Digital Forensics Analysis Report

Mustafa Ranapurwala | Ross Barber | Carina Martinez-Lopez | Zoe Medina | Randall Seymore

4 December 2023

CYBR 512

For issues with embedded content, please use the Google Doc
https://docs.google.com/document/d/1jBRXcKGiRQbR4SdLMf6jP7YJBft0JtK2L2omHfSE2OA/edit?usp=sharing

Table of Contents

Executive Summary

In November 2023, USD CYBR-512 students were arranged into a forensic investigation team to conduct a computer forensics analysis of files from a Windows XP image (nps-2009-domexusers.E01). The team will provide law enforcement with any evidence of communication artifacts to determine if a crime has been committed. The primary test objective for this project is to identify if any users on the system communicated with, and sent any files to remote users.

Evidence Acquisition Processing Procedures

Testers received the disk image file “nps-2009-domexusers.E01” on November 28th, 2023 from the Digital Corpora website. This image was uploaded into Autopsy and ingested with all available modules selected. All analysis completed on the disk image file data was performed using Autopsy 4.21.0 and RegRipper.

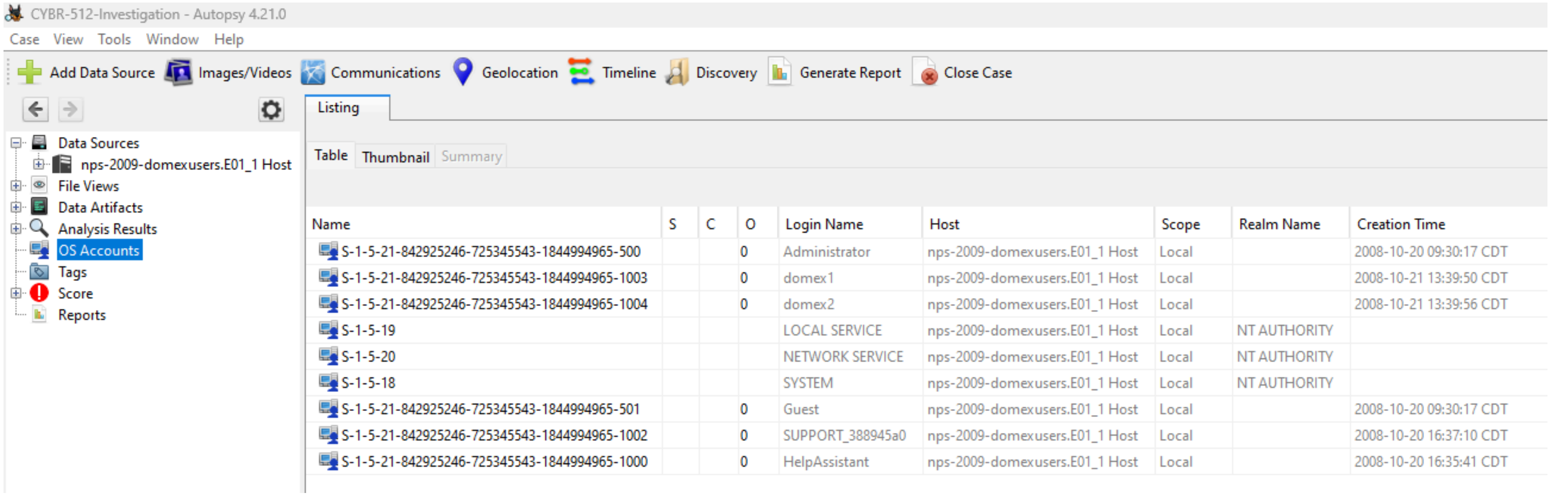
Analysis

System Users and Associated Security Identifiers

Nine total users were identified on the processed image by drilling into results in the ‘OS Accounts’ section of Autopsy results. All users appear to be local to the system, suggesting the device was not joined to a domain. Included is a list of users by Security ID along with the corresponding Login Name.

Security ID	Login Name
S-1-5-21-842925246-725345543-1844994965-500	Administrator
S-1-5-21-842925246-725345543-1844994965-1003	domex1
S-1-5-21-842925246-725345543-1844994965-1004	domex2
S-1-5-19	LOCAL SERVICE
S-1-5-20	NETWORK SERVICE
S-1-5-18	SYSTEM
S-1-5-21-842925246-725345543-1844994965-501	Guest
S-1-5-21-842925246-725345543-1844994965-1002	SUPPORT_388945a0
S-1-5-21-842925246-725345543-1844994965-1000	HelpAssistant

Evidence



Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-842925246-725345543-1844994965-500			0	Administrator	nps-2009-domexusers.E01_1 Host	Local		2008-10-20 09:30:17 CDT
S-1-5-21-842925246-725345543-1844994965-1003			0	domex1	nps-2009-domexusers.E01_1 Host	Local		2008-10-21 13:39:50 CDT
S-1-5-21-842925246-725345543-1844994965-1004			0	domex2	nps-2009-domexusers.E01_1 Host	Local		2008-10-21 13:39:56 CDT
S-1-5-19				LOCAL SERVICE	nps-2009-domexusers.E01_1 Host	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	nps-2009-domexusers.E01_1 Host	Local	NT AUTHORITY	
S-1-5-18				SYSTEM	nps-2009-domexusers.E01_1 Host	Local	NT AUTHORITY	
S-1-5-21-842925246-725345543-1844994965-501			0	Guest	nps-2009-domexusers.E01_1 Host	Local		2008-10-20 09:30:17 CDT
S-1-5-21-842925246-725345543-1844994965-1002			0	SUPPORT_388945a0	nps-2009-domexusers.E01_1 Host	Local		2008-10-20 16:37:10 CDT
S-1-5-21-842925246-725345543-1844994965-1000			0	HelpAssistant	nps-2009-domexusers.E01_1 Host	Local		2008-10-20 16:35:41 CDT

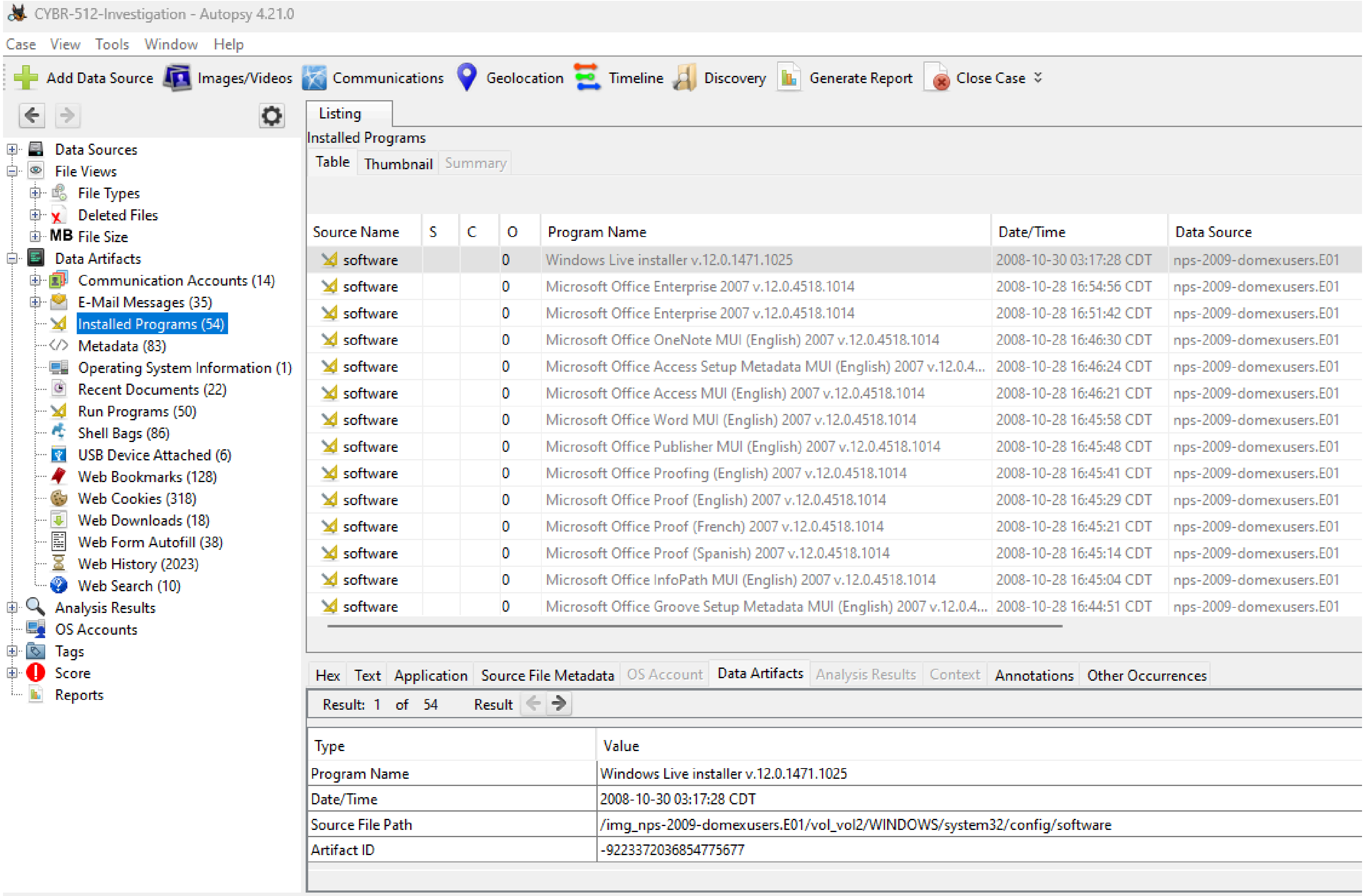
“OS Accounts” section of the Autopsy tool

Installed Applications and Software

Leveraging the ‘Installed Programs’ section of Autopsy results, a total of 54 applications were identified on the system. Six of these applications were identified as software that could be used for communication, which are highlighted below in Orange.

Software			
Windows Live installer	Microsoft Office Groove MUI (English) 2007	AOL Diagnostics_N	ICW
Microsoft Office Enterprise 2007	Microsoft Software Update for Web Folders (English) 12	Pidgin v.2.5.2	NetMeeting
Microsoft Office Enterprise 2007	Microsoft Office PowerPoint MUI (English) 2007	GTK+ Runtime 2.12.12 rev a (remove only)	OutlookExpress
Microsoft Office OneNote MUI (English)	Microsoft Office Outlook MUI (English) 2007	Mozilla Firefox (3.0.3) (en-US)	DirectDrawEx
Microsoft Office Access Setup Metadata MUI (English) 2007	Microsoft Office Excel MUI (English) 2007	Google Gears	Fontcore
Microsoft Office Access MUI (English) 2007	Microsoft Office Shared Setup Metadata MUI (English) 2007	WIC	IE40
Microsoft Office Word MUI (English) 2007	Microsoft Office Shared MUI (English) 2007	Windows XP Service Pack 3	IE4Data
Microsoft Office Publisher MUI (English)	WebFldrs XP	Windows Genuine Advantage Validation Tool (KB892130)	IE5BAKEX
Microsoft Office Proofing (English) 2007	MPlayer2	Windows Genuine Advantage Validation Tool (KB892130)	IEData
Microsoft Office Proof (English) 2007	Picasa 3 v.3.0	VMware Tools	MobileOptionPack
Microsoft Office Proof (French) 2007	Mozilla Thunderbird (2.0.0.17) (en-US)	DXM_Runtime	SchedulingAgent
Microsoft Office Proof (Spanish) 2007	Viewpoint Media Player	PCHealth	Connection Manager
Microsoft Office InfoPath MUI (English) 2007	AIM 6	AddressBook	
Microsoft Office Groove Setup Metadata MUI (English) 2007	AOLOCP_Y	DirectAnimation	

Evidence



Source Name	S	C	O	Program Name	Date/Time	Data Source
software			0	Windows Live installer v.12.0.1471.1025	2008-10-30 03:17:28 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Enterprise 2007 v.12.0.4518.1014	2008-10-28 16:54:56 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Enterprise 2007 v.12.0.4518.1014	2008-10-28 16:51:42 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office OneNote MUI (English) 2007 v.12.0.4518.1014	2008-10-28 16:46:30 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Access Setup Metadata MUI (English) 2007 v.12.0.4...	2008-10-28 16:46:24 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Access MUI (English) 2007 v.12.0.4518.1014	2008-10-28 16:46:21 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Word MUI (English) 2007 v.12.0.4518.1014	2008-10-28 16:45:58 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Publisher MUI (English) 2007 v.12.0.4518.1014	2008-10-28 16:45:48 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Proofing (English) 2007 v.12.0.4518.1014	2008-10-28 16:45:41 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Proof (English) 2007 v.12.0.4518.1014	2008-10-28 16:45:29 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Proof (French) 2007 v.12.0.4518.1014	2008-10-28 16:45:21 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Proof (Spanish) 2007 v.12.0.4518.1014	2008-10-28 16:45:14 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office InfoPath MUI (English) 2007 v.12.0.4518.1014	2008-10-28 16:45:04 CDT	nps-2009-domexusers.E01
software			0	Microsoft Office Groove Setup Metadata MUI (English) 2007 v.12.0.4...	2008-10-28 16:44:51 CDT	nps-2009-domexusers.E01

Type	Value
Program Name	Windows Live installer v.12.0.1471.1025
Date/Time	2008-10-30 03:17:28 CDT
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/WINDOWS/system32/config/software
Artifact ID	-9223372036854775677

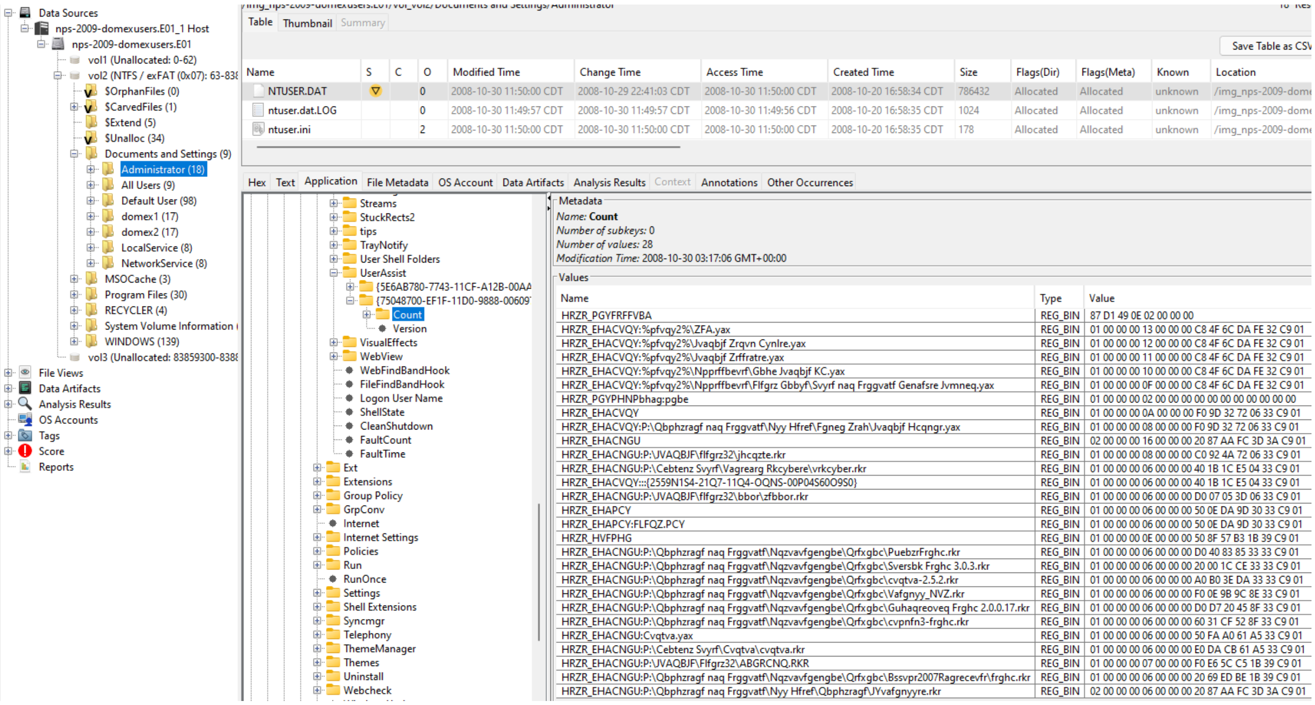
"Installed Programs" section of the Autopsy tool

Communication-Based Applications Run By Users

In order to identify which communication-based applications were run by users on the system, the NTUSER.DAT hive files within each user's profile folder in the C:\Documents and Settings directory were analyzed. ROT-13 encoded values of 'UserAssist' keys (HKCU\Software\Microsoft\Windows\CurrentVersion \Explorer\UserAssist) using Autopsy were decoded using the RegRipper tool to populate the below table.

Communication-Based Application	Executed?	Associated User(s)
Microsoft Office Outlook	Yes	domex1 domex2
Mozilla Thunderbird	Yes	domex1 domex2
AIM	Yes	domex1
Pidgin	Yes	Administrator domex1 domex2
NetMeeting	No	N/A
OutlookExpress	No	N/A

Evidence



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
NTUSER.DAT	▽		0	2008-10-30 11:50:00 CDT	2008-10-29 22:41:03 CDT	2008-10-30 11:50:00 CDT	2008-10-20 16:58:34 CDT	786432	Allocated	Allocated	unknown	/img_nps-2009-dome
ntuser.dat.LOG			0	2008-10-30 11:49:57 CDT	2008-10-30 11:49:57 CDT	2008-10-30 11:49:56 CDT	2008-10-20 16:58:35 CDT	1024	Allocated	Allocated	unknown	/img_nps-2009-dome
ntuser.ini			2	2008-10-30 11:50:00 CDT	2008-10-30 11:50:00 CDT	2008-10-30 11:50:00 CDT	2008-10-20 16:58:35 CDT	178	Allocated	Allocated	unknown	/img_nps-2009-dome

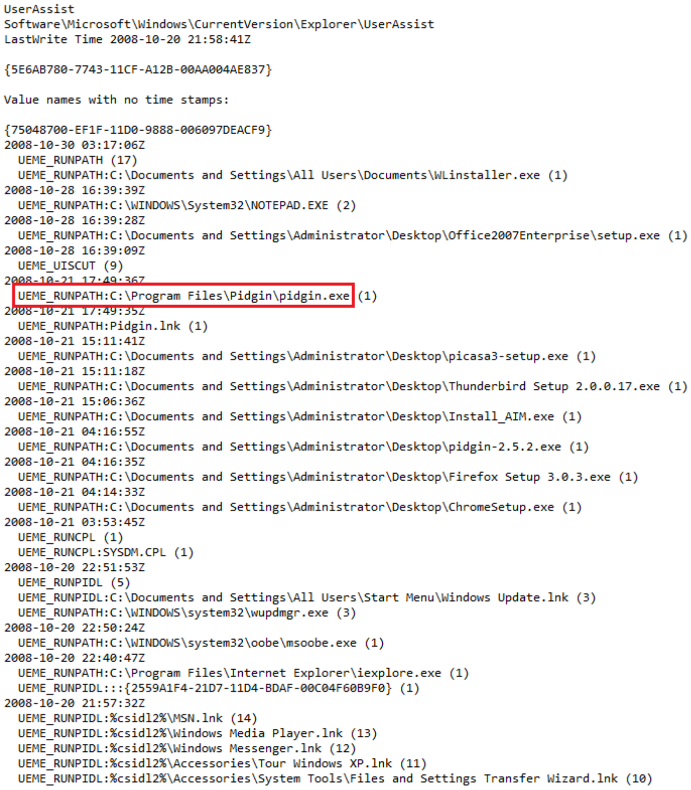
Metadata

Name: **Count**
Number of subkeys: 0
Number of values: 28
Modification Time: 2008-10-30 03:17:06 GMT+00:00

Values

Name	Type	Value
HRZR_PGYFRFFVBA	REG_BIN	87 D1 49 0E 02 00 00 00
HRZR_EHACVQY:%pfvqy2%\ZFA.yax	REG_BIN	01 00 00 00 13 00 00 00 C8 4F 6C DA FE 32 C9 01
HRZR_EHACVQY:%pfvqy2%\Jvaqbjf Zrqvn Cynlre.yax	REG_BIN	01 00 00 00 12 00 00 00 C8 4F 6C DA FE 32 C9 01
HRZR_EHACVQY:%pfvqy2%\Jvaqbjf Zrffratre.yax	REG_BIN	01 00 00 00 11 00 00 00 C8 4F 6C DA FE 32 C9 01
HRZR_EHACVQY:%pfvqy2%\Npprffbevrf\Gbhe Jvaqbjf KC.yax	REG_BIN	01 00 00 00 10 00 00 00 C8 4F 6C DA FE 32 C9 01
HRZR_EHACVQY:%pfvqy2%\Npprffbevrf\Flfgrz Gbbyf\Svyrf naq Frggvatf Genafsre Jvmneq.yax	REG_BIN	01 00 00 00 0F 00 00 00 C8 4F 6C DA FE 32 C9 01
HRZR_PGYPHNPbhag:pgbe	REG_BIN	01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
HRZR_EHACVQY	REG_BIN	01 00 00 00 0A 00 00 00 F0 9D 32 72 06 33 C9 01
HRZR_EHACVQY:P:\Qbphzragf naq Frggvatf\Nyy Hfref\Fgneg Zrah\Jvaqbjf Hcqngr.yax	REG_BIN	01 00 00 00 08 00 00 00 F0 9D 32 72 06 33 C9 01
HRZR_EHACNGU	REG_BIN	02 00 00 00 16 00 00 00 20 87 AA FC 3D 3A C9 01
HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\jhcqzte.rkr	REG_BIN	01 00 00 00 08 00 00 00 C0 92 4A 72 06 33 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Vagrearg Rkcybere\vrkcyber.rkr	REG_BIN	01 00 00 00 06 00 00 00 40 1B 1C E5 04 33 C9 01
HRZR_EHACVQY:::{2559N1S4-21Q7-11Q4-OQNS-00P04S60O9S0}	REG_BIN	01 00 00 00 06 00 00 00 40 1B 1C E5 04 33 C9 01
HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\bbor\zfbbor.rkr	REG_BIN	01 00 00 00 06 00 00 00 D0 07 05 3D 06 33 C9 01
HRZR_EHAPCY	REG_BIN	01 00 00 00 06 00 00 00 50 0E DA 9D 30 33 C9 01
HRZR_EHAPCY:FLFQZ.PCY	REG_BIN	01 00 00 00 06 00 00 00 50 0E DA 9D 30 33 C9 01
HRZR_HVFPHG	REG_BIN	01 00 00 00 0E 00 00 00 50 8F 57 B3 1B 39 C9 01
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\PuebzrFrghc.rkr	REG_BIN	01 00 00 00 06 00 00 00 D0 40 83 85 33 33 C9 01
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\Sversbk Frghc 3.0.3.rkr	REG_BIN	01 00 00 00 06 00 00 00 20 00 1C CE 33 33 C9 01
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\cvqtva-2.5.2.rkr	REG_BIN	01 00 00 00 06 00 00 00 A0 B0 3E DA 33 33 C9 01
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\Vafgnyy_NVZ.rkr	REG_BIN	01 00 00 00 06 00 00 00 F0 0E 9B 9C 8E 33 C9 01
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\Guhaqreoveq Frghc 2.0.0.17.rkr	REG_BIN	01 00 00 00 06 00 00 00 D0 D7 20 45 8F 33 C9 01
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\cvpnfn3-frghc.rkr	REG_BIN	01 00 00 00 06 00 00 00 60 31 CF 52 8F 33 C9 01
HRZR_EHACNGU:Cvqtva.yax	REG_BIN	01 00 00 00 06 00 00 00 50 FA A0 61 A5 33 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Cvqtva\cvqtva.rkr	REG_BIN	01 00 00 00 06 00 00 00 E0 DA CB 61 A5 33 C9 01
HRZR_EHACNGU:P:\JVAQBJF\Flfgrz32\ABGRCNQ.RKR	REG_BIN	01 00 00 00 07 00 00 00 F0 E6 5C C5 1B 39 C9 01
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\Qrfxgbc\Bssvpr2007Ragrecevfr\frghc.rkr	REG_BIN	01 00 00 00 06 00 00 00 20 69 ED BE 1B 39 C9 01
HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nyy Hfref\Qbphzragf\JYvafgnyyre.rkr	REG_BIN	02 00 00 00 06 00 00 00 20 87 AA FC 3D 3A C9 01

*ROT-13 encoded UserAssist registry keys for the ‘**Administrator**’ user in Autopsy*



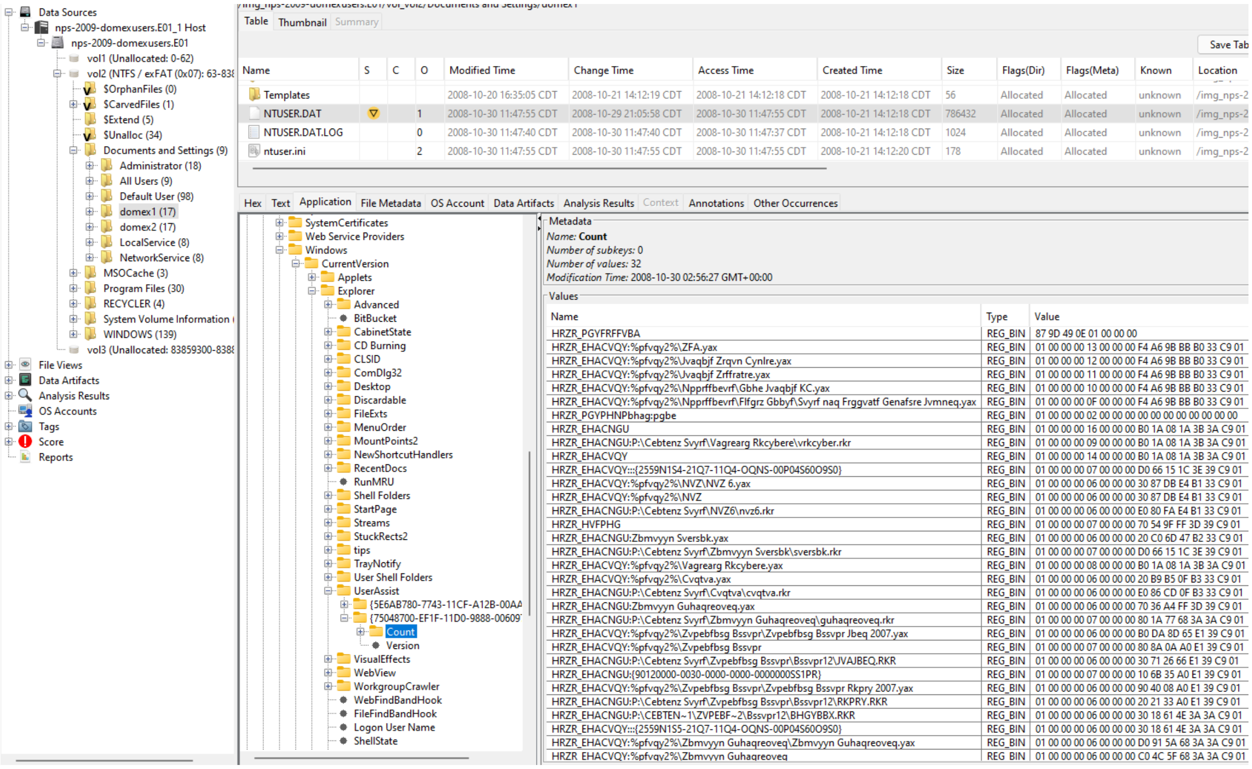
```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2008-10-20 21:58:41Z

{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 (1)
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)
```

*Evidence of the ’**Administrator**’ user running communication applications decoded with RegRipper tool*



```
Data Sources
  nps-2009-domexusers.E01_1 Host
    nps-2009-domexusers.E01
      vol1 (Unallocated: 0-62)
      vol2 (NTFS / exFAT (0x07): 63-838
        $OrphanFiles (0)
        $CarvedFiles (1)
        $Extend (5)
        $Unalloc (34)
        Documents and Settings (9)
          Administrator (18)
          All Users (9)
          Default User (98)
          domex1 (17)
          domex2 (17)
          LocalService (8)
          NetworkService (8)
        MSOCache (3)
        Program Files (30)
        RECYCLER (4)
        System Volume Information (
        WINDOWS (139)
      vol3 (Unallocated: 83859300-8388
File Views
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
```

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Templates				2008-10-20 16:35:05 CDT	2008-10-21 14:12:19 CDT	2008-10-21 14:12:18 CDT	2008-10-21 14:12:18 CDT	56	Allocated	Allocated	unknown	/img_nps-2
NTUSER.DAT	▽		1	2008-10-30 11:47:55 CDT	2008-10-29 21:05:58 CDT	2008-10-30 11:47:55 CDT	2008-10-21 14:12:18 CDT	786432	Allocated	Allocated	unknown	/img_nps-2
NTUSER.DAT.LOG			0	2008-10-30 11:47:40 CDT	2008-10-30 11:47:40 CDT	2008-10-30 11:47:37 CDT	2008-10-21 14:12:18 CDT	1024	Allocated	Allocated	unknown	/img_nps-2
ntuser.ini			2	2008-10-30 11:47:55 CDT	2008-10-30 11:47:55 CDT	2008-10-30 11:47:55 CDT	2008-10-21 14:12:20 CDT	178	Allocated	Allocated	unknown	/img_nps-2

```
SystemCertificates
Web Service Providers
Windows
  CurrentVersion
    Applets
    Explorer
      Advanced
      BitBucket
      CabinetState
      CD Burning
      CLSID
      ComDlg32
      Desktop
      Discardable
      FileExts
      MenuOrder
      MountPoints2
      NewShortcutHandlers
      RecentDocs
      RunMRU
      Shell Folders
      StartPage
      Streams
      StuckRects2
      tips
      TrayNotify
      User Shell Folders
      UserAssist
        {5E6AB780-7743-11CF-A12B-00AA
        {75048700-EF1F-11D0-9888-00609
          Count
          Version
      VisualEffects
      WebView
      WorkgroupCrawler
      WebFindBandHook
      FileFindBandHook
      Logon User Name
      ShellState
```

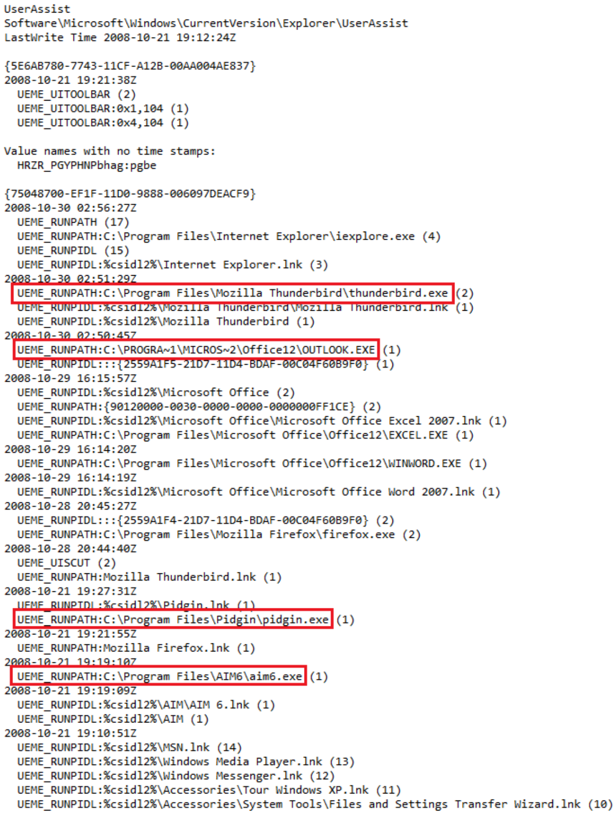
Metadata

Name: **Count**
Number of subkeys: 0
Number of values: 32
Modification Time: 2008-10-30 02:56:27 GMT+00:00

Values

Name	Type	Value
HRZR_PGYFRFFVBA	REG_BIN	87 9D 49 0E 01 00 00 00
HRZR_EHACVQY:%pfvqy2%\ZFA.yax	REG_BIN	01 00 00 00 13 00 00 00 F4 A6 9B BB B0 33 C9 01
HRZR_EHACVQY:%pfvqy2%\Jvaqbjf Zrqvn Cynlre.yax	REG_BIN	01 00 00 00 12 00 00 00 F4 A6 9B BB B0 33 C9 01
HRZR_EHACVQY:%pfvqy2%\Jvaqbjf Zrffratre.yax	REG_BIN	01 00 00 00 11 00 00 00 F4 A6 9B BB B0 33 C9 01
HRZR_EHACVQY:%pfvqy2%\Npprffbevrf\Gbhe Jvaqbjf KC.yax	REG_BIN	01 00 00 00 10 00 00 00 F4 A6 9B BB B0 33 C9 01
HRZR_EHACVQY:%pfvqy2%\Npprffbevrf\Flfgrz Gbbyf\Svyrf naq Frggvatf Genafsre Jvmneq.yax	REG_BIN	01 00 00 00 0F 00 00 00 F4 A6 9B BB B0 33 C9 01
HRZR_PGYPHNPbhag:pgbe	REG_BIN	01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
HRZR_EHACNGU	REG_BIN	01 00 00 00 16 00 00 00 B0 1A 08 1A 3B 3A C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Vagrearg Rkcybere\vrkcyber.rkr	REG_BIN	01 00 00 00 09 00 00 00 B0 1A 08 1A 3B 3A C9 01
HRZR_EHACVQY	REG_BIN	01 00 00 00 14 00 00 00 B0 1A 08 1A 3B 3A C9 01
HRZR_EHACVQY:::{2559N1S4-21Q7-11Q4-OQNS-00P04S60O9S0}	REG_BIN	01 00 00 00 07 00 00 00 D0 66 15 1C 3E 39 C9 01
HRZR_EHACVQY:%pfvqy2%\NVZ\NVZ 6.yax	REG_BIN	01 00 00 00 06 00 00 00 30 87 DB E4 B1 33 C9 01
HRZR_EHACVQY:%pfvqy2%\NVZ	REG_BIN	01 00 00 00 06 00 00 00 30 87 DB E4 B1 33 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\NVZ6\nvz6.rkr	REG_BIN	01 00 00 00 06 00 00 00 E0 80 FA E4 B1 33 C9 01
HRZR_HVFPHG	REG_BIN	01 00 00 00 07 00 00 00 70 54 9F FF 3D 39 C9 01
HRZR_EHACNGU:Zbmvyyn Sversbk.yax	REG_BIN	01 00 00 00 06 00 00 00 20 C0 6D 47 B2 33 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Zbmvyyn Sversbk\sversbk.rkr	REG_BIN	01 00 00 00 07 00 00 00 D0 66 15 1C 3E 39 C9 01
HRZR_EHACVQY:%pfvqy2%\Vagrearg Rkcybere.yax	REG_BIN	01 00 00 00 08 00 00 00 B0 1A 08 1A 3B 3A C9 01
HRZR_EHACVQY:%pfvqy2%\Cvqtva.yax	REG_BIN	01 00 00 00 06 00 00 00 20 B9 B5 0F B3 33 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Cvqtva\cvqtva.rkr	REG_BIN	01 00 00 00 06 00 00 00 E0 86 CD 0F B3 33 C9 01
HRZR_EHACNGU:Zbmvyyn Guhaqreoveq.yax	REG_BIN	01 00 00 00 06 00 00 00 70 36 A4 FF 3D 39 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Zbmvyyn Guhaqreoveq\guhaqreoveq.rkr	REG_BIN	01 00 00 00 07 00 00 00 80 1A 77 68 3A 3A C9 01
HRZR_EHACVQY:%pfvqy2%\Zvpebfbsg Bssvpr\Zvpebfbsg Bssvpr Jbeq 2007.yax	REG_BIN	01 00 00 00 06 00 00 00 B0 DA 8D 65 E1 39 C9 01
HRZR_EHACVQY:%pfvqy2%\Zvpebfbsg Bssvpr	REG_BIN	01 00 00 00 07 00 00 00 80 8A 0A A0 E1 39 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Zvpebfbsg Bssvpr\Bssvpr12\JVAJBEQ.RKR	REG_BIN	01 00 00 00 06 00 00 00 30 71 26 66 E1 39 C9 01
HRZR_EHACNGU:{90120000-0030-0000-0000-0000000SS1PR}	REG_BIN	01 00 00 00 07 00 00 00 10 6B 35 A0 E1 39 C9 01
HRZR_EHACVQY:%pfvqy2%\Zvpebfbsg Bssvpr\Zvpebfbsg Bssvpr Rkpry 2007.yax	REG_BIN	01 00 00 00 06 00 00 00 90 40 08 A0 E1 39 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Zvpebfbsg Bssvpr\Bssvpr12\RKPRY.RKR	REG_BIN	01 00 00 00 06 00 00 00 20 21 33 A0 E1 39 C9 01
HRZR_EHACNGU:P:\CEBTEN~1\ZVPEBF~2\Bssvpr12\BHGYBBX.RKR	REG_BIN	01 00 00 00 06 00 00 00 30 18 61 4E 3A 3A C9 01
HRZR_EHACVQY:::{2559N1S5-21Q7-11Q4-OQNS-00P04S60O9S0}	REG_BIN	01 00 00 00 06 00 00 00 30 18 61 4E 3A 3A C9 01
HRZR_EHACVQY:%pfvqy2%\Zbmvyyn Guhaqreoveq\Zbmvyyn Guhaqreoveq.yax	REG_BIN	01 00 00 00 06 00 00 00 D0 91 5A 68 3A 3A C9 01
HRZR_EHACVQY:%pfvqy2%\Zbmvyyn Guhaqreoveq	REG_BIN	01 00 00 00 06 00 00 00 C0 4C 5F 68 3A 3A C9 01

*ROT-13 encoded UserAssist registry keys for the '**domex1**' user in Autopsy*



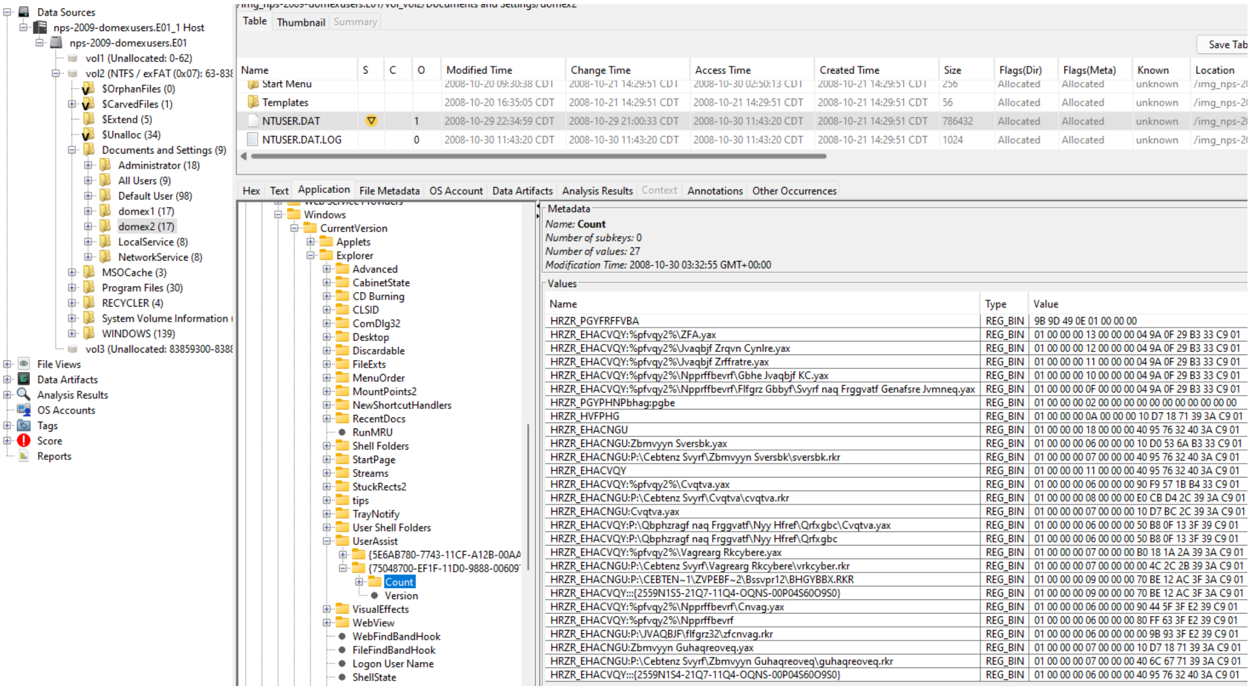
```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2008-10-21 19:12:24Z

{5E6AB780-7743-11CF-A12B-00AA004AE837}
2008-10-21 19:21:38Z
  UEME_UITOOLBAR (2)
  UEME_UITOOLBAR:0x1,104 (1)
  UEME_UITOOLBAR:0x4,104 (1)

Value names with no time stamps:
  HRZR_PGYPHNPbhag:pgbe

{75048700-EF1F-11D0-9888-006097DEACF9}
2008-10-30 02:56:27Z
  UEME_RUNPATH (17)
  UEME_RUNPATH:C:\Program Files\Internet Explorer\iexplore.exe (4)
  UEME_RUNPIDL (15)
  UEME_RUNPIDL:%csidl2%\Internet Explorer.lnk (3)
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)
2008-10-30 02:50:45Z
  UEME_RUNPATH:C:\PROGRA~1\MICROS~2\Office12\OUTLOOK.EXE (1)
  UEME_RUNPIDL:::{2559A1F5-21D7-11D4-BDAF-00C04F60B9F0} (1)
2008-10-29 16:15:57Z
  UEME_RUNPIDL:%csidl2%\Microsoft Office (2)
  UEME_RUNPATH:{90120000-0030-0000-0000-0000000FF1CE} (2)
  UEME_RUNPIDL:%csidl2%\Microsoft Office\Microsoft Office Excel 2007.lnk (1)
  UEME_RUNPATH:C:\Program Files\Microsoft Office\Office12\EXCEL.EXE (1)
2008-10-29 16:14:20Z
  UEME_RUNPATH:C:\Program Files\Microsoft Office\Office12\WINWORD.EXE (1)
2008-10-29 16:14:19Z
  UEME_RUNPIDL:%csidl2%\Microsoft Office\Microsoft Office Word 2007.lnk (1)
2008-10-28 20:45:27Z
  UEME_RUNPIDL:::{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0} (2)
  UEME_RUNPATH:C:\Program Files\Mozilla Firefox\firefox.exe (2)
2008-10-28 20:44:40Z
  UEME_UISCUT (2)
  UEME_RUNPATH:Mozilla Thunderbird.lnk (1)
2008-10-21 19:27:31Z
  UEME_RUNPIDL:%csidl2%\Pidgin.lnk (1)
  UEME_RUNPATH:C:\Program Files\Pidgin\pidgin.exe (1)
2008-10-21 19:21:55Z
  UEME_RUNPATH:Mozilla Firefox.lnk (1)
2008-10-21 19:19:10Z
  UEME_RUNPATH:C:\Program Files\AIM6\aim6.exe (1)
2008-10-21 19:19:09Z
  UEME_RUNPIDL:%csidl2%\AIM\AIM 6.lnk (1)
  UEME_RUNPIDL:%csidl2%\AIM (1)
2008-10-21 19:10:51Z
  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)
```

*Evidence of the '**domex1**' user running communication applications decoded with RegRipper tool*



/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex2

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Start Menu				2008-10-20 09:30:38 CDT	2008-10-21 14:29:51 CDT	2008-10-30 02:50:13 CDT	2008-10-21 14:29:51 CDT	256	Allocated	Allocated	unknown	/img_nps-2
Templates				2008-10-20 16:35:05 CDT	2008-10-21 14:29:51 CDT	2008-10-21 14:29:51 CDT	2008-10-21 14:29:51 CDT	56	Allocated	Allocated	unknown	/img_nps-2
NTUSER.DAT	▽		1	2008-10-29 22:34:59 CDT	2008-10-29 21:00:33 CDT	2008-10-30 11:43:20 CDT	2008-10-21 14:29:51 CDT	786432	Allocated	Allocated	unknown	/img_nps-2
NTUSER.DAT.LOG			0	2008-10-30 11:43:20 CDT	2008-10-30 11:43:20 CDT	2008-10-30 11:43:20 CDT	2008-10-21 14:29:51 CDT	1024	Allocated	Allocated	unknown	/img_nps-2

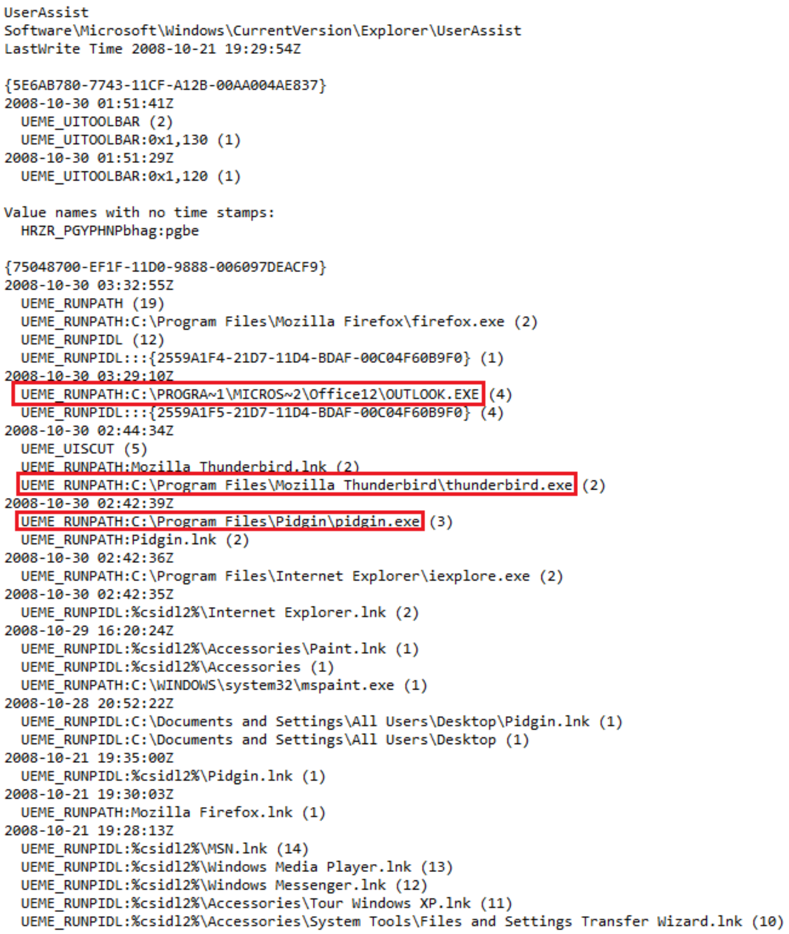
Metadata

Name: **Count**
Number of subkeys: 0
Number of values: 27
Modification Time: 2008-10-30 03:32:55 GMT+00:00

Values

Name	Type	Value
HRZR_PGYFRFFVBA	REG_BIN	9B 9D 49 0E 01 00 00 00
HRZR_EHACVQY:%pfvqy2%\ZFA.yax	REG_BIN	01 00 00 00 13 00 00 00 04 9A 0F 29 B3 33 C9 01
HRZR_EHACVQY:%pfvqy2%\Jvaqbjf Zrqvn Cynlre.yax	REG_BIN	01 00 00 00 12 00 00 00 04 9A 0F 29 B3 33 C9 01
HRZR_EHACVQY:%pfvqy2%\Jvaqbjf Zrffratre.yax	REG_BIN	01 00 00 00 11 00 00 00 04 9A 0F 29 B3 33 C9 01
HRZR_EHACVQY:%pfvqy2%\Nppreffbevrf\Gbhe Jvaqbjf KC.yax	REG_BIN	01 00 00 00 10 00 00 00 04 9A 0F 29 B3 33 C9 01
HRZR_EHACVQY:%pfvqy2%\Nppreffbevrf\Flfgrz Gbbyf\Svyrf naq Frggvatf Genafsre Jvmneq.yax	REG_BIN	01 00 00 00 0F 00 00 00 04 9A 0F 29 B3 33 C9 01
HRZR_PGYPHNPbhag:pgbe	REG_BIN	01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00
HRZR_HVFPHG	REG_BIN	01 00 00 00 0A 00 00 00 10 D7 18 71 39 3A C9 01
HRZR_EHACNGU	REG_BIN	01 00 00 00 18 00 00 00 40 95 76 32 40 3A C9 01
HRZR_EHACNGU:Zbmvyyn Sversbk.yax	REG_BIN	01 00 00 00 06 00 00 00 10 D0 53 6A B3 33 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Zbmvyyn Sversbk\sversbk.rkr	REG_BIN	01 00 00 00 07 00 00 00 40 95 76 32 40 3A C9 01
HRZR_EHACVQY	REG_BIN	01 00 00 00 11 00 00 00 40 95 76 32 40 3A C9 01
HRZR_EHACVQY:%pfvqy2%\Cvqtva.yax	REG_BIN	01 00 00 00 06 00 00 00 90 F9 57 1B B4 33 C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Cvqtva\cvqtva.rkr	REG_BIN	01 00 00 00 08 00 00 00 E0 CB D4 2C 39 3A C9 01
HRZR_EHACNGU:Cvqtva.yax	REG_BIN	01 00 00 00 07 00 00 00 10 D7 BC 2C 39 3A C9 01
HRZR_EHACVQY:P:\Qbphzragf naq Frggvatf\Nyy Hfref\Qrfxgbc\Cvqtva.yax	REG_BIN	01 00 00 00 06 00 00 00 50 B8 0F 13 3F 39 C9 01
HRZR_EHACVQY:P:\Qbphzragf naq Frggvatf\Nyy Hfref\Qrfxgbc	REG_BIN	01 00 00 00 06 00 00 00 50 B8 0F 13 3F 39 C9 01
HRZR_EHACVQY:%pfvqy2%\Vagrearg Rkcybere.yax	REG_BIN	01 00 00 00 07 00 00 00 B0 18 1A 2A 39 3A C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Vagrearg Rkcybere\vrkcyber.rkr	REG_BIN	01 00 00 00 07 00 00 00 00 4C 2C 2B 39 3A C9 01
HRZR_EHACNGU:P:\CEBTEN~1\ZVPEBF~2\Bssvpr12\BHGYBBX.RKR	REG_BIN	01 00 00 00 09 00 00 00 70 BE 12 AC 3F 3A C9 01
HRZR_EHACVQY:::{2559N1S5-21Q7-11Q4-OQNS-00P04S60O9S0}	REG_BIN	01 00 00 00 09 00 00 00 70 BE 12 AC 3F 3A C9 01
HRZR_EHACVQY:%pfvqy2%\Nppreffbevrf\Cnvag.yax	REG_BIN	01 00 00 00 06 00 00 00 90 44 5F 3F E2 39 C9 01
HRZR_EHACVQY:%pfvqy2%\Nppreffbevrf	REG_BIN	01 00 00 00 06 00 00 00 80 FF 63 3F E2 39 C9 01
HRZR_EHACNGU:P:\JVAQBJF\flfgrz32\zfcnvag.rkr	REG_BIN	01 00 00 00 06 00 00 00 00 9B 93 3F E2 39 C9 01
HRZR_EHACNGU:Zbmvyyn Guhaqreoveq.yax	REG_BIN	01 00 00 00 07 00 00 00 10 D7 18 71 39 3A C9 01
HRZR_EHACNGU:P:\Cebtenz Svyrf\Zbmvyyn Guhaqreoveq\guhaqreoveq.rkr	REG_BIN	01 00 00 00 07 00 00 00 40 6C 67 71 39 3A C9 01
HRZR_EHACVQY:::{2559N1S4-21Q7-11Q4-OQNS-00P04S60O9S0}	REG_BIN	01 00 00 00 06 00 00 00 40 95 76 32 40 3A C9 01

*ROT-13 encoded UserAssist registry keys for the ‘**domex2**’ user in Autopsy*



```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2008-10-21 19:29:54Z

{5E6AB780-7743-11CF-A12B-00AA004AE837}
2008-10-30 01:51:41Z
  UEME_UITOOLBAR (2)
  UEME_UITOOLBAR:0x1,130 (1)
2008-10-30 01:51:29Z
  UEME_UITOOLBAR:0x1,120 (1)

Value names with no time stamps:
  HRZR_PGYPHNPbhag:pgbe

{75048700-EF1F-11D0-9888-006097DEACF9}
2008-10-30 03:32:55Z
  UEME_RUNPATH (19)
  UEME_RUNPATH:C:\Program Files\Mozilla Firefox\firefox.exe (2)
  UEME_RUNPIDL (12)
  UEME_RUNPIDL:::{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0} (1)
2008-10-30 03:29:10Z
  UEME_RUNPATH:C:\PROGRA~1\MICROS~2\Office12\OUTLOOK.EXE (4)
  UEME_RUNPIDL:::{2559A1F5-21D7-11D4-BDAF-00C04F60B9F0} (4)
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
  UEME_RUNPATH:C:\Program Files\Pidgin\pidgin.exe (3)
  UEME_RUNPATH:Pidgin.lnk (2)
2008-10-30 02:42:36Z
  UEME_RUNPATH:C:\Program Files\Internet Explorer\iexplore.exe (2)
2008-10-30 02:42:35Z
  UEME_RUNPIDL:%csidl2%\Internet Explorer.lnk (2)
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)
2008-10-28 20:52:22Z
  UEME_RUNPIDL:C:\Documents and Settings\All Users\Desktop\Pidgin.lnk (1)
  UEME_RUNPIDL:C:\Documents and Settings\All Users\Desktop (1)
2008-10-21 19:35:00Z
  UEME_RUNPIDL:%csidl2%\Pidgin.lnk (1)
2008-10-21 19:30:03Z
  UEME_RUNPATH:Mozilla Firefox.lnk (1)
2008-10-21 19:28:13Z
  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)
```

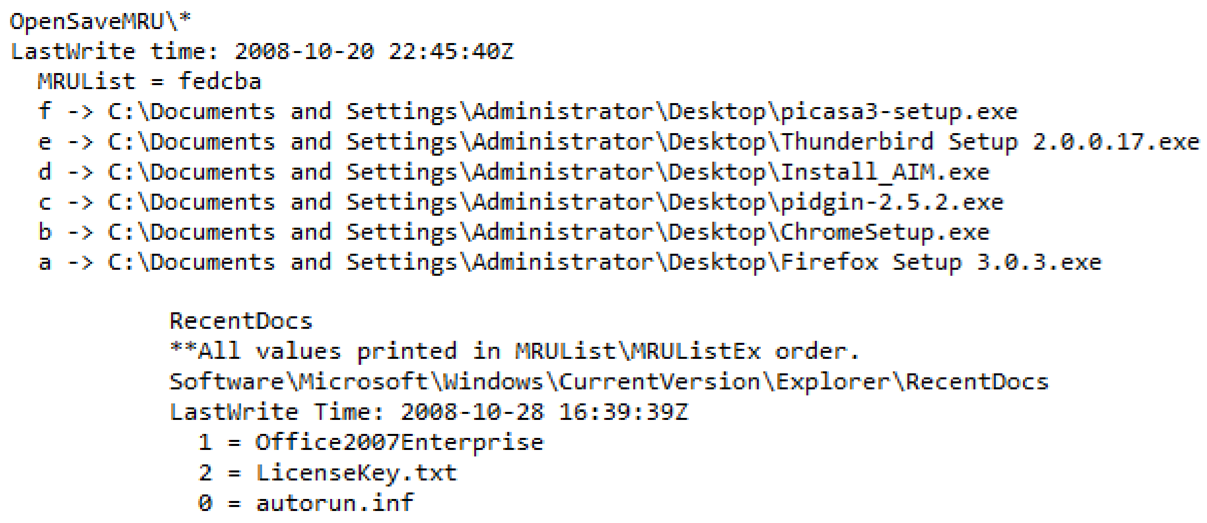
*Evidence of the ’**domex2**’ user running communication applications decoded with RegRipper tool*

Recently Accessed Files

Available NTUSER.DAT Hive files were analyzed further in order to identify files and documents recently accessed per user. Testers again leveraged the RegRipper tool to decode OpenSave and RecentDocs MRU registry list keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs / OpenSaveMRU) and locate files accessed.

User	File(s) / Document(s) Accessed
Administrator	Firefox Setup 3.0.3.exe
	ChromeSetup.exe
	pidgin-2.5.2.exe
	Install_AIM.exe
	Thunderbird Setup 2.0.0.17.exe
	picasa3-setup.exe
	LicenseKey.txt
	autorun.inf
domex1	This is a word document sent by domex user 1.docx
	This is a spreadsheet sent by domex user 1.xlsx
	web-mail-1-3-2.xpi
	This is a word document by domex user 1.docx
	This is a spreadsheet deleted by domex user 1.xlsx
	This is a spreadsheet by domex user 1.xlsx
	This is a word document deleted by domex user 1.docx
domex2	WLinstaller.exe
	domexuser2.JPG

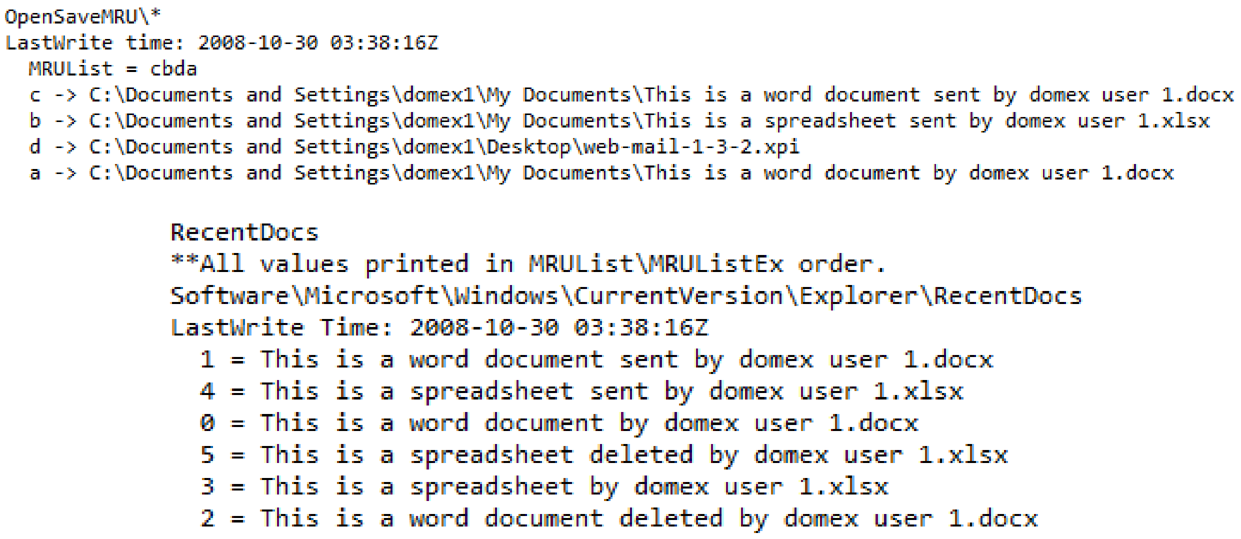
Evidence



```
OpenSaveMRU\*
LastWrite time: 2008-10-20 22:45:40Z
  MRUList = fedcba
  f -> C:\Documents and Settings\Administrator\Desktop\picasa3-setup.exe
  e -> C:\Documents and Settings\Administrator\Desktop\Thunderbird Setup 2.0.0.17.exe
  d -> C:\Documents and Settings\Administrator\Desktop\Install_AIM.exe
  c -> C:\Documents and Settings\Administrator\Desktop\pidgin-2.5.2.exe
  b -> C:\Documents and Settings\Administrator\Desktop\ChromeSetup.exe
  a -> C:\Documents and Settings\Administrator\Desktop\Firefox Setup 3.0.3.exe

            RecentDocs
            **All values printed in MRUList\MRUListEx order.
            Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
            LastWrite Time: 2008-10-28 16:39:39Z
              1 = Office2007Enterprise
              2 = LicenseKey.txt
              0 = autorun.inf
```

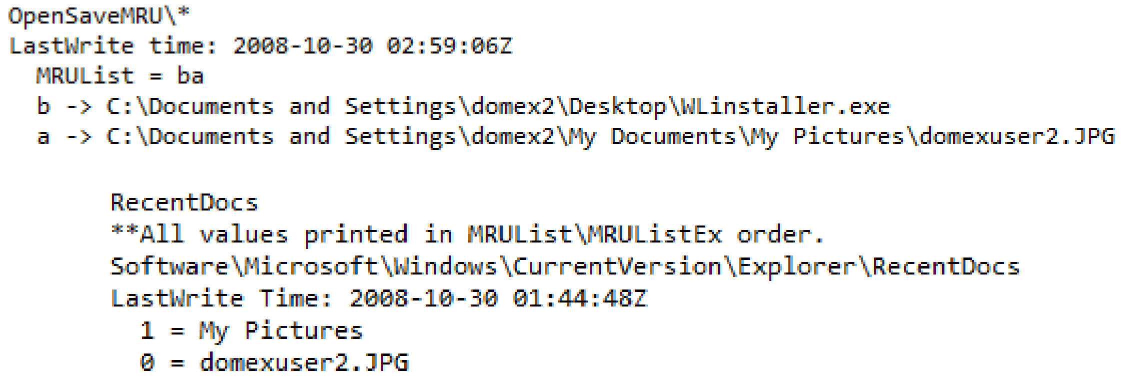
*RegRipper tool output of recently accessed files for the '**Administrator**' user*



```
OpenSaveMRU\*
LastWrite time: 2008-10-30 03:38:16Z
  MRUList = cbda
  c -> C:\Documents and Settings\domex1\My Documents\This is a word document sent by domex user 1.docx
  b -> C:\Documents and Settings\domex1\My Documents\This is a spreadsheet sent by domex user 1.xlsx
  d -> C:\Documents and Settings\domex1\Desktop\web-mail-1-3-2.xpi
  a -> C:\Documents and Settings\domex1\My Documents\This is a word document by domex user 1.docx

            RecentDocs
            **All values printed in MRUList\MRUListEx order.
            Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
            LastWrite Time: 2008-10-30 03:38:16Z
              1 = This is a word document sent by domex user 1.docx
              4 = This is a spreadsheet sent by domex user 1.xlsx
              0 = This is a word document by domex user 1.docx
              5 = This is a spreadsheet deleted by domex user 1.xlsx
              3 = This is a spreadsheet by domex user 1.xlsx
              2 = This is a word document deleted by domex user 1.docx
```

*RegRipper tool output of recently accessed files for the '**domex1**' user*



```
OpenSaveMRU\*
LastWrite time: 2008-10-30 02:59:06Z
  MRUList = ba
  b -> C:\Documents and Settings\domex2\Desktop\WLinstaller.exe
  a -> C:\Documents and Settings\domex2\My Documents\My Pictures\domexuser2.JPG

       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
```

*RegRipper tool output of recently accessed files for the '**domex2**' user*

Contents of Office Files Recently Accessed by User

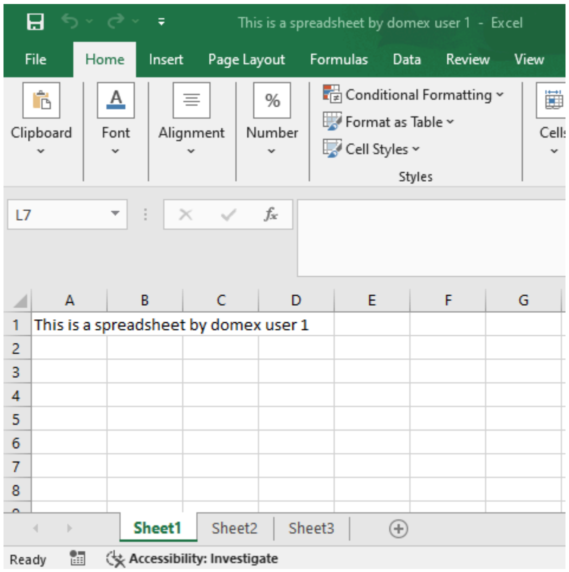
Testers proceeded with a targeted analysis of the **domex1** user's interactions with Microsoft Office files identified in the previous section based on suggestions from law enforcement to focus on Office files. The Autopsy navigator was used to browse the image filesystem path to each document found in evidence from the previous section and inspect contents.

All documents observed in the C:\My Documents folder were found to have plain text matching their filename (i.e. the 'This is a spreadsheet by domex user 1.docx' contains the text, "This is a spreadsheet by domex user 1").

The 'This is a word document deleted by domex user 1.docx' file value was identified in the C:\RECYCLER key, but with a different name than the original file observed in the MRU List - "Dc3.docx". The same file was identified in the CarvedFiles key, indicating there was an attempt to delete the file permanently.

The 'This is a spreadsheet deleted by domex user 1.xlsx' file value was identified in the C:\RECYCLER key, but with a different name than the original file observed in the MRU List - "Dc4.xlsx"

Evidence

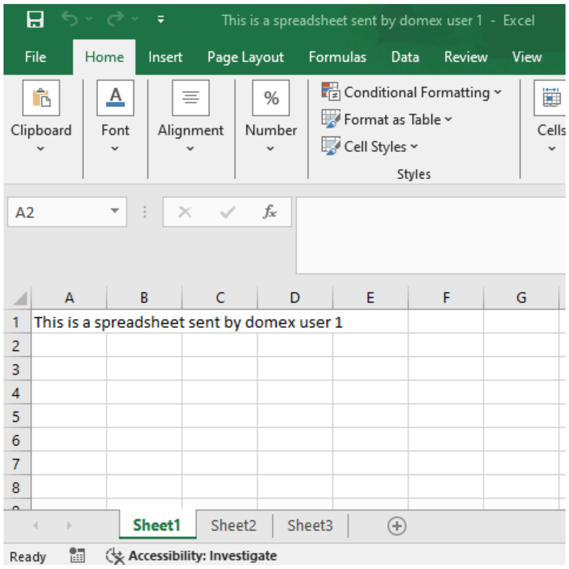


This is a spreadsheet by domex user 1 - Excel

L7

1 This is a spreadsheet by domex user 1

"This is a spreadsheet by domex user 1.xlsx"

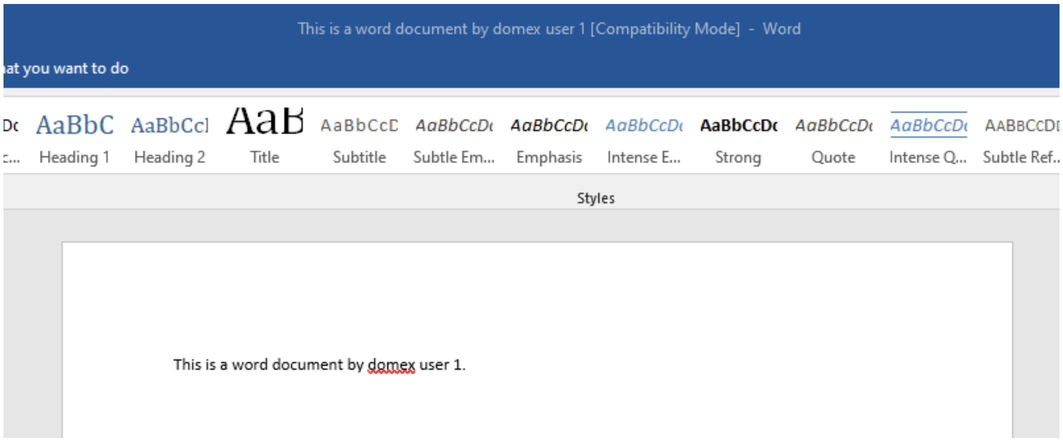


This is a spreadsheet sent by domex user 1 - Excel

A2

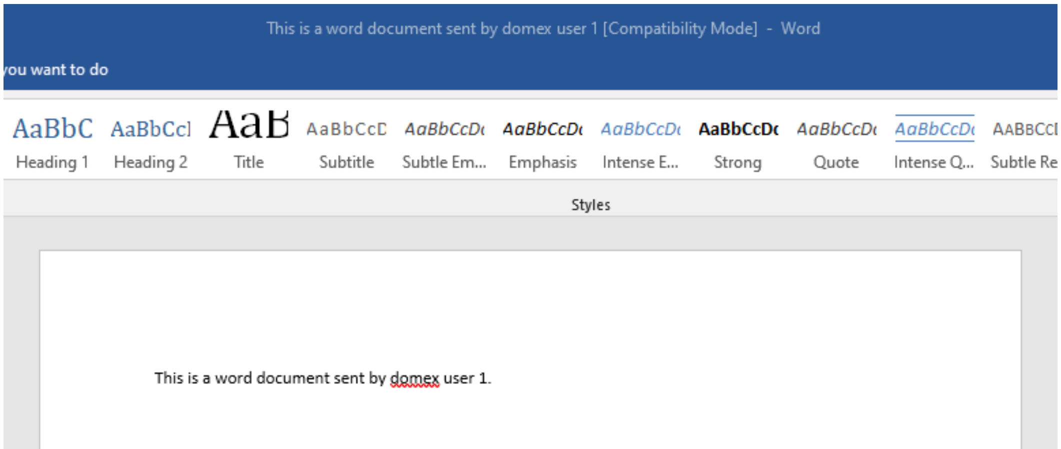
1 This is a spreadsheet sent by domex user 1

"This is a spreadsheet sent by domex user 1.xlsx"



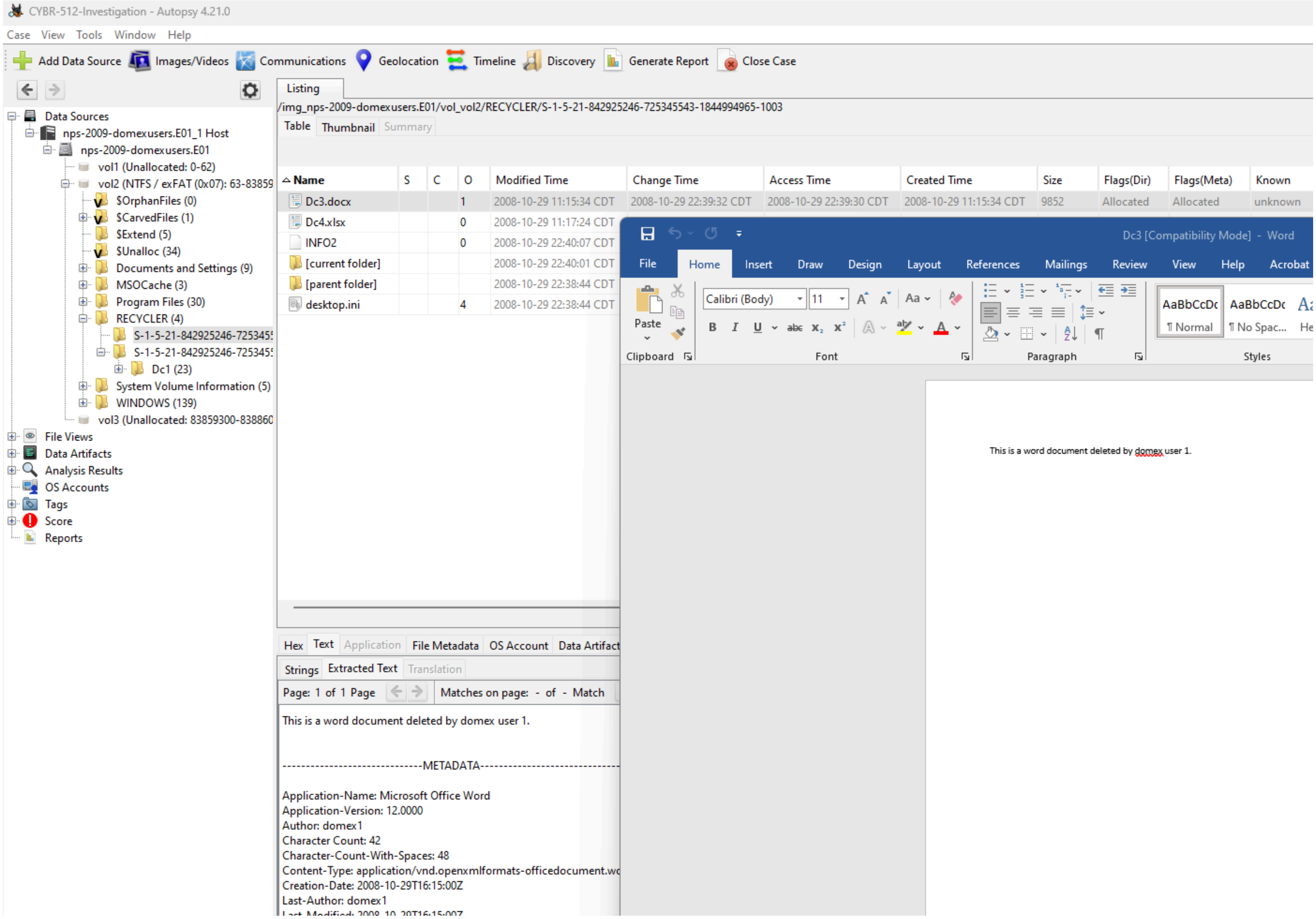
This is a word document by domex user 1.

“This is a word document by domex user 1.docx”



This is a word document sent by domex user 1.

“This is a word document sent by domex user 1.docx”


CYBR-512-Investigation - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Data Sources
nps-2009-domexusers.E01_1 Host
nps-2009-domexusers.E01
vol1 (Unallocated: 0-62)
vol2 (NTFS / exFAT (0x07): 63-83859
$OrphanFiles (0)
$CarvedFiles (1)
$Extend (5)
$Unalloc (34)
Documents and Settings (9)
MSOCache (3)
Program Files (30)
RECYCLER (4)
S-1-5-21-842925246-725345
S-1-5-21-842925246-725345
Dc1 (23)
System Volume Information (5)
WINDOWS (139)
vol3 (Unallocated: 83859300-838860
File Views
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
Table Thumbnail Summary
Hex Text Application File Metadata OS Account Data Artifact
Strings Extracted Text Translation
Page: 1 of 1 Page
Matches on page: - of - Match
Dc3 [Compatibility Mode] - Word
File Home Insert Draw Design Layout References Mailings Review View Help Acrobat
Paste
Clipboard
Calibri (Body) 11
Font
Paragraph
AaBbCcDc ¶ Normal
AaBbCcDc ¶ No Spac...
Styles

/img_nps-2009-domexusers.E01/vol_vol2/RECYCLER/S-1-5-21-842925246-725345543-1844994965-1003

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
Dc3.docx			1	2008-10-29 11:15:34 CDT	2008-10-29 22:39:32 CDT	2008-10-29 22:39:30 CDT	2008-10-29 11:15:34 CDT	9852	Allocated	Allocated	unknown
Dc4.xlsx			0	2008-10-29 11:17:24 CDT							
INFO2			0	2008-10-29 22:40:07 CDT							
[current folder]				2008-10-29 22:40:01 CDT							
[parent folder]				2008-10-29 22:38:44 CDT							
desktop.ini			4	2008-10-29 22:38:44 CDT							

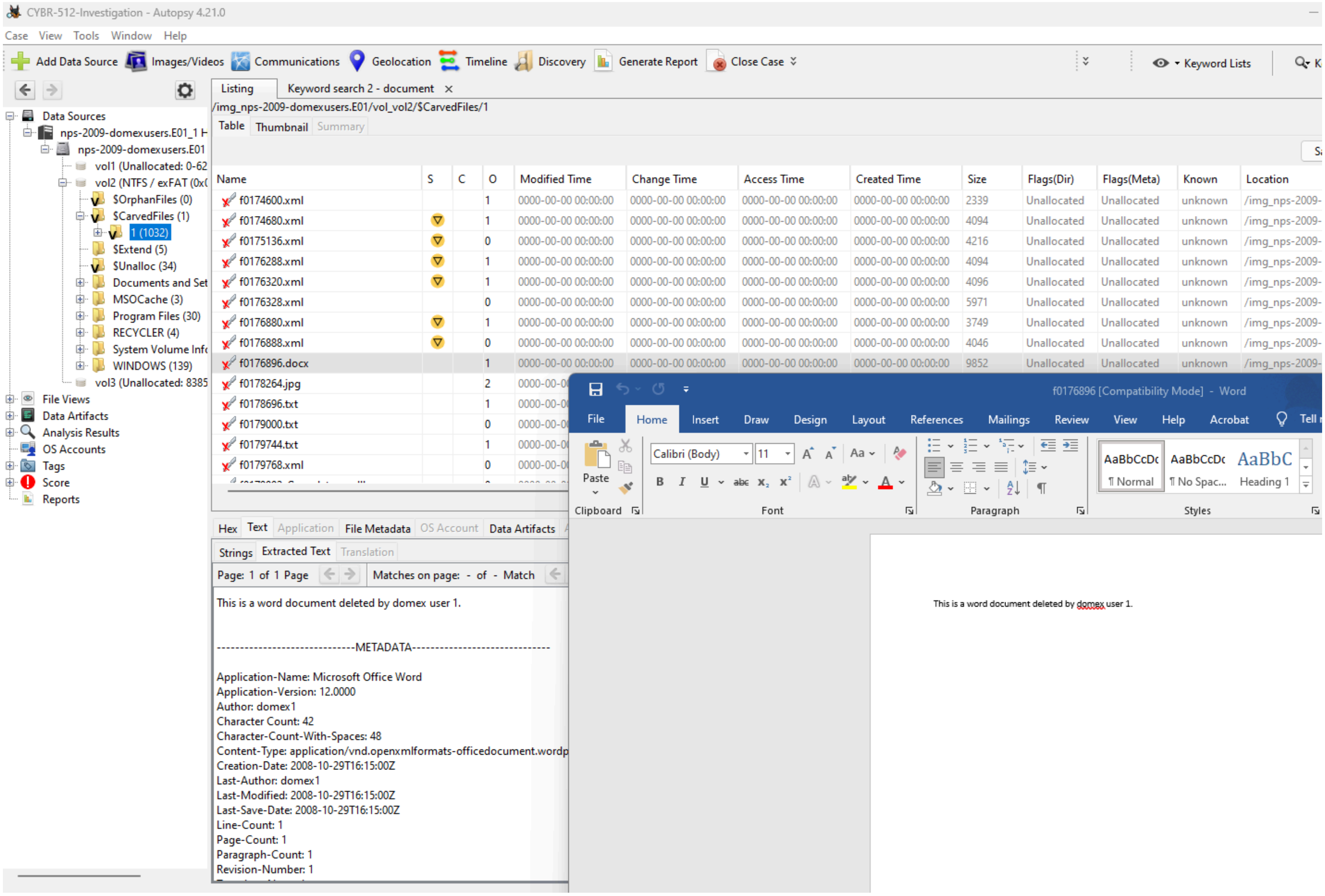
```
This is a word document deleted by domex user 1.

-----------------------------METADATA-----------------------------

Application-Name: Microsoft Office Word
Application-Version: 12.0000
Author: domex1
Character Count: 42
Character-Count-With-Spaces: 48
Content-Type: application/vnd.openxmlformats-officedocument.wo
Creation-Date: 2008-10-29T16:15:00Z
Last-Author: domex1
Last-Modified: 2008-10-29T16:15:00Z
```

This is a word document deleted by domex user 1.

“This is a word document deleted by domex user 1.docx” identified in C:\RECYCLER (Dc3.docx)



/img_nps-2009-domexusers.E01/vol_vol2/$CarvedFiles/1

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
f0174600.xml			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	2339	Unallocated	Unallocated	unknown	/img_nps-2009-
f0174680.xml	▽		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	4094	Unallocated	Unallocated	unknown	/img_nps-2009-
f0175136.xml	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4216	Unallocated	Unallocated	unknown	/img_nps-2009-
f0176288.xml	▽		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	4094	Unallocated	Unallocated	unknown	/img_nps-2009-
f0176320.xml	▽		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	4096	Unallocated	Unallocated	unknown	/img_nps-2009-
f0176328.xml			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	5971	Unallocated	Unallocated	unknown	/img_nps-2009-
f0176880.xml	▽		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	3749	Unallocated	Unallocated	unknown	/img_nps-2009-
f0176888.xml	▽		0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	4046	Unallocated	Unallocated	unknown	/img_nps-2009-
f0176896.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	9852	Unallocated	Unallocated	unknown	/img_nps-2009-
f0178264.jpg			2	0000-00-0								
f0178696.txt			1	0000-00-0								
f0179000.txt			0	0000-00-0								
f0179744.txt			1	0000-00-0								
f0179768.xml			0	0000-00-0								

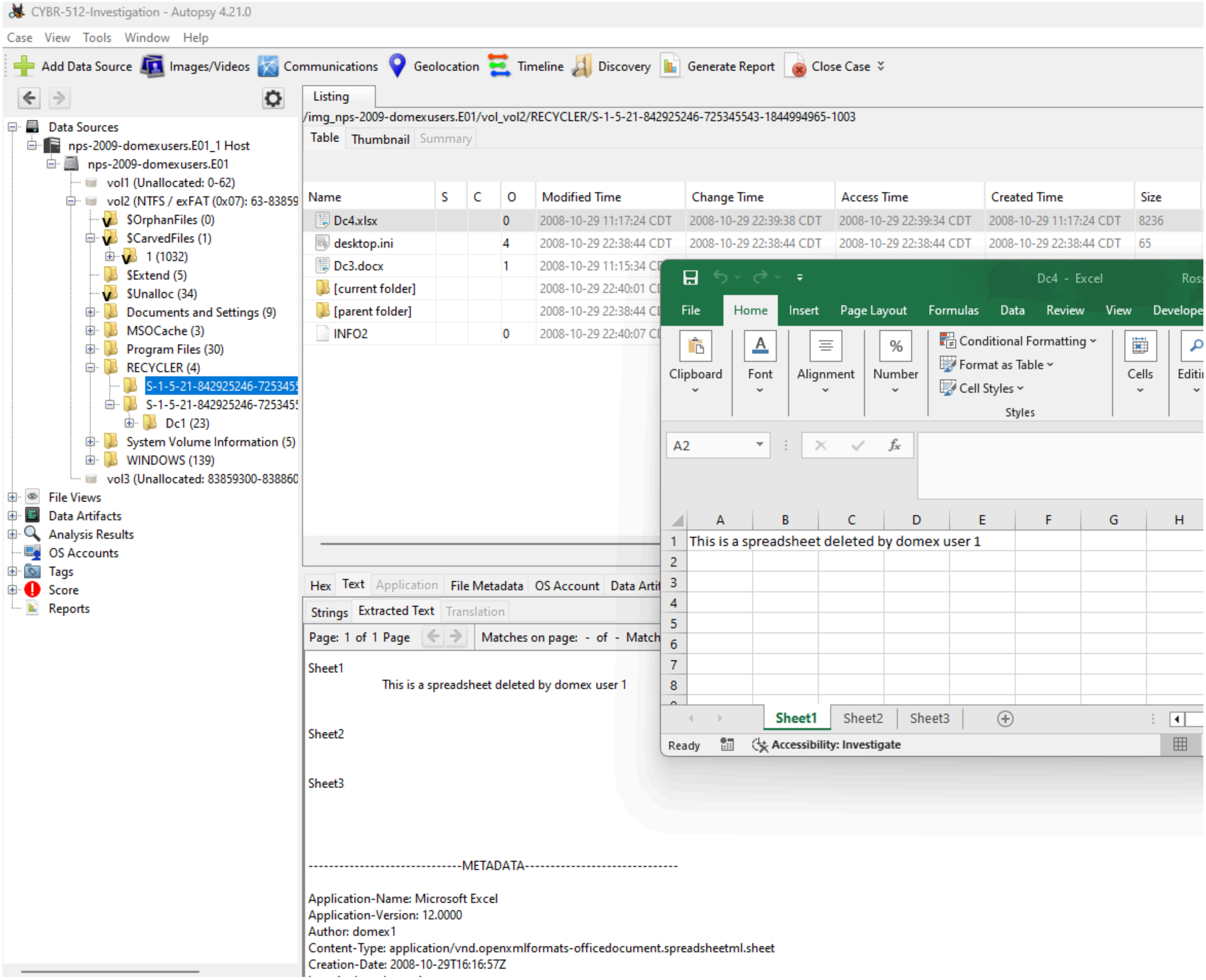
```
This is a word document deleted by domex user 1.


-----------------------------METADATA-----------------------------

Application-Name: Microsoft Office Word
Application-Version: 12.0000
Author: domex1
Character Count: 42
Character-Count-With-Spaces: 48
Content-Type: application/vnd.openxmlformats-officedocument.wordp
Creation-Date: 2008-10-29T16:15:00Z
Last-Author: domex1
Last-Modified: 2008-10-29T16:15:00Z
Last-Save-Date: 2008-10-29T16:15:00Z
Line-Count: 1
Page-Count: 1
Paragraph-Count: 1
Revision-Number: 1
```

This is a word document deleted by domex user 1.

"This is a word document deleted by domex user 1.docx" identified in CarvedFiles (f0176896.docx)



/img_nps-2009-domexusers.E01/vol_vol2/RECYCLER/S-1-5-21-842925246-725345543-1844994965-1003

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Dc4.xlsx			0	2008-10-29 11:17:24 CDT	2008-10-29 22:39:38 CDT	2008-10-29 22:39:34 CDT	2008-10-29 11:17:24 CDT	8236
desktop.ini			4	2008-10-29 22:38:44 CDT	2008-10-29 22:38:44 CDT	2008-10-29 22:38:44 CDT	2008-10-29 22:38:44 CDT	65
Dc3.docx			1	2008-10-29 11:15:34 C				
[current folder]				2008-10-29 22:40:01 C				
[parent folder]				2008-10-29 22:38:44 C				
INFO2			0	2008-10-29 22:40:07 C				

	A	B	C	D	E	F	G	H
1	This is a spreadsheet deleted by domex user 1							
2								
3								
4								
5								
6								
7								
8								

```
Sheet1
        This is a spreadsheet deleted by domex user 1


Sheet2


Sheet3



----------------------------METADATA----------------------------

Application-Name: Microsoft Excel
Application-Version: 12.0000
Author: domex1
Content-Type: application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Creation-Date: 2008-10-29T16:16:57Z
```

"This is a spreadsheet deleted by domex user 1.xlsx" identified in C:\RECYCLER (Dc4.xlsx)

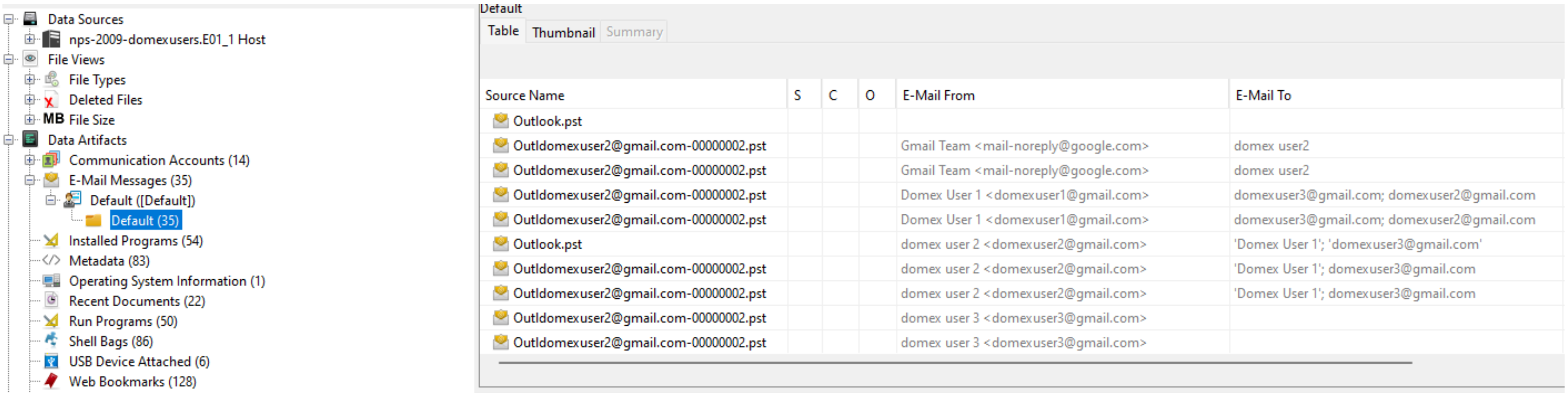
Emails Sent by Users, Recipient(s), and File Attachments

Testers investigated the email correspondence of users using Autopsy, focusing on those who used Outlook based on suggestions from law enforcement. Autopsy found 35 data artifacts involving Outlook emails, many of which were simply email header data. Artifacts that contained email plaintext were analyzed to piece together the email chain between “domex user 1”, “domex user 2”, and “domex user 3” using domains from gmail, hotmail, and live.

“Domex user 2” sent a photo attachment within one of the emails to the other two users. This photo attachment had the path:
/img_nps-2009-domexusers.E01/vol_vol2/”Documents and Settings”/domex2/”Local Settings”/”Application Data” /Microsoft/Outlook/Outlook.pst/domexuser2.JPG

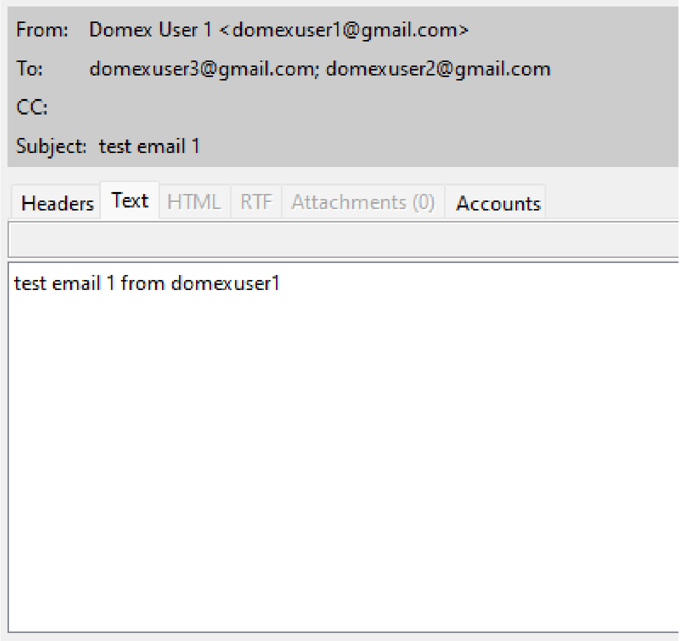
“Domex user 1” sent two file attachments within one of the emails to the other two users. These file attachments had the paths:
/img_nps-2009-domexusers.E01/vol_vol2/”Documents and Settings”/domex2/”Local Settings”/”Application Data”/Microsoft/Outlook/Outldomexuser2@gmail.com-00000002.pst/”This is a spreadsheet sent by domex user 1”.xlsx
/img_nps-2009-domexusers.E01/vol_vol2/”Documents and Settings”/domex2/”Local Settings”/”Application Data"/Microsoft/Outlook/Outldomexuser2@gmail.com-00000002.pst/”This is a word document sent by domex user 1”.docx

Evidence



Source Name	S	C	O	E-Mail From	E-Mail To
Outlook.pst					
Outldomexuser2@gmail.com-00000002.pst				Gmail Team <mail-noreply@google.com>	domex user2
Outldomexuser2@gmail.com-00000002.pst				Gmail Team <mail-noreply@google.com>	domex user2
Outldomexuser2@gmail.com-00000002.pst				Domex User 1 <domexuser1@gmail.com>	domexuser3@gmail.com; domexuser2@gmail.com
Outldomexuser2@gmail.com-00000002.pst				Domex User 1 <domexuser1@gmail.com>	domexuser3@gmail.com; domexuser2@gmail.com
Outlook.pst				domex user 2 <domexuser2@gmail.com>	'Domex User 1'; 'domexuser3@gmail.com'
Outldomexuser2@gmail.com-00000002.pst				domex user 2 <domexuser2@gmail.com>	'Domex User 1'; domexuser3@gmail.com
Outldomexuser2@gmail.com-00000002.pst				domex user 2 <domexuser2@gmail.com>	'Domex User 1'; domexuser3@gmail.com
Outldomexuser2@gmail.com-00000002.pst				domex user 3 <domexuser3@gmail.com>	
Outldomexuser2@gmail.com-00000002.pst				domex user 3 <domexuser3@gmail.com>	

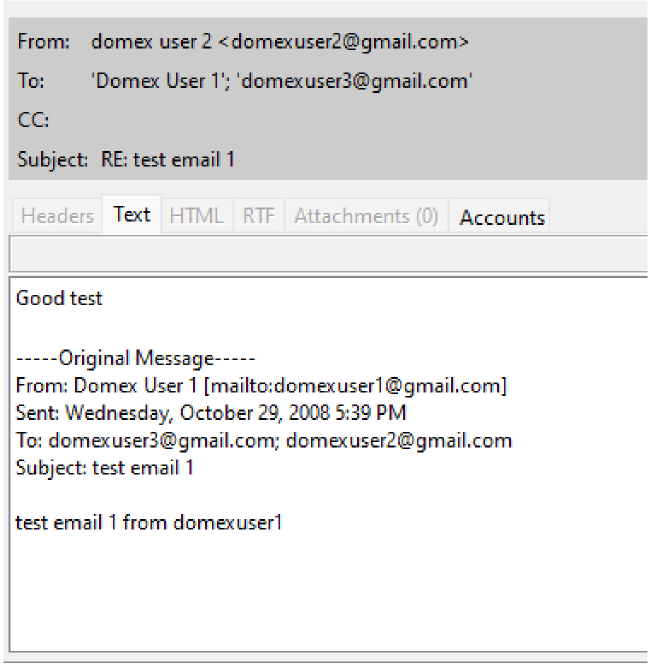
Outlook emails found in “Data Artifacts” > “E-Mail Messages” > “Default” > “Default”



From: Domex User 1 <domexuser1@gmail.com>
To: domexuser3@gmail.com; domexuser2@gmail.com
CC:
Subject: test email 1

test email 1 from domexuser1

1/11 - Email Message from domexuser1@gmail.com to domexuser3@gmail.com and domexuser2@gmail.com



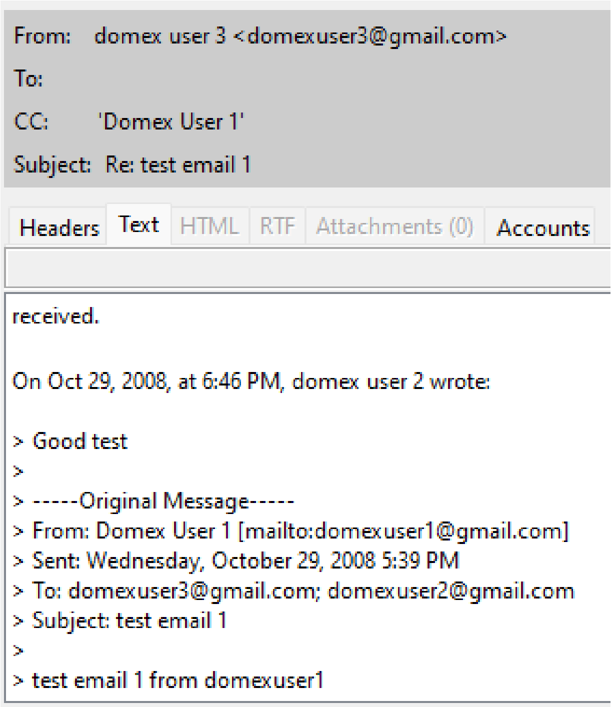
From: domex user 2 <domexuser2@gmail.com>
To: 'Domex User 1'; 'domexuser3@gmail.com'
CC:
Subject: RE: test email 1

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

2/11 - Email Message from domexuser2@gmail.com to domexuser3@gmail.com and domexuser1@gmail.com



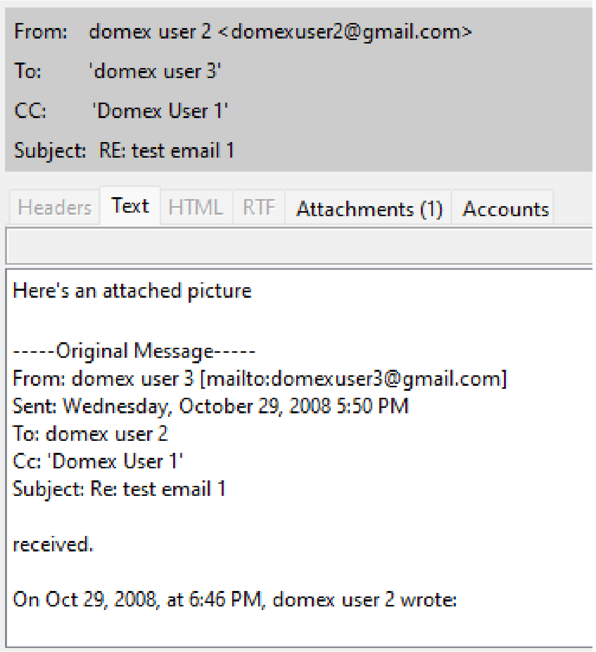
From: domex user 3 <domexuser3@gmail.com>
To:
CC: 'Domex User 1'
Subject: Re: test email 1

```
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
```

3/11 - Email Message from domexuser3@gmail.com that CCs domexuser1@gmail.com



From: domex user 2 <domexuser2@gmail.com>
To: 'domex user 3'
CC: 'Domex User 1'
Subject: RE: test email 1

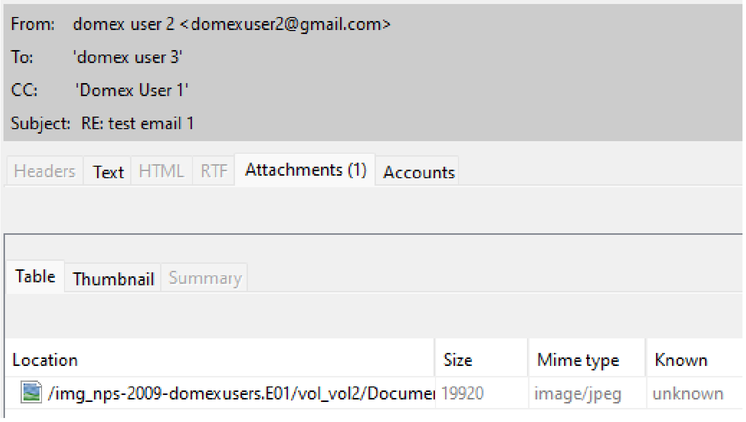
```
Here's an attached picture

-----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:
```

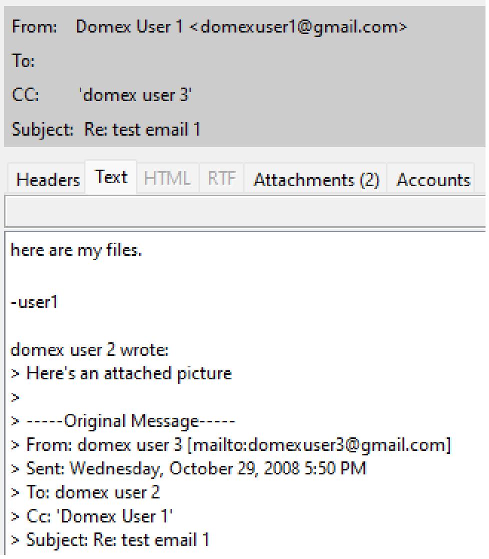
4/11 - Email Message from domexuser2@gmail.com to domexuser3@gmail.com and CCs domexuser1@gmail.com



From: domex user 2 <domexuser2@gmail.com>
To: 'domex user 3'
CC: 'Domex User 1'
Subject: RE: test email 1

Location	Size	Mime type	Known
/img_nps-2009-domexusers.E01/vol_vol2/Documei	19920	image/jpeg	unknown

5/11 - Photo Attachment in Image “4/11” from domexuser2@gmail.com to domexuser3@gmail.com and CCs domexuser1@gmail.com



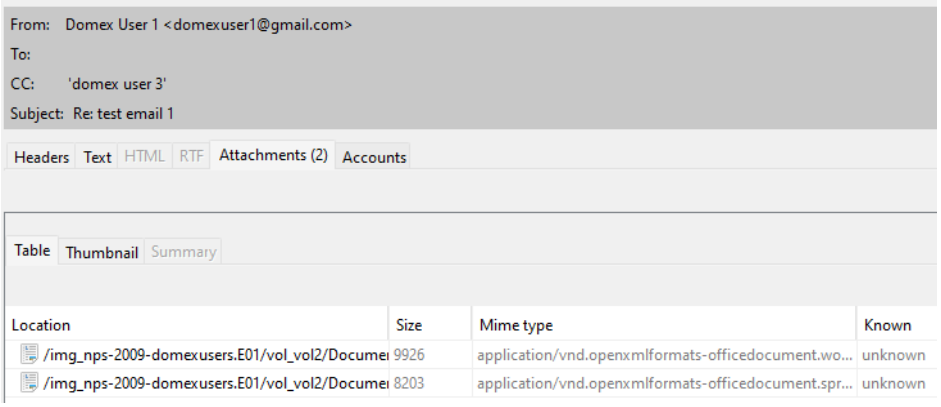
From: Domex User 1 <domexuser1@gmail.com>
To:
CC: 'domex user 3'
Subject: Re: test email 1

```
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
```

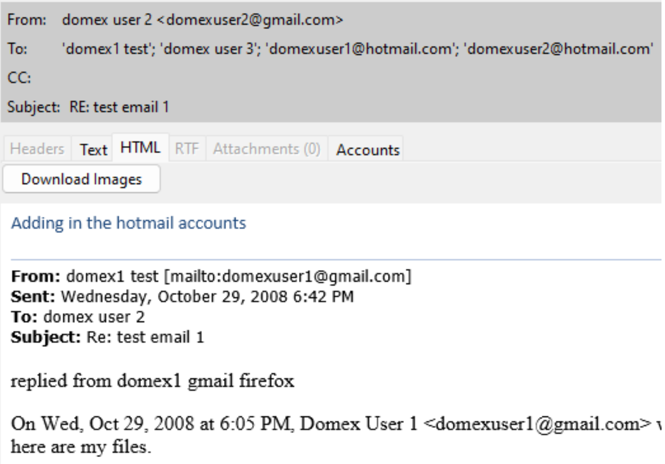
6/11 - Email Message from domexuser1@gmail.com that CCs domexuser3@gmail.com



From: Domex User 1 <domexuser1@gmail.com>
To:
CC: 'domex user 3'
Subject: Re: test email 1

Location	Size	Mime type	Known
/img_nps-2009-domexusers.E01/vol_vol2/Documei	9926	application/vnd.openxmlformats-officedocument.wo...	unknown
/img_nps-2009-domexusers.E01/vol_vol2/Documei	8203	application/vnd.openxmlformats-officedocument.spr...	unknown

7/11 - File Attachments in Image “6/11” from domexuser1@gmail.com that CCs domexuser3@gmail.com



From: domex user 2 <domexuser2@gmail.com>
To: 'domex1 test'; 'domex user 3'; 'domexuser1@hotmail.com'; 'domexuser2@hotmail.com'
CC:
Subject: RE: test email 1

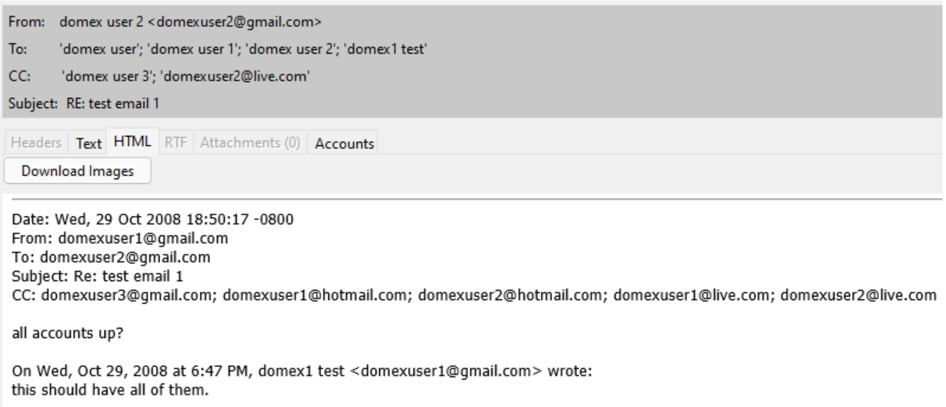
Adding in the hotmail accounts

From: domex1 test [mailto:domexuser1@gmail.com]
Sent: Wednesday, October 29, 2008 6:42 PM
To: domex user 2
Subject: Re: test email 1

replied from domex1 gmail firefox

On Wed, Oct 29, 2008 at 6:05 PM, Domex User 1 <domexuser1@gmail.com>
here are my files.

8/11 - Email Message from domexuser2@gmail.com to domexuser3@gmail.com, domexuser1@gmail.com, domexuser1@hotmail.com, domexuser2@hotmail.com



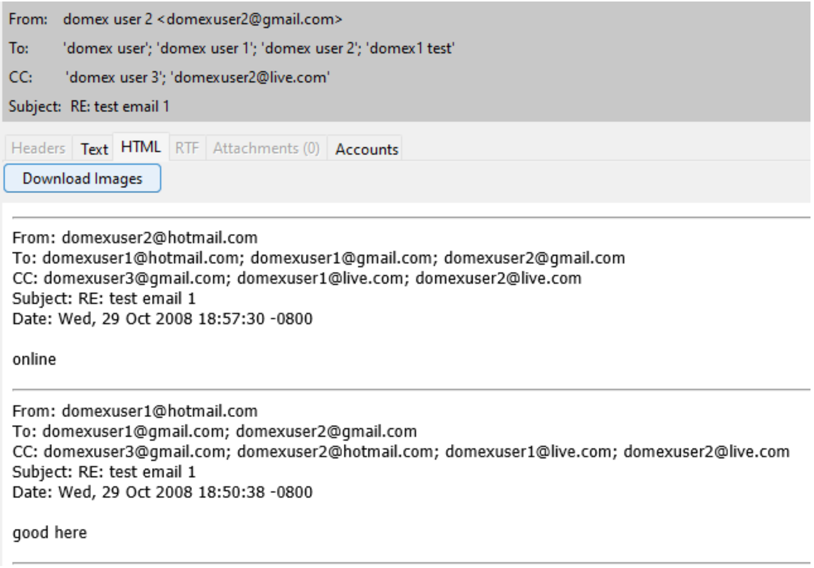
From: domex user 2 <domexuser2@gmail.com>
To: 'domex user'; 'domex user 1'; 'domex user 2'; 'domex1 test'
CC: 'domex user 3'; 'domexuser2@live.com'
Subject: RE: test email 1

Date: Wed, 29 Oct 2008 18:50:17 -0800
From: domexuser1@gmail.com
To: domexuser2@gmail.com
Subject: Re: test email 1
CC: domexuser3@gmail.com; domexuser1@hotmail.com; domexuser2@hotmail.com; domexuser1@live.com; domexuser2@live.com

all accounts up?

On Wed, Oct 29, 2008 at 6:47 PM, domex1 test <domexuser1@gmail.com> wrote:
this should have all of them.

9/11 - Start of Email Chain from domexuser1@gmail.com to domexuser2@gmail.com and that CCs domexuser3@gmail.com, domexuser1@hotmail.com, domexuser2@hotmail.com, domexuser1@live.com, and domexuser2@live.com



From: domex user 2 <domexuser2@gmail.com>
To: 'domex user'; 'domex user 1'; 'domex user 2'; 'domex1 test'
CC: 'domex user 3'; 'domexuser2@live.com'
Subject: RE: test email 1

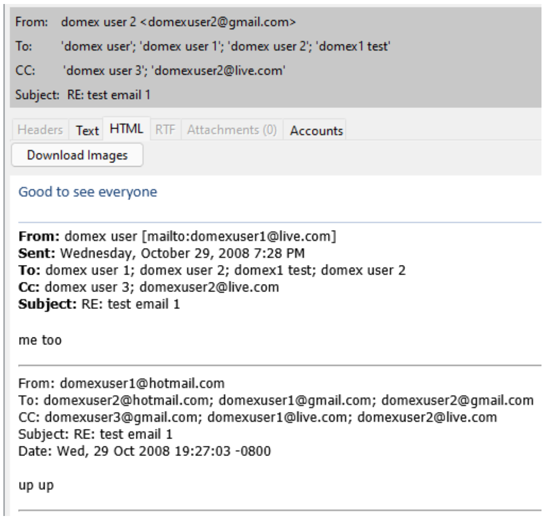
From: domexuser2@hotmail.com
To: domexuser1@hotmail.com; domexuser1@gmail.com; domexuser2@gmail.com
CC: domexuser3@gmail.com; domexuser1@live.com; domexuser2@live.com
Subject: RE: test email 1
Date: Wed, 29 Oct 2008 18:57:30 -0800

online

From: domexuser1@hotmail.com
To: domexuser1@gmail.com; domexuser2@gmail.com
CC: domexuser3@gmail.com; domexuser2@hotmail.com; domexuser1@live.com; domexuser2@live.com
Subject: RE: test email 1
Date: Wed, 29 Oct 2008 18:50:38 -0800

good here

10/11 - Continuation of Email Chain from domexuser1@hotmail.com to domexuser1@gmail.com and domexuser2@gmail.com and that CCs domexuser3@gmail.com, domexuser2@hotmail.com, domexuser1@live.com, and domexuser2@live.com;



From: domex user 2 <domexuser2@gmail.com>
To: 'domex user'; 'domex user 1'; 'domex user 2'; 'domex1 test'
CC: 'domex user 3'; 'domexuser2@live.com'
Subject: RE: test email 1

Good to see everyone

From: domex user [mailto:domexuser1@live.com]
Sent: Wednesday, October 29, 2008 7:28 PM
To: domex user 1; domex user 2; domex1 test; domex user 2
Cc: domex user 3; domexuser2@live.com
Subject: RE: test email 1

me too

From: domexuser1@hotmail.com
To: domexuser2@hotmail.com; domexuser1@gmail.com; domexuser2@gmail.com
CC: domexuser3@gmail.com; domexuser1@live.com; domexuser2@live.com
Subject: RE: test email 1
Date: Wed, 29 Oct 2008 19:27:03 -0800

up up

11/11 - End of Email Chain from domexuser2@gmail.com to domexuser1@gmail.com, domexuser1@live.com, domexuser1@hotmail.com, and domexuser2@hotmail.com and that CCs domexuser3@gmail.com and domexuser2@live.com

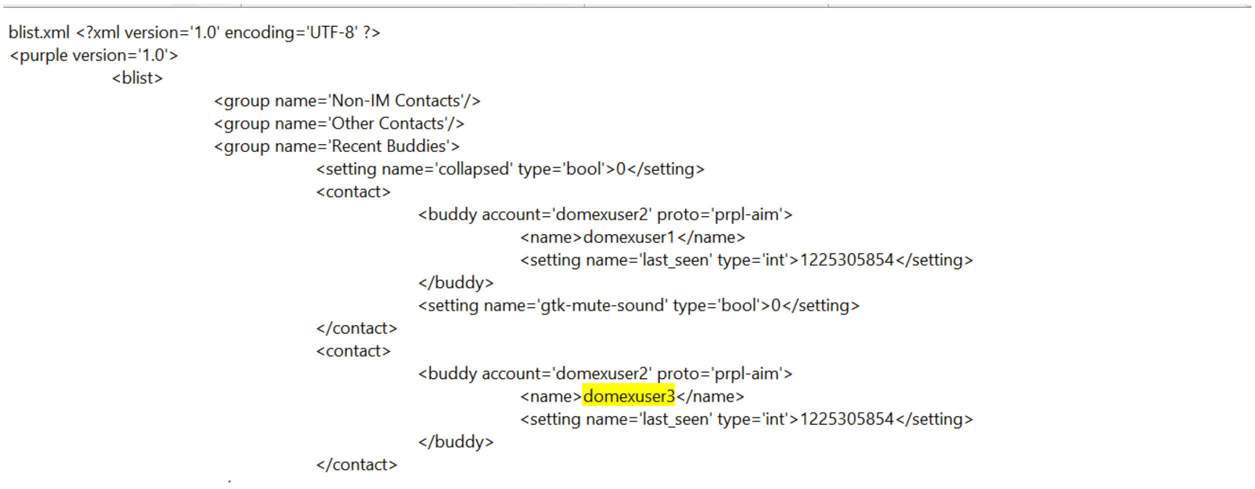
“Pidgin Messenger” Software and Transmission Analysis

Using the “Keyword Search” function in Autopsy, testers were able to parse through the “Data Artifacts” and locate metadata on .xml files sent through Pidgin Messenger. The text data on this specific “blist.xml” file provides a “Recent Buddies” address listing for domexuser2. In this group, both domexuser1 and domexuser3 exist.

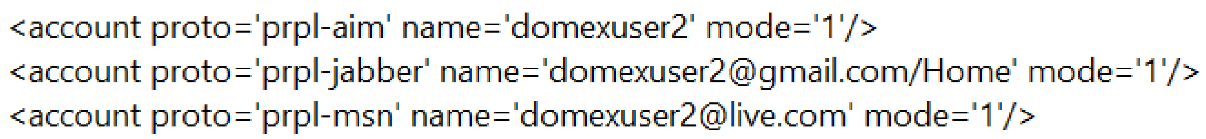
It is revealed within the data that domexuser2 is utilizing protocol “prpl-aim”. At the bottom of the file it can be seen that domexuser2’s account utilizes three different protocols to interact with Pidgin messenger:

1. “prpl-aim”
2. “prpl-jabber”
3. “prpl-msn”

Evidence



```
blist.xml <?xml version='1.0' encoding='UTF-8' ?>
<purple version='1.0'>
        <blist>
                <group name='Non-IM Contacts'/>
                <group name='Other Contacts'/>
                <group name='Recent Buddies'>
                        <setting name='collapsed' type='bool'>0</setting>
                        <contact>
                                <buddy account='domexuser2' proto='prpl-aim'>
                                        <name>domexuser1</name>
                                        <setting name='last_seen' type='int'>1225305854</setting>
                                </buddy>
                                <setting name='gtk-mute-sound' type='bool'>0</setting>
                        </contact>
                        <contact>
                                <buddy account='domexuser2' proto='prpl-aim'>
                                        <name>domexuser3</name>
                                        <setting name='last_seen' type='int'>1225305854</setting>
                                </buddy>
                        </contact>
```

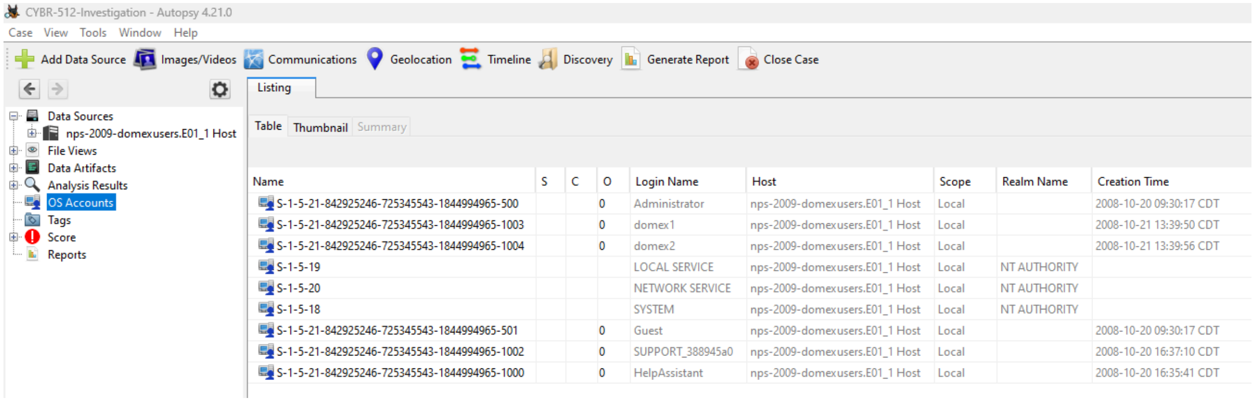


```
<account proto='prpl-aim' name='domexuser2' mode='1'/>
<account proto='prpl-jabber' name='domexuser2@gmail.com/Home' mode='1'/>
<account proto='prpl-msn' name='domexuser2@live.com' mode='1'/>
```

Files Transmitted to Remote Users

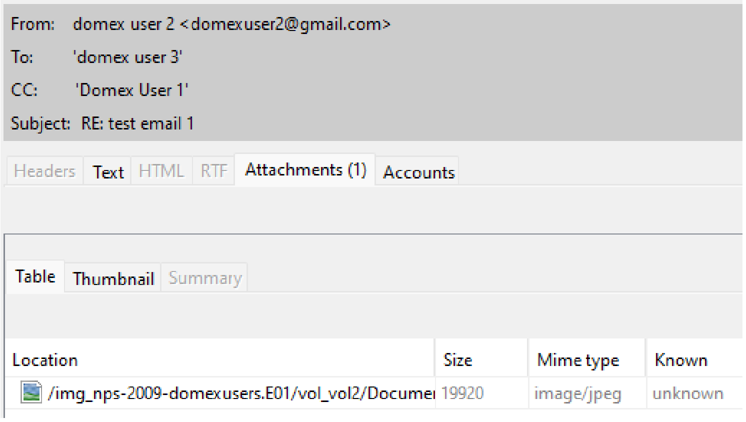
In light of all the evidence presented in the previous sections, the testers have found that there is strong evidence to suggest that users on the system were communicating and sending files to a remote user. When looking at the user account list in the first section of the analysis, it is clear that there are only two domex users on the local system: domex1 and domex2. Yet, when sifting through the email communications from domex1 and domex2, it can be seen that they are communicating with a third party known as domex3. In section 6 of the analysis, there are data artifacts of domex2 sending domex3 a photo attachment and domex1 sending domex3 two file attachments via email. In section 7 of the analysis, there is a data artifact of the user account domex2 having an account called domex3 on their buddy list that they communicate with. All of this evidence points to the conclusion that there are users on the system that are communicating and sending files to a remote user.

Evidence



Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-842925246-725345543-1844994965-500			0	Administrator	nps-2009-domexusers.E01_1 Host	Local		2008-10-20 09:30:17 CDT
S-1-5-21-842925246-725345543-1844994965-1003			0	domex1	nps-2009-domexusers.E01_1 Host	Local		2008-10-21 13:39:50 CDT
S-1-5-21-842925246-725345543-1844994965-1004			0	domex2	nps-2009-domexusers.E01_1 Host	Local		2008-10-21 13:39:56 CDT
S-1-5-19				LOCAL SERVICE	nps-2009-domexusers.E01_1 Host	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	nps-2009-domexusers.E01_1 Host	Local	NT AUTHORITY	
S-1-5-18				SYSTEM	nps-2009-domexusers.E01_1 Host	Local	NT AUTHORITY	
S-1-5-21-842925246-725345543-1844994965-501			0	Guest	nps-2009-domexusers.E01_1 Host	Local		2008-10-20 09:30:17 CDT
S-1-5-21-842925246-725345543-1844994965-1002			0	SUPPORT_388945a0	nps-2009-domexusers.E01_1 Host	Local		2008-10-20 16:37:10 CDT
S-1-5-21-842925246-725345543-1844994965-1000			0	HelpAssistant	nps-2009-domexusers.E01_1 Host	Local		2008-10-20 16:35:41 CDT

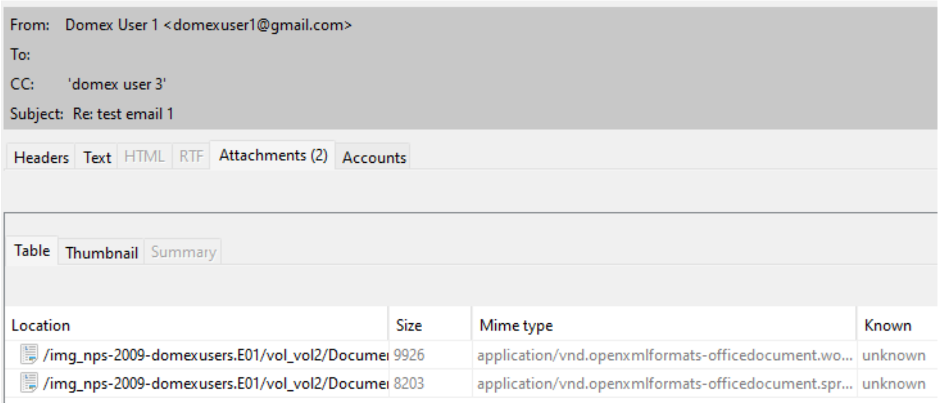
All of the user accounts on the local machine. Domex1 and Domex2 are present but not Domex3.



From: domex user 2 <domexuser2@gmail.com>
To: 'domex user 3'
CC: 'Domex User 1'
Subject: RE: test email 1

Location	Size	Mime type	Known
/img_nps-2009-domexusers.E01/vol_vol2/Documei	19920	image/jpeg	unknown

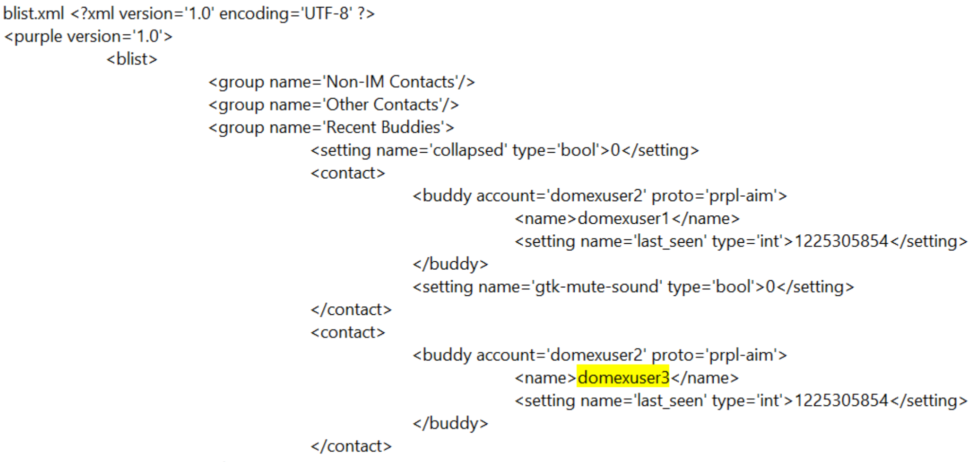
Evidence of Domex User 2 sending a photo attachment to Domex User 3.



From: Domex User 1 <domexuser1@gmail.com>
To:
CC: 'domex user 3'
Subject: Re: test email 1

Location	Size	Mime type	Known
/img_nps-2009-domexusers.E01/vol_vol2/Documei	9926	application/vnd.openxmlformats-officedocument.wo...	unknown
/img_nps-2009-domexusers.E01/vol_vol2/Documei	8203	application/vnd.openxmlformats-officedocument.spr...	unknown

Evidence of Domex User1 sending two file attachments to Domex User 3.



```
blist.xml <?xml version='1.0' encoding='UTF-8' ?>
<purple version='1.0'>
        <blist>
                <group name='Non-IM Contacts'/>
                <group name='Other Contacts'/>
                <group name='Recent Buddies'>
                        <setting name='collapsed' type='bool'>0</setting>
                        <contact>
                                <buddy account='domexuser2' proto='prpl-aim'>
                                        <name>domexuser1</name>
                                        <setting name='last_seen' type='int'>1225305854</setting>
                                </buddy>
                                <setting name='gtk-mute-sound' type='bool'>0</setting>
                        </contact>
                        <contact>
                                <buddy account='domexuser2' proto='prpl-aim'>
                                        <name>domexuser3</name>
                                        <setting name='last_seen' type='int'>1225305854</setting>
                                </buddy>
                        </contact>
```

Evidence of Domex User 2 having Domex User 3 as a buddy on Pidgin Messenger for communication.