Assignment 6.1: Forensic Investigation

Allison Manning

Shiley-Marcos School of Engineering, University of San Diego

CYBR-512-01B: Incident Detection and Handling

December 03, 2023

Executive Summary

We were tasked with discovering if any users on the system communicated with and sent any files to remote users. We obtained a copy of the hard drive of the computer in question and conducted a thorough analysis in order to answer the questions posed. We found that the computer has several messaging programs installed such as Windows Messenger. Our investigation revealed that the system housed several communication applications, including Windows Messenger, Thunderbird and various email programs. We discovered evidence of local users engaging in communications with remote users through these messaging platforms. Notably, our analysis of email communications indicated the transmission of files to remote users. This was solidified by examining email headers, attachments, and the creation and modification details of the documents involved.

This investigation highlights the capabilities of tools like Autopsy, FRED, RegRipper, PST Viewer Pro, and Rifiuti2 in conducting detailed digital forensic analyses. Our analysis not only answered the primary inquiry but also provided a broad picture of user activities and interactions within the system. Through our examination, we have successfully established that there was indeed communication with, and transmission of files to, remote users.

Introduction

This report presents the findings of a comprehensive digital forensic investigation conducted on a specific computer system. The primary objective of this investigation was to ascertain whether any of the system's users communicated with or transmitted files to remote users. This involved a detailed analysis of user profiles, installed software, file access patterns, email communications, and instant messaging artifacts. The analysis aimed to provide a clear understanding of the activities carried out by the users of the system and to identify any potential unauthorized or suspicious communications.

Methodology

The investigation was conducted using a systematic approach, utilizing a range of digital forensic tools and techniques. Key steps in the methodology included:

- **Data Acquisition**: The system's data was acquired using forensic imaging techniques to ensure the integrity and reliability of the evidence. This step was crucial to preserve the original state of the data and prevent any alterations during the analysis.
- **Data Analysis**:
    - **User Profile Analysis**: Utilized tools like FRED, RegRipper and Autopsy to extract and analyze user profiles from the SAM file and OS Accounts. This helped in identifying the users of the system along with the security identifiers.
    - **Software Inventory**: Examined the list of installed applications, with a specific focus on communication tools.

- **Program Usage**: Analyzed Shell Bags data to determine which programs were run by each user, providing insights into user behavior and application usage patterns.
- **File Access Patterns**: Investigated recently accessed Office documents and other files for each user, using Shell Bags data to track file interaction histories.
- **Email Communication Analysis**: Extracted and analyzed email communications from Outlook PST files using PST Viewer Pro 24. This included examining the contents of the emails, recipients, and any attached files.

- **Artifact Analysis**:

  - **Pidgin Messenger Artifacts**: Searched for and analyzed artifacts related to the Pidgin Messenger program to understand the instant messaging protocols used and the identities of the contacts communicated with.

Deliverables

1. **Who are the users on the system? What are their "security identifiers" (i.e., Windows userIDs)?**

Artifacts for users on the system are found at C://WINDOWS/system32/config/SAM. As well, in Autopsy, these programs are listed under Data Artifacts/OS Accounts.

We used Reg Ripper 3.0 on the SAM file and that produced the following:

User Information

Username : Administrator [500]

SID : S-1-5-21-842925246-725345543-1844994965-500

Full Name :

User Comment : Built-in account for administering the computer/domain

Account Type : Default Admin User

Account Created : Mon Oct 20 14:30:17 2008 Z

Name :

Last Login Date : Thu Oct 30 07:36:09 2008 Z

Pwd Reset Date : Mon Oct 20 14:33:37 2008 Z

Pwd Fail Date : Never

Login Count : 14

--> Password does not expire

--> Normal user account

Username : Guest [501]

SID : S-1-5-21-842925246-725345543-1844994965-501

Full Name :

User Comment : Built-in account for guest access to the computer/domain

Account Type : Default Guest Acct

Account Created : Mon Oct 20 14:30:17 2008 Z

Name :

Last Login Date : Never

Pwd Reset Date : Never

Pwd Fail Date : Never

Login Count : 0

--> Password does not expire

--> Account Disabled

--> Password not required

--> Normal user account

Username : HelpAssistant [1000]

SID : S-1-5-21-842925246-725345543-1844994965-1000

Full Name : Remote Desktop Help Assistant Account

User Comment : Account for Providing Remote Assistance

Account Type : Custom Limited Acct

Account Created : Mon Oct 20 21:35:41 2008 Z

Name :

Last Login Date : Never

Pwd Reset Date : Mon Oct 20 21:35:41 2008 Z

Pwd Fail Date : Never

Login Count : 0

--> Password does not expire

--> Account Disabled

--> Normal user account

Username : SUPPORT_388945a0 [1002]

SID : S-1-5-21-842925246-725345543-1844994965-1002

Full Name : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US

User Comment : This is a vendor's account for the Help and Support Service

Account Type : Custom Limited Acct

Account Created : Mon Oct 20 21:37:10 2008 Z

Name :

Last Login Date : Never

Pwd Reset Date : Mon Oct 20 21:37:10 2008 Z

Pwd Fail Date : Never

Login Count : 0

--> Password does not expire

--> Account Disabled

--> Normal user account

Username : domex1 [1003]

SID : S-1-5-21-842925246-725345543-1844994965-1003

Full Name : domex1

User Comment :

Account Type : Default Admin User

Account Created : Tue Oct 21 18:39:50 2008 Z

Name :

Last Login Date : Thu Oct 30 07:50:08 2008 Z

Pwd Reset Date : Never

Pwd Fail Date : Never

Login Count : 34

--> Password does not expire

--> Normal user account

Username : domex2 [1004]

SID : S-1-5-21-842925246-725345543-1844994965-1004

Full Name : domex2

User Comment :

Account Type : Custom Limited Acct

Account Created : Tue Oct 21 18:39:56 2008 Z

Name :

Last Login Date : Thu Oct 30 03:28:44 2008 Z

Pwd Reset Date : Never

Pwd Fail Date : Never

Login Count : 34

--> Password does not expire

--> Normal user account

The following is a screenshot from Data Artifacts/OS Accounts showing the same information:

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-18				SYSTEM	PhysicalDrive0_1 Host	Local	NT AUTHORITY	
S-1-5-21-842925246-725345543-1844994965-500			0	Administrator	nps-2009-domexusers.E01_3696 Host	Local		2008-10-20 07:30:17 PDT
S-1-5-21-842925246-725345543-1844994965-1003			0	domex1	nps-2009-domexusers.E01_3696 Host	Local		2008-10-21 11:39:50 PDT
S-1-5-21-842925246-725345543-1844994965-1004			0	domex2	nps-2009-domexusers.E01_3696 Host	Local		2008-10-21 11:39:56 PDT
S-1-5-19				LOCAL SERVICE	nps-2009-domexusers.E01_3696 Host	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	nps-2009-domexusers.E01_3696 Host	Local	NT AUTHORITY	
S-1-5-18				SYSTEM	nps-2009-domexusers.E01_3696 Host	Local	NT AUTHORITY	
S-1-5-21-842925246-725345543-1844994965-501			0	Guest	nps-2009-domexusers.E01_3696 Host	Local		2008-10-20 07:30:17 PDT
S-1-5-21-842925246-725345543-1844994965-1002			0	SUPPORT_388945a0	nps-2009-domexusers.E01_3696 Host	Local		2008-10-20 14:37:10 PDT
S-1-5-21-842925246-725345543-1844994965-1000			0	HelpAssistant	nps-2009-domexusers.E01_3696 Host	Local		2008-10-20 14:35:41 PDT

2. **What application software is installed on the system? Which of the applications can be used for communication purposes?**

   Artifacts for application software installed on the system are found at **C://WINDOWS/system32/config/software**. As well, in Autopsy, these programs are listed under Data Artifacts/Installed Programs. Applications that can be used for communication purposes are highlighted in yellow. The software Pidgin gives access to multiple other communication softwares and that is further discussed in #7.

Application Software on System (for communication)
Windows Live installer v.12.0.1471.1025
Microsoft Office Enterprise 2007 v.12.0.4518.1014
Microsoft Office Enterprise 2007 v.12.0.4518.1014
Microsoft Office OneNote MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Access Setup Metadata MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Access MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Word MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Publisher MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Proofing (English) 2007 v.12.0.4518.1014
Microsoft Office Proof (English) 2007 v.12.0.4518.1014
Microsoft Office Proof (French) 2007 v.12.0.4518.1014
Microsoft Office Proof (Spanish) 2007 v.12.0.4518.1014
Microsoft Office InfoPath MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Groove Setup Metadata MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Groove MUI (English) 2007 v.12.0.4518.1014

Microsoft Software Update for Web Folders (English) 12 v.12.0.4518.1014
Microsoft Office PowerPoint MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Outlook MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Excel MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Shared Setup Metadata MUI (English) 2007 v.12.0.4518.1014
Microsoft Office Shared MUI (English) 2007 v.12.0.4518.1014
WebFldrs XP v.9.50.7523
MPlayer2
Picasa 3 v.3.0
Mozilla Thunderbird (2.0.0.17) v.2.0.0.17 (en-US)
Viewpoint Media Player
AIM 6
AOLOCP_Y
AOL Diagnostics_N
Pidgin v.2.5.2
GTK+ Runtime 2.12.12 rev a (remove only)
Mozilla Firefox (3.0.3) v.3.0.3 (en-US)
Google Gears v.0.4.24.0
WIC
Windows XP Service Pack 3 v.20080414.031525
Windows Genuine Advantage Validation Tool (KB892130) v.1.7.0069.2
Windows Genuine Advantage Validation Tool (KB892130)
VMware Tools v.7.9.3.2574

DXM_Runtime
PCHealth
AddressBook
DirectAnimation
ICW
NetMeeting
OutlookExpress
DirectDrawEx
Fontcore
IE40
IE4Data
IE5BAKEX
IEData
MobileOptionPack
SchedulingAgent
Connection Manager

3. **Did anyone on the system ever run these programs? Which programs did each user run?**

Artifacts for the Pidgin Messenger, AIM, and Mozilla Thunderbird are located at: **C://Documents and Settings/USER/NTUSER.DAT**, where "USER" denotes the account name to be searched. The analysis focused on the three user accounts that were discovered: Administrator, domex1, and domex2. All three

communication applications were run by domex1, domex2, and Admin, as shown in the screenshots below. We did not find .lnk files for Admin for AIM or Thunderbird, however upon further investigation, these were found to be in the “All Users” directory.

Type	Value
Path	Pidgin.lnk
Key	Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last Write	2008-10-30 16:47:15 PDT
Date Modified	2008-10-21 04:18:58 PDT
Date Created	2008-10-21 04:18:58 PDT
Date Accessed	2008-10-28 20:59:58 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/NTUSER.DAT
Artifact ID	-9223372036854775726

```
2008-10-21 19:27:31Z
  UEME_RUNPIDL:%csidl2%\Pidgin.lnk (1)
  UEME_RUNPATH:C:\Program Files\Pidgin\pidgin.exe (1)
```

Type	Value
Path	Pidgin.lnk
Key	Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last Write	2008-10-30 03:34:52 PDT
Date Modified	2008-10-21 04:18:58 PDT
Date Created	2008-10-21 04:18:58 PDT
Date Accessed	2008-10-30 02:42:40 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex2/NTUSER.DAT
Artifact ID	-9223372036854775696

```
2008-10-30 02:42:39Z
  UEME_RUNPATH:C:\Program Files\Pidgin\pidgin.exe (3)
  UEME_RUNPATH:Pidgin.lnk (2)
```

Type	Value
Path	Pidgin.lnk
Key	Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last Write	2008-10-30 16:49:48 PDT
Date Modified	2008-10-21 04:18:58 PDT
Date Created	2008-10-21 04:18:58 PDT
Date Accessed	2008-10-30 02:42:40 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/Administrator/NTUSER.DAT
Artifact ID	-9223372036854775759

```
2008-10-21 17:49:36Z
  UEME_RUNPATH:C:\Program Files\Pidgin\pidgin.exe (1)
2008-10-21 17:49:35Z
  UEME_RUNPATH:Pidgin.lnk (1)
```

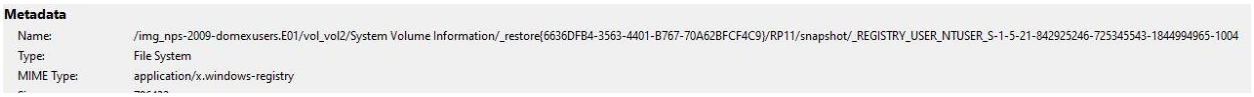
a. AIM6 was run by domex1, domex2, and Admin.

Type	Value
Path	AIM 6.lnk
Key	Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last Write	2008-10-30 16:47:15 PDT
Date Modified	2008-10-21 15:09:34 PDT
Date Created	2008-10-21 15:09:34 PDT
Date Accessed	2008-10-22 21:16:28 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/NTUSER.DAT
Artifact ID	-9223372036854775730

```
2008-10-21 19:19:09Z
  UEME_RUNPIDL:%csidl2%\AIM\AIM 6.lnk (1)
  UEME_RUNPIDL:%csidl2%\AIM (1)
```

Type	Value
Path	AIM 6.lnk
Key	Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last Write	2008-10-30 03:34:52 PDT
Date Modified	2008-10-21 15:09:34 PDT
Date Created	2008-10-21 15:09:34 PDT
Date Accessed	2008-10-30 02:54:26 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex2/NTUSER.DAT
Artifact ID	-9223372036854775700

Note: This .lnk file was not present in the user's DAT file when ripped by Reg Ripper. Upon further investigation, it was found in a system restore point for domex2.



Type	Value
Path	AIM 6.lnk
Key	Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last Write	2008-10-30 16:49:48 PDT
Date Modified	2008-10-21 15:09:34 PDT
Date Created	2008-10-21 15:09:34 PDT
Date Accessed	2008-10-30 02:54:26 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/Administrator/NTUSER.DAT
Artifact ID	-9223372036854775771

Though this file path is to the Admin's NTUSER.DAT file, this .lnk file was not present in this user's DAT file. The .lnk file was present in **C://Documents and Settings/All Users/Desktop** however, there was no DAT file present for extraction and ripping.

Not having the .lnk file in the Admin's NTUSER.DAT indicates that the shortcut was not a part of the admin's personal user settings or desktop environment and it wasn't used by the admin account. Finding the .lnk file in the C://Documents and Settings/All Users/Desktop directory points to its general accessibility. This directory is a shared space, implying the shortcut was meant for use by all users on the system and came as default.

Below is the screenshot showing the .lnk file as shown in Autopsy.

/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/All Users/Desktop

Table | Thumbnail | Summary

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2008-10-21 08:12:43 PDT	2008-10-21 08:12:43 PDT	2008-10-30 00:36:23 PDT
[parent folder]				2008-10-20 14:36:42 PDT	2008-10-20 14:36:42 PDT	2008-10-30 09:43:17 PDT
AIM 6.lnk			0	2008-10-21 08:09:32 PDT	2008-10-21 08:09:32 PDT	2008-10-29 20:17:31 PDT
Mozilla Firefox.lnk			0	2008-10-20 21:16:49 PDT	2008-10-20 21:16:49 PDT	2008-10-29 20:38:01 PDT
Mozilla Thunderbird.lnk			0	2008-10-21 08:11:33 PDT	2008-10-21 08:11:33 PDT	2008-10-29 20:17:31 PDT
Picasa 3.lnk			0	2008-10-21 08:12:43 PDT	2008-10-21 08:12:43 PDT	2008-10-29 20:17:31 PDT
Pidgin.lnk			0	2008-10-20 21:18:56 PDT	2008-10-20 21:18:56 PDT	2008-10-29 19:42:39 PDT

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Basic Properties

Login: Administrator
Full Name:
Address: S-1-5-21-842925246-725345543-1844994965-500
Type:
Creation Date: 2008-10-20 07:30:17 PDT
Object ID: 3702

b. Mozilla Thunderbird was accessed by domex1, domex2, and Admin.

Type	Value
Path	Mozilla Thunderbird.lnk
Key	Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last Write	2008-10-30 16:47:15 PDT
Date Modified	2008-10-21 15:11:34 PDT
Date Created	2008-10-21 15:11:34 PDT
Date Accessed	2008-10-30 01:52:10 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/NTUSER.DAT
Artifact ID	-9223372036854775728

```
2008-10-30 02:51:29Z
  UEME_RUNPATH:C:\Program Files\Mozilla Thunderbird\thunderbird.exe (2)
  UEME_RUNPIDL:%csidl2%\Mozilla Thunderbird\Mozilla Thunderbird.lnk (1)
  UEME_RUNPIDL:%csidl2%\Mozilla Thunderbird (1)
```

Type	Value
Path	Mozilla Thunderbird.lnk
Key	Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last Write	2008-10-30 03:34:52 PDT
Date Modified	2008-10-21 15:11:34 PDT
Date Created	2008-10-21 15:11:34 PDT
Date Accessed	2008-10-30 02:54:26 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex2/NTUSER.DAT
Artifact ID	-9223372036854775698

```
2008-10-30 02:44:34Z
  UEME_UISCUT (5)
  UEME_RUNPATH:Mozilla Thunderbird.lnk (2)
  UEME_RUNPATH:C:\Program Files\Mozilla Thunderbird\thunderbird.exe (2)
2008-10-30 02:42:39Z
```

Type	Value
Path	Mozilla Thunderbird.lnk
Key	Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last Write	2008-10-30 16:49:48 PDT
Date Modified	2008-10-21 15:11:34 PDT
Date Created	2008-10-21 15:11:34 PDT
Date Accessed	2008-10-30 02:54:26 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/Administrator/NTUSER.DAT
Artifact ID	-9223372036854775769

Though this file path is to the Admin's NTUSER.DAT file, this .lnk file was not present in this user's DAT file. The .lnk file was present in **C://Documents and Settings/All Users/Desktop** however, there was no DAT file present for extraction and ripping.

Not having the .lnk file in the Admin's NTUSER.DAT indicates that the shortcut was not a part of the admin's personal user settings or desktop environment and it wasn't used by the admin account. Finding the .lnk file in the C://Documents and Settings/All Users/Desktop directory points to its general accessibility. This directory is a shared space, implying the shortcut was meant for use by all users on the system and came as default. Below is the screenshot showing the .lnk file as shown in Autopsy.

/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/All Users/Desktop

Table | Thumbnail | Summary

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2008-10-21 08:12:43 PDT	2008-10-21 08:12:43 PDT	2008-10-30 00:36:23 PDT
[parent folder]				2008-10-20 14:36:42 PDT	2008-10-20 14:36:42 PDT	2008-10-30 09:43:17 PDT
AIM 6.lnk			0	2008-10-21 08:09:32 PDT	2008-10-21 08:09:32 PDT	2008-10-29 20:17:31 PDT
Mozilla Firefox.lnk			0	2008-10-20 21:16:49 PDT	2008-10-20 21:16:49 PDT	2008-10-29 20:38:01 PDT
Mozilla Thunderbird.lnk			0	2008-10-21 08:11:33 PDT	2008-10-21 08:11:33 PDT	2008-10-29 20:17:31 PDT
Picasa 3.lnk			0	2008-10-21 08:12:43 PDT	2008-10-21 08:12:43 PDT	2008-10-29 20:17:31 PDT
Pidgin.lnk			0	2008-10-20 21:18:56 PDT	2008-10-20 21:18:56 PDT	2008-10-29 19:42:39 PDT

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Basic Properties

Login:	Administrator
Full Name:	
Address:	S-1-5-21-842925246-725345543-1844994965-500
Type:	
Creation Date:	2008-10-20 07:30:17 PDT
Object ID:	3702

4. **What files (Office documents, in particular) did each user recently access?**

    a. Domex1 accessed and sent a Word document and Excel spreadsheet.

Type	Value
Path	This is a word document sent by domex user 1.docx
Key	Software\Microsoft\Windows\ShellNoRoam\Bags\2\Shell
Date Modified	2008-10-29 16:15:22 PDT
Date Created	2008-10-29 16:15:22 PDT
Date Accessed	2008-10-30 03:38:20 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/NTUSER.DAT
Artifact ID	-9223372036854775714

Type	Value
Path	This is a spreadsheet sent by domex user 1.xlsx
Key	Software\Microsoft\Windows\ShellNoRoam\Bags\2\Shell
Date Modified	2008-10-29 16:16:54 PDT
Date Created	2008-10-29 16:16:52 PDT
Date Accessed	2008-10-30 03:38:12 PDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/NTUSER.DAT
Artifact ID	-9223372036854775716

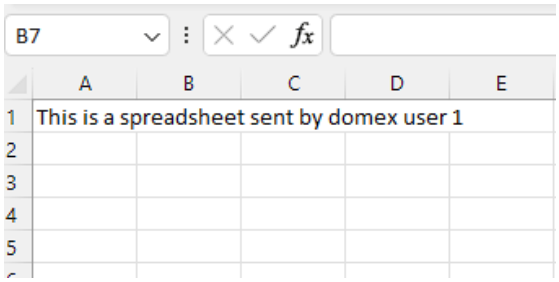
    b. A jpg was created by domex2 in MsPaint.

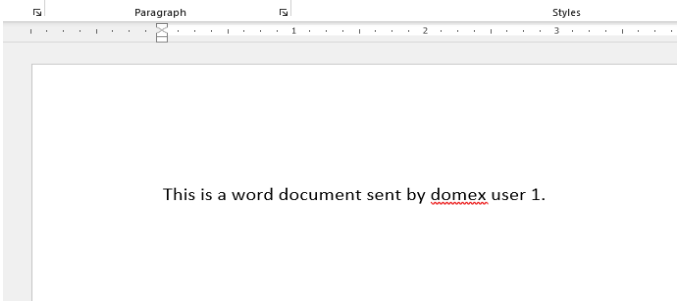
```
RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time: 2008-10-30 01:44:48Z
  1 = My Pictures
  0 = domexuser2.JPG

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.JPG
LastWrite Time 2008-10-30 01:59:11Z
MRUListEx = 0
  0 = domexuser2.JPG


2008-10-29 16:20:24Z
  UEME_RUNPIDL:%csidl2%\Accessories\Paint.lnk (1)
  UEME_RUNPIDL:%csidl2%\Accessories (1)
  UEME_RUNPATH:C:\WINDOWS\system32\mspaint.exe (1)
```

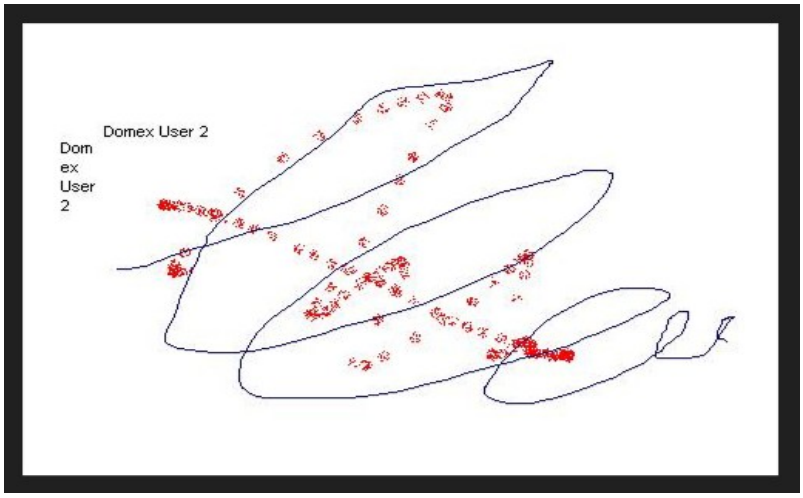
5. **Find the files (including any traces of deleted files) on the system that you listed in your answer to the previous question. What are the contents of each file?**

The following 3 files were located on the system. Their contents can be found in the screenshots

1. This_is_a_spreadsheet_sent_by_domex_user_1.xlsx
2. This_is_a_word_document_sent_by_domex_user_1.docx below.
3. domexuser2.jpg



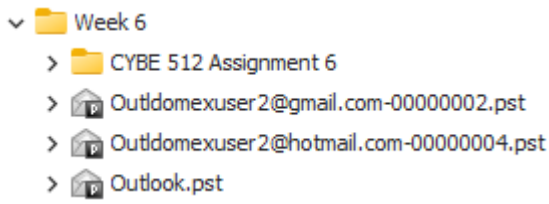




6. **What emails (restrict your search to Outlook, unless you are very ambitious) did users on the system send? To whom did they send them? Were there any file attachments?**

The following 3 outlook PSTs were extracted from autopsy and ingested into PST Viewer Pro 24 for ease of use and analyzation:

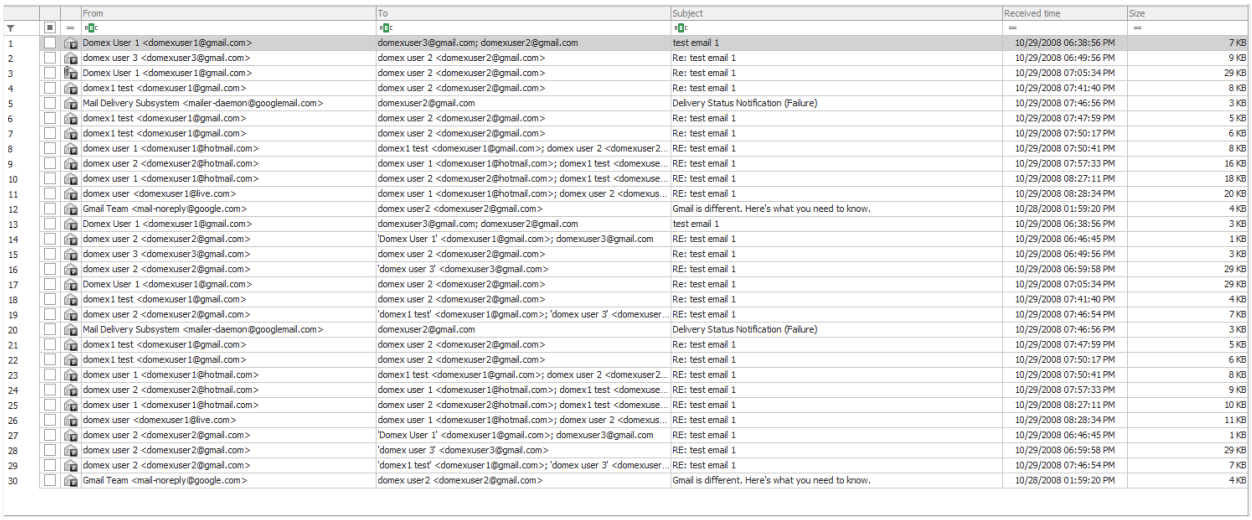
1. Outlookdomexuser2@gmail.com-00000002.pst
2. Outlookdomexuser2@gmail.com-00000004.pst
3. Outlook.pst



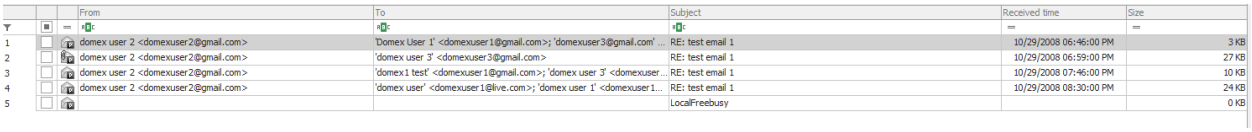
Two of the PST contained various test emails between the following users:

- domexuser1@live.com
- domexuser1@hotmail.com
- donexuser2@hotmail.com
- domexuser1@gmail.com
- domexuser2@gmail.com
- domexuser3@gmail.com
- domexuser2@live.com

RE: test email 1
domex user <domexuser1@live.com>
Sent time: 10/29/2008 08:28:28 PM
Received time: 10/29/2008 08:28:34 PM
To: domex user 1 <domexuser1@hotmail.com>; domex user 2 <domexuser2@hotmail.com>; domex1 test <domexuser1@gmail.com>; domex user 2 <domexuser2@gmail.com>
Cc: domex user 3 <domexuser3@gmail.com>; domexuser2@live.com



	From	To	Subject	Received time	Size
1	Domex User 1 <domexuser1@gmail.com>	domexuser3@gmail.com; domexuser2@gmail.com	test email 1	10/29/2008 06:38:56 PM	7 KB
2	domex user 3 <domexuser3@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 06:49:56 PM	9 KB
3	Domex User 1 <domexuser1@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 07:05:34 PM	29 KB
4	domex1 test <domexuser1@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 07:41:40 PM	8 KB
5	Mail Delivery Subsystem <mailer-daemon@googlemail.com>	domexuser2@gmail.com	Delivery Status Notification (Failure)	10/29/2008 07:46:56 PM	3 KB
6	domex1 test <domexuser1@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 07:47:59 PM	5 KB
7	domex1 test <domexuser1@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 07:50:17 PM	6 KB
8	domex user 1 <domexuser1@hotmail.com>	domex1 test <domexuser1@gmail.com>; domex user 2 <domexuser2...	RE: test email 1	10/29/2008 07:50:41 PM	8 KB
9	domex user 2 <domexuser2@hotmail.com>	domex user 1 <domexuser1@hotmail.com>; domex1 test <domexuse...	RE: test email 1	10/29/2008 07:57:33 PM	16 KB
10	domex user 1 <domexuser1@hotmail.com>	domex user 2 <domexuser2@hotmail.com>; domex1 test <domexuse...	RE: test email 1	10/29/2008 08:27:11 PM	18 KB
11	domex user <domexuser1@live.com>	domex user 1 <domexuser1@hotmail.com>; domex user 2 <domexus...	RE: test email 1	10/29/2008 08:28:34 PM	20 KB
12	Gmail Team <mail-noreply@google.com>	domex user2 <domexuser2@gmail.com>	Gmail is different. Here's what you need to know.	10/28/2008 01:59:20 PM	4 KB
13	Domex User 1 <domexuser1@gmail.com>	domexuser3@gmail.com; domexuser2@gmail.com	test email 1	10/29/2008 06:38:56 PM	3 KB
14	domex user 2 <domexuser2@gmail.com>	'Domex User 1' <domexuser1@gmail.com>; domexuser3@gmail.com	RE: test email 1	10/29/2008 06:46:45 PM	1 KB
15	domex user 3 <domexuser3@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 06:49:56 PM	3 KB
16	domex user 2 <domexuser2@gmail.com>	'domex user 3' <domexuser3@gmail.com>	RE: test email 1	10/29/2008 06:59:58 PM	29 KB
17	Domex User 1 <domexuser1@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 07:05:34 PM	29 KB
18	domex1 test <domexuser1@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 07:41:40 PM	4 KB
19	domex user 2 <domexuser2@gmail.com>	'domex1 test' <domexuser1@gmail.com>; 'domex user 3' <domexuser...	RE: test email 1	10/29/2008 07:46:54 PM	7 KB
20	Mail Delivery Subsystem <mailer-daemon@googlemail.com>	domexuser2@gmail.com	Delivery Status Notification (Failure)	10/29/2008 07:46:56 PM	3 KB
21	domex1 test <domexuser1@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 07:47:59 PM	5 KB
22	domex1 test <domexuser1@gmail.com>	domex user 2 <domexuser2@gmail.com>	Re: test email 1	10/29/2008 07:50:17 PM	6 KB
23	domex user 1 <domexuser1@hotmail.com>	domex1 test <domexuser1@gmail.com>; domex user 2 <domexuser2...	RE: test email 1	10/29/2008 07:50:41 PM	8 KB
24	domex user 2 <domexuser2@hotmail.com>	domex user 1 <domexuser1@hotmail.com>; domex1 test <domexuse...	RE: test email 1	10/29/2008 07:57:33 PM	9 KB
25	domex user 1 <domexuser1@hotmail.com>	domex user 2 <domexuser2@hotmail.com>; domex1 test <domexuse...	RE: test email 1	10/29/2008 08:27:11 PM	10 KB
26	domex user <domexuser1@live.com>	domex user 1 <domexuser1@hotmail.com>; domex user 2 <domexus...	RE: test email 1	10/29/2008 08:28:34 PM	11 KB
27	domex user 2 <domexuser2@gmail.com>	'Domex User 1' <domexuser1@gmail.com>; domexuser3@gmail.com	RE: test email 1	10/29/2008 06:46:45 PM	1 KB
28	domex user 2 <domexuser2@gmail.com>	'domex user 3' <domexuser3@gmail.com>	RE: test email 1	10/29/2008 06:59:58 PM	29 KB
29	domex user 2 <domexuser2@gmail.com>	'domex1 test' <domexuser1@gmail.com>; 'domex user 3' <domexuser...	RE: test email 1	10/29/2008 07:46:54 PM	7 KB
30	Gmail Team <mail-noreply@google.com>	domex user2 <domexuser2@gmail.com>	Gmail is different. Here's what you need to know.	10/28/2008 01:59:20 PM	4 KB



	From	To	Subject	Received time	Size
1	domex user 2 <domexuser2@gmail.com>	'Domex User 1' <domexuser1@gmail.com>; 'domexuser3@gmail.com' ...	RE: test email 1	10/29/2008 06:46:00 PM	3 KB
2	domex user 2 <domexuser2@gmail.com>	'domex user 3' <domexuser3@gmail.com>	RE: test email 1	10/29/2008 06:59:00 PM	27 KB
3	domex user 2 <domexuser2@gmail.com>	'domex1 test' <domexuser1@gmail.com>; 'domex user 3' <domexuser...	RE: test email 1	10/29/2008 07:46:00 PM	10 KB
4	domex user 2 <domexuser2@gmail.com>	'domex user' <domexuser1@live.com>; 'domex user 1' <domexuser1...	RE: test email 1	10/29/2008 08:30:00 PM	24 KB
5			LocalFreebusy		0 KB

There are 2 specific emails where users emailed files to other users. The first being an email from domexuser1@gmail.com to domexuser2@gmail.com and domexuser3@gmail.com on 10/29/2008 at 07:05:24 PM. This email had the following files attached:

- This_is_a_spreadsheet_sent_by_domex_user_1.xlsx

- This_is_a_word_document_sent_by_domex_user_1.docx

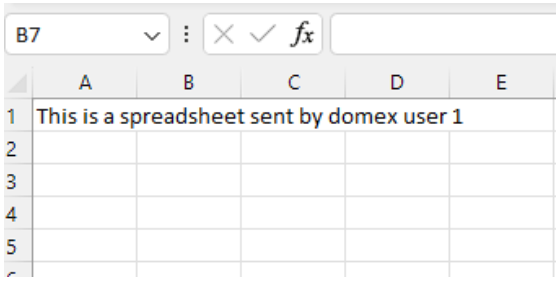
Re: test email 1

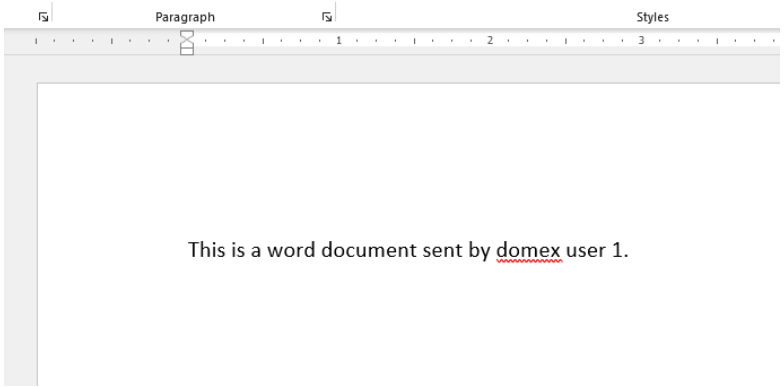
Domex User 1 <domexuser1@gmail.com>
Sent time: 10/29/2008 07:05:24 PM
Received time: 10/29/2008 07:05:34 PM
To: domex user 2 <domexuser2@gmail.com>
Cc: 'domex user 3' <domexuser3@gmail.com>
Attachments: This is a spreadsheet sent by domex user 1.xlsx This is a word document sent by domex user 1.docx

here are my files.

-user1

domex user 2 wrote:
> Here's an attached picture
>
> -----Original Message-----
> From: domex user 3 [mailto:domexuser3@gmail.com]
> Sent: Wednesday, October 29, 2008 5:50 PM
> To: domex user 2
> Cc: 'Domex User 1'
> Subject: Re: test email 1
>
> received.
>
> On Oct 29, 2008, at 6:46 PM, domex user 2 wrote:
>
>
>> Good test
>>
>> -----Original Message-----
>> From: Domex User 1 [mailto:domexuser1@gmail.com]
>> Sent: Wednesday, October 29, 2008 5:39 PM
>> To: domexuser3@gmail.com; domexuser2@gmail.com
>> Subject: test email 1
>>
>> test email 1 from domexuser1
>>
>
>
>
>
> ---
>



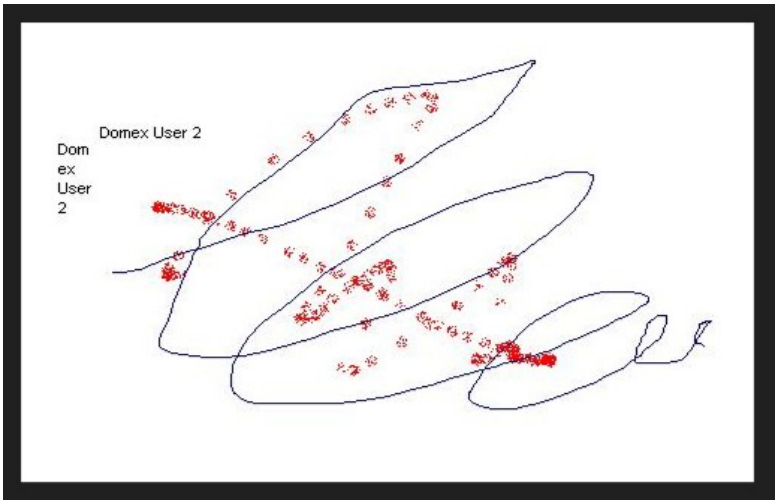


The second email was sent by domexuser2@gmail.com to domexuser3@gmail.com and domexuser1@gmail.com on 10/29/2008 at 06:59:49 PM. The email had the following file attached:

- domexuser2.jpg

RE: test email 1
domex user 2 <domexuser2@gmail.com>
Sent time: 10/29/2008 06:59:49 PM
Received time: 10/29/2008 06:59:00 PM
To: 'domex user 3' <domexuser3@gmail.com>
Cc: 'Domex User 1' <domexuser1@gmail.com>
Attachments: domexuser2.JPG

```
Here's an attached picture

-----Original Message-----
From: domex user 3 [mailto:domexuser3@gmail.com]
Sent: Wednesday, October 29, 2008 5:50 PM
To: domex user 2
Cc: 'Domex User 1'
Subject: Re: test email 1

received.

On Oct 29, 2008, at 6:46 PM, domex user 2 wrote:

> Good test
>
> -----Original Message-----
> From: Domex User 1 [mailto:domexuser1@gmail.com]
> Sent: Wednesday, October 29, 2008 5:39 PM
> To: domexuser3@gmail.com; domexuser2@gmail.com
> Subject: test email 1
>
> test email 1 from domexuser1
>
```

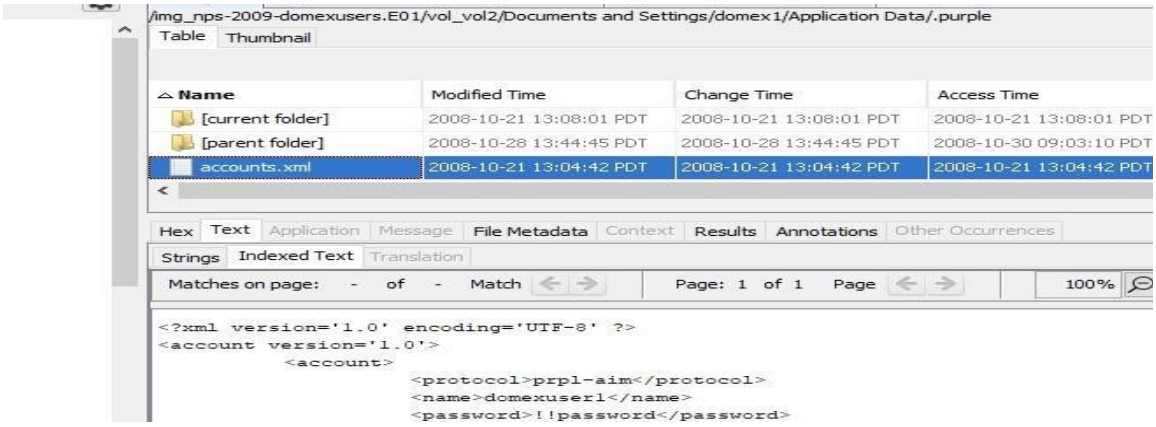


4. **Find any artifacts of the "Pidgin Messenger" program that you can. What instant messaging (IM) protocols did the users connect to using Pidgin and who were the "buddies" that they likely communicated with?**

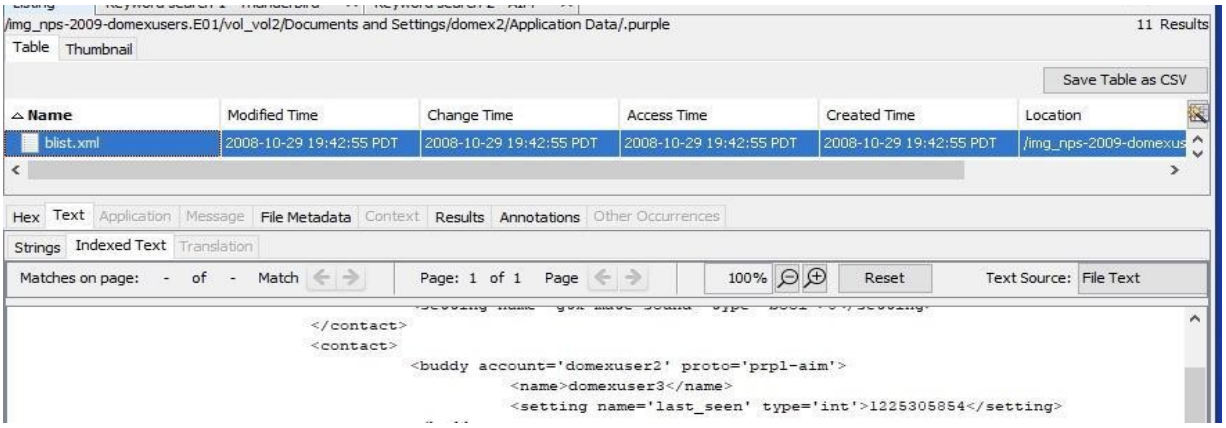
   Artifacts for the Pidgin Messenger are located at: **C://Documents and Settings/USER/Application Data/.purple** , where "USER" denotes the account name to be searched. The analysis focused on the three user accounts that were discovered, Administrator, domex1, and domex2.

   This folder contains several files that contain various user configuration settings. The files that were analyzed were: Accounts.xml, blist.xml, and prefs.xml, accels. The following is a basic overview of the information contained within these files.

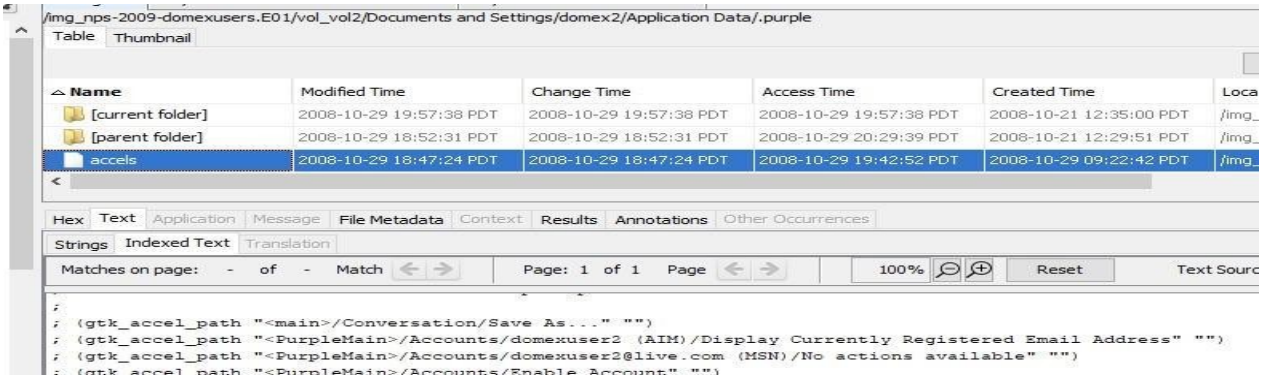
   - Accounts.xml: Messaging protocols that Pidgin is integrated with along with their respective usernames and passwords. (See screenshot below)



   - blist.xml: List of buddies, by username, for each integrated messaging protocol. (See screenshot below)



- prefs.xml: User preferences and various configuration settings.
- accels: Evidence of deleted messages or account deletion. (See screenshot below)



A breakdown of the information gleaned and complete listing of usernames uncovered from these artifacts/files are contained in the attached Pidgin Artifact Report. The messaging protocols that Pidgin was integrated with were AIM, Jabber, and MSN Messenger. Notably, the domexuser2 Pidgin account, which is associated with the domex2 (-1004) local computer account, has user domexuser3 listed as a buddy which is not a local user. This is an indication that communication may have taken place via the Pidgin messenger through one of the three listed protocols to a remote user, domexuser3. The prefs.xml file did not indicate that logging or history was enabled for any user. For this reason we opted to not include a screenshot for that file. Subsequent searches for messenger log files yielded no results. The accels file was found only in the domexuser2 account. The file indicates that conversations took place via Pidgin using the AIM and MSN protocols. Actual conversation logs could not be located.

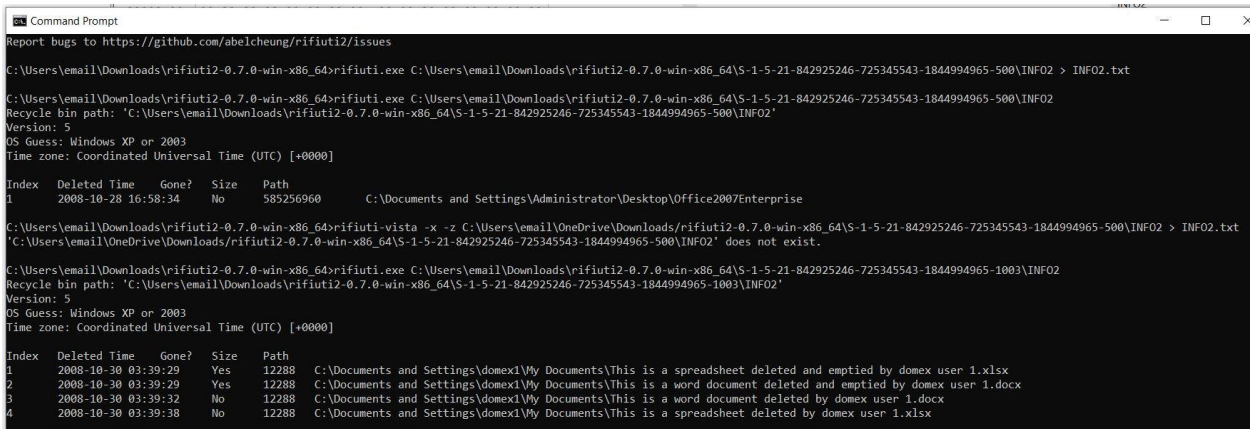
8. The main question: Did any users on the system communicate with and send any files to remote users? If so, with whom did they communicate and what files, if any, were transmitted?

In our investigation we found evidence of communication and transfer of files between domex1, domex2 and domex3 through a thorough exam of all the systems email logs and file data.

We found evidence that domex1 sent a Word document and Excel spreadsheet to domex2 and CC'd domex3. This was done by analyzing the headers and attachments in the sent items in domex1's email. The data we found in the word doc and excel doc confirmed this when we looked at the creation dates, modified dates and the originating user's details.
We also found that domex2 sent a .jpg file to domex3 and CC'd domex1. This was verified by inspecting the attachment details in the email data and cross referencing the hash of the .jpg file of the file we extracted from the outlook email and compared with the hash of the .jpg found in autopsy.

We also looked at web activities to confirm this. We looked at all .HTML files on the system for traces of file transfer and communication. While doing this it was noted that there was FTP usage in browser history and the cache.
We also found traces of potential remote assistance activities that might indicate remote desktop or support sessions. This was found from the system's .HTML logs. However, there is a lack of concrete evidence to support this.

We also used Rifiuti2.0 to examine the Recycler contents, however, this only confirmed what Autopsy had revealed about the deleted documents.



So, we have evidence of email file transmissions among domex1, domex2, and domex3 but our findings for FTP and RDP are inconclusive. We would need further access to external server logs or system data to determine these activities.

Conclusion

This lab successfully demonstrates the extremely impressive functionality and power of the Autopsy tool when conducting forensic analysis of large datasets. Additionally, it effectively demonstrates Autopsy's ability to accurately depict data to assist in forming a comprehensive picture of the events leading up to the incident under investigation. Although there was no need to use third party software, we decided that by leveraging the following tools: Forensic Registry EDitor (FRED), RegRipper, PST Viewer Pro, and Rifiuti2, we would be able to include cleaner and more user-friendly data in or report of the events in question.