes the following tasks:

1. Email Messages and Programs
2. Examining Emails in Network Traffic

## Objective: User Communications Analysis

Performing this lab will provide the student with a hands-on lab experience meeting the User Communications Analysis 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 litigation in general. Forensic Software like EnCase and FTK will allow you to view the email messages from programs like Outlook and Outlook Express.

**POP3** – Post Office Protocol Version 3. Uses Port 110 by default to receive mail.

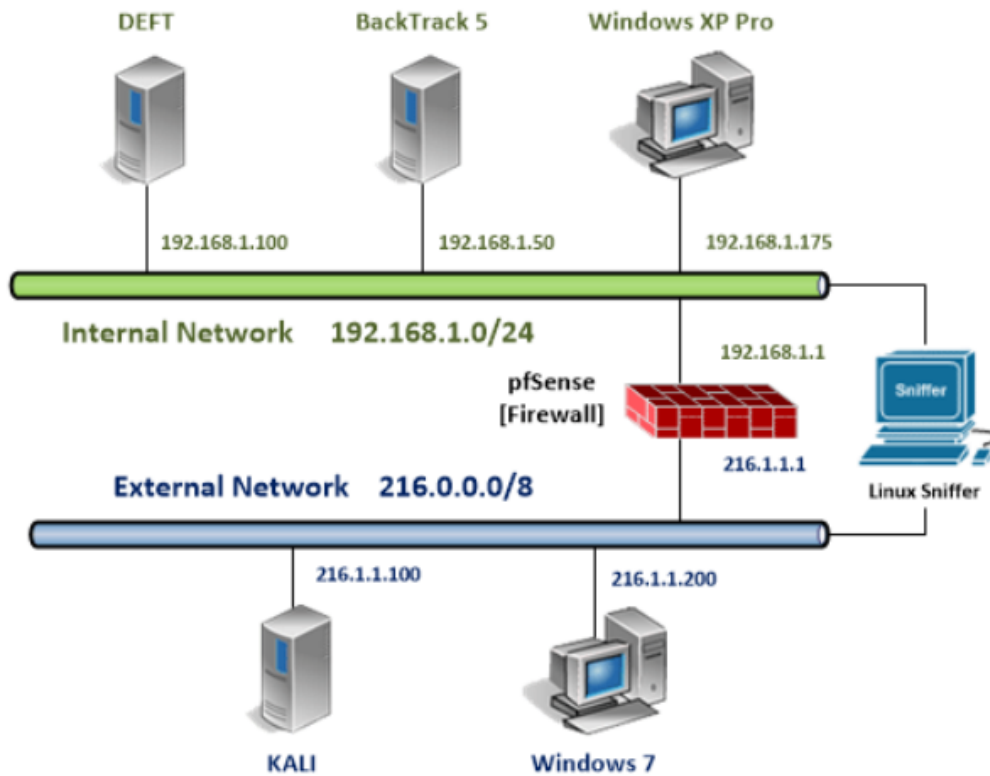
**SMTP** – Simple Mail Transfer Protocol. Uses Port 25 by default to send mail.

**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](http://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	216.1.1.200	student	password

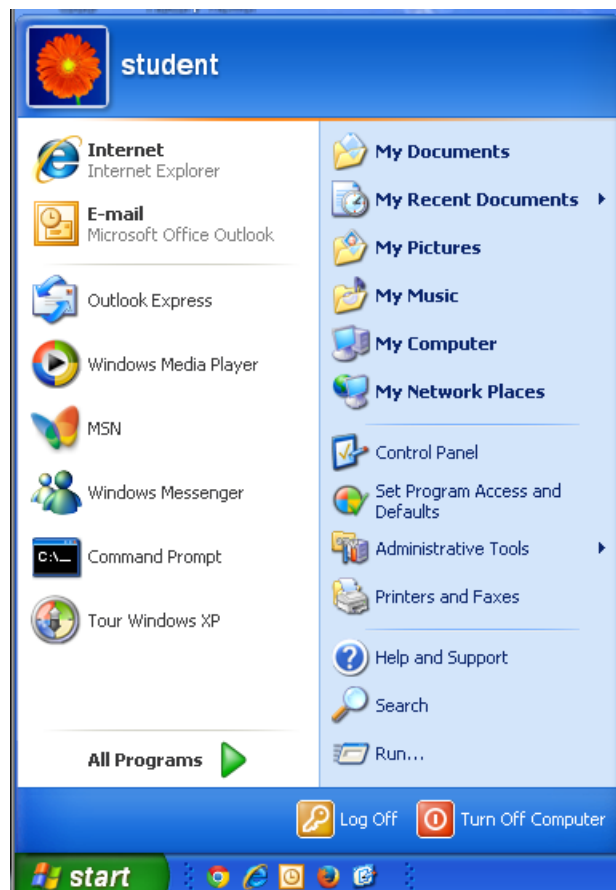


## 1 Email Messages and Programs

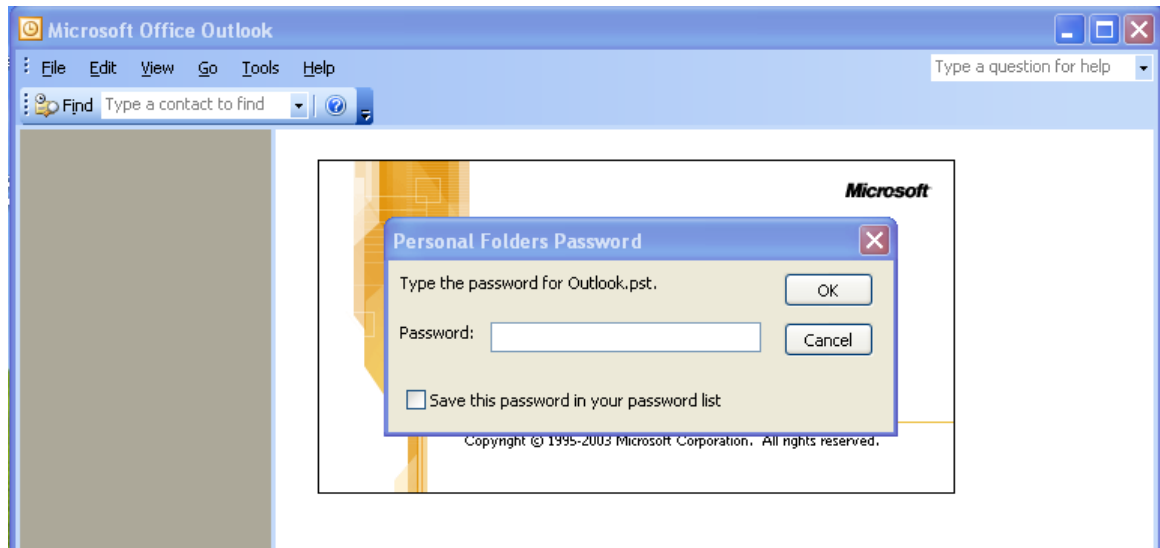
Email messages can play a critical role in criminal investigations, the e-discovery process, and litigation in general. Forensic software like EnCase and FTK will allow you to view email messages from programs like Outlook and Outlook Express. Outlook comes with Microsoft Office, and Outlook Express 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 these 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 My Computer.



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

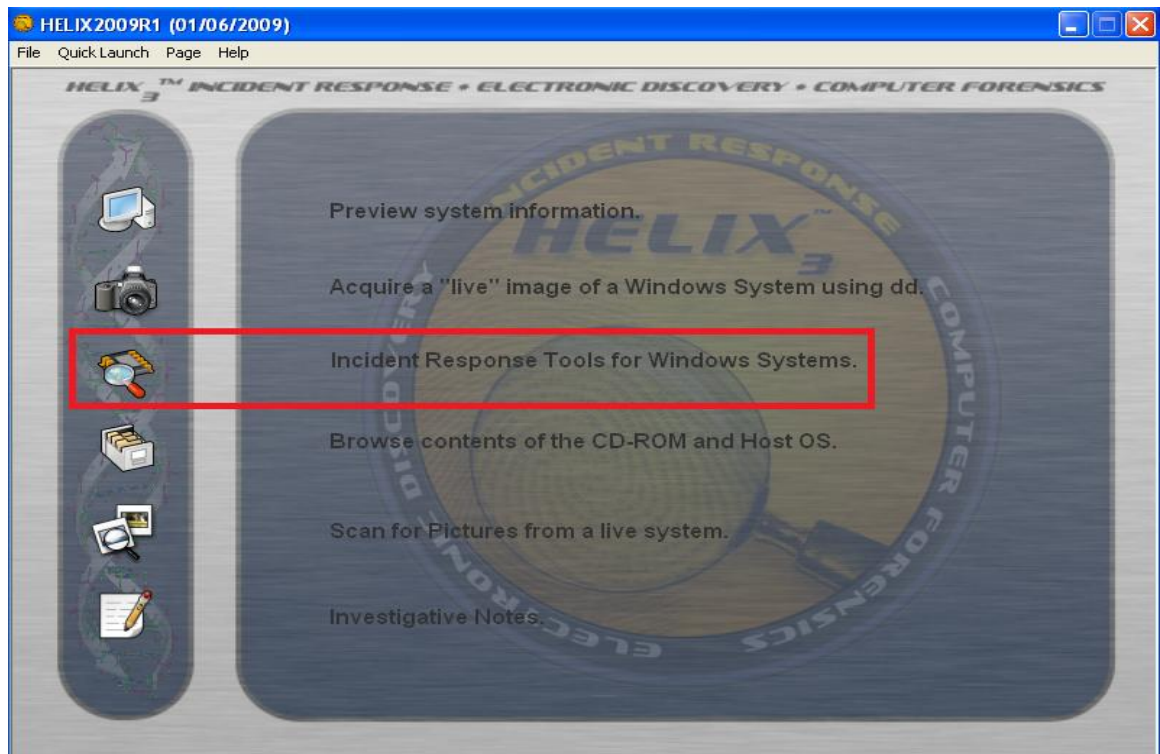


- Click **Accept** to Accept the HELIX warning.

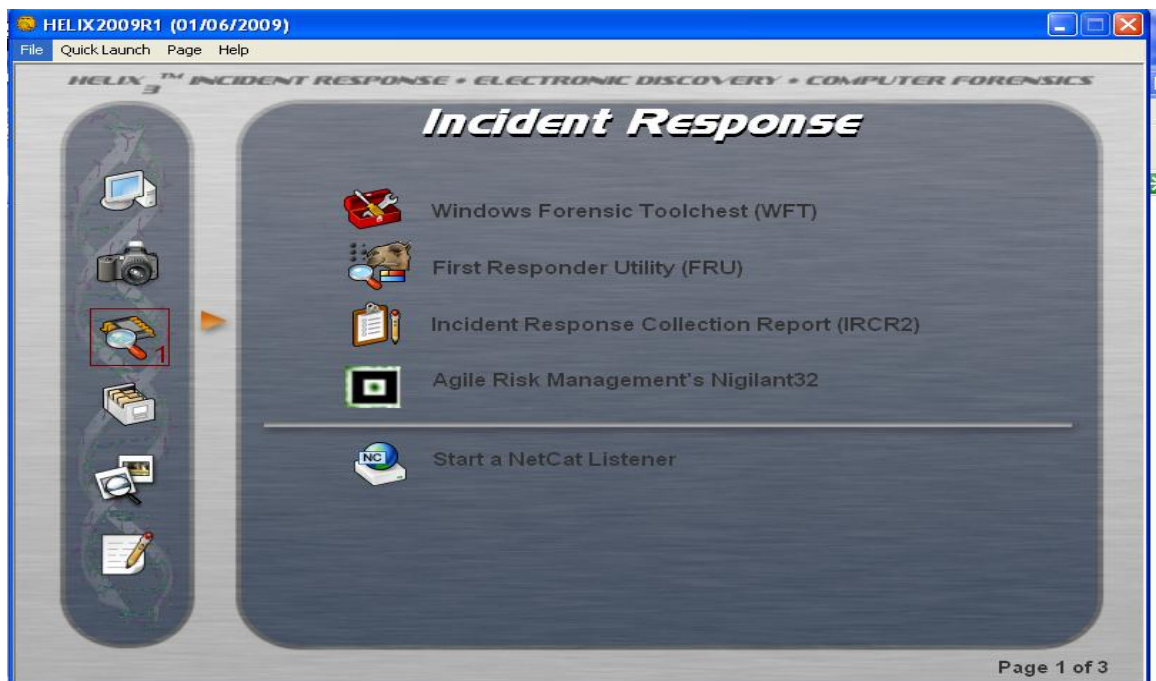




- Click on the icon to select the **Incident Response Tools for Windows Systems**.



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

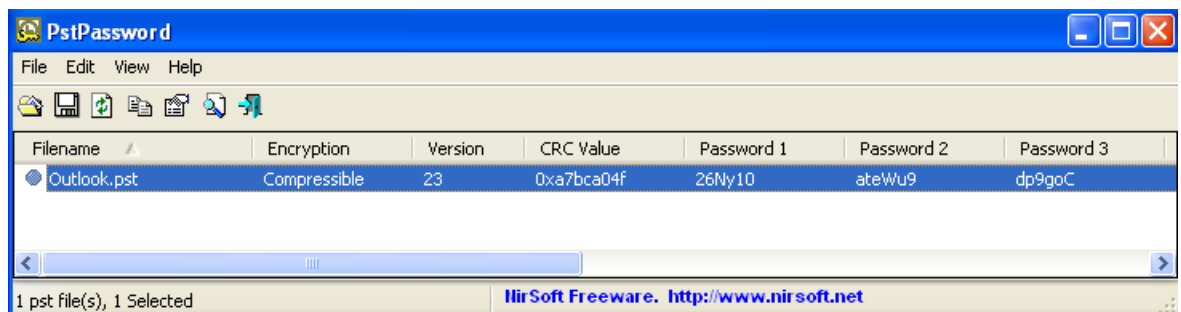


8. Click the icon in front of the **PST Password Viewer**. Click **Yes** in response to, IS THIS OK?



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

Make note of these passwords for later use.

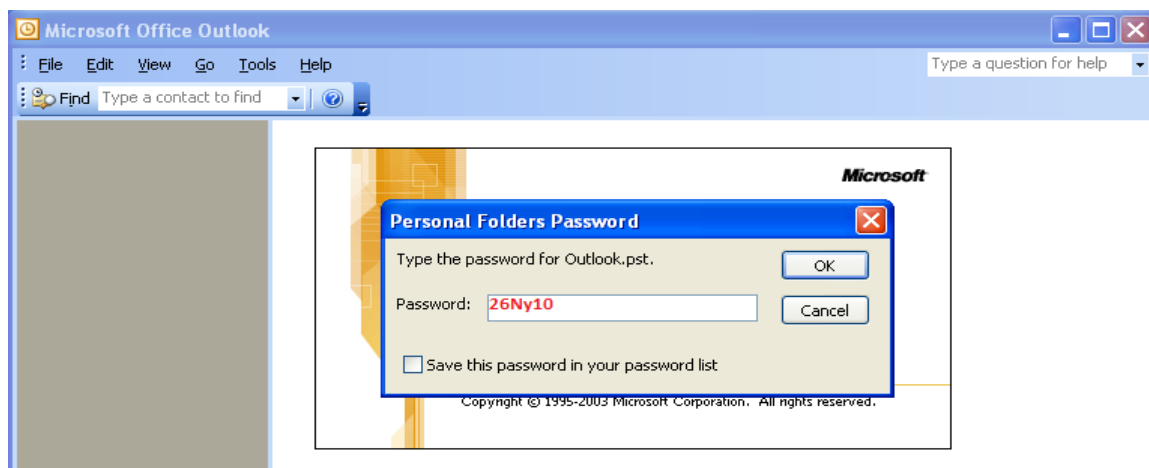


10. Once again, on the Windows XP Pro Internal Machine, click on the Start button and select E-mail.



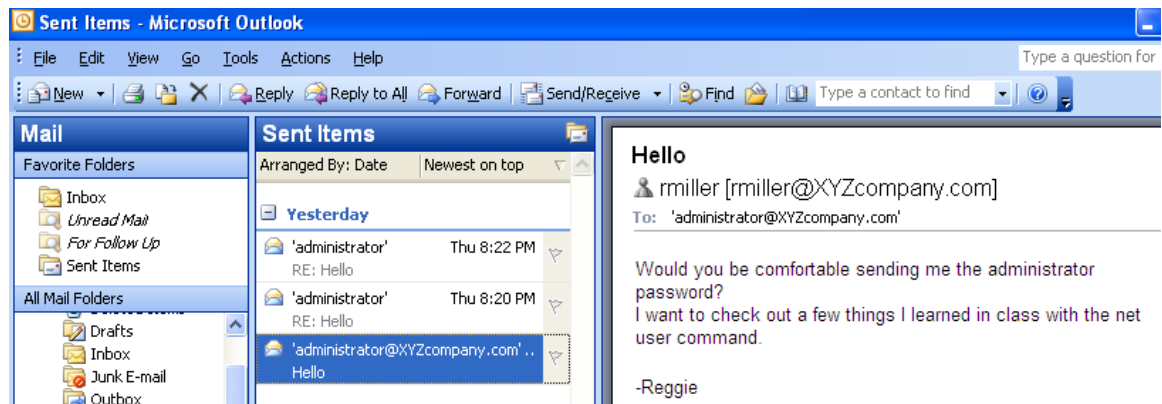
11. You are prompted for a Personal Folders Password. Enter one of the three passwords that PSTPassword provided (in the example below, we use the password **26Ny10**, see Step 9) and click **OK**.

Be aware that passwords are case sensitive.

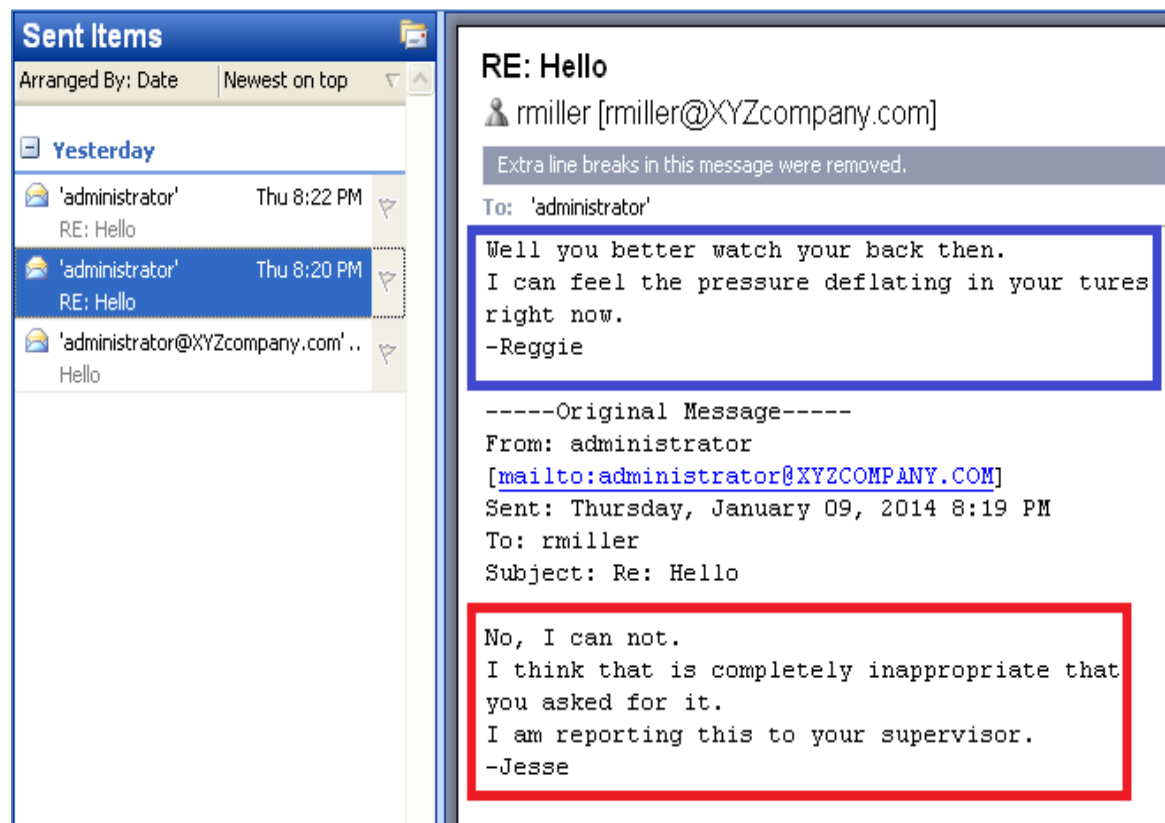


12. Click **Cancel** on the Identity Login screen.

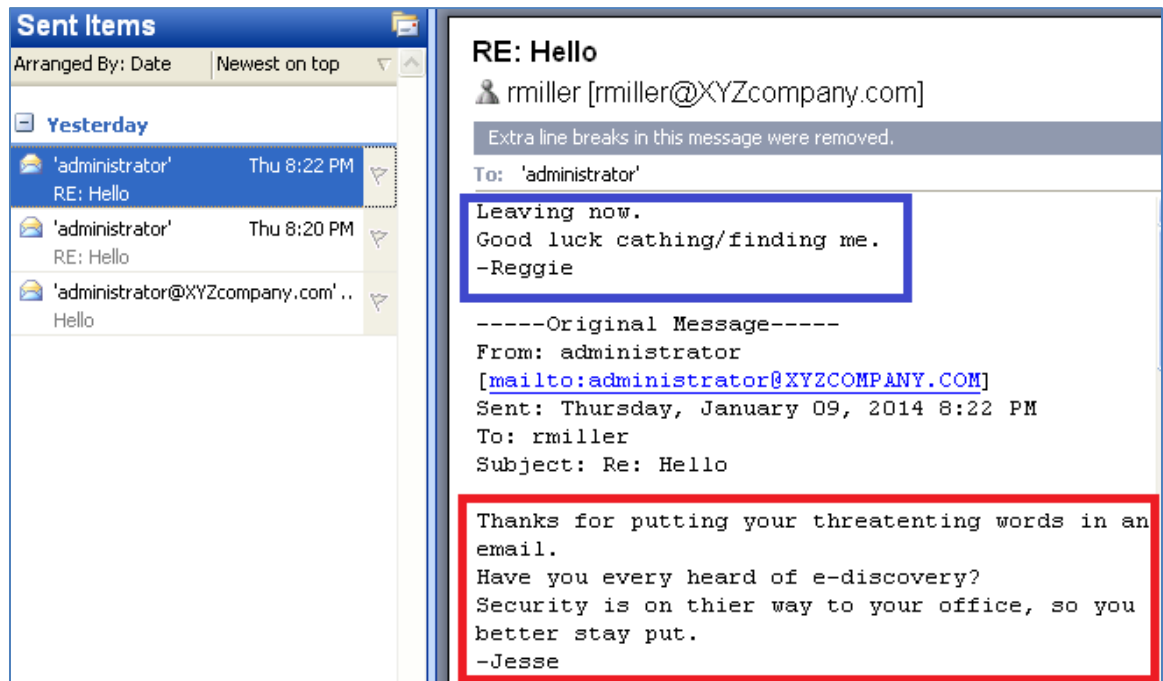
13. Click on the **Sent Items** folder. Select the email at the bottom of the list and read it.



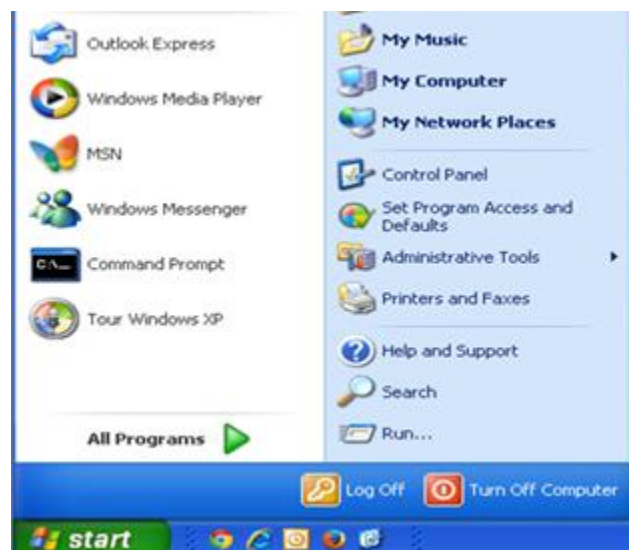
14. In the **Sent Items** folder, select the middle email in the list and read it.



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



16. Close Outlook when you are finished viewing the email correspondence.
17. On the Windows XP Pro Internal Machine, click on the **Start button**, select **Outlook Express** (if Outlook express is not displayed on the start menu, select **Start > All Programs > Outlook Express**).





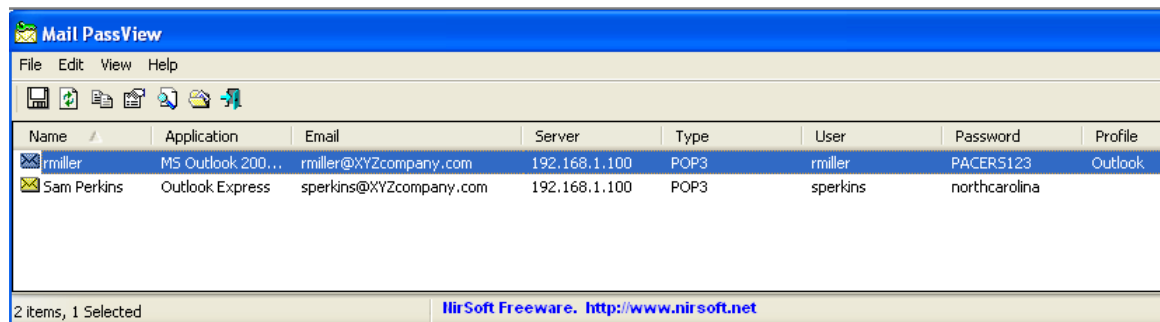
18. Click Main Identity. We do not know the password.



19. 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?



## 20. View the extracted passwords for Outlook and Outlook Express.



Name	Application	Email	Server	Type	User	Password	Profile
rmiller	MS Outlook 200...	rmiller@XYZcompany.com	192.168.1.100	POP3	rmiller	PACER5123	Outlook
Sam Perkins	Outlook Express	sperkins@XYZcompany.com	192.168.1.100	POP3	sperkins	northcarolina	

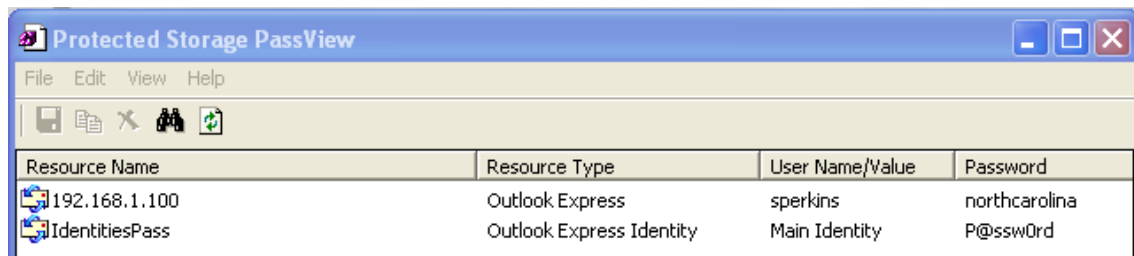
2 items, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

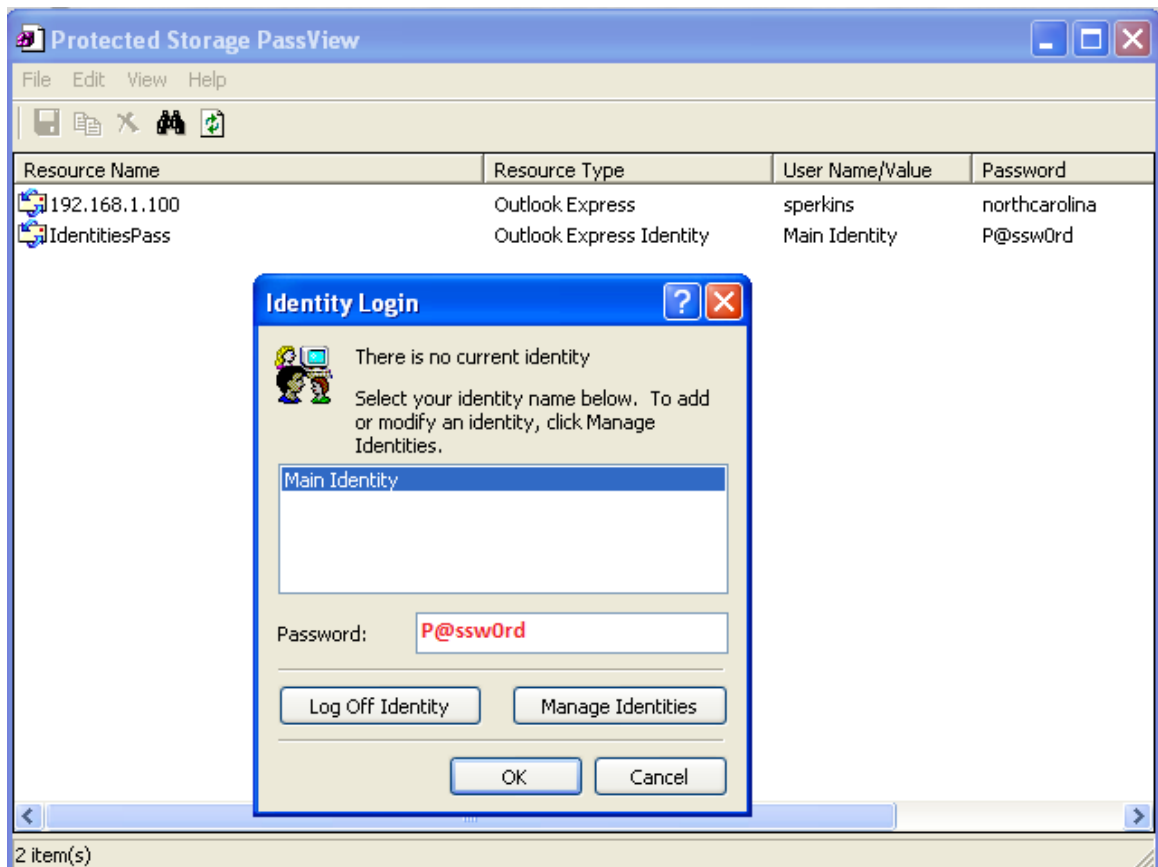
While those passwords we extracted are the passwords for the email accounts, they will not work if the user has selected a different Personal Folder password in Outlook or a Login Identity password in Outlook Express. HELIX provided the PST password, but that will not work for Outlook Express. We can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

21. 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?

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

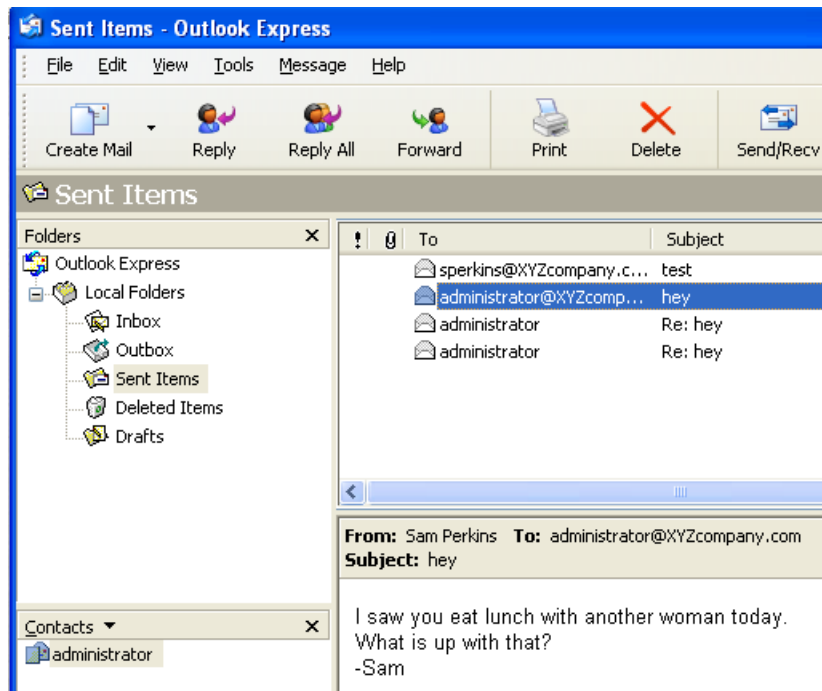


23. Return to the Outlook Express Identity Login window. Click Main Identity and type **P@ssw0rd**. Close the connection error window.

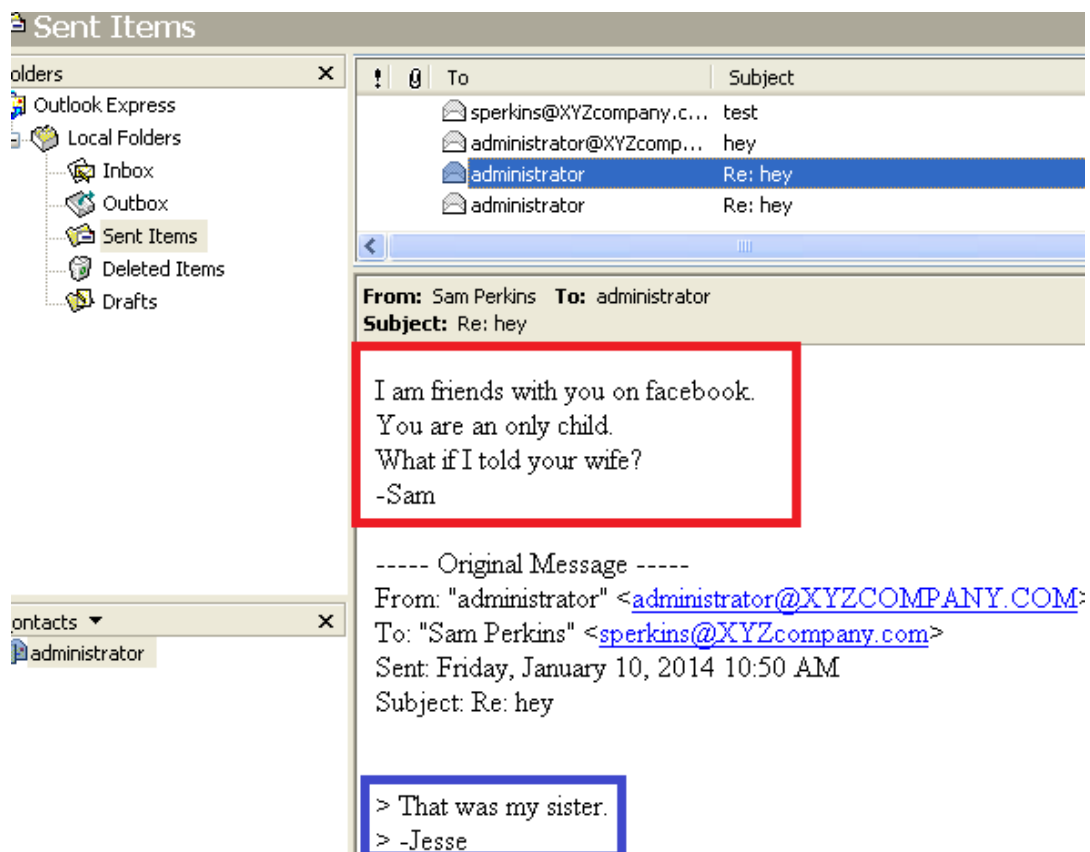




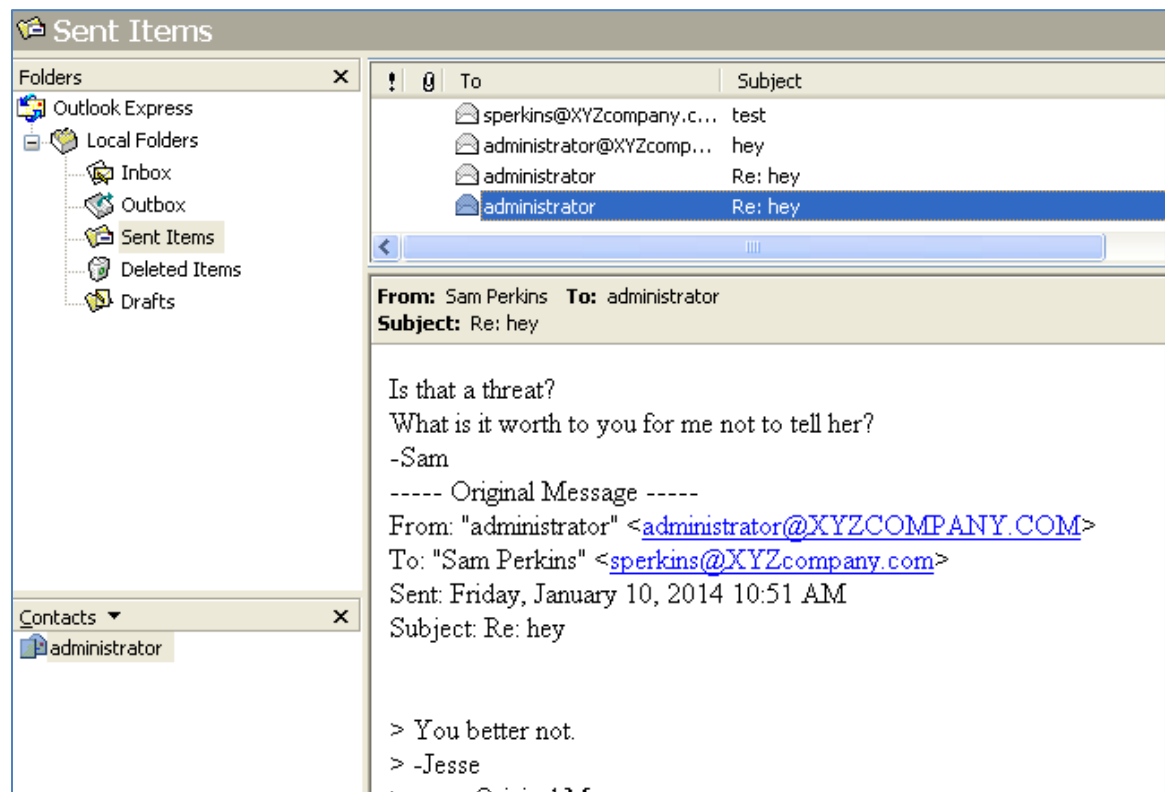
24. Click the **Sent Items** folder. Read the second email (from the top).



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



26. Click the **Sent Items** folder. Read the fourth email (from the top).



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

28. 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

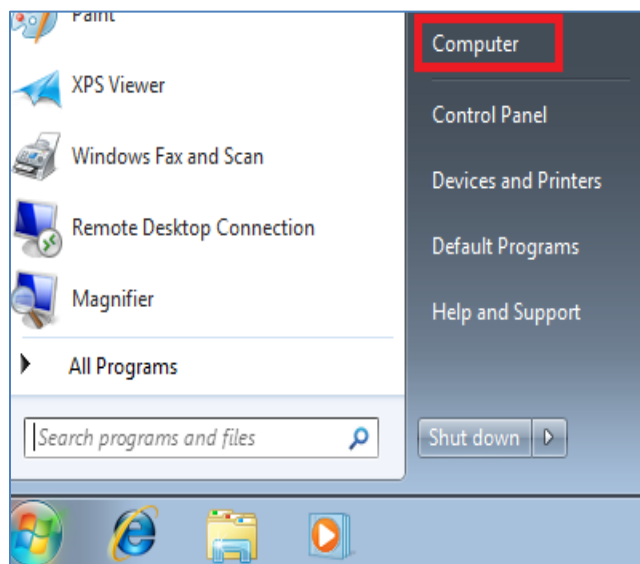
In the first task, we looked at email messages on the system. In this task, we will examine email messages in network traffic. You can get information about sent messages as well as view email passwords if the communication is not encrypted. Tools like Wireshark and Network Miner will allow you to view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

### 2.1 Viewing File Systems

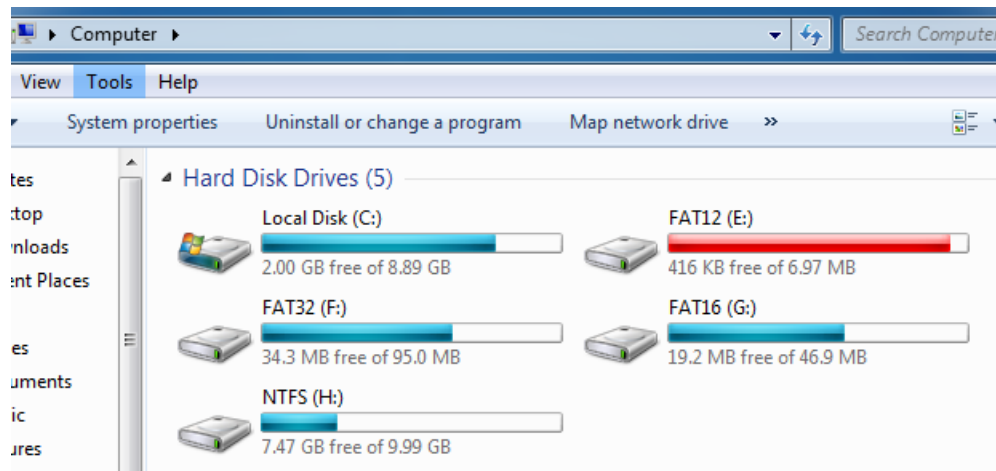
1. To log into the **Windows 7 External Machine**, click on the **Windows 7** icon on the topology.
2. If required, enter the username, **student**.
3. Type in the password, **password**, and press **Enter** to log in.



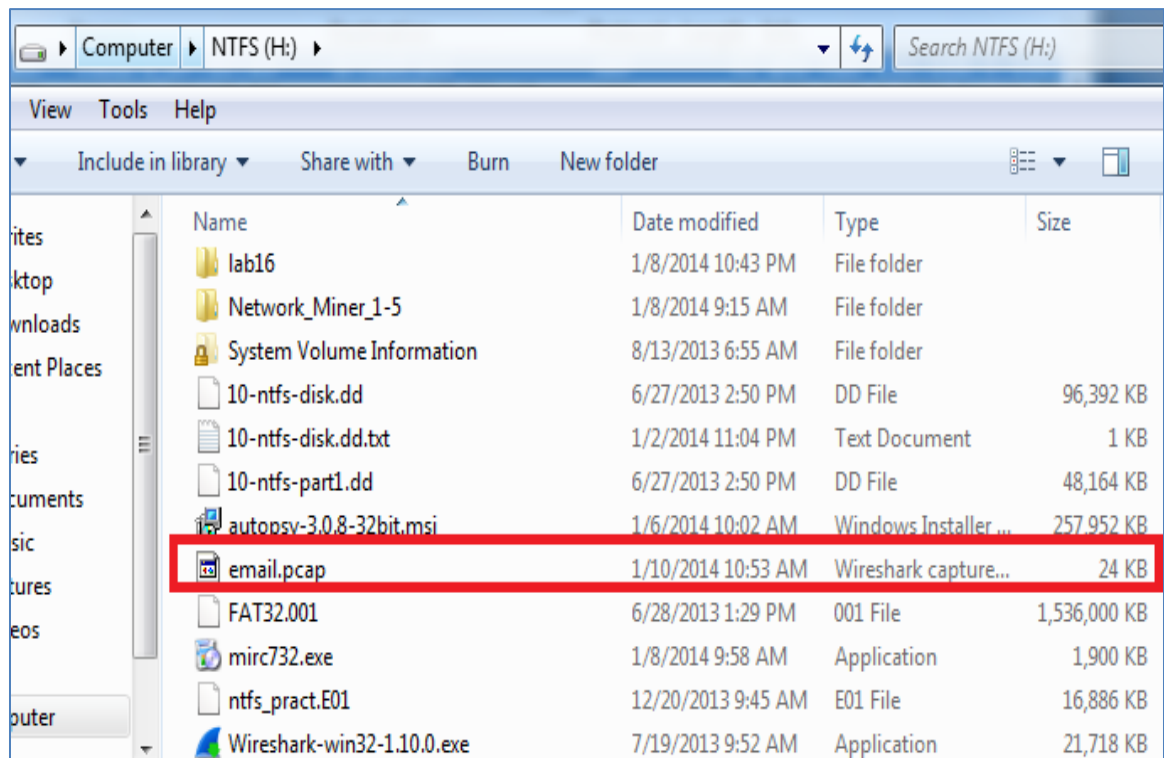
4. Click on the Start button and click on the link to **Computer**.



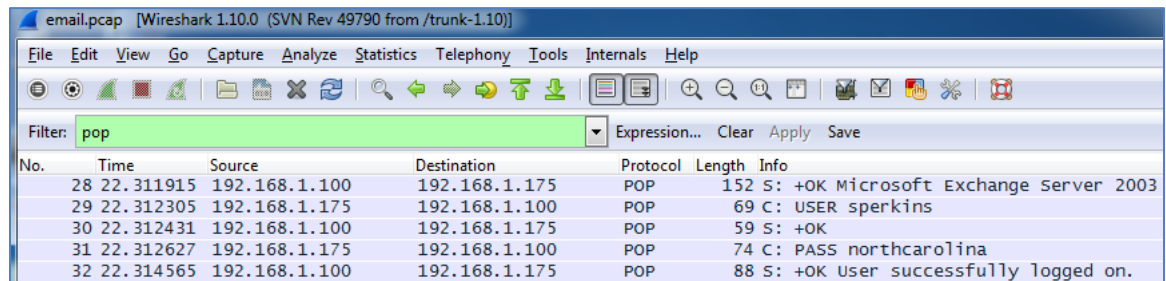
- Double-click on the **NTFS (H:)** Drive to access the email capture file.



- 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.

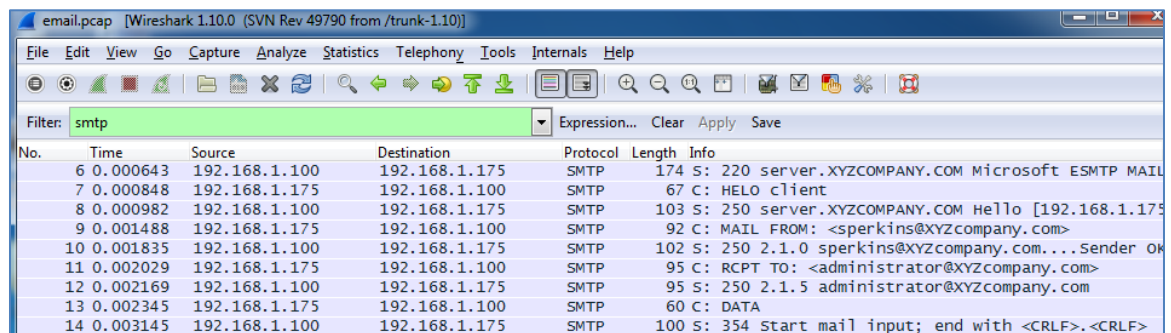


email.pcap [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]

Filter: **pop** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
28	22.311915	192.168.1.100	192.168.1.175	POP	152	S: +OK Microsoft Exchange Server 2003
29	22.312305	192.168.1.175	192.168.1.100	POP	69	C: USER sperkins
30	22.312431	192.168.1.100	192.168.1.175	POP	59	S: +OK
31	22.312627	192.168.1.175	192.168.1.100	POP	74	C: PASS northcarolina
32	22.314565	192.168.1.100	192.168.1.175	POP	88	S: +OK User successfully logged on.

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

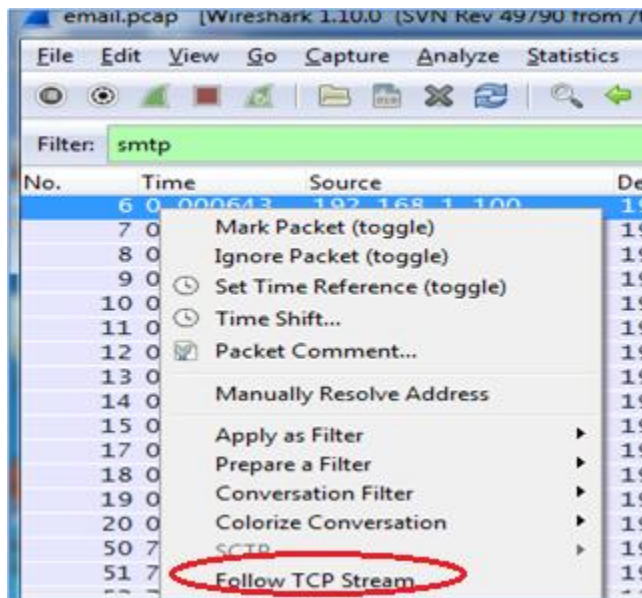


email.pcap [Wireshark 1.10.0 (SVN Rev 49790 from /trunk-1.10)]

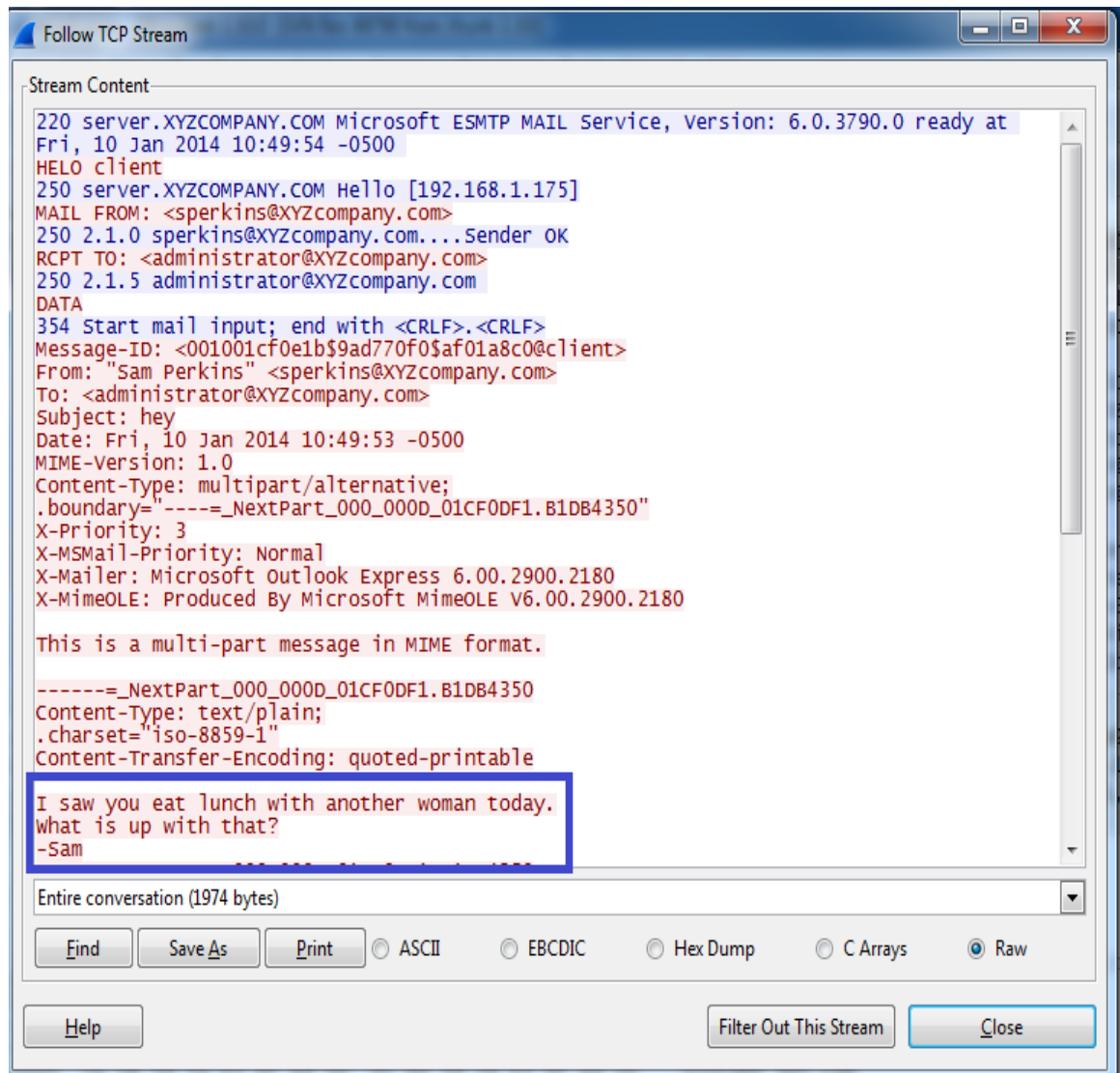
Filter: **smtp** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6	0.000643	192.168.1.100	192.168.1.175	SMTP	174	S: 220 server.XYZCOMPANY.COM Microsoft ESMTPL MAIL
7	0.000848	192.168.1.175	192.168.1.100	SMTP	67	C: HELO client
8	0.000982	192.168.1.100	192.168.1.175	SMTP	103	S: 250 server.XYZCOMPANY.COM Hello [192.168.1.175]
9	0.001488	192.168.1.175	192.168.1.100	SMTP	92	C: MAIL FROM: <sperkins@xyzcompany.com>
10	0.001835	192.168.1.100	192.168.1.175	SMTP	102	S: 250 2.1.0 sperkins@xyzcompany.com... Sender OK
11	0.002029	192.168.1.175	192.168.1.100	SMTP	95	C: RCPT TO: <administrator@xyzcompany.com>
12	0.002169	192.168.1.100	192.168.1.175	SMTP	95	S: 250 2.1.5 administrator@xyzcompany.com
13	0.002345	192.168.1.175	192.168.1.100	SMTP	60	C: DATA
14	0.003145	192.168.1.100	192.168.1.175	SMTP	100	S: 354 Start mail input; end with <CRLF>.<CRLF>

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

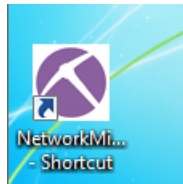


## 10. View the email message contained with the TCP Stream.

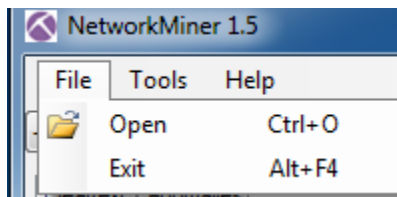


## 11. Close the TCP Stream and close Wireshark by clicking the red X in the upper-right corner.

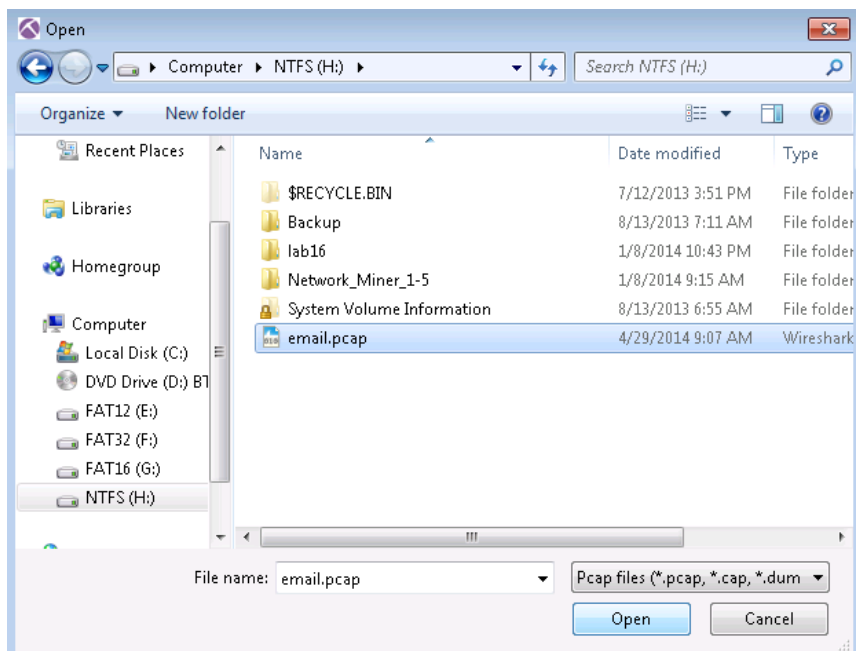
- Click the shortcut to Network Miner on the Windows 7 External Machine desktop.



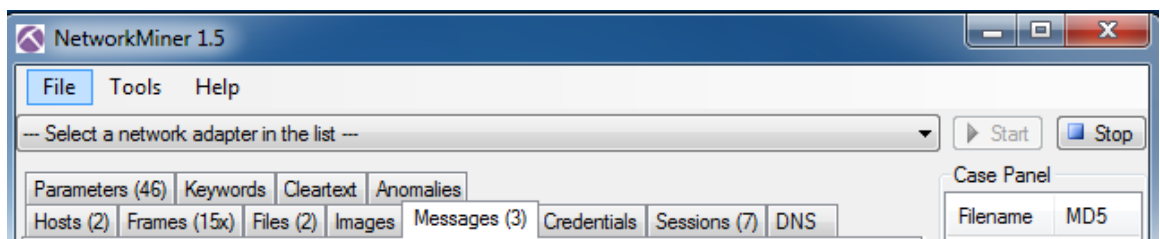
- Select **File** from the Menu bar and then select **Open**.



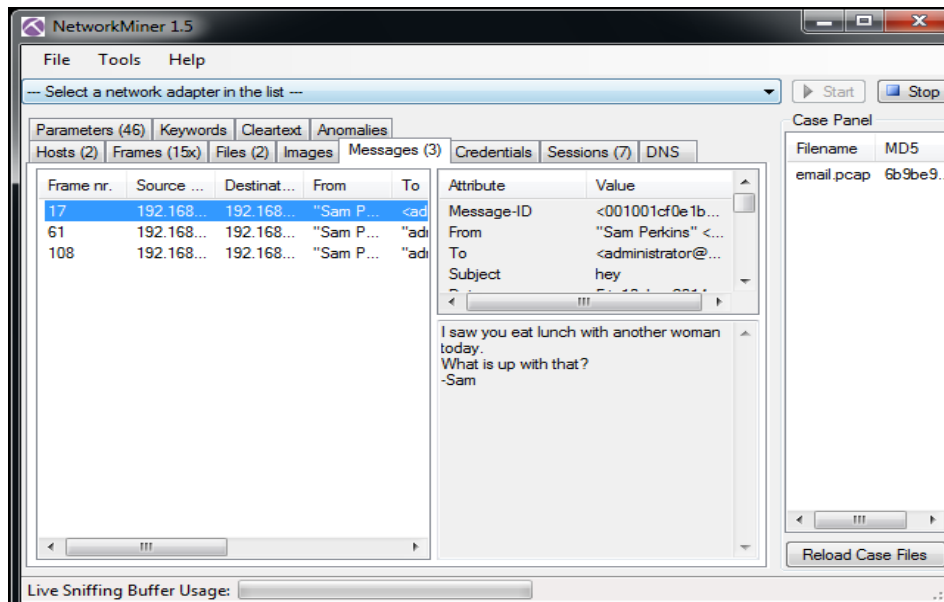
- Navigate to NTFS (H:), Click on email.pcap and click **Open**.



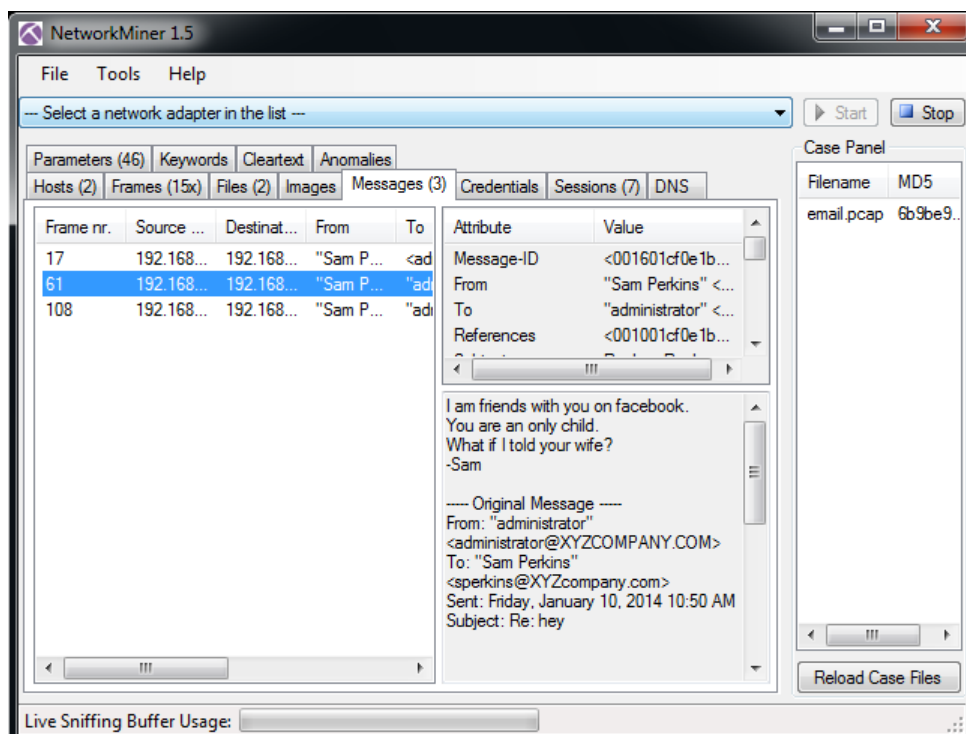
- Click on the Messages tab within Network Miner.



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

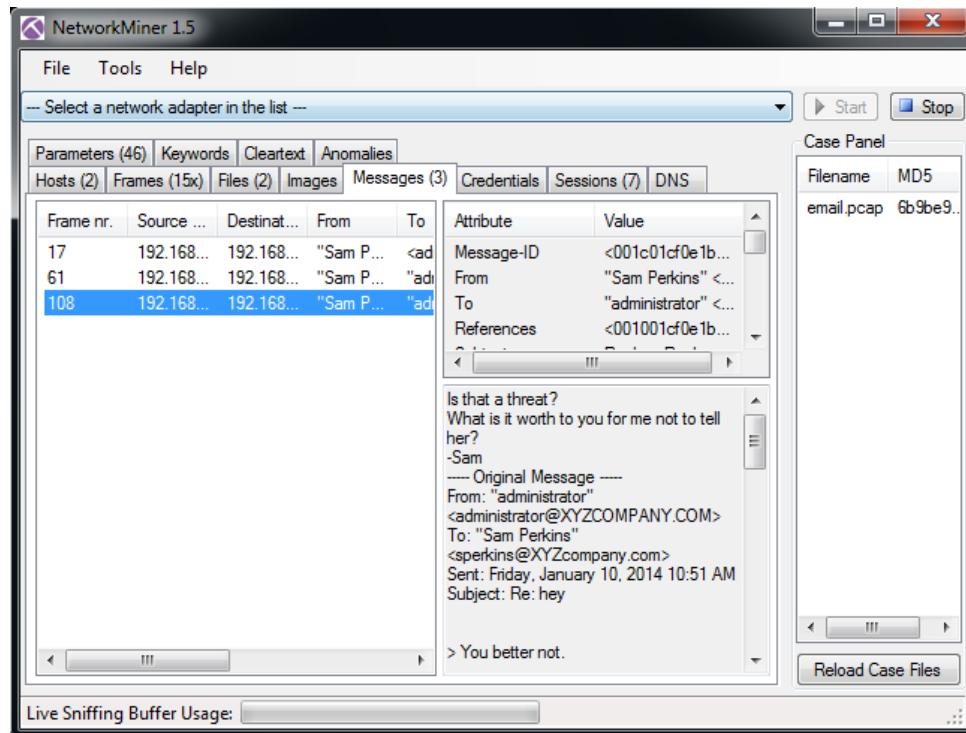


17. Click on the second email message (middle) in the list. Read the email.





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



19. 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?



## References

1. Outlook Express:  
[http://en.wikipedia.org/wiki/Outlook\\_Express](http://en.wikipedia.org/wiki/Outlook_Express)
2. Microsoft Outlook:  
<http://office.microsoft.com/en-us/outlook/>
3. Simple Mail Transfer Protocol:  
[http://en.wikipedia.org/wiki/Simple\\_Mail\\_Transfer\\_Protocol](http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol)
4. Post Office Protocol (Version 3):  
[http://en.wikipedia.org/wiki/Post\\_Office\\_Protocol](http://en.wikipedia.org/wiki/Post_Office_Protocol)

