GUIDANCE SOFTWARE

From beginning to endpoint.

Examination Report

Case Information

Case Number	123456789
Examiner Name	Sahifa Syed
Description	The Hunter Case

Evidence

Name	Acquisition MD5	Verification MD5	Evidence Number	Examiner Name
Hunter XP	dfcfe9ab9a60c6ad4a314656b687226b	dfcfe9ab9a60c6ad4a314656b687226b	1	

Examiner Notes

The following notes were prepared as part of the examination.

Documents of Interest

Documents

The below bookmarks represent documents that are potentially relevant to this case.

1) Banking Information.txt

Item Path	Hunter XP\C\Documents and Settings\Bob Hunter\My Documents\Banking Information.txt
File Created	03/06/02 16:09:08
Last Written	03/06/02 16:09:36
Last Accessed	03/06/02 16:09:36
MD5	2f3bf3218f3863fcb5990f64fb137ee4
Comment	

Pictures

The below bookmarks represent pictures that are potentially relevant to this case.

2) 101-0188_IMG.JPG

Item Path	Web Site\101-0188_IMG.JPG
File Created	
Last Written	
Last Accessed	
MD5	5ead9d1c32a5deb91600b0783b7b4699
Comment	

3) evidence

- Email
  - Web Site
  - Web Page
  - Fwd: Delivery Status Notification (Failure)

4) wbkC1.tmp

Item Path	Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Temporary Internet Files\Content.IE5\8XGPQD6L\wbkC1.tmp
File Created	03/06/02 12:37:06
Last Written	03/06/02 12:37:06
Last Accessed	03/06/02 12:37:06
MD5	cec6f1262f2563db19574238c959d5f7
Comment	

5) 102-0229_IMG.JPG

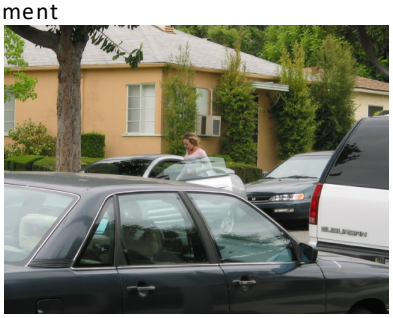
Item Path	Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Application Data\Microsoft\CD Burning\Hunter Pics\Christina Detsiwt\102-0229_IMG.JPG
File Created	14/05/02 13:02:15
Last Written	24/04/02 15:54:00
Last Accessed	04/06/02 19:04:18
MD5	39021a9ea60f0b9e43410dec5b769931
Comment	

6) 103-0383_IMG.JPG

Item Path	Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Application Data\Microsoft\CD Burning\Hunter Pics\Christina Detsiwt\103-0383_IMG.JPG
File Created	14/05/02 13:02:25
Last Written	25/04/02 18:04:00
Last Accessed	04/06/02 19:04:26
MD5	e6231f5e49907b1892e7c1c61f82f0d1
Comment	

7) 104-0438_IMG.JPG

Item Path	Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Application Data\Microsoft\CD Burning\Hunter Pics\Christina Detsiwt\104-0438_IMG.JPG
File Created	14/05/02 13:02:37
Last Written	29/04/02 17:12:00
Last Accessed	04/06/02 19:04:31
MD5	f8b5f2b5a5e3d2eba5821d4e7e3f3d66
Comment	



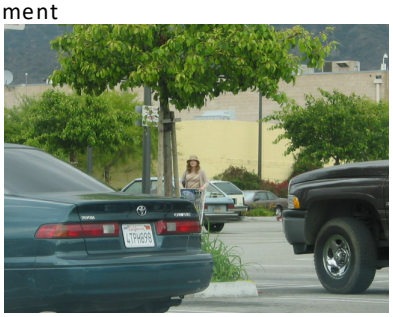
8) 104-0438_IMG.JPG

Item Path	Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Application Data\Microsoft\CD Burning\Hunter Pics\Christina Detsiwt\104-0438_IMG.JPG
File Created	14/05/02 13:02:37
Last Written	29/04/02 17:12:00
Last Accessed	04/06/02 19:04:31

MD5 f8b5f2b5a5e3d2eba5821d4e7e3f3d66
Comment

9) 104-0480_IMG.JPG

Item Path Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Application Data\Microsoft\CD Burning\Hunter Pics\Sabrina Dewercs\104-0480_IMG.JPG
File Created 14/05/02 13:02:34
Last Written 29/04/02 17:13:00
Last Accessed 04/06/02 19:02:48
MD5 93c43d482d3a289a2ffb47620eb4a33b
Comment



clean up and wiping utilities

Pictures of Interest

Email of Interest

Email

The below bookmarks represent emails that are potentially relevant to this case.

10) Re: Web Page on Christina

Comment

From	Billy Ray <billyray150@hotmail.com>
To	chaser1191@hotmail.com
Sent	30/05/02 19:11:11
Subject	Re: Web Page on Christina

yes I saw that too I will fix it, hold off on the email I tested his address its not working

>From: "IC YOU" <chaser1191@hotmail.com>
>To: billyray150@hotmail.com
>Subject: Web Page on Christina
>Date: Thu, 23 May 2002 08:48:19 -0500
>
>Billy,
>
>Page looks good, the old man should pay up. on one of the photos though you are in the reflection of the window, what where you thinking. Get that off of there, I will email dad today after you fix it.
>
>Bob
>

11) Web Site

Comment

From	Billy Ray <billyray150@hotmail.com>
To	chaser1191@hotmail.com
Sent	22/05/02 09:01:21
Subject	Web Site

Bob here are some of the pics from the web page we are doing. I will be posting it later today, then we can send the letter to the ole man. if all goes well we will be rich men this summer.

I could not send all of the photos because of this hotmail limit, but we can hook up later by phone or IM or yahoo or something and I will show you the page.

Billy

Attachments

Name	101-0188_IMG.JPG
Logical Size	122,102

101-0188_IMG.JPG

Name	101-0192_IMG.JPG
Logical Size	99,921

101-0192_IMG.JPG

Name	101-0195_IMG.JPG
Logical Size	102,586

101-0195_IMG.JPG

Name	102-0206_IMG.JPG
Logical Size	101,309

102-0206_IMG.JPG

Name	102-0212_IMG.JPG
Logical Size	80,666

102-0212_IMG.JPG

Name	102-0226_IMG.JPG
Logical Size	93,654

102-0226_IMG.JPG

Name	102-0244_IMG.JPG
Logical Size	105,807

102-0244_IMG.JPG

Name	102-0271_IMG.JPG
Logical Size	95,932

102-0271_IMG.JPG

Name	102-0271_IMG.JPG
Logical Size	95,932

102-0271_IMG.JPG

Name	102-0283_IMG.JPG
Logical Size	111,983

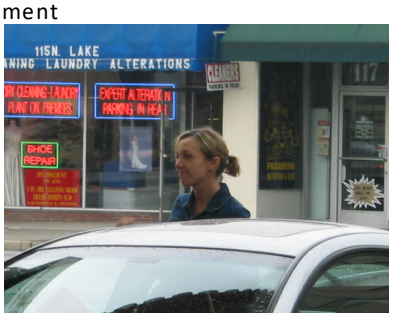
102-0283_IMG.JPG

12) 101-0188_IMG.JPG

Item Path Web Site\101-0188_IMG.JPG
File Created
Last Written
Last Accessed
MD5 5ead9d1c32a5deb91600b0783b7b4699
Comment

13) 101-0192_IMG.JPG

Item Path Web Site\101-0192_IMG.JPG
File Created
Last Written
Last Accessed
MD5 2f35b6db61617b096bda629678f9cca7
Comment

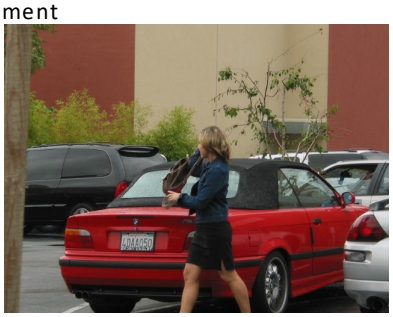


14) 101-0195_IMG.JPG

Item Path Web Site\101-0195_IMG.JPG
File Created
Last Written
Last Accessed
MD5 eed38cd7639fc1cb14f486e2f7d29546
Comment

15) 102-0206_IMG.JPG

Item Path Web Site\102-0206_IMG.JPG
File Created
Last Written
Last Accessed
MD5 ec20cf24abcee99cbccd60f19913e0e8
Comment



16) 102-0212_IMG.JPG

Item Path Web Site\102-0212_IMG.JPG
File Created
Last Written
Last Accessed
MD5 db36fb3c0170105aaa12b18f34a6b4a1
Comment

17) 102-0226_IMG.JPG

Item Path Web Site\102-0226_IMG.JPG
File Created
Last Written
Last Accessed
MD5 4e86632343cae9ff63551a3baa9da3f5
Comment

18) 102-0244_IMG.JPG

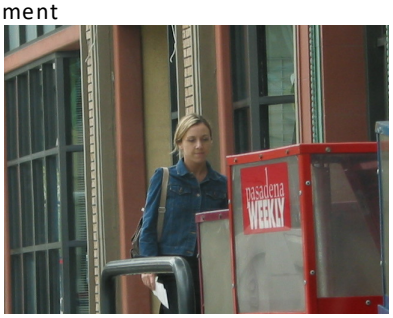
Item Path Web Site\102-0244_IMG.JPG
File Created
Last Written
Last Accessed
MD5 1de4d799f5ac1f0d1d63f69070fef0e4
Comment

19) 102-0271_IMG.JPG

Item Path Web Site\102-0271_IMG.JPG
File Created
Last Written
Last Accessed
MD5 f4e3609bf826ee29f52efffb8a5dec9e
Comment

20) 102-0271_IMG.JPG

Item Path Web Site\102-0271_IMG.JPG
File Created
Last Written
Last Accessed
MD5 f4e3609bf826ee29f52efffb8a5dec9e
Comment



21) 102-0283_IMG.JPG

Item Path Web Site\102-0283_IMG.JPG
File Created
Last Written
Last Accessed
MD5 cec6f1262f2563db19574238c959d5f7
Comment

Internet Artifacts of Interest

Internet Artifacts

The below bookmarks represent Internet artifacts that are potentially relevant to this case.

internet history

22) evidence

Typed URL

23) 00018.SPL

True Path	Hunter\Hunter XP\C\WINDOWS\system32\spool\PRINTERS\00018.SPL
File Created	04/06/02 19:11:37
Last Written	04/06/02 19:11:37
Last Accessed	04/06/02 19:11:37
MD5	0a0eeb854bbe032e54fb46d7eaf7f5da
Start Sector	1,437,739
Sector offset	80
File Offset	80
Length	41
Comment	stalking and blackmailing

24) NTUSER.DAT

Item Path Internet Explorer (Windows)\History\Typed URL\NTUSER.DAT
Comment

Internet Artifact Type	History\Typed URL
Title	url6
Url Name	www.thestalkershomepage.com
Url Host	www.thestalkershomepage.com
Last Modification Time	03/06/02 15:15:54
Browser Type	Internet Explorer (Windows)
Profile Name	Bob Hunter
Message Size	58

25) Christina Sabrina URL

Item Path Christina Sabrina URL
Comment Internet visits by URL, collected by the Internet Artifacts module.

	URL
1	http://www.guidancesw.com/christina_sabrina.htm

26) stalking website

Item Path stalking website
Comment Internet visits by URL, collected by the Internet Artifacts module.

	URL
1	http://www.glr.com/stalk.html

Printer information related to 00018.SPL file

27) Dewercs related message

Item Path Dewercs related message
Comment Displays Yahoo Instant Messages.

	Text
1	Yeah I know I just need to figure out what to do with Dewercs

Other Findings

The below bookmarks represent other information that is potentially relevant to this case.

28) 00006432_101-0192_IMG.JPG_FO-2.mp3

Item Path Billy.dbx\Web Site\101-0192_IMG.JPG\101-0192_IMG.JPG\00006432_101-0192_IMG.JPG_FO-2.mp3
File Created
Last Written
Last Accessed
MD5 2665df0614cfdd8c380083a769187fd9
Comment

29) StandardName

Item Path $$$PROTO.HIV\ControlSet001\Control\TimeZoneInformation\StandardName
File Created
Last Written
Last Accessed
MD5 568e5255f001440322030e808dacbaf3
Comment

30) Html Body

Item Path chaser1191\Slack Table\Your Daughters Safety Depends on This!!!\Html Body
File Created
Last Written
Last Accessed
MD5
Comment

31) Html Body

Item Path chaser1191\Chaser1191\Mail\Mail You've Sent\If you love your daughter\Html Body
File Created
Last Written
Last Accessed
MD5
Comment

32) login_title_logo[1].gif

Item Path Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Temporary Internet Files\Content.IE5\042WFPGU\login_title_logo[1].gif
File Created 31/03/02 09:25:43
Last Written 31/03/02 09:25:43
Last Accessed 31/03/02 09:25:43
MD5 99bc335305e3d3b3554b9c5ac8c2a726
Comment

USB Drives

Found external drives on USB records. Two files were shown

33) lnk file system information

Item Path lnk file system information
Comment Provides information about Link Files, collected by the Windows Artifact Parser module, that link to executable files.

	File Attributes
1	32

34) oembios.bin

Item Path Hunter XP\C\WINDOWS\system32\oembios.bin
File Created 23/08/01 07:00:00
Last Written 23/08/01 07:00:00
Last Accessed 28/02/02 16:00:02
MD5 6d0bd10dd99ae61ba6e8a1a3e697dfcd
Comment

35) sabrina recycle bin

Item Path sabrina recycle bin
Comment Files found in the Recycle Bin, collected by the Windows Artifact Parser module.

	Deleted
1	05/06/02 01:49:16

36) User Accounts

Item Path User Accounts
Comment
Users from the Windows Registry, collected by the System Information module, derived from the following registry keys:
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList",
"HKEY_LOCAL_MACHINE\SAM".
- the information may be duplicated because the same entry can be found in both registry locations
- the SID and Profile Path information may be empty for entries found in HKEY_LOCAL_MACHINE\SAM.

	User
1	Administrator
2	Bob Hunter
3	Guest

37) External Drives

Item Path External Drives
Comment
USB Devices from the Windows Registry, collected by the System Information module, derived from the following registry keys:
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR",
"HKEY_LOCAL_MACHINE\System\MountedDevices",
"HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}",
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList",
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProductName".

	Device
1	Netac OnlyDisk USB Device

38) Christina and Sabrina related Content

Item Path Christina and Sabrina related Content
Comment MFT entries parsed from $Logfile, collected by the Windows Artifact Parser module.

	Target
1	Hunter XP
2	Hunter XP

39) Timezone

Item Path Timezone
Comment
Time Zone from the Windows Registry, collected by the System Information module, derived from the following registry keys:
If collected from Windows NT-
- "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\NetworkCards",
- "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services",
- "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\Root".
If collected from Windows XP-
- "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation",
- "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones".
If collected from Windows Vista (or above)-
- "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation",
- "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones",
- "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones".

	Standard Name
1	Central Standard Time

examination of files types

40) realplay.exe

Item Path Hunter XP\C\Program Files\Real\RealPlayer\realplay.exe
File Created 01/03/02 09:09:53
Last Written 01/03/02 09:09:53
Last Accessed 04/06/02 18:01:46
MD5 849d97fe4cc09cfc2772d10f641e1baf
Comment

41) cleanmgr.exe

Item Path Hunter XP\C\WINDOWS\system32\cleanmgr.exe
File Created 23/08/01 07:00:00
Last Written 23/08/01 07:00:00
Last Accessed 03/06/02 12:08:40
MD5 482b5e753b543abd23d2a7c85c29f148
Comment

42) 102-0283_IMG[1].jpg

Item Path Hunter XP\C\Documents and Settings\Bob Hunter\Local Settings\Temporary Internet Files\Content.IE5\8XGPQD6L\102-0283_IMG[1].jpg
File Created 03/06/02 14:04:23
Last Written 03/06/02 14:04:23
Last Accessed 03/06/02 14:04:23
MD5 c955bd8edabb7ca88e72cc2c389633db
Comment

43) Recycle bin content

Item Path Recycle bin content
Comment Files found in the Recycle Bin, collected by the Windows Artifact Parser module.

	Deleted
1	05/06/02 01:50:06
2	05/06/02 01:49:16
3	05/06/02 01:49:46