PRECIOUS REPORT

10/12/2025
Report by
Anthony
Smithmyer

Executive Summary

The main user on this Windows XP computer is Frodo Baggins. This person enjoys Lord of the Rings. The baseline activity for this user is browsing the web, sending emails, and looking at images related to Lord of the Rings. The computer is set to Mountain Time, and there is evidence that suggests the user is getting interested in digital forensics. There are deleted files on the computer that were recovered, although they do not raise concern considering the fact that the main user was working on a disk image, which is a bit-by-bit copy of a hard drive or other storage device. Overall, this user is a big fan of the Lord of the Rings series that is also getting involved in digital forensics.

Methods

Tools used:

- Autopsy 4.22.1 (The latest version)
- Windows Registry Explorer
- Windows Event Viewer
- PicPick Screenshot Tool

The process:

I downloaded the disk image of Precious's computer and started a new case in Autopsy 4.22.1. I selected the disk image as a data source. I began to look through the files on the image to find the essential flags. The flags are listed below:

1) User Account Discovery: What is the name of the main Windows user account?
2) Operating System Version: What operating system is installed?
3) Time Zone: What time zone is the computer set to?
4) USB Device History: Find one USB storage device that was connected to the computer and provide the make/model/serial number.
5) Browser History: Identify one website the user visited that could indicate personal interests.
6) Email Attachments: Find at least one email attachment that the user sent.
7) Recent Documents: Find one document that the user recently opened.
8) Email Artifacts: Locate at least one email address used on the computer.
9) Pictures: Identify at least three images that could be meaningful.
10) Software: Identify at least three programs that are installed on the computer.
11) System Boot: When is the last recorded system shutdown date and time?
12) Deleted Files: Identify and recover a deleted file.
13) Did you discover any other interesting evidence on the computer?
14) Bonus Question: Find evidence that the computer printed a document. What

was the document? What do you know about it? (This is a bit tricky and will require outside research.)

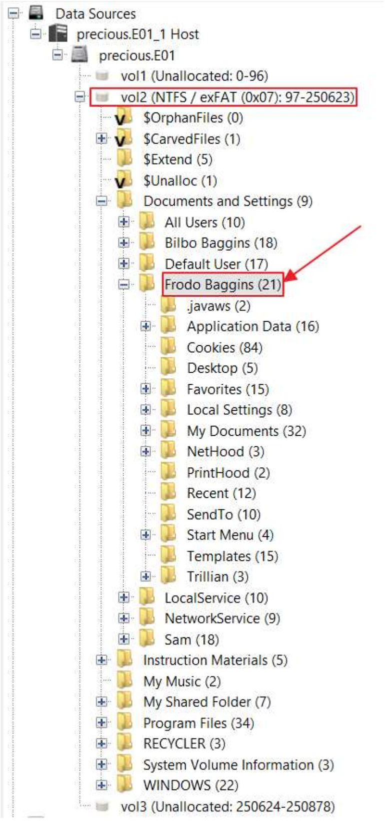
15) Bonus Question: Does this user seem to like music? What evidence supports your answer?

Verification:

I verified the flags and artifacts by using the built-in data artifacts section in Autopsy, finding the flags within the files on the disk image, and exploring the registry hives in Registry Explorer.

Findings

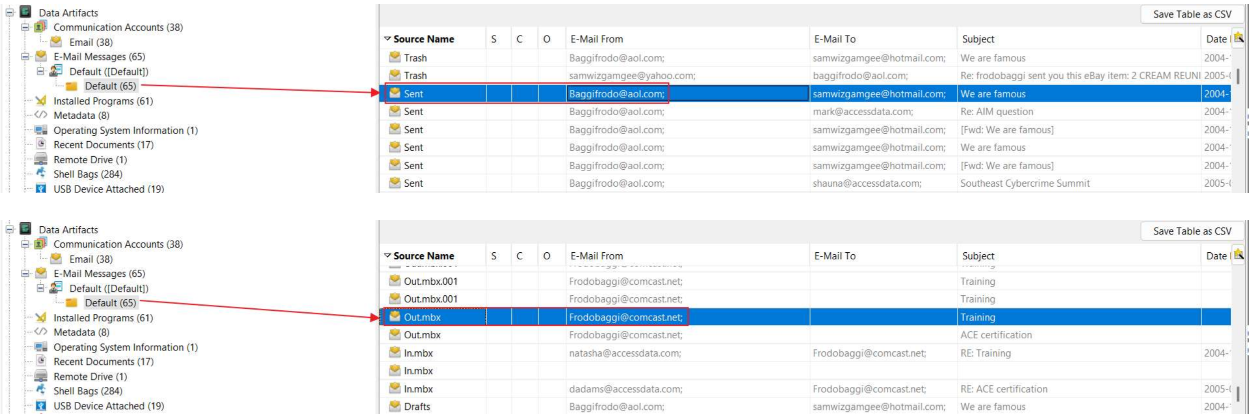
I found the first flag by determining the main user on the computer to be the user called "Frodo Baggins." I arrived at this conclusion by viewing the Documents and Settings folder within volume 2 of the disk image, which contains the main file system for the computer. There are several user folders within the Documents and Settings folder. The user folder for Frodo Baggins contains the most subfolders and data out of all the users on the computer, as shown in Figure 1.



```
Data Sources
  precious.E01_1 Host
    precious.E01
      vol1 (Unallocated: 0-96)
      vol2 (NTFS / exFAT (0x07): 97-250623)
        $OrphanFiles (0)
        $CarvedFiles (1)
        $Extend (5)
        $Unalloc (1)
        Documents and Settings (9)
          All Users (10)
          Bilbo Baggins (18)
          Default User (17)
          Frodo Baggins (21)
            .javaws (2)
            Application Data (16)
            Cookies (84)
            Desktop (5)
            Favorites (15)
            Local Settings (8)
            My Documents (32)
            NetHood (3)
            PrintHood (2)
            Recent (12)
            SendTo (10)
            Start Menu (4)
            Templates (15)
            Trillian (3)
          LocalService (10)
          NetworkService (9)
          Sam (18)
        Instruction Materials (5)
        My Music (2)
        My Shared Folder (7)
        Program Files (34)
        RECYCLER (3)
        System Volume Information (3)
        WINDOWS (22)
      vol3 (Unallocated: 250624-250878)
```

Figure 1: File system and user folders shown on Autopsy

Another piece of evidence that proves Frodo Baggins is the main user on the computer is the email addresses. Most of the emails sent on the computer are from Frodo's email addresses. Frodo's addresses are Baggifrodo@aol.com and Frodobaggi@comcast.net. This information was obtained in Autopsy. These email addresses are shown in Figure 2.

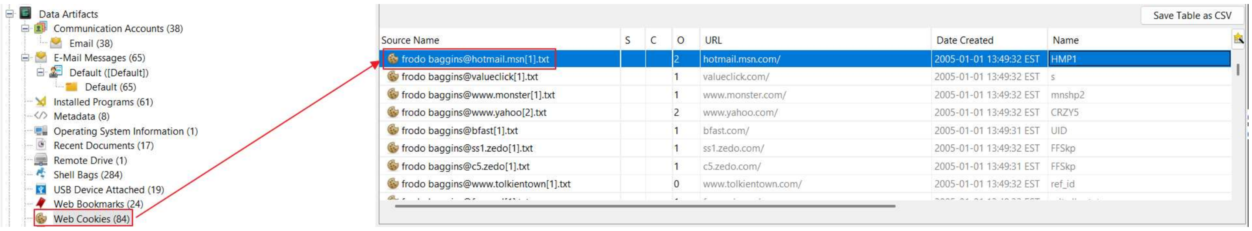


Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date
Trash				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	We are famous	2004-
Trash				samwizgamgee@yahoo.com;	baggifrodo@aol.com;	Re: frodobaggi sent you this eBay item: 2 CREAM REUNI	2005-
Sent				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	We are famous	2004-
Sent				Baggifrodo@aol.com;	mark@accessdata.com;	Re: AIM question	2004-
Sent				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	[Fwd: We are famous]	2004-
Sent				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	We are famous	2004-
Sent				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	[Fwd: We are famous]	2004-
Sent				Baggifrodo@aol.com;	shauna@accessdata.com;	Southeast Cybercrime Summit	2005-

Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date
Out.mbx.001				Frodobaggi@comcast.net;		Training	
Out.mbx.001				Frodobaggi@comcast.net;		Training	
Out.mbx				Frodobaggi@comcast.net;		Training	
Out.mbx				Frodobaggi@comcast.net;		ACE certification	
In.mbx				natasha@accessdata.com;	Frodobaggi@comcast.net;	RE: Training	2004-
In.mbx							
In.mbx				dadams@accessdata.com;	Frodobaggi@comcast.net;	RE: ACE certification	2005-
Drafts				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	We are famous	2004-

Figure 2: Frodo Baggins's email addresses

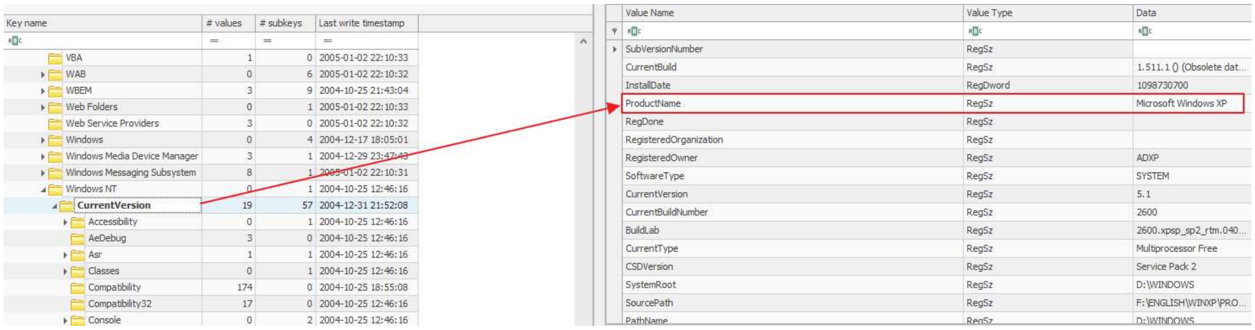
Other evidence that suggests Frodo Baggins is the main user is the web cookies. All of the cookies on the drive are for Frodo's accounts. This is shown below in Figure 3.



Source Name	S	C	O	URL	Date Created	Name
frodo baggins@hotmail.msn[1].txt			2	hotmail.msn.com/	2005-01-01 13:49:32 EST	HMP1
frodo baggins@valueclick[1].txt			1	valueclick.com/	2005-01-01 13:49:32 EST	s
frodo baggins@www.monster[1].txt			1	www.monster.com/	2005-01-01 13:49:32 EST	mnshp2
frodo baggins@www.yahoo[2].txt			2	www.yahoo.com/	2005-01-01 13:49:32 EST	CRZY5
frodo baggins@bfast[1].txt			1	bfast.com/	2005-01-01 13:49:31 EST	UID
frodo baggins@ss1.zedo[1].txt			1	ss1.zedo.com/	2005-01-01 13:49:32 EST	FFSkp
frodo baggins@c5.zedo[1].txt			1	c5.zedo.com/	2005-01-01 13:49:31 EST	FFSkp
frodo baggins@www.tolkientown[1].txt			0	www.tolkientown.com/	2005-01-01 13:49:32 EST	ref_id

Figure 3: Frodo Baggins web cookies

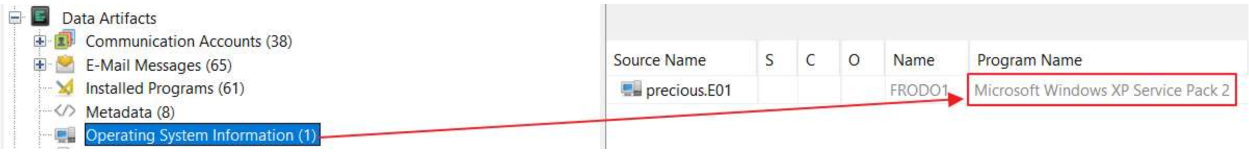
I discovered the second flag by looking at the Software hive in Registry Explorer. I obtained this registry hive from WINDOWS>system32>config on the disk image. In order to obtain the Operating System information, I went to SOFTWARE\Microsoft\Windows NT\CurrentVersion in Registry Explorer. From here, I determined the OS to be Microsoft Windows XP. I validated this information with the Operating System Information artifact in Autopsy. See Figures 4 and 5 for a visual representation. Note that the computer name in Figure 5 says "FRODO1"



Key name	# values	# subkeys	Last write timestamp
VBA	1	0	2005-01-02 22:10:33
WAB	0	6	2005-01-02 22:10:32
WBEM	3	9	2004-10-25 21:43:04
Web Folders	0	1	2005-01-02 22:10:33
Web Service Providers	3	0	2005-01-02 22:10:32
Windows	0	4	2004-12-17 18:05:01
Windows Media Device Manager	3	1	2004-12-29 23:47:43
Windows Messaging Subsystem	8	1	2005-01-02 22:10:31
Windows NT	0	1	2004-10-25 12:46:16
CurrentVersion	19	57	2004-12-31 21:52:08
Accessibility	0	1	2004-10-25 12:46:16
AeDebug	3	0	2004-10-25 12:46:16
Asr	1	1	2004-10-25 12:46:16
Classes	0	1	2004-10-25 12:46:16
Compatibility	174	0	2004-10-25 18:55:08
Compatibility32	17	0	2004-10-25 12:46:16
Console	0	2	2004-10-25 12:46:16

Value Name	Value Type	Data
SubVersionNumber	RegSz	
CurrentBuild	RegSz	1.511.1 () (Obsolete dat...
InstallDate	RegDword	1098730700
ProductName	RegSz	Microsoft Windows XP
RegDone	RegSz	
RegisteredOrganization	RegSz	
RegisteredOwner	RegSz	ADXP
SoftwareType	RegSz	SYSTEM
CurrentVersion	RegSz	5.1
CurrentBuildNumber	RegSz	2600
BuildLab	RegSz	2600.xpsp_sp2_rtm.040...
CurrentType	RegSz	Multiprocessor Free
CSDVersion	RegSz	Service Pack 2
SystemRoot	RegSz	D:\WINDOWS
SourcePath	RegSz	F:\ENGLISH\WINXP\PRO...
PathName	RegSz	D:\WINDOWS

Figure 4: OS Information shown in Registry Explorer

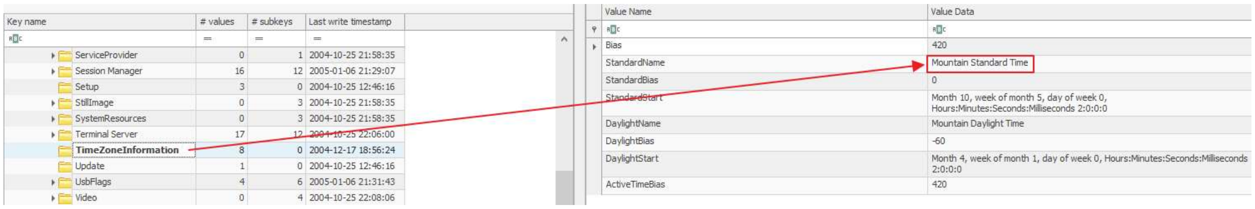


Data Artifacts
- Communication Accounts (38)
- E-Mail Messages (65)
- Installed Programs (61)
- Metadata (8)
- Operating System Information (1)

Source Name	S	C	O	Name	Program Name
precious.E01				FRODO1	Microsoft Windows XP Service Pack 2

Figure 5: OS Information shown in Autopsy

I discovered the third flag by looking through the System hive in Registry Explorer. By going to SYSTEM\CurrentControlSet\Control\TimeZoneInformation, I determined that the time zone the computer is set to is Mountain Standard Time. This is shown in Figure 6.

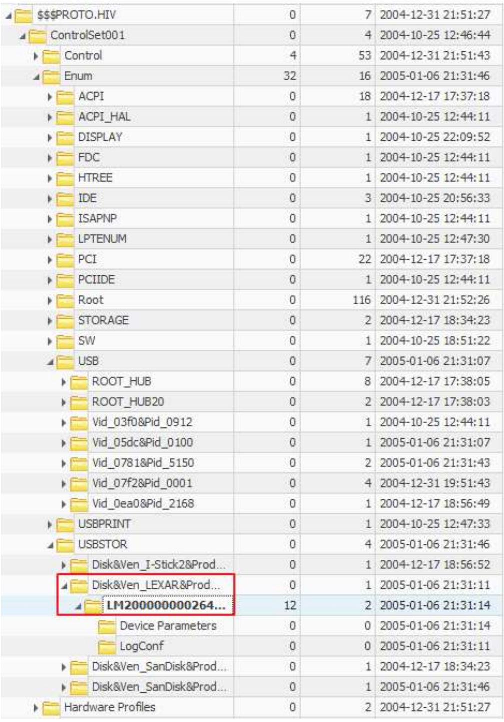


Key name	# values	# subkeys	Last write timestamp
ServiceProvider	0	1	2004-10-25 21:58:35
Session Manager	16	12	2005-01-06 21:29:07
Setup	3	0	2004-10-25 12:46:16
StillImage	0	3	2004-10-25 21:58:35
SystemResources	0	3	2004-10-25 21:58:35
Terminal Server	17	12	2004-10-25 22:06:00
TimeZoneInformation	8	0	2004-12-17 18:56:24
Update	1	0	2004-10-25 12:46:16
UsbFlags	4	6	2005-01-06 21:31:43
Video	0	4	2004-10-25 22:08:06

Value Name	Value Data
Bias	420
StandardName	Mountain Standard Time
StandardBias	0
StandardStart	Month 10, week of month 5, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
DaylightName	Mountain Daylight Time
DaylightBias	-60
DaylightStart	Month 4, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
ActiveTimeBias	420

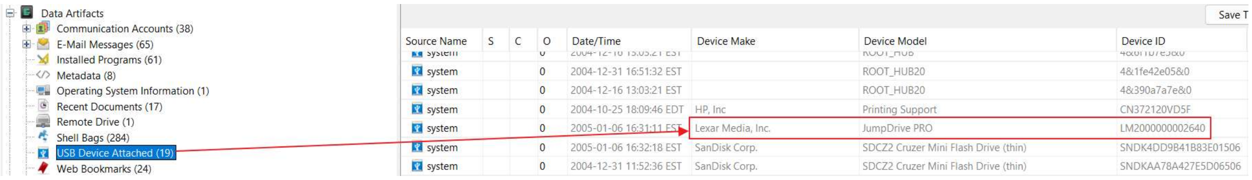
Figure 6: Time zone information shown in Registry Explorer

After finding the time zone information, I set out to find USB device history. By looking in the System hive and going to SYSTEM\CurrentControlSet\Enum\USBSTOR, I discovered a USB device that was previously attached to the computer. The device was a Lexar Media, Inc. JumpDrive PRO with the serial number LM2000000002640. This information was verified in Autopsy and is shown in Figures 7 and 8.



$$$PROTO.HIV	0	7	2004-12-31 21:51:27
ControlSet001	0	4	2004-10-25 12:46:44
Control	4	53	2004-12-31 21:51:43
Enum	32	16	2005-01-06 21:31:46
ACPI	0	18	2004-12-17 17:37:18
ACPI_HAL	0	1	2004-10-25 12:44:11
DISPLAY	0	1	2004-10-25 22:09:52
FDC	0	1	2004-10-25 12:44:11
HTREE	0	1	2004-10-25 12:44:11
IDE	0	3	2004-10-25 20:56:33
ISAPNP	0	1	2004-10-25 12:44:11
LPTENUM	0	1	2004-10-25 12:47:30
PCI	0	22	2004-12-17 17:37:18
PCIIDE	0	1	2004-10-25 12:44:11
Root	0	116	2004-12-31 21:52:26
STORAGE	0	2	2004-12-17 18:34:23
SW	0	1	2004-10-25 18:51:22
USB	0	7	2005-01-06 21:31:07
ROOT_HUB	0	8	2004-12-17 17:38:05
ROOT_HUB20	0	2	2004-12-17 17:38:03
Vid_03f0&Pid_0912	0	1	2004-10-25 12:44:11
Vid_05dc&Pid_0100	0	1	2005-01-06 21:31:07
Vid_0781&Pid_5150	0	2	2005-01-06 21:31:43
Vid_07f2&Pid_0001	0	4	2004-12-31 19:51:43
Vid_0ea0&Pid_2168	0	1	2004-12-17 18:56:49
USBPRINT	0	1	2004-10-25 12:47:33
USBSTOR	0	4	2005-01-06 21:31:46
Disk&Ven_I-Stick2&Prod...	0	1	2004-12-17 18:56:52
Disk&Ven_LEXAR&Prod...	0	1	2005-01-06 21:31:11
LM200000000264...	12	2	2005-01-06 21:31:14
Device Parameters	0	0	2005-01-06 21:31:14
LogConf	0	0	2005-01-06 21:31:11
Disk&Ven_SanDisk&Prod...	0	1	2004-12-17 18:34:23
Disk&Ven_SanDisk&Prod...	0	1	2005-01-06 21:31:46
Hardware Profiles	0	2	2004-12-31 21:51:27

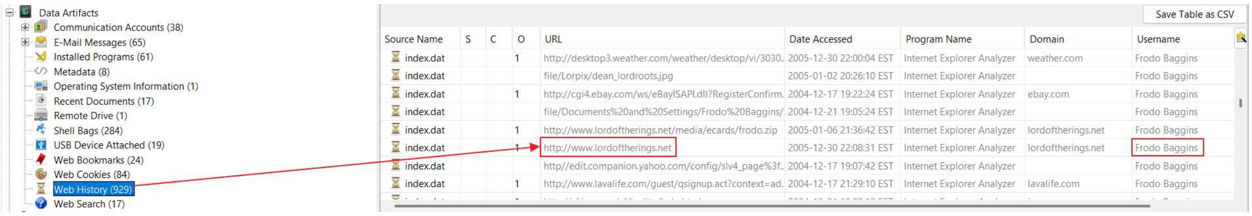
Figure 7: USB device shown in Registry Explorer



Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID
system			0	2004-12-31 16:51:32 EST		ROOT_HUB20	4&1fe42e05&0
system			0	2004-12-16 13:03:21 EST		ROOT_HUB20	4&390a7a7e&0
system			0	2004-10-25 18:09:46 EDT	HP, Inc	Printing Support	CN372120VD5F
system			0	2005-01-06 16:31:11 EST	Lexar Media, Inc.	JumpDrive PRO	LM2000000002640
system			0	2005-01-06 16:32:18 EST	SanDisk Corp.	SDCZ2 Cruzer Mini Flash Drive (thin)	SNDK4DD9B41B83E01506
system			0	2004-12-31 11:52:36 EST	SanDisk Corp.	SDCZ2 Cruzer Mini Flash Drive (thin)	SNDKAA78A427E5D06506

Figure 8: USB device shown in Autopsy

For the fifth flag, I looked in the Web History tab in Autopsy to find a website that shows the user's personal interests. Figure 9 shows Frodo Baggins visited http://lordoftherings.net. The user of this computer enjoys Lord of the Rings because not only is the main user called Frodo Baggins, which is a character in the movie series, but one of the websites visited by this user is a Lord of the Rings website.

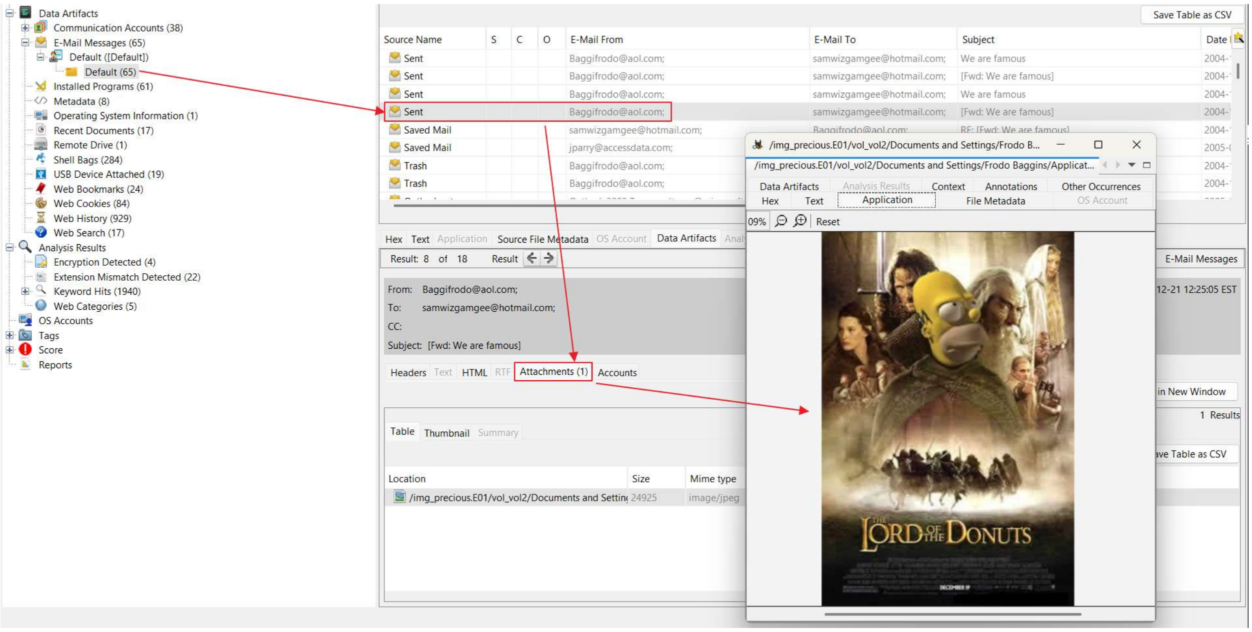


Source Name	S	C	O	URL	Date Accessed	Program Name	Domain	Username
index.dat			1	http://desktop3.weather.com/weather/desktop/vi/3030..	2005-12-30 22:00:04 EST	Internet Explorer Analyzer	weather.com	Frodo Baggins
index.dat				file/Lorpix/dean_lordroots.jpg	2005-01-02 20:26:10 EST	Internet Explorer Analyzer		Frodo Baggins
index.dat			1	http://cgi4.ebay.com/ws/eBayISAPI.dll?RegisterConfirm.	2004-12-17 19:22:24 EST	Internet Explorer Analyzer	ebay.com	Frodo Baggins
index.dat				file/Documents%20and%20Settings/Frodo%20Baggins/	2004-12-21 19:05:24 EST	Internet Explorer Analyzer		Frodo Baggins
index.dat			1	http://www.lordoftherings.net/media/ecards/frodo.zip	2005-01-06 21:36:42 EST	Internet Explorer Analyzer	lordoftherings.net	Frodo Baggins
index.dat			1	http://www.lordoftherings.net	2005-12-30 22:08:31 EST	Internet Explorer Analyzer	lordoftherings.net	Frodo Baggins
index.dat				http//edit.companion.yahoo.com/config/slv4_page%3f..	2004-12-17 19:07:42 EST	Internet Explorer Analyzer		Frodo Baggins
index.dat			1	http://www.lavalife.com/guest/qsignup.act?context=ad.	2004-12-17 21:29:10 EST	Internet Explorer Analyzer	lavalife.com	Frodo Baggins

Figure 9: http://lordoftherings.net, a website visited by Frodo Baggins

I discovered the sixth flag by looking through the emails sent on the computer. I sorted the list to show emails with attachments first. I then clicked on the email, went to the Attachments tab, and opened the attachment within Autopsy. This is shown in Figure

10. The image sent in this email also shows the user’s personal interests in Lord of the Rings.



Source Name	S	C	O	E-Mail From	E-Mail To	Subject	Date
Sent				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	We are famous	2004-
Sent				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	[Fwd: We are famous]	2004-
Sent				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	We are famous	2004-
Sent				Baggifrodo@aol.com;	samwizgamgee@hotmail.com;	[Fwd: We are famous]	2004-
Saved Mail				samwizgamgee@hotmail.com;	Baggifrodo@aol.com;	RE: [Fwd: We are famous]	2004-
Saved Mail				jparry@accessdata.com;			2005-
Trash				Baggifrodo@aol.com;			2004-
Trash				Baggifrodo@aol.com;			2004-

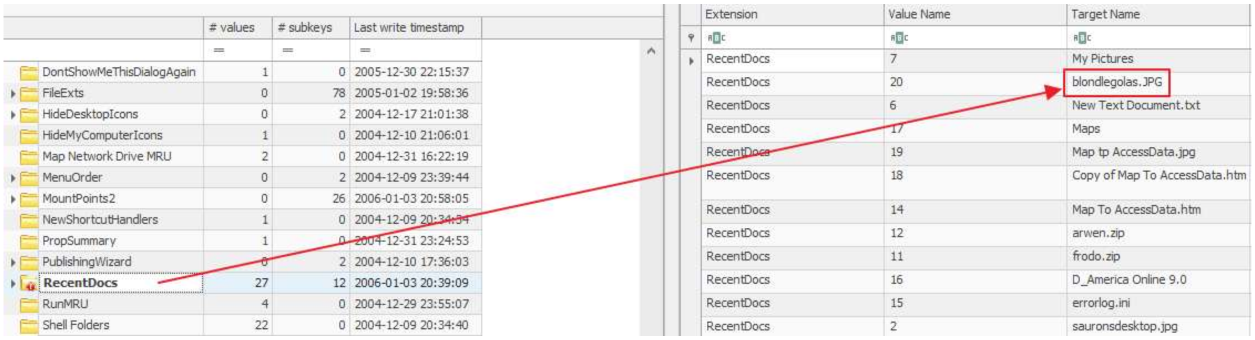
From: Baggifrodo@aol.com;
To: samwizgamgee@hotmail.com;
CC:
Subject: [Fwd: We are famous]

12-21 12:25:05 EST

Location	Size	Mime type
/img_precious.E01/vol_vol2/Documents and Settin	24925	image/jpeg

Figure 10: Email sent by Frodo with a jpeg attached

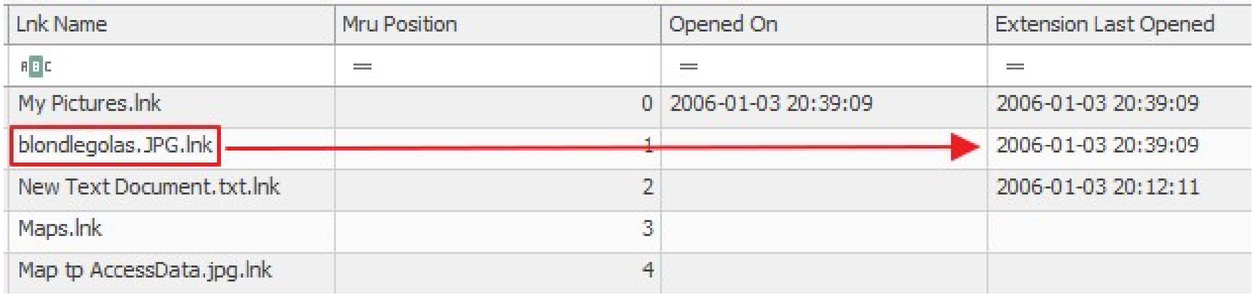
For the seventh flag, I discovered a recently opened document while looking at NTUSER.DAT in Registry Explorer. I obtained this file from Frodo Baggin’s user folder. By going to NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs, I found one of the recently opened documents. This recently accessed file is blondlegolas.JPG. See Figure 11 for more information. Figure 12 shows the date the file was opened.



	# values	# subkeys	Last write timestamp
DontShowMeThisDialogAgain	1	0	2005-12-30 22:15:37
FileExts	0	78	2005-01-02 19:58:36
HideDesktopIcons	0	2	2004-12-17 21:01:38
HideMyComputerIcons	1	0	2004-12-10 21:06:01
Map Network Drive MRU	2	0	2004-12-31 16:22:19
MenuOrder	0	2	2004-12-09 23:39:44
MountPoints2	0	26	2006-01-03 20:58:05
NewShortcutHandlers	1	0	2004-12-09 20:34:54
PropSummary	1	0	2004-12-31 23:24:53
PublishingWizard	0	2	2004-12-10 17:36:03
RecentDocs	27	12	2006-01-03 20:39:09
RunMRU	4	0	2004-12-29 23:55:07
Shell Folders	22	0	2004-12-09 20:34:40

Extension	Value Name	Target Name
RecentDocs	7	My Pictures
RecentDocs	20	blondlegolas.JPG
RecentDocs	6	New Text Document.txt
RecentDocs	17	Maps
RecentDocs	19	Map tp AccessData.jpg
RecentDocs	18	Copy of Map To AccessData.htm
RecentDocs	14	Map To AccessData.htm
RecentDocs	12	arwen.zip
RecentDocs	11	frodo.zip
RecentDocs	16	D_America Online 9.0
RecentDocs	15	errorlog.ini
RecentDocs	2	sauronsdesktop.jpg

Figure 11: Recently accessed file viewed in Registry Explorer

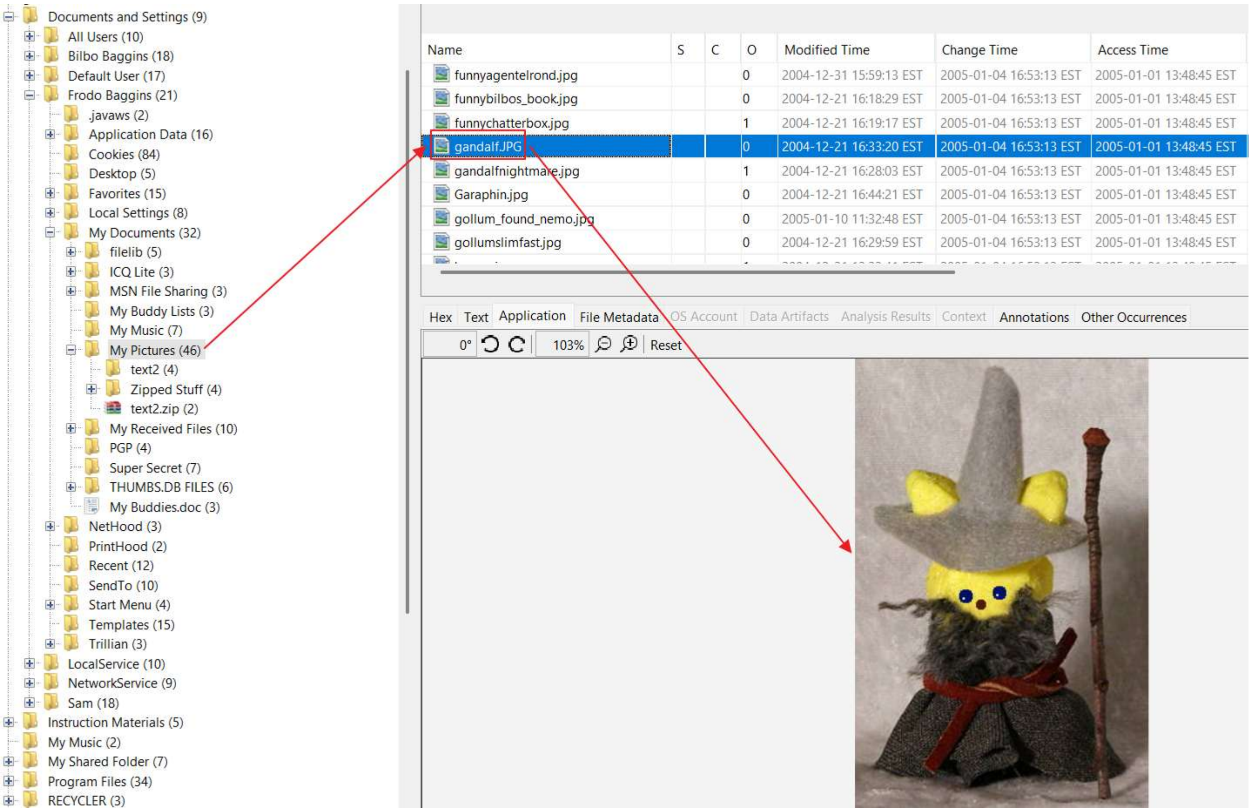


Lnk Name	Mru Position	Opened On	Extension Last Opened
ABC	=	=	=
My Pictures.lnk	0	2006-01-03 20:39:09	2006-01-03 20:39:09
blondlegolas.JPG.lnk	1		2006-01-03 20:39:09
New Text Document.txt.lnk	2		2006-01-03 20:12:11
Maps.lnk	3		
Map tp AccessData.jpg.lnk	4		

Figure 12: Timestamp for the recently accessed file

The eighth flag, which is an email address used on the computer, was covered previously. One of the email addresses primarily used on this computer is Baggifrodo@aol.com, and is shown in Figure 2.

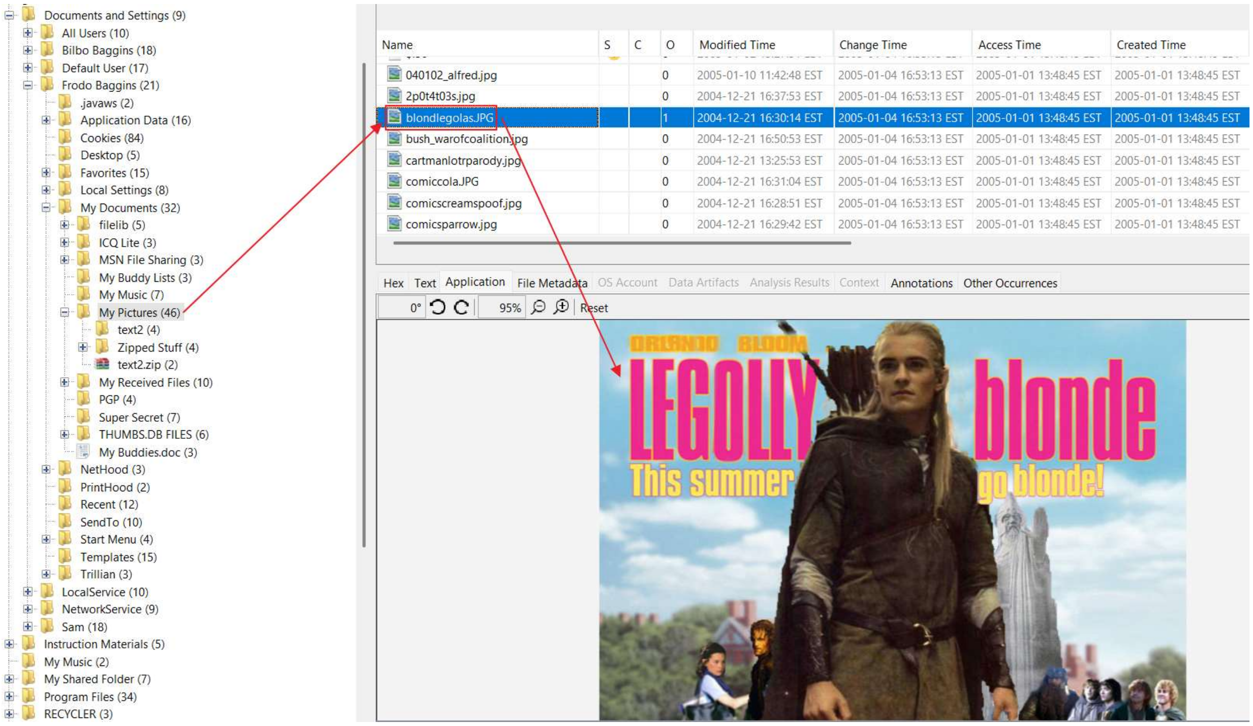
The ninth flag consists of finding three useful images on the computer. I found these pictures by looking through the My Pictures folder within Frodo Baggins's user file. All of the pictures are images and memes related to Lord of the Rings. Three of those pictures are shown in Figures 13-15.



```
Documents and Settings (9)
    All Users (10)
    Bilbo Baggins (18)
    Default User (17)
    Frodo Baggins (21)
        .javaws (2)
        Application Data (16)
        Cookies (84)
        Desktop (5)
        Favorites (15)
        Local Settings (8)
        My Documents (32)
            filelib (5)
            ICQ Lite (3)
            MSN File Sharing (3)
            My Buddy Lists (3)
            My Music (7)
            My Pictures (46)
                text2 (4)
                Zipped Stuff (4)
                text2.zip (2)
            My Received Files (10)
            PGP (4)
            Super Secret (7)
            THUMBS.DB FILES (6)
            My Buddies.doc (3)
        NetHood (3)
        PrintHood (2)
        Recent (12)
        SendTo (10)
        Start Menu (4)
        Templates (15)
        Trillian (3)
    LocalService (10)
    NetworkService (9)
    Sam (18)
Instruction Materials (5)
My Music (2)
My Shared Folder (7)
Program Files (34)
RECYCLER (3)
```

Name	S	C	O	Modified Time	Change Time	Access Time
funnyagentelrond.jpg			0	2004-12-31 15:59:13 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
funnybilbos_book.jpg			0	2004-12-21 16:18:29 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
funnychatterbox.jpg			1	2004-12-21 16:19:17 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
gandalf.JPG			0	2004-12-21 16:33:20 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
gandalfnightmare.jpg			1	2004-12-21 16:28:03 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
Garaphin.jpg			0	2004-12-21 16:44:21 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
gollum_found_nemo.jpg			0	2005-01-10 11:32:48 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
gollumslimfast.jpg			0	2004-12-21 16:29:59 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST

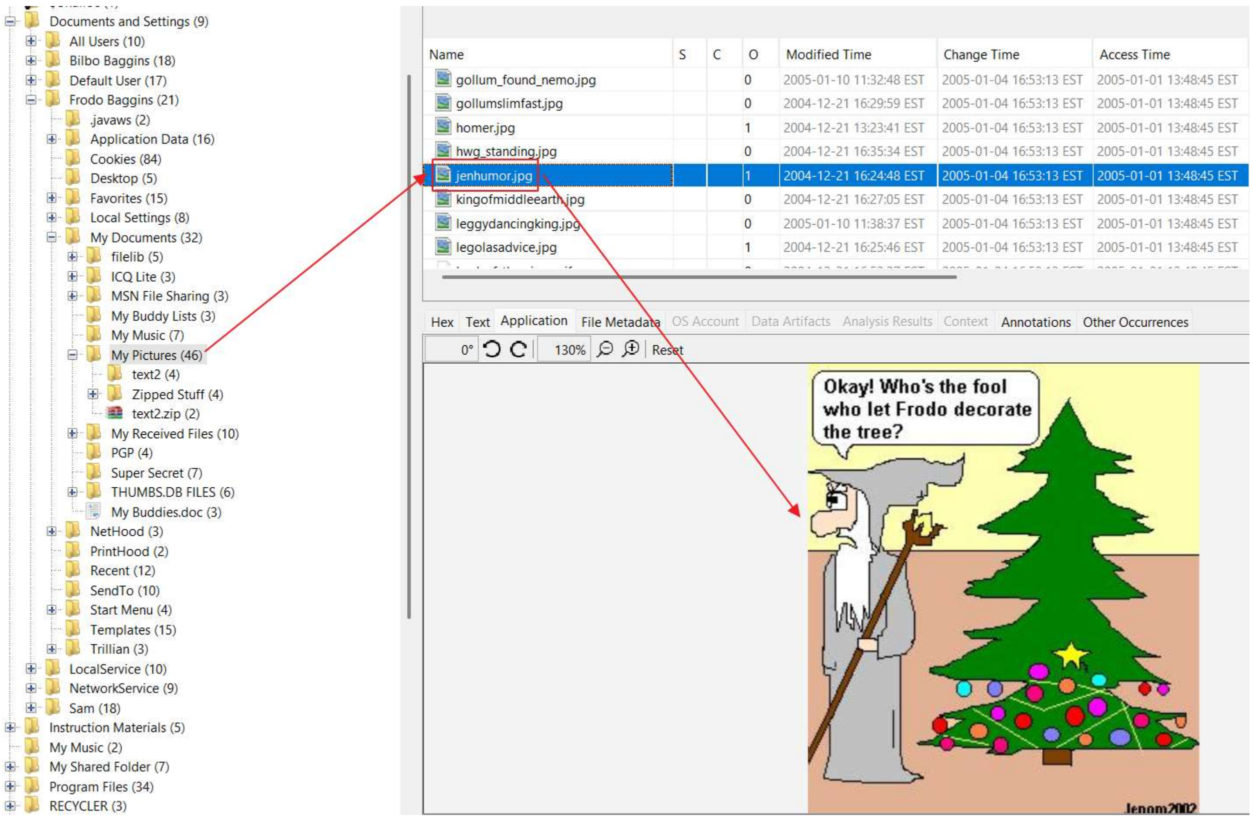
Figure 13: One picture found on the hard drive



```
Documents and Settings (9)
    All Users (10)
    Bilbo Baggins (18)
    Default User (17)
    Frodo Baggins (21)
        .javaws (2)
        Application Data (16)
        Cookies (84)
        Desktop (5)
        Favorites (15)
        Local Settings (8)
        My Documents (32)
            filelib (5)
            ICQ Lite (3)
            MSN File Sharing (3)
            My Buddy Lists (3)
            My Music (7)
            My Pictures (46)
                text2 (4)
                Zipped Stuff (4)
                text2.zip (2)
            My Received Files (10)
            PGP (4)
            Super Secret (7)
            THUMBS.DB FILES (6)
            My Buddies.doc (3)
        NetHood (3)
        PrintHood (2)
        Recent (12)
        SendTo (10)
        Start Menu (4)
        Templates (15)
        Trillian (3)
    LocalService (10)
    NetworkService (9)
    Sam (18)
Instruction Materials (5)
My Music (2)
My Shared Folder (7)
Program Files (34)
RECYCLER (3)
```

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
040102_alfred.jpg			0	2005-01-10 11:42:48 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST
2p0t4t03s.jpg			0	2004-12-21 16:37:53 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST
blondlegolas.JPG			1	2004-12-21 16:30:14 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST
bush_warofcoalition.jpg			0	2004-12-21 16:50:53 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST
cartmanlotrparody.jpg			0	2004-12-21 13:25:53 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST
comiccola.JPG			0	2004-12-21 16:31:04 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST
comicscreamspoof.jpg			0	2004-12-21 16:28:51 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST
comicsparrow.jpg			0	2004-12-21 16:29:42 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST

Figure 14: Another picture found on the hard drive

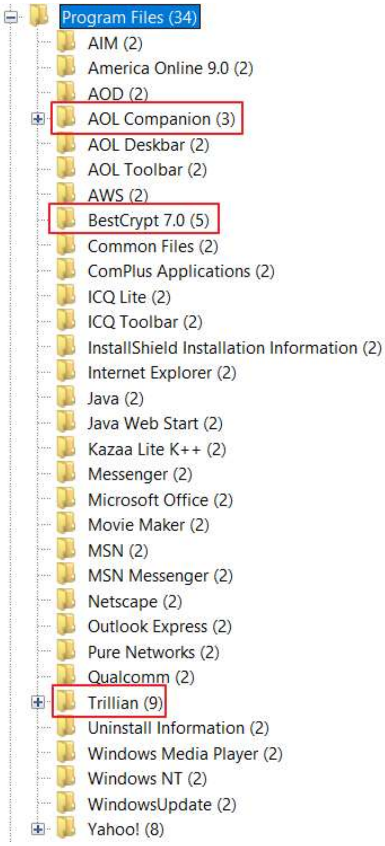


```
Documents and Settings (9)
    All Users (10)
    Bilbo Baggins (18)
    Default User (17)
    Frodo Baggins (21)
        .javaws (2)
        Application Data (16)
        Cookies (84)
        Desktop (5)
        Favorites (15)
        Local Settings (8)
        My Documents (32)
            filelib (5)
            ICQ Lite (3)
            MSN File Sharing (3)
            My Buddy Lists (3)
            My Music (7)
            My Pictures (46)
                text2 (4)
                Zipped Stuff (4)
                text2.zip (2)
            My Received Files (10)
            PGP (4)
            Super Secret (7)
            THUMBS.DB FILES (6)
            My Buddies.doc (3)
        NetHood (3)
        PrintHood (2)
        Recent (12)
        SendTo (10)
        Start Menu (4)
        Templates (15)
        Trillian (3)
    LocalService (10)
    NetworkService (9)
    Sam (18)
Instruction Materials (5)
My Music (2)
My Shared Folder (7)
Program Files (34)
RECYCLER (3)
```

Name	S	C	O	Modified Time	Change Time	Access Time
gollum_found_nemo.jpg			0	2005-01-10 11:32:48 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
gollumslimfast.jpg			0	2004-12-21 16:29:59 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
homer.jpg			1	2004-12-21 13:23:41 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
hwg_standing.jpg			0	2004-12-21 16:35:34 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
jenhumor.jpg			1	2004-12-21 16:24:48 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
kingofmiddleearth.jpg			0	2004-12-21 16:27:05 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
leggydancingking.jpg			0	2005-01-10 11:38:37 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST
legolasadvice.jpg			1	2004-12-21 16:25:46 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST

Figure 15: A third picture found on the hard drive

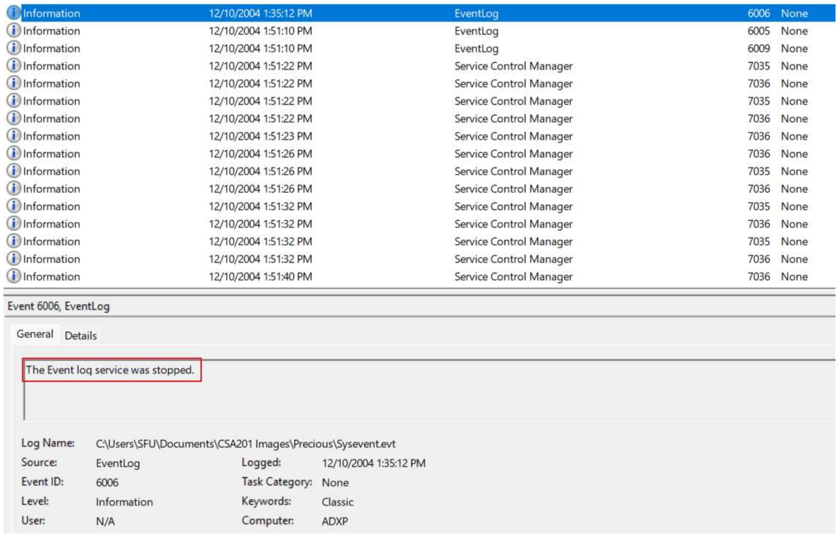
In order to find the tenth flag, I searched through the Program Files folder on the hard drive to find programs installed on the computer. Three programs installed are AOL Companion, BestCrypt 7.0, and Trillian. AOL Companion is a desktop application that provides users with quick access to various AOL services. BestCrypt 7.0 is an encryption software. Trillian is an instant messaging application. These applications are shown in Figure 16.



Program Files (34)
AIM (2)
America Online 9.0 (2)
AOD (2)
AOL Companion (3)
AOL Deskbar (2)
AOL Toolbar (2)
AWS (2)
BestCrypt 7.0 (5)
Common Files (2)
ComPlus Applications (2)
ICQ Lite (2)
ICQ Toolbar (2)
InstallShield Installation Information (2)
Internet Explorer (2)
Java (2)
Java Web Start (2)
Kazaa Lite K++ (2)
Messenger (2)
Microsoft Office (2)
Movie Maker (2)
MSN (2)
MSN Messenger (2)
Netscape (2)
Outlook Express (2)
Pure Networks (2)
Qualcomm (2)
Trillian (9)
Uninstall Information (2)
Windows Media Player (2)
Windows NT (2)
WindowsUpdate (2)
Yahoo! (8)

Figure 16: Three programs installed on the computer

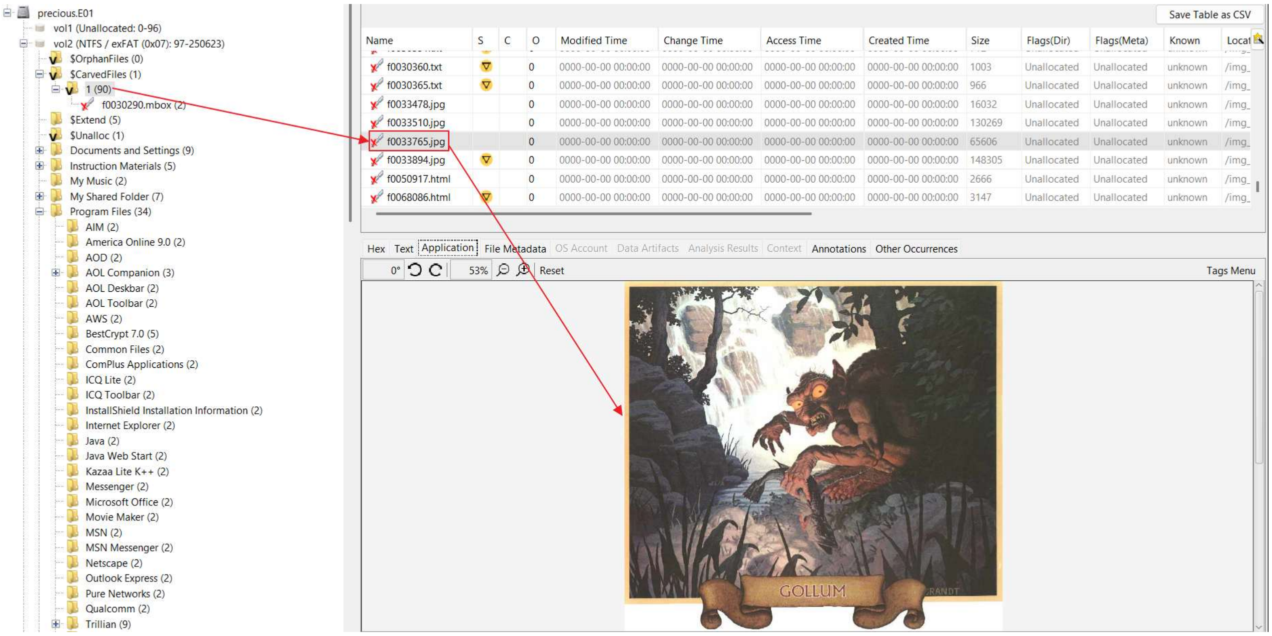
I discovered the eleventh flag by looking at the sysevent.evt log file. Unlike modern operating system event logs, the logs for Windows XP lack crucial data that can be used for an investigation. However, I saw that the event log service was stopped at 1:35:12 PM on 12/10/2004, which indicates the last successful shutdown of the computer.



```
Information   12/10/2004 1:35:12 PM   EventLog                  6006   None
Information   12/10/2004 1:51:10 PM   EventLog                  6005   None
Information   12/10/2004 1:51:10 PM   EventLog                  6009   None
Information   12/10/2004 1:51:22 PM   Service Control Manager   7035   None
Information   12/10/2004 1:51:22 PM   Service Control Manager   7036   None
Information   12/10/2004 1:51:22 PM   Service Control Manager   7035   None
Information   12/10/2004 1:51:22 PM   Service Control Manager   7036   None
Information   12/10/2004 1:51:23 PM   Service Control Manager   7036   None
Information   12/10/2004 1:51:26 PM   Service Control Manager   7036   None
Information   12/10/2004 1:51:26 PM   Service Control Manager   7035   None
Information   12/10/2004 1:51:26 PM   Service Control Manager   7036   None
Information   12/10/2004 1:51:32 PM   Service Control Manager   7035   None
Information   12/10/2004 1:51:32 PM   Service Control Manager   7036   None
Information   12/10/2004 1:51:32 PM   Service Control Manager   7035   None
Information   12/10/2004 1:51:32 PM   Service Control Manager   7036   None
Information   12/10/2004 1:51:40 PM   Service Control Manager   7036   None

Event 6006, EventLog

General   Details

The Event log service was stopped.

Log Name:   C:\Users\SFU\Documents\CSA201 Images\Precious\Sysevent.evt
Source:     EventLog       Logged:          12/10/2004 1:35:12 PM
Event ID:   6006           Task Category:   None
Level:      Information    Keywords:        Classic
User:       N/A            Computer:        ADXP
```

Figure 17: Shutdown recorded in the Windows Event Viewer

I found the twelfth flag by looking through the $CarvedFiles folder in Autopsy. This means the image was deleted but was able to be recovered since it was not completely overwritten by the file system. See Figure 18.



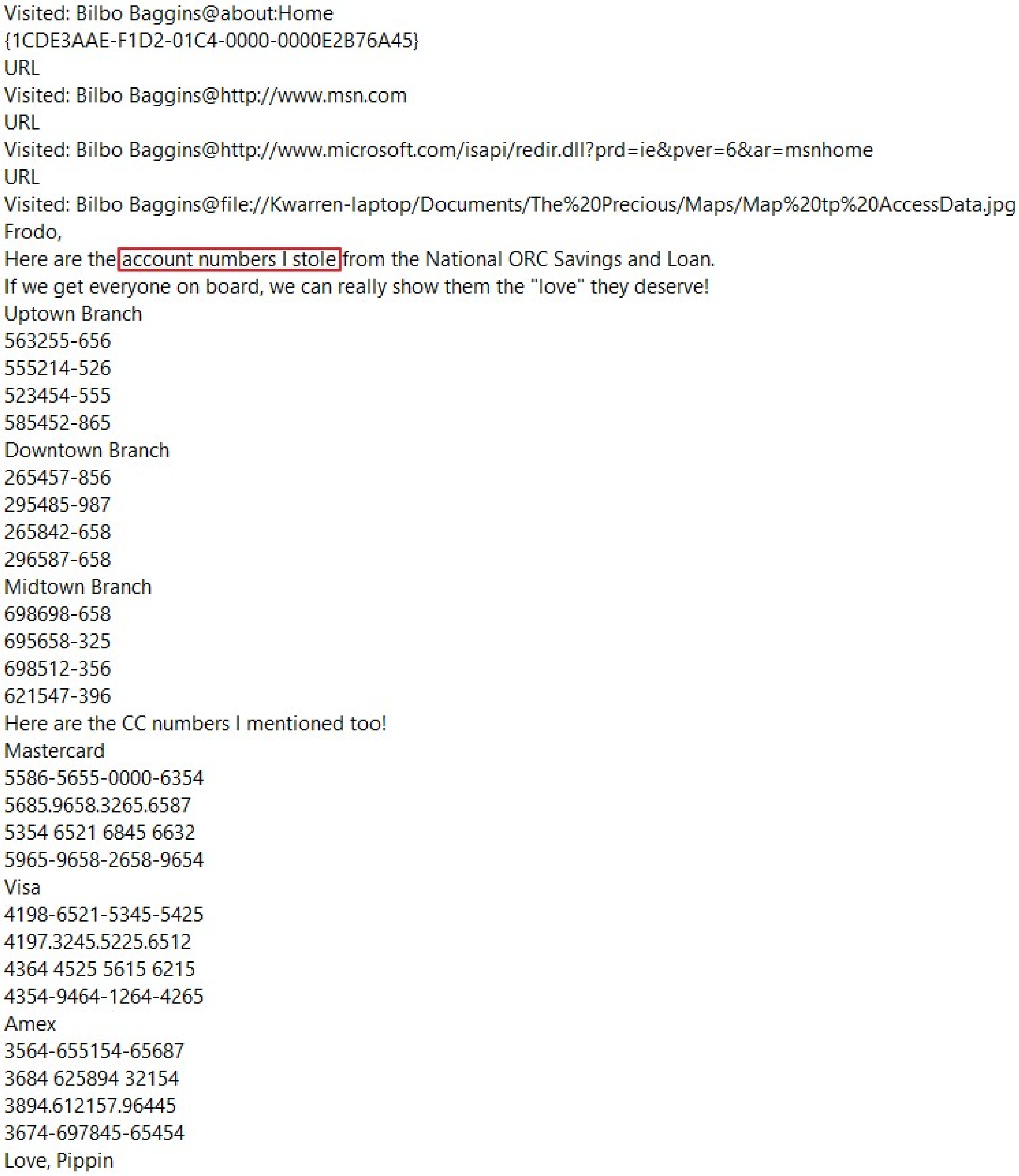
```
precious.E01
  vol1 (Unallocated: 0-96)
  vol2 (NTFS / exFAT (0x07): 97-250623)
    $OrphanFiles (0)
    $CarvedFiles (1)
      1 (90)
        f0030290.mbox (2)
    $Extend (5)
    $Unalloc (1)
    Documents and Settings (9)
    Instruction Materials (5)
    My Music (2)
    My Shared Folder (7)
    Program Files (34)
      AIM (2)
      America Online 9.0 (2)
      AOD (2)
      AOL Companion (3)
      AOL Deskbar (2)
      AOL Toolbar (2)
      AWS (2)
      BestCrypt 7.0 (5)
      Common Files (2)
      ComPlus Applications (2)
      ICQ Lite (2)
      ICQ Toolbar (2)
      InstallShield Installation Information (2)
      Internet Explorer (2)
      Java (2)
      Java Web Start (2)
      Kazaa Lite K++ (2)
      Messenger (2)
      Microsoft Office (2)
      Movie Maker (2)
      MSN (2)
      MSN Messenger (2)
      Netscape (2)
      Outlook Express (2)
      Pure Networks (2)
      Qualcomm (2)
      Trillian (9)
```

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Locat
f0030360.txt	▽		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	1003	Unallocated	Unallocated	unknown	/img_
f0030365.txt	▽		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	966	Unallocated	Unallocated	unknown	/img_
f0033478.jpg			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	16032	Unallocated	Unallocated	unknown	/img_
f0033510.jpg			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	130269	Unallocated	Unallocated	unknown	/img_
f0033765.jpg			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	65606	Unallocated	Unallocated	unknown	/img_
f0033894.jpg	▽		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	148305	Unallocated	Unallocated	unknown	/img_
f0050917.html			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	2666	Unallocated	Unallocated	unknown	/img_
f0068086.html	▽		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	3147	Unallocated	Unallocated	unknown	/img_

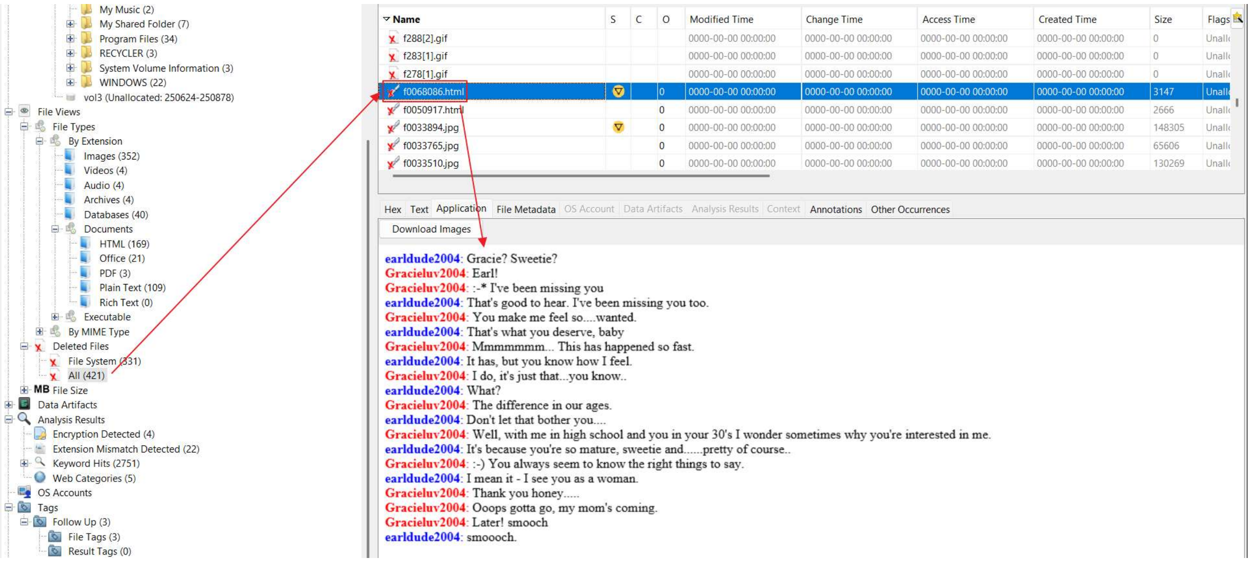
Figure 18: Recovered deleted file

For the thirteenth flag, I discovered multiple interesting pieces of evidence on the computer. First, I found a log file in the $Unalloc folder on the file system which included evidence of credit card theft, as shown in Figure 19. I also discovered a deleted html file of a chat between an alleged 30+ year old man and a high school girl, as shown in Figure 20. However, this consists of two accounts that were not on the hard drive. There is evidence that suggests Frodo was working on a disk image, so these two files could have come from that. Figure 21 shows an email sent by Frodo Baggins regarding help with a disk image.



```
Visited: Bilbo Baggins@about:Home
{1CDE3AAE-F1D2-01C4-0000-0000E2B76A45}
URL
Visited: Bilbo Baggins@http://www.msn.com
URL
Visited: Bilbo Baggins@http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
URL
Visited: Bilbo Baggins@file://Kwarren-laptop/Documents/The%20Precious/Maps/Map%20tp%20AccessData.jpg
Frodo,
Here are the account numbers I stole from the National ORC Savings and Loan.
If we get everyone on board, we can really show them the "love" they deserve!
Uptown Branch
563255-656
555214-526
523454-555
585452-865
Downtown Branch
265457-856
295485-987
265842-658
296587-658
Midtown Branch
698698-658
695658-325
698512-356
621547-396
Here are the CC numbers I mentioned too!
Mastercard
5586-5655-0000-6354
5685.9658.3265.6587
5354 6521 6845 6632
5965-9658-2658-9654
Visa
4198-6521-5345-5425
4197.3245.5225.6512
4364 4525 5615 6215
4354-9464-1264-4265
Amex
3564-655154-65687
3684 625894 32154
3894.612157.96445
3674-697845-65454
Love, Pippin
```

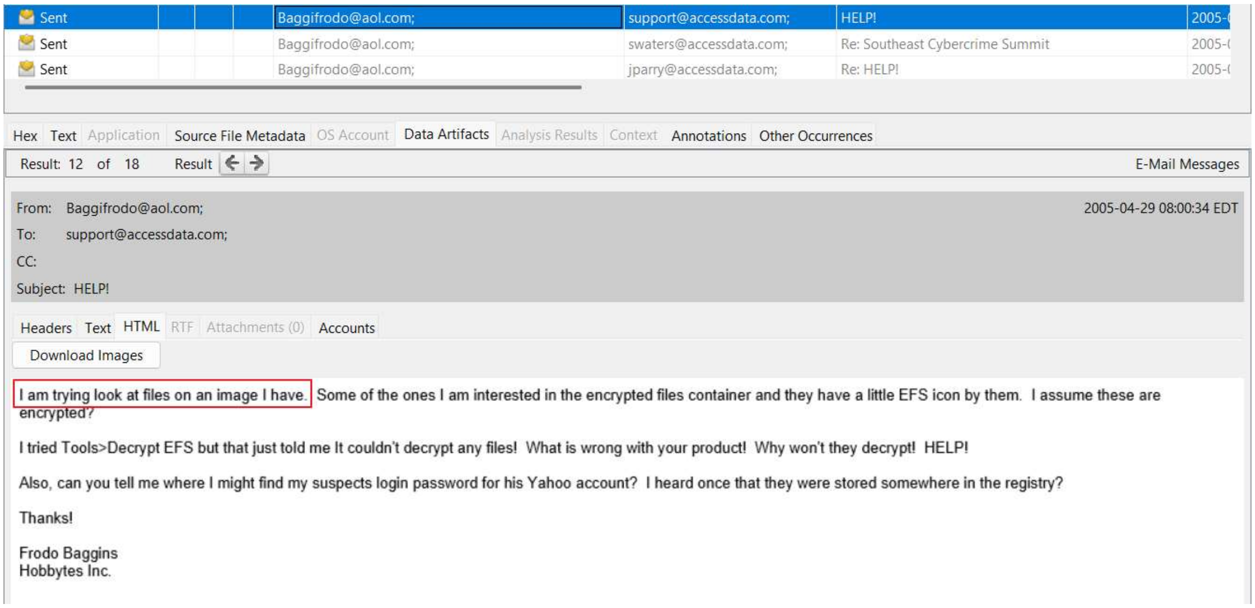
Figure 19: Possible stolen credit cards



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
f288[2].gif				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unall
f283[1].gif				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unall
f278[1].gif				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unall
f0068086.html	▽		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	3147	Unall
f0050917.html			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	2666	Unall
f0033894.jpg	▽		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	148305	Unall
f0033765.jpg			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	65606	Unall
f0033510.jpg			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	130269	Unall

earldude2004: Gracie? Sweetie?
Gracieluv2004: Earl!
Gracieluv2004: :-* I've been missing you
earldude2004: That's good to hear. I've been missing you too.
Gracieluv2004: You make me feel so....wanted.
earldude2004: That's what you deserve, baby
Gracieluv2004: Mmmmmmm... This has happened so fast.
earldude2004: It has, but you know how I feel.
Gracieluv2004: I do, it's just that...you know..
earldude2004: What?
Gracieluv2004: The difference in our ages.
earldude2004: Don't let that bother you....
Gracieluv2004: Well, with me in high school and you in your 30's I wonder sometimes why you're interested in me.
earldude2004: It's because you're so mature, sweetie and......pretty of course..
Gracieluv2004: :-) You always seem to know the right things to say.
earldude2004: I mean it - I see you as a woman.
Gracieluv2004: Thank you honey.....
Gracieluv2004: Ooops gotta go, my mom's coming.
Gracieluv2004: Later! smooch
earldude2004: smoooch.

Figure 20: Potential pedophilia



Sent	Baggifrodo@aol.com;	support@accessdata.com;	HELP!	2005-(
Sent	Baggifrodo@aol.com;	swaters@accessdata.com;	Re: Southeast Cybercrime Summit	2005-(
Sent	Baggifrodo@aol.com;	jparry@accessdata.com;	Re: HELP!	2005-(

From: Baggifrodo@aol.com; 2005-04-29 08:00:34 EDT
To: support@accessdata.com;
CC:
Subject: HELP!

I am trying look at files on an image I have. Some of the ones I am interested in the encrypted files container and they have a little EFS icon by them. I assume these are encrypted?

I tried Tools>Decrypt EFS but that just told me It couldn't decrypt any files! What is wrong with your product! Why won't they decrypt! HELP!

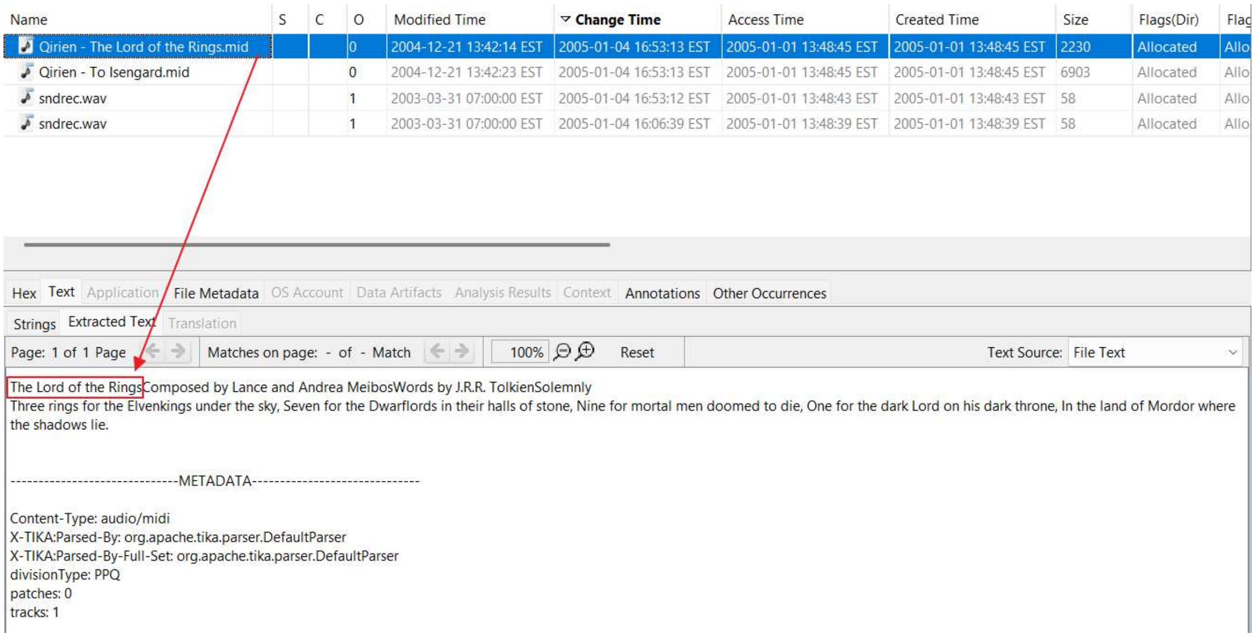
Also, can you tell me where I might find my suspects login password for his Yahoo account? I heard once that they were stored somewhere in the registry?

Thanks!

Frodo Baggins
Hobbytes Inc.

Figure 21: Evidence that shows Frodo was working on a disk image

There is also some evidence that suggests the user enjoys music, however it is just music from the Lord of the Rings. This is shown in Figure 22.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
Qirien - The Lord of the Rings.mid			0	2004-12-21 13:42:14 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST	2230	Allocated	Allo
Qirien - To Isengard.mid			0	2004-12-21 13:42:23 EST	2005-01-04 16:53:13 EST	2005-01-01 13:48:45 EST	2005-01-01 13:48:45 EST	6903	Allocated	Allo
sndrec.wav			1	2003-03-31 07:00:00 EST	2005-01-04 16:53:12 EST	2005-01-01 13:48:43 EST	2005-01-01 13:48:43 EST	58	Allocated	Allo
sndrec.wav			1	2003-03-31 07:00:00 EST	2005-01-04 16:06:39 EST	2005-01-01 13:48:39 EST	2005-01-01 13:48:39 EST	58	Allocated	Allo

Text Source: File Text

```
The Lord of the RingsComposed by Lance and Andrea MeibosWords by J.R.R. TolkienSolemnly
Three rings for the Elvenkings under the sky, Seven for the Dwarflords in their halls of stone, Nine for mortal men doomed to die, One for the dark Lord on his dark throne, In the land of Mordor where the shadows lie.


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

Content-Type: audio/midi
X-TIKA:Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA:Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
divisionType: PPQ
patches: 0
tracks: 1
```

Figure 22: Lord of the Rings music

Timeline

Date/Time	Event	Relevance
12/10/2004 13:35:12 MST	Event Log stopped	Frodo's computer was shut down
12/10/2004 13:51:10 MST	Event Log started	Frodo's computer booted up
12/21/2004 10:25:05 MST	Frodo sends email to Sam about a Lord of the Rings spoof image	Shows interest in Lord of the Rings
1/4/2005 14:42:35 MST	Frodo searches for "lotr"	Shows interest in Lord of the Rings
1/4/2005 14:42:35 MST	Frodo visits http://lordoftherings.net	Shows interest in Lord of the Rings
1/4/2005 14:53:13 MST	Several images and files related to Lord of the Rings are changed on the computer	Indicates a change in the metadata of the files, possibly due to file renaming or a location change
1/6/2005 14:31:11 MST	USB device inserted into the computer	Indicates a possible transfer of data between the computer and the USB drive
4/29/2005 6:00:34 MDT	Frodo asks for help with disk image	Shows interest in digital forensics, proves Frodo was working on a disk image

1/3/2006 14:39:09 MST	The file "blondlegolas.JPG" is accessed	Shows continued interest in Lord of the Rings

Conclusions

The main user on this Windows XP computer is Frodo Baggins. This person enjoys Lord of the Rings, as shown through the accounts, pictures, and music on the computer. The computer is set to Mountain Time, as shown in the Windows Registry. There is evidence that suggests the user is getting interested in digital forensics, such as email artifacts and deleted files found on the computer. There are deleted files on the computer that were recovered, although they do not raise concern since the main user was working on a disk image. Overall, this user is a big fan of the Lord of the Rings series. The user also has a growing interest in digital forensics.