

## **Forensic Investigation**

Kayvon Karimi

Shiley-Marcos School of Engineering, University of San Diego

CYBR-512: Incident Detection and Handling

Professor Mark Heckman, Ph.D.

December 2nd, 2024



## Executive Summary

This forensic investigation analyzed the Windows XP system image *nps-2009-domexusers.E01* to assist law enforcement in determining if sensitive data was transmitted by users of this device. The analysis included examining user accounts, installed software, program usage, recently accessed files, emails, and artifacts from instant messaging applications. In summary:

- **User Activity:** Two active user accounts, *domex1* and *domex2*, were identified, along with their Security Identifiers, SIDs, and login records. *domex1* was determined to be the primary user of the system.
- **Installed Applications:** Multiple communication programs, such as Pidgin Messenger, Outlook, and Mozilla Thunderbird, were installed and actively used.
- **Recently Accessed Files:** Six Office documents were recently accessed by *domex1*, including four still present on the system and two deleted files.
- **Email Analysis:** Evidence of email communications was found, including attachments sent to remote users. Two Office documents were confirmed as email attachments sent by *domex1*.
- **Instant Messaging:** Artifacts from Pidgin Messenger revealed active connections to AIM and Jabber/XMPP protocols, along with buddy lists indicating external communication.
- **File Transfer:** Evidence showed *domex1* sending files, including spreadsheets and Word documents, to remote users via email.

This investigation confirmed that users communicated with remote entities and transmitted files.

## Analysis

### 1. User Accounts and Security Identifiers

- a. Who are the users on the system?
- b. What are their Security Identifiers (SIDs)?

The SAM file was analyzed to gather information about the system's user accounts, including usernames, Security Identifiers (SIDs), account creation times, and login activity. Using Autopsy, the SAM file was located within the system's registry files, and RegRipper was used to parse the file and generate a detailed report, providing key insights into the system's user activity.

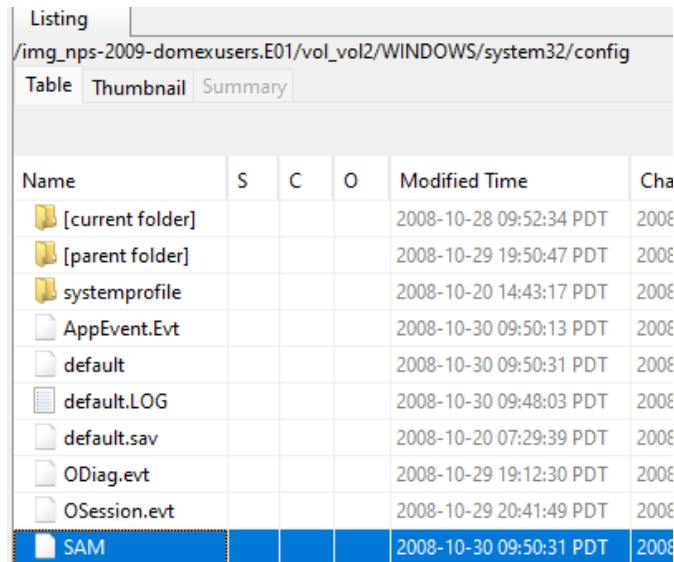
Account Type	Username	Security Identifier	Account Created	Last Login
Default Admin User	domex1[1003]	S-1-5-21-842952546-725345543-1844994965-500	2008-10-20 14:30:17 UTC	2008-10-30 07:36:09 UTC
Default Guest Account	domex2 [1004]	S-1-5-21-842952546-725345543-1844994965-501	2008-10-20 14:30:17 UTC	Never Logged In

```
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
```

## Steps Taken:

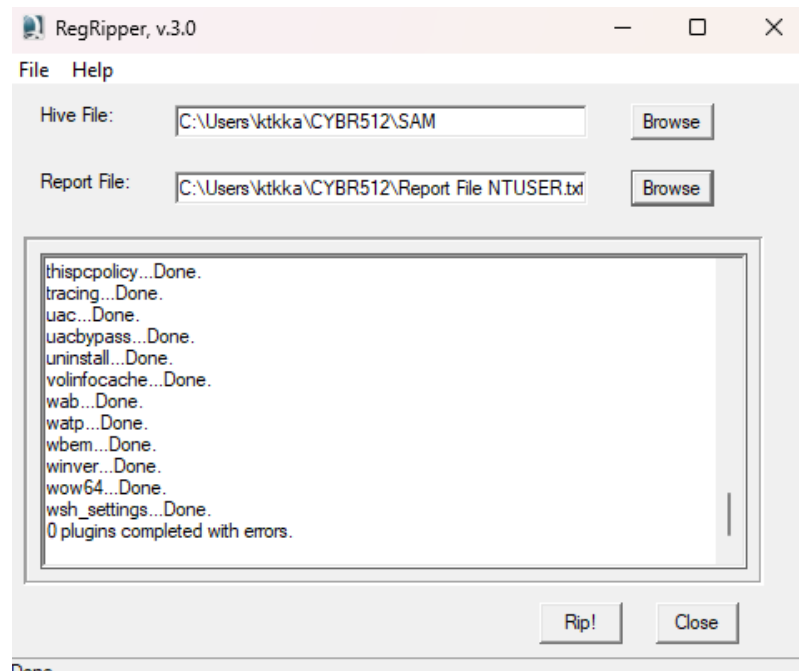
1. Extracted the SAM File from Autopsy:
  - a. Opened the Autopsy tool and navigated to the SAM file under
    - *Windows\System32\config*



The screenshot shows the 'Listing' tab in Autopsy. The path is `/img_nps-2009-domexusers.E01/vol_vol2/WINDOWS/system32/config`. The 'Table' view is selected. The file 'SAM' is highlighted in blue. The table has columns: Name, S, C, O, Modified Time, and Cha.

Name	S	C	O	Modified Time	Cha
[current folder]				2008-10-28 09:52:34 PDT	2008
[parent folder]				2008-10-29 19:50:47 PDT	2008
systemprofile				2008-10-20 14:43:17 PDT	2008
AppEvent.Evt				2008-10-30 09:50:13 PDT	2008
default				2008-10-30 09:50:31 PDT	2008
default.LOG				2008-10-30 09:48:03 PDT	2008
default.sav				2008-10-20 07:29:39 PDT	2008
ODiag.evt				2008-10-29 19:12:30 PDT	2008
OSession.evt				2008-10-29 20:41:49 PDT	2008
SAM				2008-10-30 09:50:31 PDT	2008

2. Installed RegRipper to generate a report of registry artifacts ([GitHub](#)).
3. Parsed the SAM file using RegRipper:
  - a. Opened RegRipper and entered the 'SAM' file path name in the *Hive File* field.
  - b. Entered destination folder in *Report File* field.



4. Generated the SAM Report:
  - a. Click on *Rip!* to generate detailed report
  - b. Open the resulting report file in Notepad for review and analysis

## 2. Installed Applications

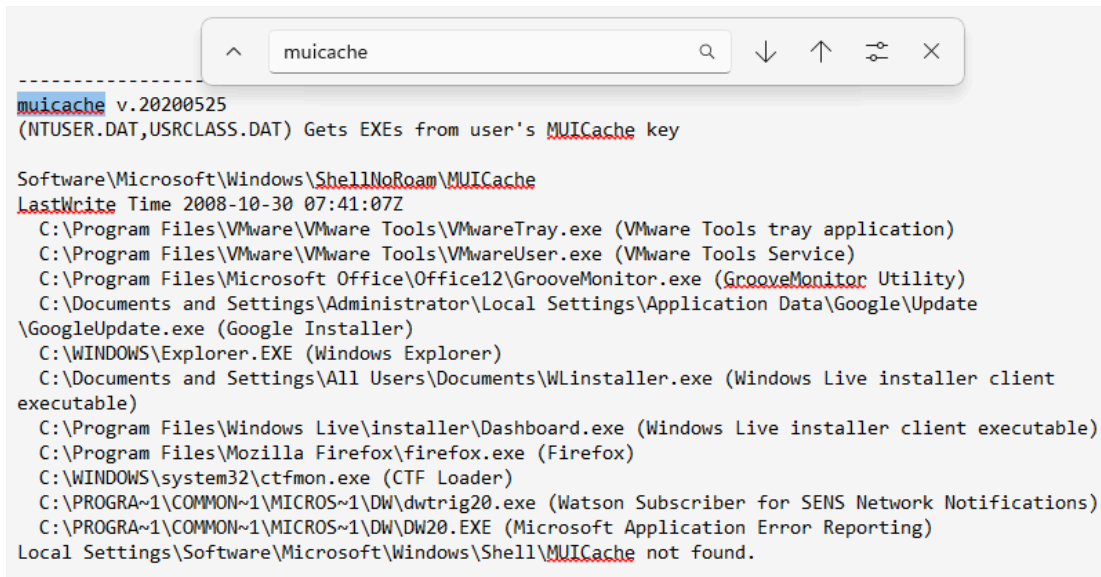
- a. What application software is installed on the system?
- b. Which of the applications can be used for communication purposes?

To identify the installed applications, we used Autopsy to analyze the 'NTUSER.DAT' file located in the *C:\Documents and Settings\Administrator* directory. Key plugins such as *listsoft* and *muicache* were applied to extract software information, including application names, executables, and associated metadata.

Application Category	Installed Applications	Can it be used for Communication?
Google Tools	Google Update.exe (google Installer), Google Gears v.0.4.24.0	No
Instant Messaging Tools	Pidgin Messenger, AIM (AOL Instant Messenger)	Yes
Media Applications	Windows Media Player, Picasa 3 v.3.0, MPlayer2, Viewpoint Media Player	No
Microsoft Office 2007	Word, Excel, PowerPoint, Outlook, and Publisher, GrooveMonitor.exe,	Outlook and GrooveMonitor can be used for communication
Mozilla Applications	Firefox web browser, Thunderbird email client	Yes
System Tools	Watson Diagnostics (DW20.exe), WebFldrs XP v.9.50.7523, PCHealth	PCHealth: Yes
VMware Tools	VMwareTray.exe, VMwareUser.exe	No
Web Browser	Google Chrome Browser, Mozilla Firefox Browser, NetscapeNavigator	Yes
Windows Tools	Windows Installer (Dashboard.exe, WLInstaller.exe)	No

## Steps Taken:

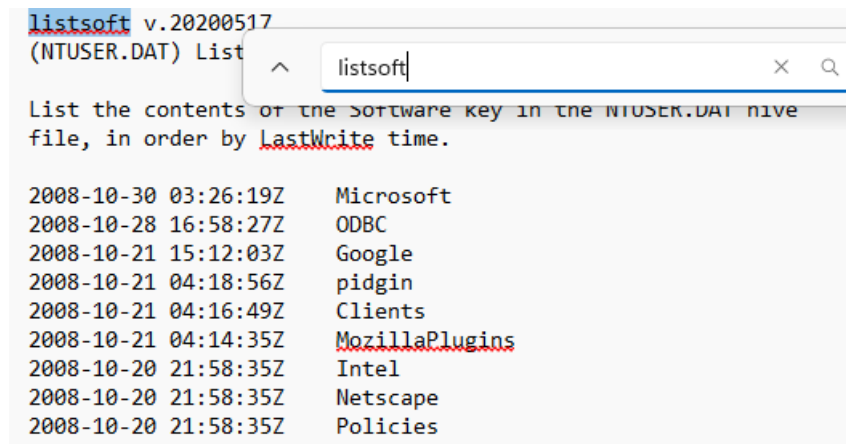
1. Identified and Extracted the 'NTUSER.DAT' File in Autopsy
  - a. Located the file under *C:\Documents and Settings\Administrator* in Autopsy.
2. Parsed the 'NTUSER.DAT' file
  - a. Selected the exported 'NTUSER.DAT file' in the *Hive File* field using the Browse option.
  - b. Specified the output destination folder for the report in the *Report File* field.
  - c. Clicked 'Rip!' to generate the report.
3. I opened the report in Notepad, and compiled the list of applications from the *muicache* and *listsoft* plugin outputs.



The screenshot shows the output of the 'muicache' plugin. At the top, there is a search bar with 'muicache' entered. Below it, the text reads: 'muicache v.20200525 (NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key'. The main body of the output lists various executables and their last write times, such as 'C:\Program Files\VMware\VMware Tools\VMwareTray.exe (VMware Tools tray application)' and 'C:\WINDOWS\Explorer.EXE (Windows Explorer)'. The list ends with 'Local Settings\Software\Microsoft\Windows\Shell\MUICache not found.'

```
muicache v.20200525
(NTUSER.DAT,USRCLASS.DAT) Gets EXEs from user's MUICache key

Software\Microsoft\Windows\ShellNoRoam\MUICache
LastWrite Time 2008-10-30 07:41:07Z
C:\Program Files\VMware\VMware Tools\VMwareTray.exe (VMware Tools tray application)
C:\Program Files\VMware\VMware Tools\VMwareUser.exe (VMware Tools Service)
C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe (GrooveMonitor Utility)
C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Update
\GoogleUpdate.exe (Google Installer)
C:\WINDOWS\Explorer.EXE (Windows Explorer)
C:\Documents and Settings\All Users\Documents\WLInstaller.exe (Windows Live installer client
executable)
C:\Program Files\Windows Live\installer\Dashboard.exe (Windows Live installer client executable)
C:\Program Files\Mozilla Firefox\firefox.exe (Firefox)
C:\WINDOWS\system32\ctfmon.exe (CTF Loader)
C:\PROGRA~1\COMMON~1\MICROS~1\DW\dwtrig20.exe (Watson Subscriber for SENS Network Notifications)
C:\PROGRA~1\COMMON~1\MICROS~1\DW\DW20.EXE (Microsoft Application Error Reporting)
Local Settings\Software\Microsoft\Windows\Shell\MUICache not found.
```



The screenshot shows the output of the 'listsoft' plugin. At the top, there is a search bar with 'listsoft' entered. Below it, the text reads: 'listsoft v.20200517 (NTUSER.DAT) List'. The main body of the output lists the contents of the Software key in the NTUSER.DAT hive file, ordered by last write time. The list includes entries like '2008-10-30 03:26:19Z Microsoft', '2008-10-28 16:58:27Z ODBC', '2008-10-21 15:12:03Z Google', '2008-10-21 04:18:56Z pidgin', '2008-10-21 04:16:49Z Clients', '2008-10-21 04:14:35Z MozillaPlugins', '2008-10-20 21:58:35Z Intel', '2008-10-20 21:58:35Z Netscape', and '2008-10-20 21:58:35Z Policies'.

```
listsoft v.20200517
(NTUSER.DAT) List

List the contents of the Software key in the NTUSER.DAT hive
file, in order by LastWrite time.

2008-10-30 03:26:19Z    Microsoft
2008-10-28 16:58:27Z    ODBC
2008-10-21 15:12:03Z    Google
2008-10-21 04:18:56Z    pidgin
2008-10-21 04:16:49Z    Clients
2008-10-21 04:14:35Z    MozillaPlugins
2008-10-20 21:58:35Z    Intel
2008-10-20 21:58:35Z    Netscape
2008-10-20 21:58:35Z    Policies
```

### 3. Program Usage

#### a. Did anyone on the system ever run these programs?

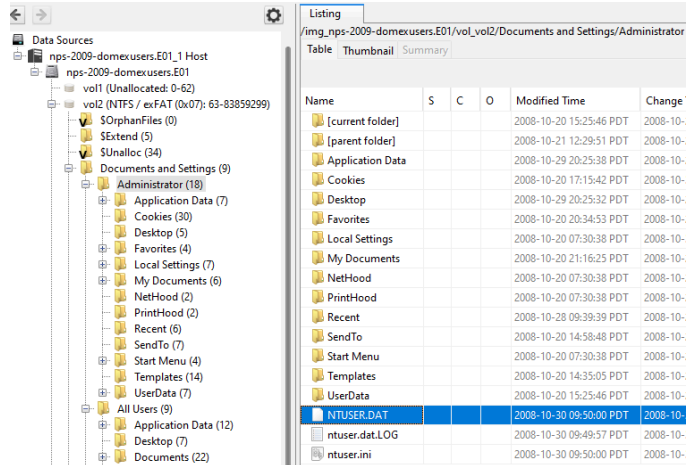
One method of collecting this data was performed by analyzing the 'NTUSER.DAT' file to determine whether the listed programs were ever run on the system. Using registry keys such as OpenSaveMRU, UserAssist, and MUICache, evidence was found showing that all of the listed applications were executed between October 20th and October 21st 2008 by the system's Administrator account. The table below summarizes the findings, including the programs, sources of evidence, and their associated timestamps.

Program	Timestamp	Run Count
Files and Settings Transfer Wizard	2008-10-20 21:57:32Z	10
Internet Explorer	2008-10-20 22:40:47Z	1
Notepad	2008-10-28 16:39:39Z	2
Pidgin Messenger	2008-10-21 17:49:36Z	1
Pidgin Shortcut	2008-10-21 17:49:35Z	1
Picasa Installer	2008-10-21 15:11:41Z	1
Thunderbird Installer	2008-10-21 15:11:18Z	1
Windows Media Player	2008-10-20 21:57:32Z	13
Windows Messenger	2008-10-20 21:57:32Z	12
Windows Update	2008-10-20 22:51:53Z	3
Windows Update Executable	2008-10-20 22:51:53Z	3

#### Steps Taken:

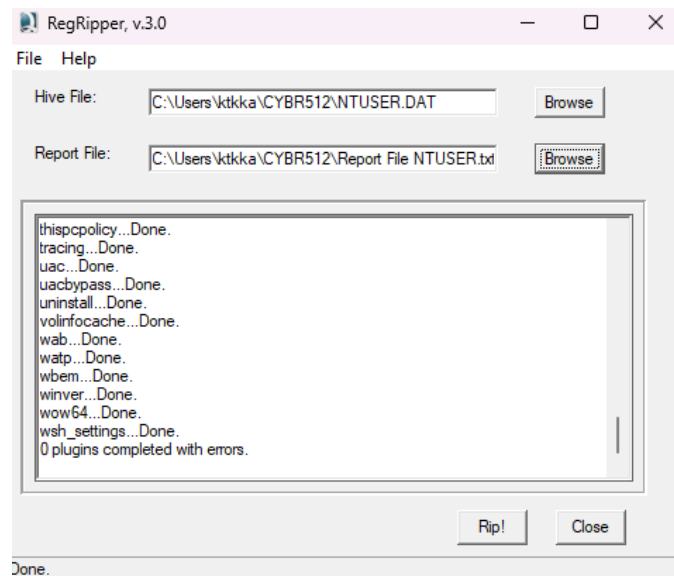
##### 1. Extracted the 'NTUSER.DAT' File

- a. Used Autopsy to locate the 'NTUSER.DAT' file for the Administrator and Guest accounts.
- b. Navigated to: Documents and Settings\Administrator\ntuser.dat and extracted file.



2. Parsed the 'NTUSER.DAT' file with RegRipper:

- Opened RegRipper and entered the 'NTUSER.DAT' file path name in the 'Hive File' field.
- Entered destination folder in Report File field.



3. Reviewed Registry Keys:

- Opened the 'NTUSER' report in a text editor (Notepad).
- Used the search function (Ctrl + F) to locate programs:
- Used *UserAssist* registry key to track programs that were interacted by the user.



Software\Microsoft\Windows\CurrentVersion\Uninstall

2008-10-21 04:15:

userassist

Google Chrome V.0.2.149.30

-----  
UserAssist

Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

LastWrite Time 2008-10-20 21:58:41Z

{5E6AB780-7743-11CF-A12B-00AA004AE837}

Value names with no time stamps:

{75048700-EF1F-11D0-9888-006097DEACF9}

2008-10-30 03:17:06Z

UEME\_RUNPATH (17)

UEME\_RUNPATH:C:\Documents and Settings\All Users\Documents\Wlinstaller.exe (1)

2008-10-28 16:39:39Z

UEME\_RUNPATH:C:\WINDOWS\System32\NOTEPAD.EXE (2)

2008-10-28 16:39:28Z

UEME\_RUNPATH:C:\Documents and Settings\Administrator\Desktop\Office2007Enterprise\setup.exe (1)

2008-10-28 16:39:09Z

UEME\_UISCUT (9)

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)

2008-10-21 15:11:41Z

UEME\_RUNPATH:C:\Documents and Settings\Administrator\Desktop\picasa3-setup.exe (1)

2008-10-21 15:11:18Z

UEME\_RUNPATH:C:\Documents and Settings\Administrator\Desktop\Thunderbird Setup 2.0.0.17.exe (1)

2008-10-21 15:06:36Z

UEME\_RUNPATH:C:\Documents and Settings\Administrator\Desktop\Install\_AIM.exe (1)

2008-10-21 04:16:55Z

UEME\_RUNPATH:C:\Documents and Settings\Administrator\Desktop\pidgin-2.5.2.exe (1)

2008-10-21 04:16:35Z

UEME\_RUNPATH:C:\Documents and Settings\Administrator\Desktop\Firefox Setup 3.0.3.exe (1)

2008-10-21 04:14:33Z

UEME\_RUNPATH:C:\Documents and Settings\Administrator\Desktop\ChromeSetup.exe (1)

2008-10-21 03:53:45Z

UEME\_RUNCPL (1)

UEME\_RUNCPL:SYSDM.CPL (1)


2008-10-20 22:51:53Z

UEME\_RUNPIDL (5)

UEME\_RUNPIDL:C:\Documents and Settings\All Users\Start Menu\Windows Update.lnk (3)

UEME\_RUNPATH:C:\WINDOWS\system32\wupdmgr.exe (3)

2008-10-20 22:50:24Z

UEME\_RUNPATH:C:\WINDOWS\system32\oobe\msoobe.exe 

2008-10-20 22:40:47Z

UEME\_RUNPATH:C:\Program Files\Internet Explorer\iexplore.exe (1)

UEME\_RUNPIDL:::{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0} (1)

2008-10-20 21:57:32Z

UEME\_RUNPIDL:%csidl2%\MSN.lnk (14)

UEME\_RUNPIDL:%csidl2%\Windows Media Player.lnk (13)

UEME\_RUNPIDL:%csidl2%\Windows Messenger.lnk (12)

UEME\_RUNPIDL:%csidl2%\Accessories\Tour Windows XP.lnk (11)

UEME\_RUNPIDL:%csidl2%\Accessories\System Tools\Files and Settings Transfer Wizard.lnk (10)

Additionally, the Autopsy “Run Programs” Data Artifacts listing provides the prefetch files detected by Autopsy in a list with the program name, path, execution time stamp, and count. Within this section, additional executed program information was extracted.

Source Name	Program Name	Time Stamp	Count
AIM6.EXE-34DC5725.pf	AIM6.EXE	2008-10-30 00:50:43 PDT	5
AOLLOAD.EXE-11F701E6.pf	AOLLOAD.EXE	2008-10-29 20:35:10 PDT	6
AOLSOFTWARE.EXE-11870E32.pf	AOLSOFTWARE.EXE	2008-10-30 09:03:10 PDT	31
DASHBOARD.EXE-1F66FC57.pf	DASHBOARD.EXE	2008-10-29 20:17:30 PDT	1
EXCEL.EXE-34CB65E9.pf	EXCEL.EXE	2008-10-29 09:15:57 PDT	1
FIREFOX.EXE-28641590.pf	FIREFOX.EXE	2008-10-30 00:51:27 PDT	16
GOOGLEUPDATE.EXE-0FED1BD9.pf	GOOGLEUPDATE.EXE	2008-10-30 09:10:59 PDT	79
GROOVEMONITOR.EXE-2606717A.pf	GROOVEMONITOR.EXE	2008-10-30 00:50:17 PDT	6
HELPER.EXE-0415776D.pf	HELPER.EXE	2008-10-21 12:30:16 PDT	2
HELPSVC.EXE-2878DDA2.pf	HELPSVC.EXE	2008-10-22 14:42:05 PDT	1
IEXPLORE.EXE-27122324.pf	IEXPLORE.EXE	2008-10-29 19:56:27 PDT	7
MSOHTMED.EXE-0712ED38.pf	MSOHTMED.EXE	2008-10-28 09:55:01 PDT	1
OUTLOOK.EXE-2FC6F8AB.pf	OUTLOOK.EXE	2008-10-29 20:29:14 PDT	5
PIDGIN.EXE-280DB919.pf	PIDGIN.EXE	2008-10-29 19:42:40 PDT	5

SETUP.EXE-17D54D77.pf	SETUP.EXE	2008-10-28 09:39:28 PDT	1
THUNDERBIRD.EXE-38CA75D9.pf	THUNDERBIRD.EXE	2008-10-29 19:54:43 PDT	10
VMIP.EXE-2BD5723A.pf	VMIP.EXE	2008-10-29 18:06:33 PDT	10
VMWARETRAY.EXE-029F476F.pf	VMWARETRAY.EXE	2008-10-30 00:50:16 PDT	12
VMWAREUSER.EXE-1F72BBE4.pf	VMWAREUSER.EXE	2008-10-30 00:50:17 PDT	12























#### 4. Recently Accessed Files

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

To determine the Office documents recently accessed by users, Autopsy's Data Artifacts module was utilized, which parses metadata and system artifacts during ingestion, including shortcut, *.lnk*, files and registry keys like *RecentDocs*. Autopsy categorizes these as Recent Documents, and identified 6 distinct Office documents associated with *domexuser1*, based on unique file paths for *.xlsx* and *.docx* located in *C:\Documents and Settings\domex1\My Documents*. Each document had corresponding *.lnk* files reflecting actions such as accessed, sent, or deleted. The unique file paths confirmed that these were separate files. Additionally, some files were no longer present in the My Documents folder, indicating they may have been deleted after being accessed. The recently accessed documents are summarized with timestamps in the table below.

User	File Name	File Hash	Timestamp
domex1	This is a spreadsheet by domex user 1.xlsx	dd0197445b07359857ea968db372fb1e	2008-10-29 12:16:28 EDT
domex1	This is a spreadsheet deleted by domex user 1.xlsx  Dc4.xlsx	a90baa95ad2974f5fb5b268bc5b68e54	2008-10-29 12:17:24 EDT
domex1	This is a spreadsheet sent by domex user 1.xlsx	2a444a21186db2b9816edc87c7b02d3f	2008-10-29 12:16:52 EDT
domex1	This is a word	53dec327aed600884f	2008-10-29 12:15:34

	document deleted by domex user 1.docx  Dc3.docx	2145fc860aaee8	EDT
domex1	This is a word document by domex user 1.docx	adbb75d83fda3d5d49f02a6b16fea9f8	2008-10-29 12:14:52 EDT
domex1	This is a word document sent by domex user 1.docx	757988c327a36d37500e56c238f15007	2008-10-29 12:15:20 EDT
SHELLNEW	EXCEL12.XLSX	0a8bf38315fe8edaf988b9fb077be18a	2008-10-28 09:42:47 PDT

Listing						
Recent Documents						
Table Thumbnail Summary						
Source Name	S	C	O	Path	Date Accessed	
 autorun.lnk				C:\Documents and Settings\Administrator\Desktop\O...	2008-10-28 12:39:19 EDT	
 LicenseKey.lnk				C:\Documents and Settings\Administrator\Desktop\O...	2008-10-28 12:39:39 EDT	
 Office2007Enterprise.lnk				C:\Documents and Settings\Administrator\Desktop\O...	2008-10-28 12:39:20 EDT	
 My Documents (2).LNK				C:\Documents and Settings\domex1\My Documents	2008-10-29 12:14:52 EDT	
 My Documents.LNK				C:\Documents and Settings\domex1\My Documents	2008-10-29 12:14:52 EDT	
 Templates.LNK				C:\Documents and Settings\domex1\Application Data...	2008-10-29 12:15:44 EDT	
 This is a spreadsheet by domex user 1.LNK				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:16:28 EDT	
 This is a spreadsheet deleted by domex user 1.LNK				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:17:24 EDT	
 This is a spreadsheet sent by domex user 1.LNK				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:16:52 EDT	
 This is a word document deleted by domex user 1.LNK				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:15:34 EDT	
 This is a spreadsheet by domex user 1.lnk				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:16:28 EDT	
 This is a spreadsheet deleted by domex user 1.lnk				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:17:24 EDT	
 This is a spreadsheet sent by domex user 1.lnk				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:16:52 EDT	
 This is a word document by domex user 1.lnk				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:14:52 EDT	
 This is a word document deleted by domex user 1.lnk				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:15:34 EDT	
 This is a word document sent by domex user 1.lnk				C:\Documents and Settings\domex1\My Documents\...	2008-10-29 12:15:20 EDT	
 domexuser2.LNK				C:\Documents and Settings\domex2\My Documents\...	2008-10-29 21:59:10 EDT	
 My Pictures.LNK				C:\Documents and Settings\domex2\My Documents\...	2008-10-29 21:59:10 EDT	
 domexuser2.lnk				C:\Documents and Settings\domex2\My Documents\...	2008-10-29 12:21:16 EDT	
 My Pictures.lnk				C:\Documents and Settings\domex2\My Documents\...	2008-10-29 12:21:16 EDT	
 NTUSER.DAT					2008-10-30 02:48:12 EDT	
 NTUSER.DAT				C:\Documents and Settings\domex2\My Documents\...		

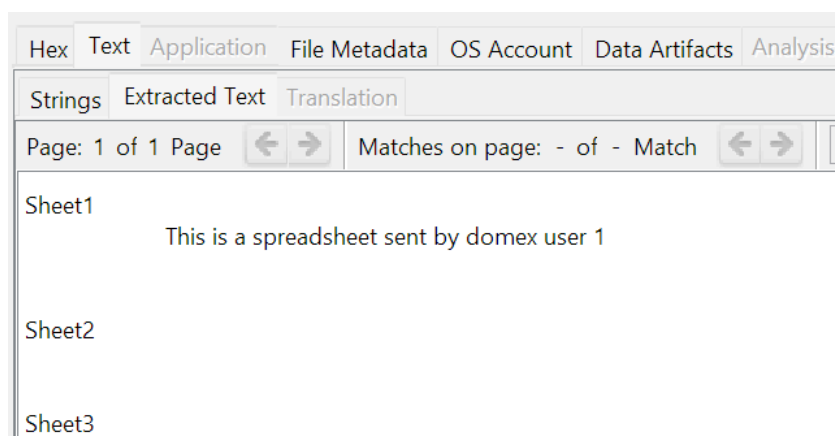
▲ Name	C	S	O	Modified Time	Change Time	Access Time	Created Time	Size
Dc3.docx			1	2008-10-29 09:15:34 PDT	2008-10-29 20:39:32 PDT	2008-10-29 20:39:30 PDT	2008-10-29 09:15:34 PDT	9852
Dc4.xlsx		▼	0	2008-10-29 09:17:24 PDT	2008-10-29 20:39:38 PDT	2008-10-29 20:39:34 PDT	2008-10-29 09:17:24 PDT	8236
EXCEL12.XLSX			0	2006-09-22 01:25:46 PDT	2008-10-28 09:42:47 PDT	2008-10-28 09:42:47 PDT	2006-09-22 01:25:46 PDT	8714
PROTTPLN.DOC			0	2004-11-01 17:56:22 PST	2008-10-28 09:42:45 PDT	2008-10-28 09:45:52 PDT	2004-11-01 17:56:22 PST	19968
PROTTPLN.PPT			0	2004-11-01 17:56:32 PST	2008-10-28 09:40:23 PDT	2008-10-28 09:44:30 PDT	2004-11-01 17:56:26 PST	12288
PROTTPLN.XLS			0	2004-11-01 17:56:40 PST	2008-10-28 09:42:45 PDT	2008-10-28 09:45:52 PDT	2004-11-01 17:56:40 PST	8704
PROTTPLV.DOC			0	2004-11-01 17:56:20 PST	2008-10-28 09:42:45 PDT	2008-10-28 09:45:52 PDT	2004-11-01 17:56:20 PST	19968
PROTTPLV.PPT			0	2004-11-01 17:56:24 PST	2008-10-28 09:40:24 PDT	2008-10-28 09:44:30 PDT	2004-11-01 17:56:24 PST	12288
PROTTPLV.XLS			0	2008-10-28 09:42:45 PDT	2008-10-28 09:42:45 PDT	2008-10-28 09:45:52 PDT	2004-11-01 17:56:32 PST	8704
PWRPNT12.PPTX			0	2006-09-22 01:32:50 PDT	2008-10-28 09:44:30 PDT	2008-10-28 09:44:30 PDT	2006-09-22 01:32:50 PDT	27140
SOLVSAMP.XLS		▼	0	2003-04-21 19:19:40 PDT	2008-10-28 09:42:54 PDT	2008-10-28 09:42:54 PDT	2003-04-21 19:19:40 PDT	118784
This is a spreadsheet by domex user 1.xlsx		▼	0	2008-10-29 09:16:28 PDT	2008-10-29 09:16:28 PDT	2008-10-29 19:04:32 PDT	2008-10-29 09:16:27 PDT	8230
This is a spreadsheet sent by domex user 1.xlsx		▼	1	2008-10-29 09:16:52 PDT	2008-10-29 09:16:52 PDT	2008-10-29 20:38:10 PDT	2008-10-29 09:16:51 PDT	8203
This is a spreadsheet sent by domex user 1.xlsx		▼	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	8203
This is a word document by domex user 1.docx			0	2008-10-29 09:14:52 PDT	2008-10-29 09:14:52 PDT	2008-10-29 09:14:52 PDT	2008-10-29 09:14:52 PDT	9844
This is a word document sent by domex user 1.docx		▼	1	2008-10-29 09:15:20 PDT	2008-10-29 09:15:20 PDT	2008-10-29 20:38:18 PDT	2008-10-29 09:15:20 PDT	9926
This is a word document sent by domex user 1.docx		▼	1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	9926
excel.xls			1	2004-08-04 05:00:00 PDT	2008-10-20 14:58:34 PDT	2008-10-20 14:58:34 PDT	2008-10-20 14:58:34 PDT	5632

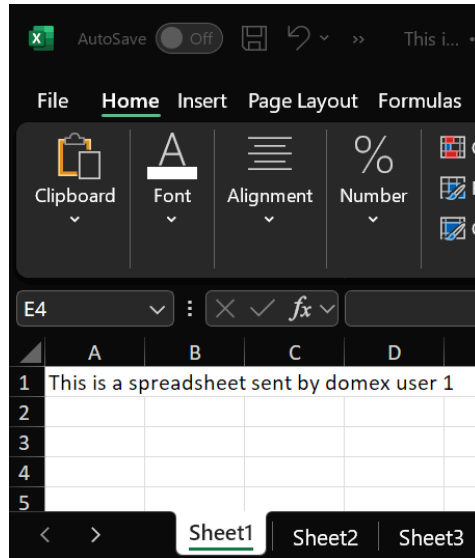
## 5. Locating Files

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

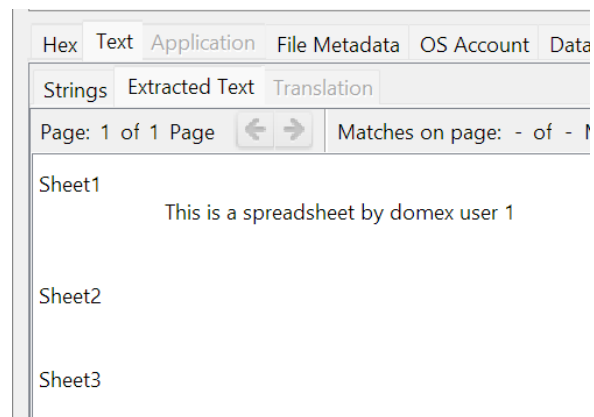
For 4 of the 6 recently accessed Office documents, the files were still accessible in the *My Documents* directory of user *domex1*. These files could easily be extracted and viewed or by using the *Extracted Text* function built-in Autopsy. As the documents contain very little information, only the first file contains the extracted view of the document.

- C:\Documents and Settings\domex1\My Documents\This is a spreadsheet sent by domex user 1.xlsx*

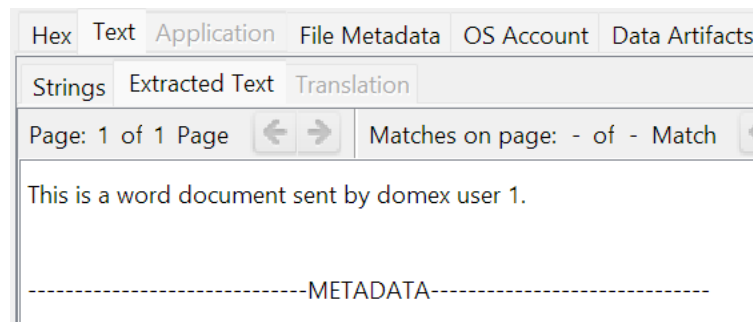




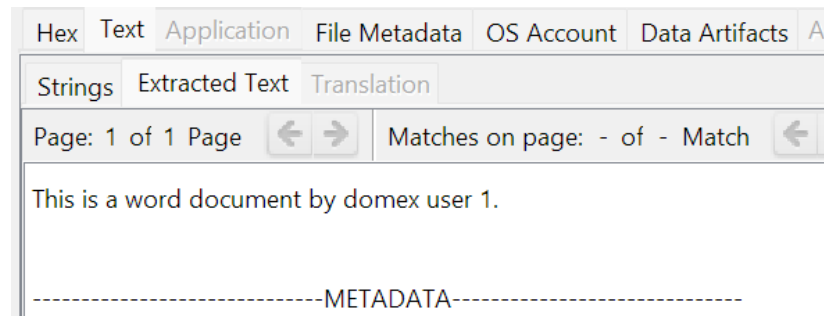
2. *C:\Documents and Settings\domex1\My Documents\This is a spreadsheet by domex user 1.xlsx*



3. *C:\Documents and Settings\domex1\My Documents\This is a word document sent by domex user 1.docx*



4. *C:\Documents and Settings\domex1\My Documents\This is a word document by domex user 1.docx*



For the remaining 2 recently accessed Office documents, which were deleted as confirmed by the files no longer being present in the *My Documents* directory of user *domex1*, traces of these files were still accessible through the Recent Documents section in Autopsy. By using the extracted text function or performing a keyword search for the file names, portions of the content were recoverable.

5. *C:\Documents and Settings\domex1\My Documents\This is a spreadsheet deleted by domex user 1.xlsx*     **DELETED**

Data Content

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset

THISIS~3.XLS  
 This is a spreadsheet deleted by domex user 1.xlsx  
 C:\Documents and Settings\domex1\My Documents\This is a spreadsheet deleted by domex user 1.xlsx  
 B..\My Documents\This is a spreadsheet deleted by domex user 1.xlsx-C:\Documents and Settings\domex1\My Documents  
 realistic\_xp

6. *C:\Documents and Settings\domex1\My Documents\This is a word document deleted by domex user 1.docx*

Data Content

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Oc

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset

THISIS~3.DOC  
 This is a word document deleted by domex user 1.docx  
 C:\Documents and Settings\domex1\My Documents\This is a word document deleted by domex user 1.docx  
 D..\My Documents\This is a word document deleted by domex user 1.docx-C:\Documents and Settings\domex1\My Documents  
 realistic\_xp

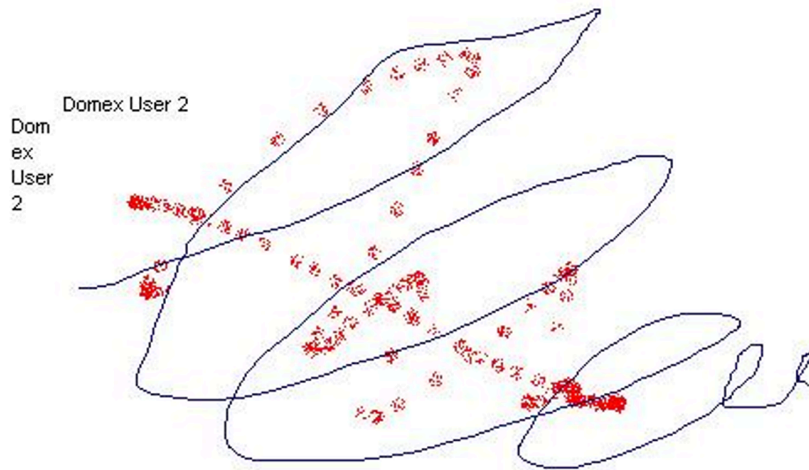
## 6. Email Analysis

- 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?

Sender	Receiver(s)	Email Subject	Message	Has Attachments	File Name	Timestamp
domexuser1@gmail.com	domexuser3@gmail.com	RE: test email 1	Good test	No	N/A	Wed, 29 Oct 18:46:00 PDT
domexuser1@gmail.com	'Domex user 3'	RE: test email 1	Here's an attached picture	Yes	domexuser2.jpg	Wed, 29 Oct 18:59:00 PDT
domexuser1@gmail.com	domexuser2@gmail.com ;	RE: test email 1	This is a spreadsheet sent by	Yes	This is a spreadsheet sent by	Wed, 29 Oct 2008 19:05:34



	domexuser3@gmail.com		domex user 1.xlsx		domex user 1.xlsx	-0700 (PDT)
domexuser1@gmail.com	domexuser2@gmail.com ; domexuser3@gmail.com	RE: test email 1	This is a word document sent by domex user 1.docx	Yes	This is a word document sent by domex user 1.docx	Wed, 29 Oct 2008 17:38:43 -0800
domexuser1@gmail.com	Domex1 test; domex user 3; domexuser1@hotmail.com; domexuser2@hotmail.com	RE: test email 1	Adding in the hotmail accounts	No	N/A	Wed, 29 Oct 2008 19:46:00 PDT
domexuser1@gmail.com	Domex user; domex user 1; domex user 2; domex1 test	RE: test email 1	Good to see everyone	No	N/A	Wed, 29 Oct 2008 20:30:00 PDT
domexuser2@gmail.com	domexuser1@gmail.com domexuser3@gmail.com	LocalFreeBusy		No	N/A	N/A



domexuser2.jpg

MD5: 1830b0f77dcfbfee91901aebc6d126f8

## 7. Pidgin Messenger Artifacts

- a. 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?

Pidgin is a GTK+ instant messaging application for Windows and Unix. It supports communication over AIM, ICQ, Jabber/XMPP, MSN, Yahoo!, Bonjour, Gadu-Gadu, IRC, QQ, SILC, SIMPLE, IRC, Novell GroupWise, Lotus Sametime, Zephyr and more.

Account protocol	Name	Password
prpl-aim	domexuser2	!!password

prpl-jabber	domexuser2@gmail.com	!!password
prpl-msn	domexuser2@live.com	!!password

File Path: *Documents and Settings/domex1/Application Data/.purple/blist.xml*

```

</blist>
<privacy>
    <account proto='prpl-aim' name='domexuser2' mode='1'/>
    <account proto='prpl-jabber' name='domexuser2@gmail.com/Home' mode='1'/>
    <account proto='prpl-msn' name='domexuser2@live.com' mode='1'/>

```

File name	Protocol	Group	Buddy Account	Name	Alias
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	SportsFanStan	All SPORTS 24-7!!!
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	IM Street	
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	Liv Greene	
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	GossipinGabby	GOSSIP all day all night!
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	USA Today	USA Today
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	VoteRedorBlue	
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	SmackTalkSports	
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	MovieFone	
blist.xml	prpl-aim	AIM Bot	domexuser1	Prof Gilzot	The Best

			domexuser2		Tutor in the Universe!
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	Spleak	
blist.xml	prpl-aim	AIM Bot	domexuser1 domexuser2	Ed Drivers	
f0147200.xml	prpl-aim	Buddies/ Family	domexuser1	domexuser2	
blist.xml	prpl-aim	Buddies/ Family	domexuser2	domexuser3	
f0282592.xml	prpl-aim	Recent Buddies	domexuser2	domexuser1	
f0147200.xml	prpl-jabber	Buddies/ Family	domexuser1@ gmail.com	domesxuser2@gmail .com	domex2 user

File Path: *Documents and Settings/domex1/Application Data/.purple/blist.xml*

```

blist.xml <?xml version='1.0' encoding='UTF-8' ?>
<purple version='1.0'>
  <blist>
    <group name='Recent Buddies'>
      <setting name='collapsed' type='bool'>0</setting>
      <contact>
        <buddy account='domexuser1' proto='prpl-aim'>
          <name>domexuser2</name>
          <setting name='last_seen' type='int'>1224619676</setting>
        </buddy>
      </contact>
    </group>
    <group name='Co-Workers' />
    <group name='Family' />
    <group name='Buddies'>
      <setting name='collapsed' type='bool'>0</setting>
      <contact>
        <buddy account='domexuser1@gmail.com/Home' proto='prpl-jabber'>
          <name>domesxuser2@gmail.com</name>
          <alias>domex2 user</alias>
          <setting name='last_seen' type='int'>1224618603</setting>
        </buddy>
      </contact>
      <contact>
        <buddy account='domexuser1@gmail.com/Home' proto='prpl-jabber'>
          <name>domesxuser2@gmail.com</name>
          <setting name='last_seen' type='int'>1224619274</setting>
        </buddy>
        <setting name='gtk-mute-sound' type='bool'>0</setting>
      </contact>
    </group>
    <group name='AIM Bots'>
      <setting name='collapsed' type='bool'>1</setting>
      <contact>
        <buddy account='domexuser1' proto='prpl-aim'>
          <name>MovieFone</name>
          <setting name='last_seen' type='int'>1224619388</setting>
        </buddy>
      </contact>
    </group>
  </blist>
</purple>

```

## 8. Communication and File transfer

- a. **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?**

The primary mode of communication between parties was email, specifically utilizing the Outlook application. The list of communicating entities is as follows:

1. “domex user 1”: domexuser1@hotmail.com
2. “domex user 2”: domexuser2@hotmail.com; domexuser2@gmail.com
3. “domex user 3”: domexuser3@gmail.com
4. “domex user”: domexuser1@live.com
5. “domex1 test”: domexuser1@gmail.com

Method	File Name	File Hash	Sender	Receiver	Date/Time
Outlook	This is a spreadsheet sent by domex user 1.xlsx	2a444a21186db2b9816edc87c7b02d3f	domexuser1@gmail.com	domexuser2@gmail.com; domexuser3@gmail.com	Wed, 29 Oct 2008 19:05:34 -0700 (PDT)
Outlook	This is a word document sent by domex user 1.docx	757988c327a36d37500e56c238f15007	domexuser1@gmail.com	domexuser2@gmail.com; domexuser3@gmail.com	Wed, 29 Oct 2008 17:38:43 -0800
Outlook	domexuser2.jpg	1830b0f77dcfbfee91901aebc6d126f8	domexuser2@gmail.com	domexuser3@gmail.com; domexuser1@gmail.com	Wed, 29 Oct 2008 18:49:47 -0700
WLM	Unknown	Unknown	domexuser2@hotmail.com	domexuser1@hotmail.com; domexuser1@gmail.com; domexuser2@gmail.com; domexuser3@gmail.com; domexuser1@live.com; domexuser2@live.com	2008-10-29 19:57:30 PDT

Additional method of communication identified:

## Windows Live™ Messenger Beta (WLM) (MSN Messenger)

File Path:

*img\_nps-2009-domexusers.E01/vol\_vol2/Documents and Settings/domex2/Local  
Settings/Temporary Internet  
Files/Content.IE5/0LYRGTUN/SendMessageLight[1].aspx/SendMessageLight[1].aspx/0*

Windows Live™ Home Hotmail Spaces OneCare MSN    domexuser2@hotmail.com Sign out

- New
- Options

**Your message has been sent to the following recipients:**

domex user 1	Not yet a contact
domex user 2	Not yet a contact
domex user 3	Not yet a contact
domex1 test	Not yet a contact
domexuser1@live.com	Not yet a contact
domexuser2@live.com	Not yet a contact

**Add contacts**

- ☒ domexuser1@hotmail.com
  - First name
  - Last name
- ☒ domexuser2@gmail.com
  - First name
  - Last name
- ☒ domexuser3@gmail.com
  - First name
  - Last name
- ☒ domexuser1@gmail.com
  - First name
  - Last name
- ☒ domexuser1@live.com
  - First name
  - Last name
- ☒ domexuser2@live.com
  - First name
  - Last name

[Return to message](#)

- Inbox
- Junk
- Drafts
- Sent
- Deleted

Page folders  
My Mail Contacts Calendar