LEGAL REPORT

Case: Hunter XP Forensic Image Analysis

Examiner: Raunak Kr. Singh

Requested By: Mukesh Tiwari

1. Introduction

1.1 Purpose of the Report

This legal report consists of findings of a digital disk image i.e. Hunter XP Dongled v6 which was provided to us by Mr. Mukesh Tiwari for digital forensic examination. This digital forensic examination is carried out to identify, analyse, and interpret digital evidences or artefacts relevant to suspected criminal activity involving four major offences i.e. Stalking, Extortion (Blackmailing), Conspiracy and use of anti-forensic and encryption tools.

1.2 Scope of Examination

The digital forensic examination was commenced from 8 December, 2025 where I focused on exploring all the partition of disk image. While exploring and completing other components of this module, I added the notable tag for the digital evidence which would help me to prove that criminal offence. The analysis was limited strictly to the supplied forensic image and did not involve any other digital device or digital interaction.

1.3 Examiner Credentials

The forensic examination was conducted by Raunak Kr. Singh, a cybersecurity and digital forensics student of The British College trained in the used of industry-standard forensic tools i.e. Autopsy, FTK Imager, KAPE, RegRipper, Event Log Explorer, 7-Zip, and Hex Editor.
While using all the listed tools, Chain of custody and required digital forensics principles has been followed.

2. Evidence Summary

Evidence Name	Hunter XP Dongled v6. E01
Used Tool	Autopsy v4.22.1
Stored Hash (MD5)	dfcfe9ab9a60c6ad4a314656b687226b
Calculated Hash (MD5)	dfcfe9ab9a60c6ad4a314656b687226b

3. Examination Method and Summary

The forensic examination was conducted using knowledge obtained during class and listed tools. Tools such as Autopsy, FTK Imager, were used to analyse and explore the file system, where as Reg Ripper and Registry Viewer is used to gather detailed information from the extracted registry hive. Hex Editor was used to verify the integrity of binary or hex value of the file.

Key findings included:

1. User Account Information
2. System Configuration and OS Artefacts
3. Image files and Metadata
4. E-mails
5. Internet Browsing History
6. Evidence of Anti-Forensic Software and its execution

4.File System Examination and Analysis

4.1 User Account Information

Username:	Bob Hunter [1004]
User Type:	Default Admin User
Last Login Date:	Tue Jun 4 23:01:54 2002 UTC
Password Reset Date:	Thu Feb 28 22:22:17 2002 UTC
Password Fail Date:	NONE
Login Count:	37
Password:	NO PASSWORD
Account Created:	Thu Feb 28 22:22:17 2002 UTC
Account Type:	Normal User Account
Source:	SAM Registry Hive

4.2 System Configuration and OS Artefacts

Information about the Operating System:

PC Name: Microsoft Windows XP

Install Date: 2002-02-28 22:02:39 UTC

Source: Software Registry Hive

Location:	/Img_Hunter XP for Dongled v6.EO1/Vol-Vol2/Windows/System32/Config/Software
Size:	9175040
MD5:	dbda9a624d0ca6c78f2a76dfe4e17f30
SHA-256:	5afab1494089c1f63a3f9a1902f25a01dde72c1f1b0783112bde0261eb0c9d36

Information about the Time Zone:

Time Zone: Central Standard Time (UTC)

Source: System Registry Hive

Location:	/Img_Hunter XP for Dongled v6.EO1/Vol-Vol2/Windows/System32/Config/System
Size:	2883584
MD5:	e481dace1baf5277c9934f9912e41f65
SHA-256:	8f736ab40c3a1ae90d5c8126046821eb4bd74ddb3344dfdeee4f75e5e304e55e

4.3 Image files and Metadata

1. Df829.JPG

The photograph of the victim, **Christina Detsiwt** taken on 2002-05-14 18:02:29 GMT and modified on 2002-04-25 23:05:00 GMT.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/**

Name	**Df829.JPG**
Camera Model	**Canon Powershot G2**
Internal Object ID	**9866**
MD-5 Hash	**54941a5d04408303bd6768e0d9c5fd4b**
Width-Height	**640-480**

2. **Df876.JPG**

The photograph of the victim, **Sabrina Dewrcs** taken on 2002-05-14 18:02:35 GMT and modified on 2002-04-29 22:14:00 GMT.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/**

Name	**Df876.JPG**
Camera Model	**Canon Powershot G2**
Internal Object ID	**9948**
MD-5 Hash	**7ac4e43399bc91f20c7f8dcd483738b2**
Width-Height	**640-480**

3. Df826.JPG

The photograph of the **victim and suspect**, taken on 2002-05-14 18:02:36 GMT and modified on 2002-04-25 23:05:00 GMT.

Path**: /img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/**

Name	**Df826.JPG**
Camera Model	**Canon Powershot G2**
Internal Object ID	**9860**
MD-5 Hash	**3428d550b20e4c39df0b99c8425807d6**
Width-Height	**640-480**

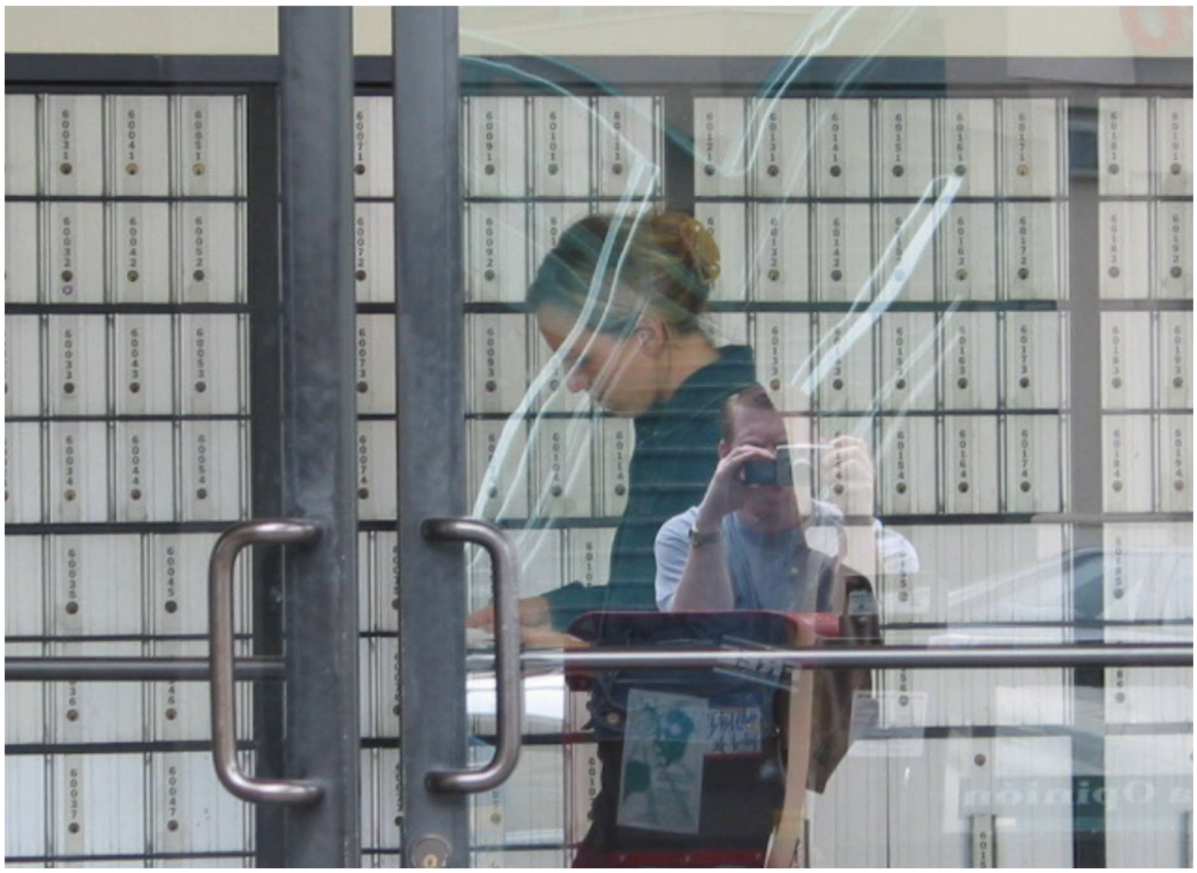
4. Df463.JPG

The photograph of the victims, **Sabrina Dewrcs and Christina Detsiwt** together taken on 2002-05-14 18:02:30 GMT and modified on 2002-04-25 23:06:00 GMT.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/**

Name	**Df463.JPG**
Camera Model	**Canon Powershot G2**
Internal Object ID	**9372**
MD-5 Hash	**fa64b24f10df62fb7c22241e75aa7929**
Width-Height	**640-480**

5. Df748.JPG



The photograph of the **suspect** taking picture of the **victim**, taken on 2002-05-14 18:02:12 GMT and modified on 2002-04-24 20:57:00 GMT.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/**

Name	**Df748.JPG**
Camera Model	**Canon Powershot G2**
Internal Object ID	**9737**
MD-5 Hash	**cec6f1262f2563db19574238c959d5f7**
Width-Height	**640-480**

6. Df384.JPG

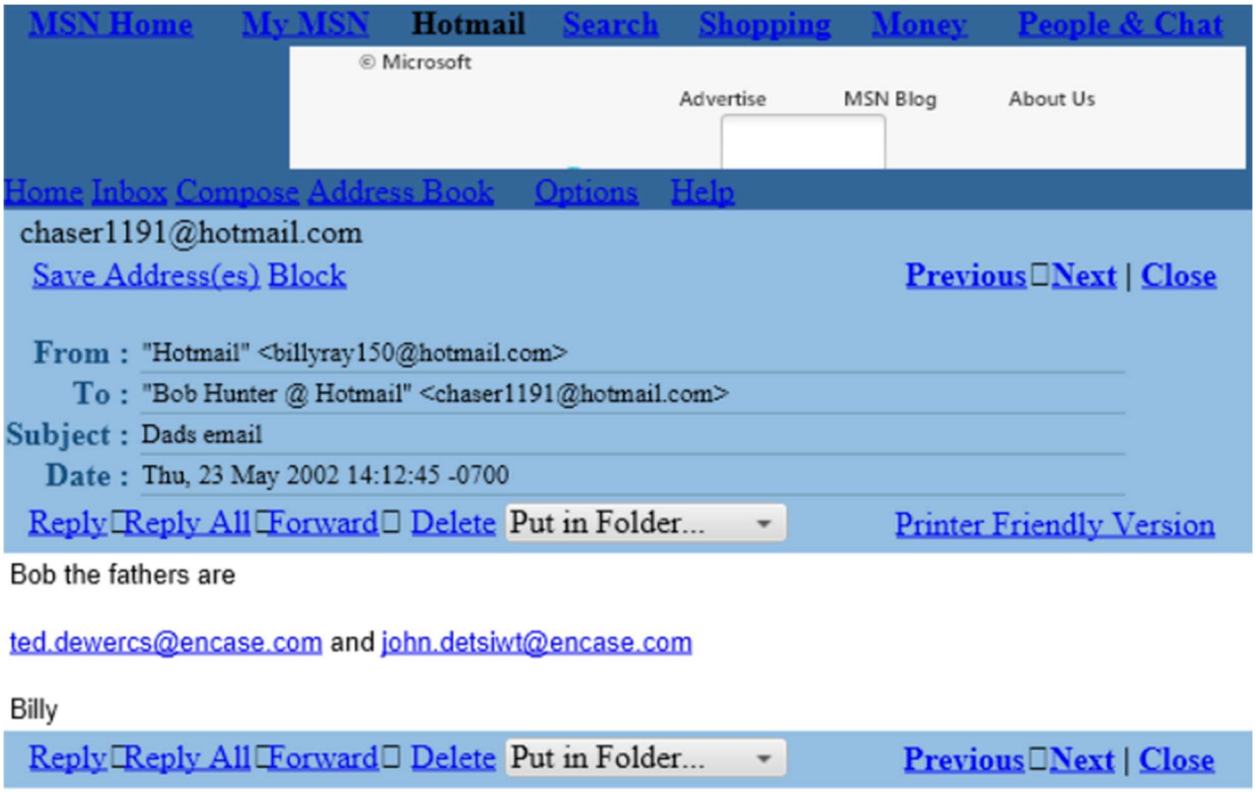
The photograph of the **suspect** taking picture of the **victim** inside the house, taken on 2002-05-14 18:02:27 GMT and modified on 2002-04-25 23:03:00 GMT.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/**

Name	**Df384.JPG**
Camera Model	**Canon Powershot G2**
Internal Object ID	**9240**
MD-5 Hash	**1ec7f4f7d3b4b071189fc5d6c9a181ab**
Width-Height	**640-480**

4.4 E-mails

1. getmsg [4].htm



In this Screenshot, we can see that **Billy Ray** used Hotmail to send information about the fathers of both **Sabrina** and **Christina** to suspect **Bob Hunter**.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/042WFPGU/getmsg [4].htm**

Created On	2002-06-04 23:42:55 GMT
Modified On	2002-06-04 23:42:56 GMT
SHA-256	c35bf65601381dfc40df3a558d1e961478d9bfdc3d02d270e27aa169c2f868f8
MD-5	d6b0d3119d7095d9908cb79ce8e8374c
Size	24807

2. getmsg [9].htm

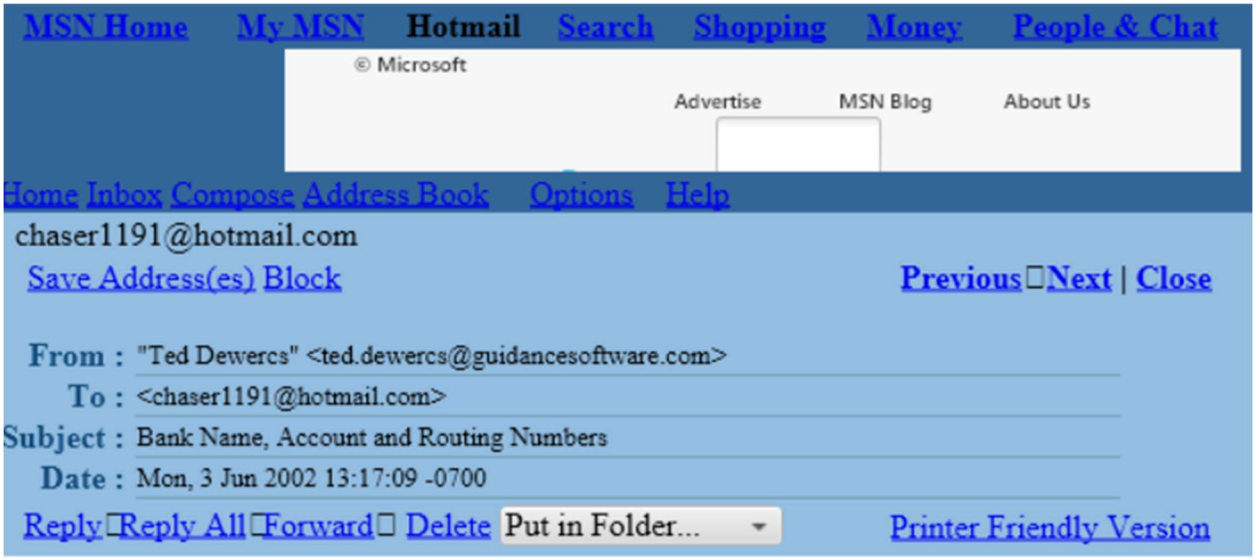
In this Screenshot, we can see that **Billy Ray** used Hotmail to send information about the threat given to father of both **Sabrina** to suspect **Bob Hunter**.

It is basically a forwarded mail to the Bob Hunter (chaser1191@hotmail.com).

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/6ZSJ6T6D/getmsg [9].htm**

Created On	2002-06-04 23:42:32 GMT
Modified On	2002-06-04 23:42:33 GMT
SHA-256	93f443cabfe3d4479ec274e8ad0e6e1f9ef48a46490dcf39d374ba1e3b5e4d45
MD-5	22ac9303494ba3239311f48352a74932
Size	2509

3. getmsg [5].htm



In this Screenshot, we can see that **Ted Dewercs** used Hotmail to reply back to **Hunter Bob** Hotmail account.

Ted didn't proceed with giving them his bank account details. Instead, he replied them back furiously.

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/042WFPGU/getmsg [5].htm

Created On	**2002-06-04 23:44:29 GMT**
Modified On	**2002-06-04 23:44:31 GMT**
SHA-256	**b4d557f06075640a88b1b7d3ec89e5a334a201a69238d3fafb22ccc0abd9ee72**
MD-5	**f15acdd11b55300b78919eeaa5c97bbc**
Size	**21052**

4. getmsg [3].htm


Hotmail® chaser1191@hotmail.com

Inbox | Previous Page

From : "John Detsiwt" <John.Detsiwt@guidancesoftware.com>
To : <chaser1191@hotmail.com>
Subject : Bank Name, Account and Routing Numbers
Date : Mon, 3 Jun 2002 13:12:02 -0700

Bank of America
14921-24927
294812918

Please don't hurt her!

In this Screenshot, we can see that **John Detsiwt** used Hotmail to reply back to **Hunter Bob** Hotmail account.

John proceeded with giving them his bank account details.

Details:

Bank of America

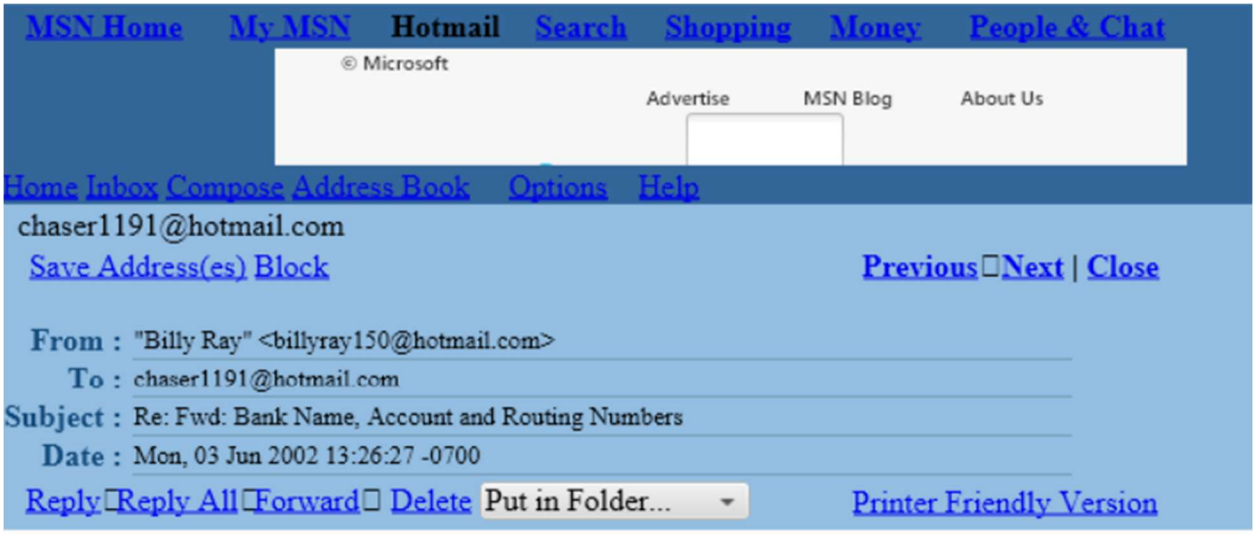
14921-24927

294812918

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/042WFPGU/getmsg [3].htm

Created On	**2002-06-03 20:17:39 GMT**
Modified On	**2002-06-03 20:17:40 GMT**
SHA-256	**a9f0ad9ac2deb07e729613c5074b7c8f88984346444c34d3581fec6ca91fa32b**
MD-5	**bd000ceb79c7d4d5e0318791d4aaf8a0**
Size	**4474**

5. getmsg [10].htm



> From: "IC YOU" <chaser1191@hotmail.com>
> To: billyray150@hotmail.com
> Subject: Fwd: Bank Name, Account and Routing Numbers
> Date: Mon, 03 Jun 2002 15:23:09 -0500
>
> Check this clown out, we need to do something
>
> > From: "Ted Dewercs" <ted.dewercs@guidancesoftware.com>
> > To: <chaser1191@hotmail.com>
> > Subject: Bank Name, Account and Routing Numbers
> > Date: Mon, 3 Jun 2002 13:17:09 -0700
> >
> > What is this, some sort of joke? Who are you??

In this Screenshot, we can see that **Billy Ray** used Hotmail to send information about the threat given to father of both **Sabrina** to suspect **Bob Hunter**.

Basically, in this screenshot, they are mocking the reply of **father of Sabrina**.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/6ZSJ6T6D/getmsg [10].htm**

Created On	**2002-06-04 23:43:50 GMT**
Modified On	**2002-06-04 23:43:52 GMT**
SHA-256	**ee4c1ea0053599e7d99f5ef39d0e48401f08c43899892adab66c71d923de6b7b**
MD-5	80099a52567b3fe6fcd467704dfd87e0
Size	**25444**

4.5 Internet Browsing History

1. f0004544.html

bsp;

STALKERS
... **STALKING** THE STARS by Bill Kelly. Most of us are satisfied with an autographed photo of our favorite Hollywood personality – if we are lucky enough to obtain ...
Description: A history of celebrity **stalking** in Hollywood.
Category: Society > Crime > Prevention > Stalking
crimemagazine.com/stalkers.htm - 41k - Cached - Similar pages

The Bread Bakers Guild of America: **Stalking** the World-Wide ...
Stalking the World-Wide Breads. "...I once ate a dishonest loaf. It was good, but afterward I felt so used." ...Thomas Pickett. ...
Description: International and special diet recipes, tips and tricks. Also offers many articles on baking.
Category: Home > Cooking > Baking and Confections > Breads
www.bbga.org/breads.html - 28k - Cached - Similar pages

Justice Information Center (NCJRS): Victims **Stalking**
Victims. **STALKING**. Documents. Are You Being Stalked? Tips for Protection http://www ...
www.ncjrs.org/victstlk.htm - 4k - Cached - Similar pages
[More results from www.ncjrs.org]

Cyberstalking & Harassment
Safetyed runs a cyber **stalking** department and we have long experience in assisting and advising targets of online harassment. Colin Gabriel Hatcher, SafetyEd's ...
Description: Information from the cyberstalking department at SafetyEd International. General information, advice,...
Category: Computers > Internet > Abuse > Cyberstalking
www.safetyed.org/help/stalking/ - 4k - Cached - Similar pages

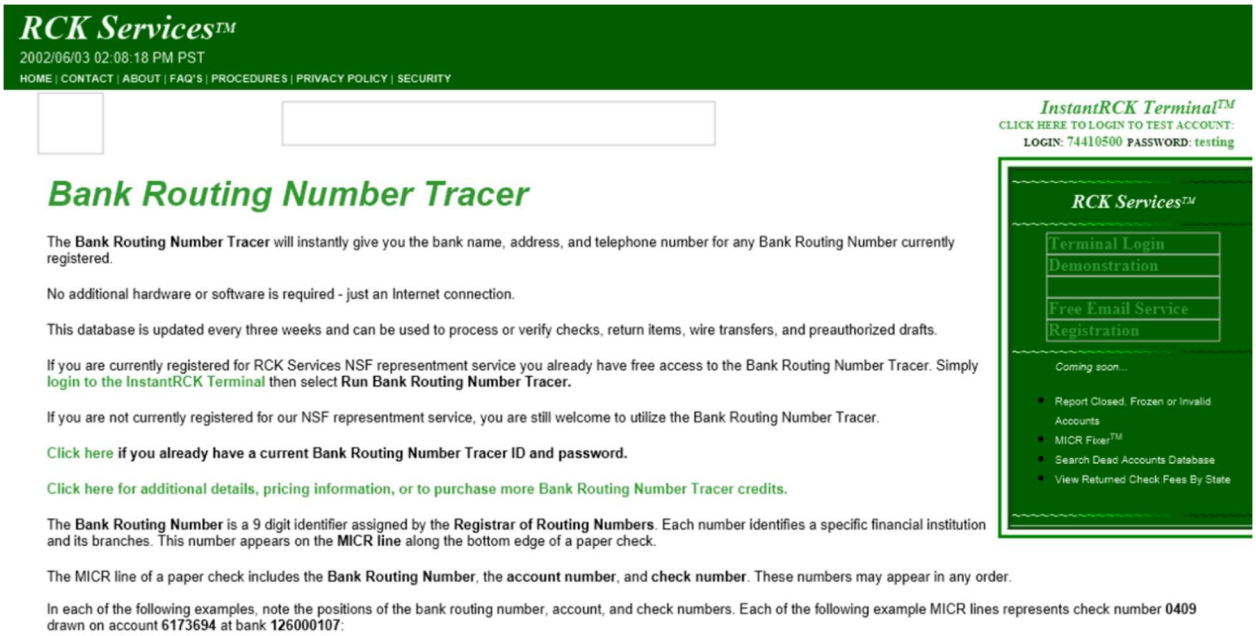
Stalking The Deadly Hantavirus: A Study In Teamwork
Stalking The Deadly Hantavirus: A Study In Teamwork.
KAREN YOUNG KREEGER. Excerpted from: The ...
Description: A look at the discovery of the newest Hantavirus.
Category: Health > Conditions and Diseases > ... > Viral > Hemorrhagic Fevers > Hantavirus
www.bocklabs.wisc.edu/ed/newhant1.html - 15k - Cached - Similar pages

While exploring internet browsing history, Bob Hunter searched something related to Stalking which is also seen in this screenshot.

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/$CarvedFiles/1/f0004544.html

Created On	**0000-00-00 00:00:00**
Modified On	**0000-00-00 00:00:00**
SHA-256	**0ee489b9baca9dc9b7e83c54e0234e05bc30c38f7dfcf1a193191a871ad444d0**
MD-5	**b26216e8a266f48525409c24762ddda5**
Size	**11207**

2. abatrace [1].htm



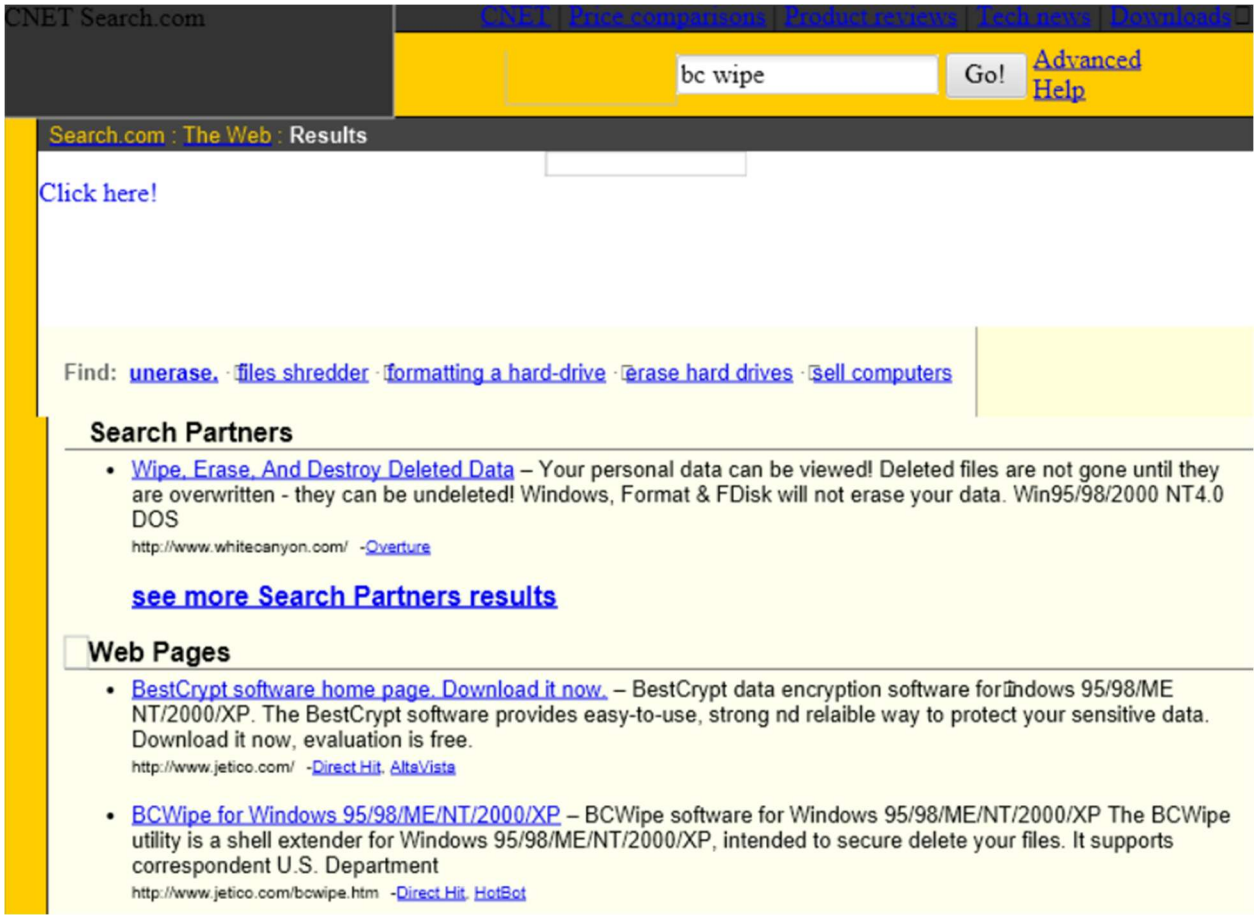
While exploring internet browsing history, Bob Hunter searched way to trace **Banking Routing Number**.

He visited **RCK Services**.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/UFK38B83/abatrace[1].htm**

Created On	**2002-06-03 21:11:19 GMT**
Modified On	**2002-06-03 21:11:20 GMT**
SHA-256	**2537116080838d41d13de6d27d88a49073449221314b58d415078f46e37391f6**
MD-5	**feed989d407f697c3603ab869085d46e**
Size	**18844**

3. f0004740_Search_com_bc_wipe.html



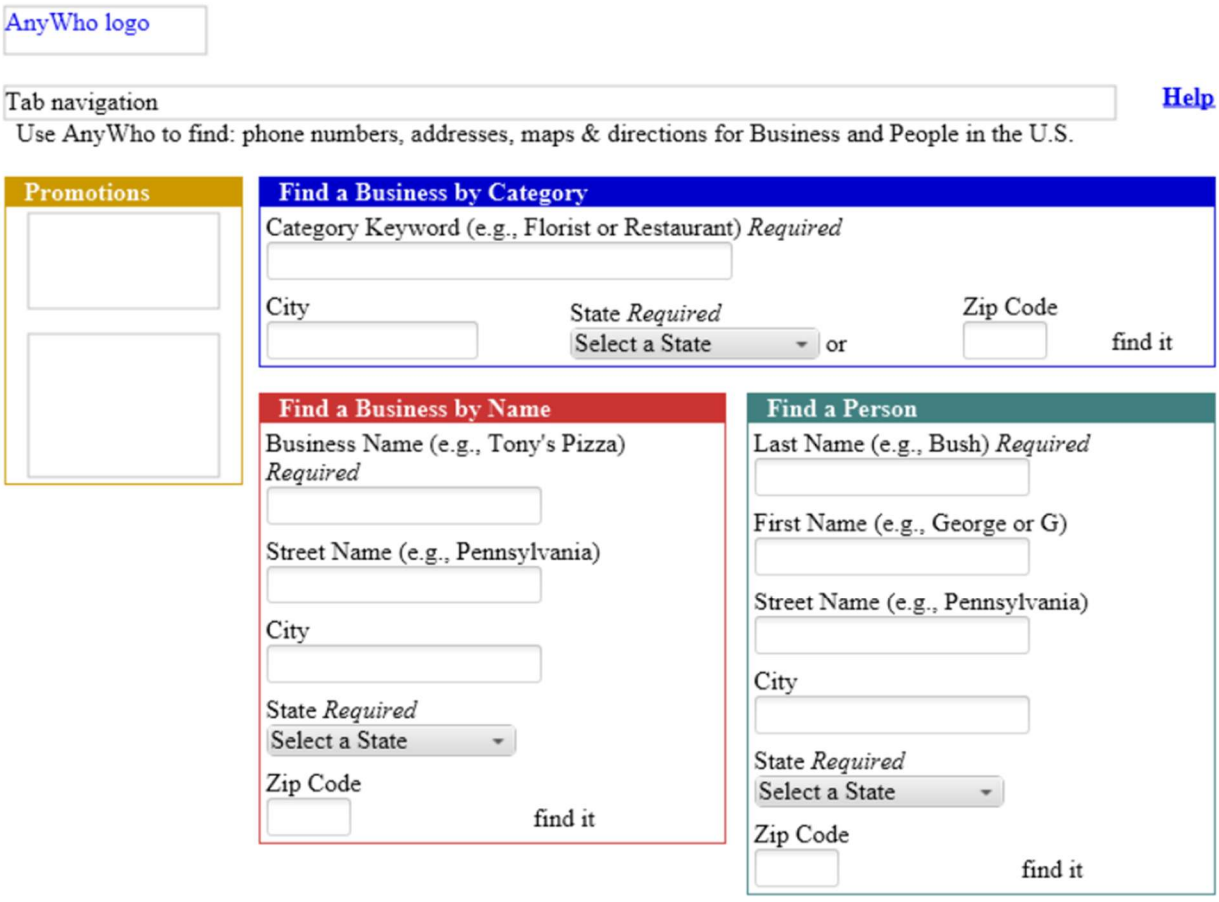
While exploring internet browsing history, Bob Hunter searched about **BC Wipe**.

BC Wipe is an anti-forensic tool used for wiping all the data way permanently.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/$CarvedFiles/1/f0004740_Search_com_bc_wipe.html**

Created On	**0000-00-00 00:00:00**
Modified On	**0000-00-00 00:00:00**
SHA-256	**448a242b6baa5d31c0388c126ce8e83336dd3f6d4da81964365c9a4ae7522fda**
MD-5	**ade4e1d441aa7b906ce2cba729981db0**
Size	**14336**

4. f0000768_AnyWho_Internet_Directory_Assistance_Yellow_Pages_White_Pages_Toll_Free_Numbers_Maps_and_Directions.html



While exploring internet browsing history, Bob Hunter searched about **AnyWho**.

AnyWho is a web service which gives detailed information about anyone who is registered within the nation.

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/$CarvedFiles/1/f0000768_AnyWho_Internet_Directory_Assistance_Yellow_Pages_White_Pages_Toll_Free_Numbers_Maps_and_Directions.html**

Created On	**0000-00-00 00:00:00**
Modified On	**0000-00-00 00:00:00**
SHA-256	**d3d3bf2f8e4444183b83e11b2fe47e7fb251cca5bcb2e0167357f028e2efc20e**
MD-5	**2033b4cd5931a43a3de9d4df069b90ac**
Size	**22649**

5. **xyz [1].htm**

While exploring internet browsing history, Bob Hunter searched about **Criminal Defense**.

More precisely, He visited:

Criminal Defense Juvenile Crimes

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/8XGPQD6L/xyz[1].htm

Created On	**2002-06-03 18:08:28 GMT**
Modified On	**2002-06-03 18:08:29 GMT**
SHA-256	**9e38fe0e2623993dfd961082f67603cfa9c4b6728415db8230b94b08758feb47**
MD-5	**0a03ec269fc46dc104a4575704344574**
Size	**26239**

6. f0000000_The_Stalker_s_Home_Page_No_More_Privacy_As_Seen_on_the_LEEZA_ShowIs_Big_Brother_Watching.html

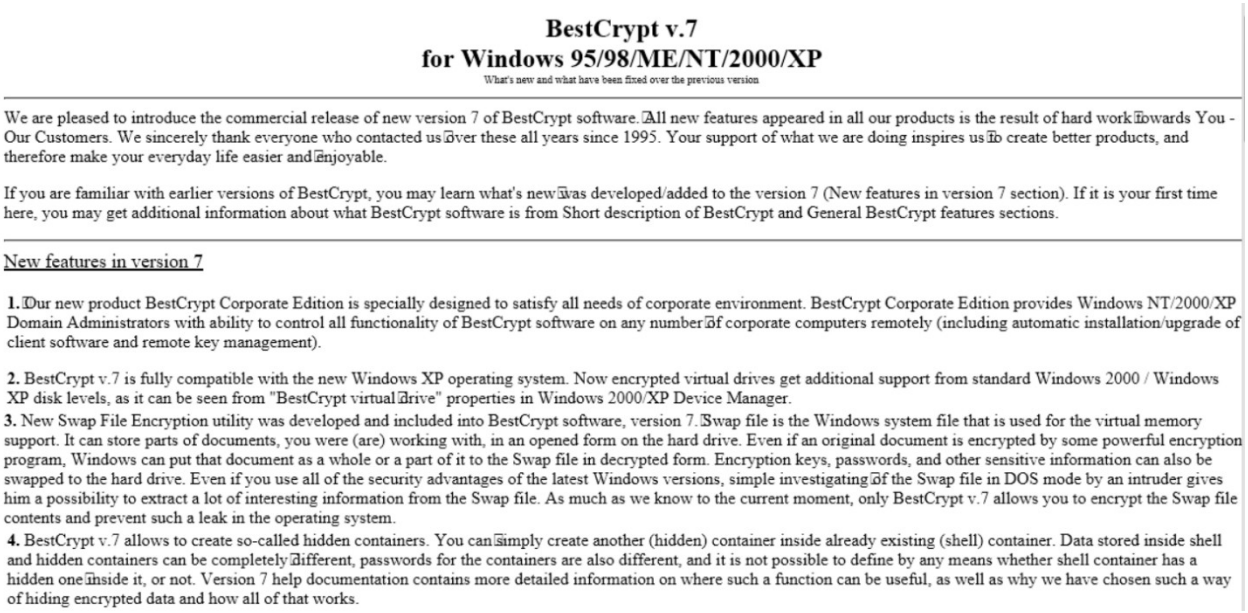
While exploring internet browsing history, Bob Hunter visited **The Stalker's Home Page**.

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/$CarvedFiles/1/f0000000_The_Stalker_s_Home_Page_No_More_Privacy_As_Seen_on_the_LEEZA_ShowIs_Big_Brother_Watching.html

Created On	**0000-00-00 00:00:00**
Modified On	**0000-00-00 00:00:00**
SHA-256	**7865a22837b4f6112ee18dbd99cc9e8e70a37472d449442598d8d10e0e2681fe**
MD-5	**ca2308cae91a8d9fd7a180420b02ab6f**
Size	**8192**

4.6 Use of Anti-Forensic and Encryption Tools

1. bcrypt7[2].htm



BestCrypt v.7
for Windows 95/98/ME/NT/2000/XP
What's new and what have been fixed over the previous version

We are pleased to introduce the commercial release of new version 7 of BestCrypt software. All new features appeared in all our products is the result of hard work towards You - Our Customers. We sincerely thank everyone who contacted us over these all years since 1995. Your support of what we are doing inspires us to create better products, and therefore make your everyday life easier and enjoyable.

If you are familiar with earlier versions of BestCrypt, you may learn what's new was developed/added to the version 7 (New features in version 7 section). If it is your first time here, you may get additional information about what BestCrypt software is from Short description of BestCrypt and General BestCrypt features sections.

New features in version 7

1. Our new product BestCrypt Corporate Edition is specially designed to satisfy all needs of corporate environment. BestCrypt Corporate Edition provides Windows NT/2000/XP Domain Administrators with ability to control all functionality of BestCrypt software on any number of corporate computers remotely (including automatic installation/upgrade of client software and remote key management).

2. BestCrypt v.7 is fully compatible with the new Windows XP operating system. Now encrypted virtual drives get additional support from standard Windows 2000 / Windows XP disk levels, as it can be seen from "BestCrypt virtual drive" properties in Windows 2000/XP Device Manager.

3. New Swap File Encryption utility was developed and included into BestCrypt software, version 7. Swap file is the Windows system file that is used for the virtual memory support. It can store parts of documents, you were (are) working with, in an opened form on the hard drive. Even if an original document is encrypted by some powerful encryption program, Windows can put that document as a whole or a part of it to the Swap file in decrypted form. Encryption keys, passwords, and other sensitive information can also be swapped to the hard drive. Even if you use all of the security advantages of the latest Windows versions, simple investigating of the Swap file in DOS mode by an intruder gives him a possibility to extract a lot of interesting information from the Swap file. As much as we know to the current moment, only BestCrypt v.7 allows you to encrypt the Swap file contents and prevent such a leak in the operating system.

4. BestCrypt v.7 allows to create so-called hidden containers. You can simply create another (hidden) container inside already existing (shell) container. Data stored inside shell and hidden containers can be completely different, passwords for the containers are also different, and it is not possible to define by any means whether shell container has a hidden one inside it, or not. Version 7 help documentation contains more detailed information on where such a function can be useful, as well as why we have chosen such a way of hiding encrypted data and how all of that works.

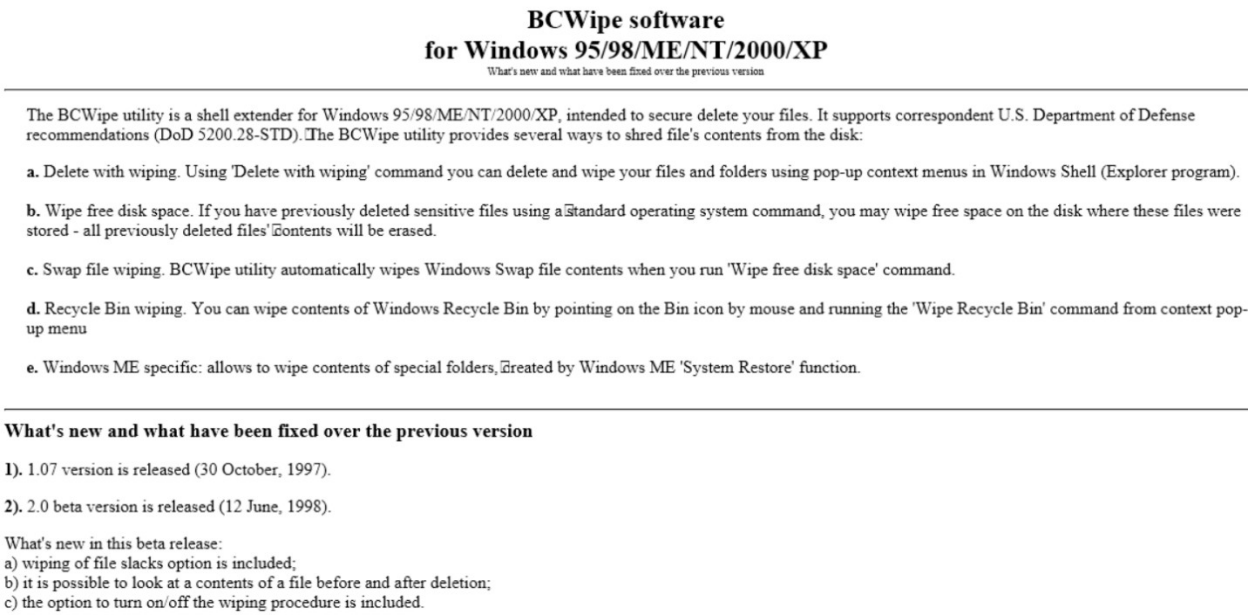
BestCrypt V.7 was installed in this PC.

BestCrypt is an anti-forensic tool used for securing data using passwords or any other type of encryption.

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/8XGPQD6L/bcrypt7[2].htm

Created On	**2002-06-05 00:21:46 GMT**
Modified On	**2002-06-05 00:21:46 GMT**
SHA-256	**2579ca9853bed672caf38bc5234960f060e7757675c80b272372eeb4468ad8e2**
MD-5	**afdb3a304ffcdb1314b78201ff6a4104**
Size	**16244**

2. bcwipe [1].htm



BCWipe software
for Windows 95/98/ME/NT/2000/XP
What's new and what have been fixed over the previous version

The BCWipe utility is a shell extender for Windows 95/98/ME/NT/2000/XP, intended to secure delete your files. It supports correspondent U.S. Department of Defense recommendations (DoD 5200.28-STD). The BCWipe utility provides several ways to shred file's contents from the disk:

a. Delete with wiping. Using 'Delete with wiping' command you can delete and wipe your files and folders using pop-up context menus in Windows Shell (Explorer program).

b. Wipe free disk space. If you have previously deleted sensitive files using a standard operating system command, you may wipe free space on the disk where these files were stored - all previously deleted files' contents will be erased.

c. Swap file wiping. BCWipe utility automatically wipes Windows Swap file contents when you run 'Wipe free disk space' command.

d. Recycle Bin wiping. You can wipe contents of Windows Recycle Bin by pointing on the Bin icon by mouse and running the 'Wipe Recycle Bin' command from context pop-up menu

e. Windows ME specific: allows to wipe contents of special folders, created by Windows ME 'System Restore' function.

What's new and what have been fixed over the previous version

1). 1.07 version is released (30 October, 1997).

2). 2.0 beta version is released (12 June, 1998).

What's new in this beta release:
a) wiping of file slacks option is included;
b) it is possible to look at a contents of a file before and after deletion;
c) the option to turn on/off the wiping procedure is included.

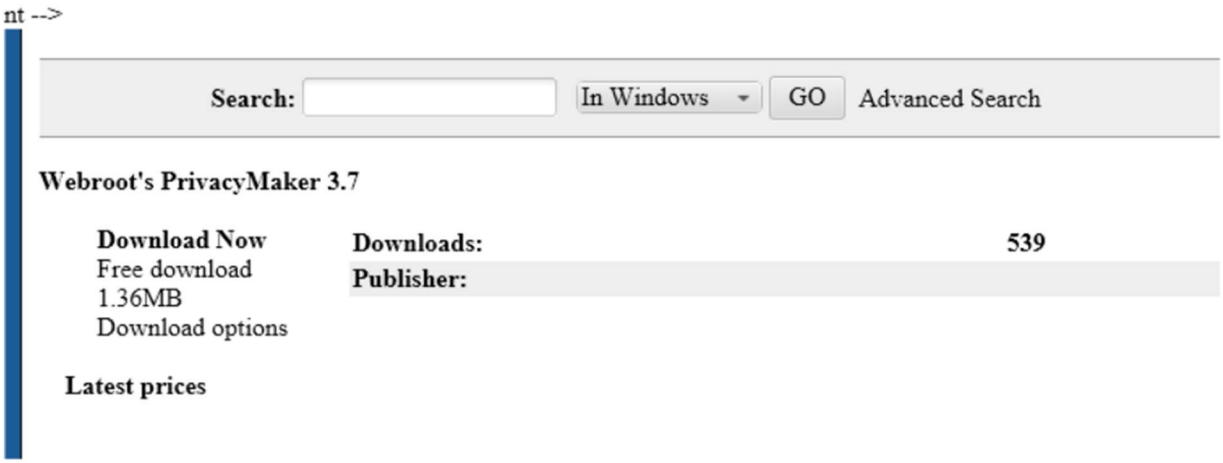
BCWipe was installed in this PC.

BCWipe is an anti-forensic tool used for permanently deleting files which can frustrate forensic investigation.

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/8XGPQD6L/bcwipe[1].htm

Created On	**2002-06-05 00:15:37 GMT**
Modified On	**2002-06-05 00:15:37 GMT**
SHA-256	**97a0e03b202bd8d53b2e1c629f683416b9104aa8803195925108da07f5294188**
MD-5	**db92bcfd8f6a8e14cb138acdbb084c68**
Size	**6273**

3. f0002800.html



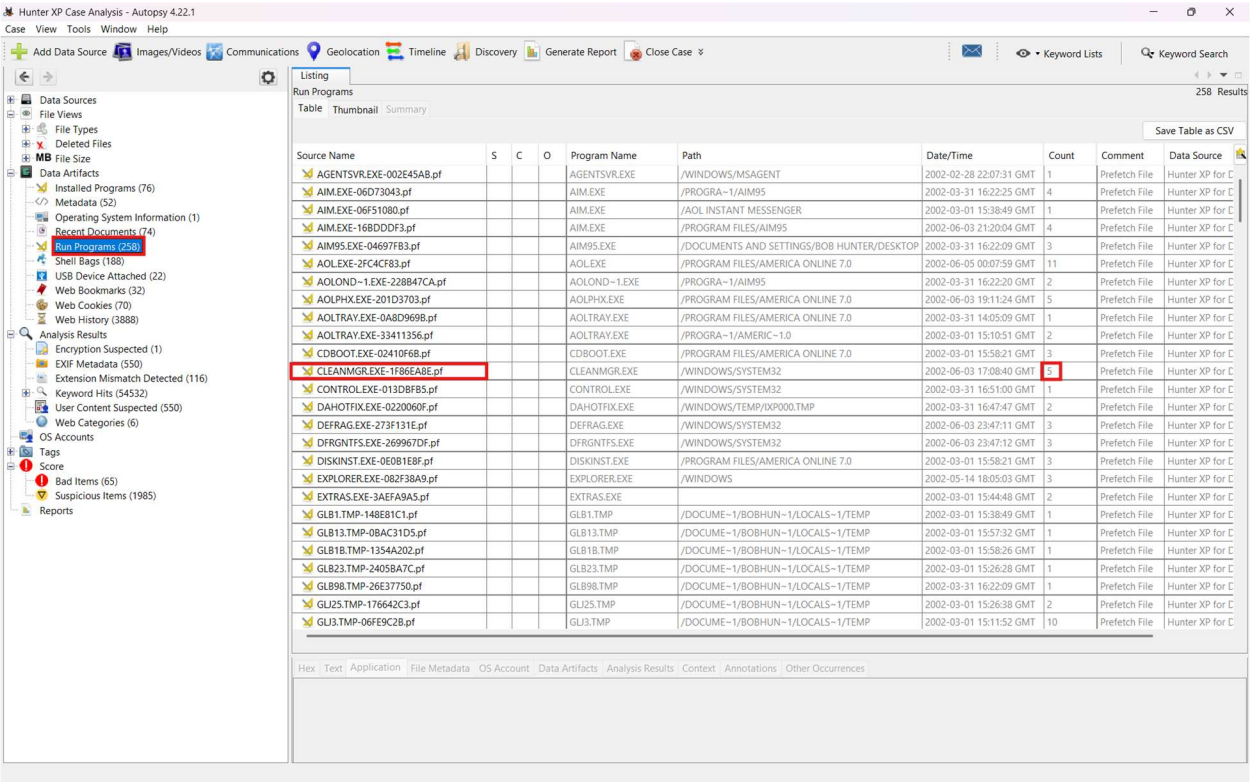
Webroot's PrivacyMaker 3.7 was searched in this PC.

Webroot's PrivacyMaker 3.7 is an anti-forensic tool used for protecting passwords, cookies and all information's related to website accessed or logged in.

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/$CarvedFiles/1/f0002800.html

Created On	**0000-00-00 00:00:00**
Modified On	**0000-00-00 00:00:00**
SHA-256	**f2d7924345f3392b33aaa5e77a59203169b3d3a098dc95904846a1e4c82eac67**
MD-5	**278aead0ac6f08d16b69e8efe46e5c51**
Size	**6144**

4. CLEANMGR.EXE



CLEANMGR was installed in this PC.

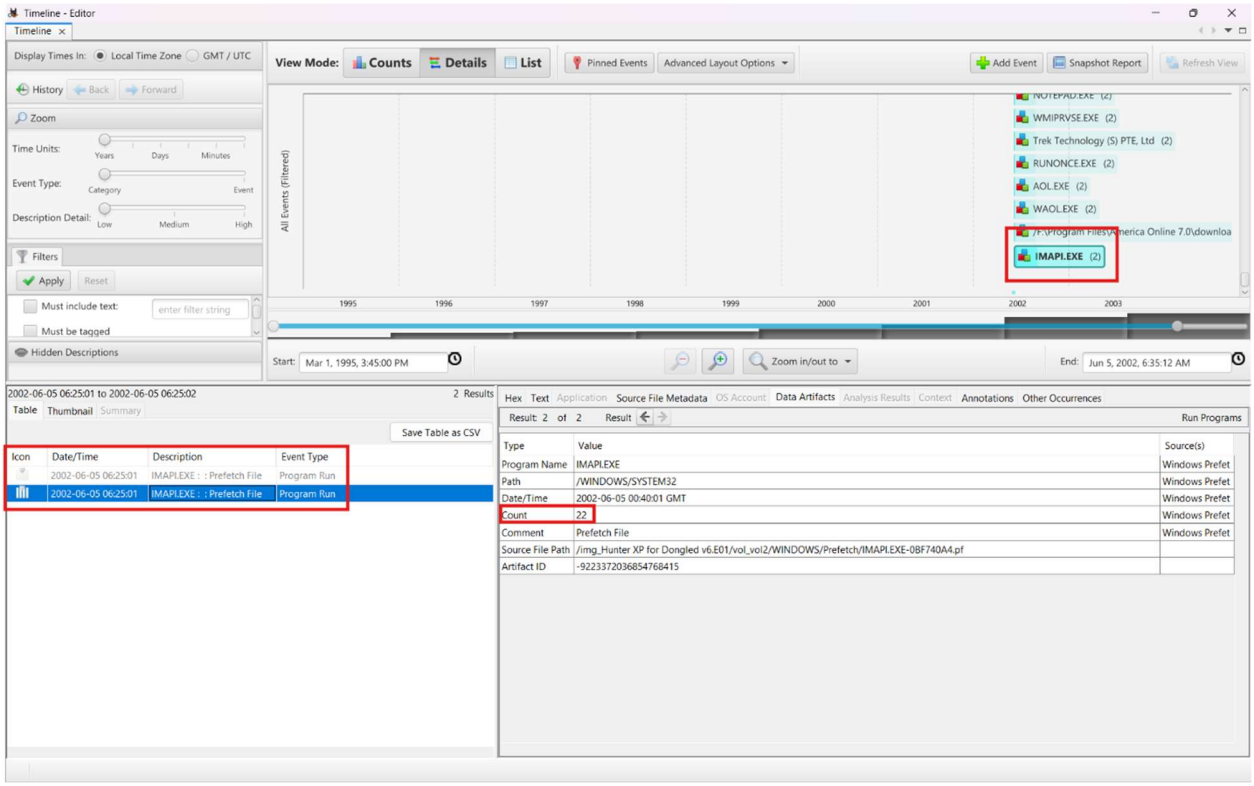
CLEANMGR is an anti-forensic tool used for permanently deleting files which can frustrate forensic investigation.

Run Count: 5

Path: **/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/Prefetch/CLEANMGR.EXE-1F86EA8E.pf**

Created On	**2002-03-31 16:48:26 GMT**
Modified On	**2002-06-03 17:08:44 GMT**
SHA-256	**884581440fc05570c28aeac18b276a17691c8703ebd0a19fd167bf23c64a9a2b**
MD-5	**5860a113b3e1b5fcb3c5fd9f35e2e0f7**
Size	**45730**

5. IMAPI.EXE



IMAPI.EXE was installed in this PC.

IMAPI.EXE is an anti-forensic tool used for permanently deleting files which can frustrate forensic investigation. It was also last run programme in this pc.

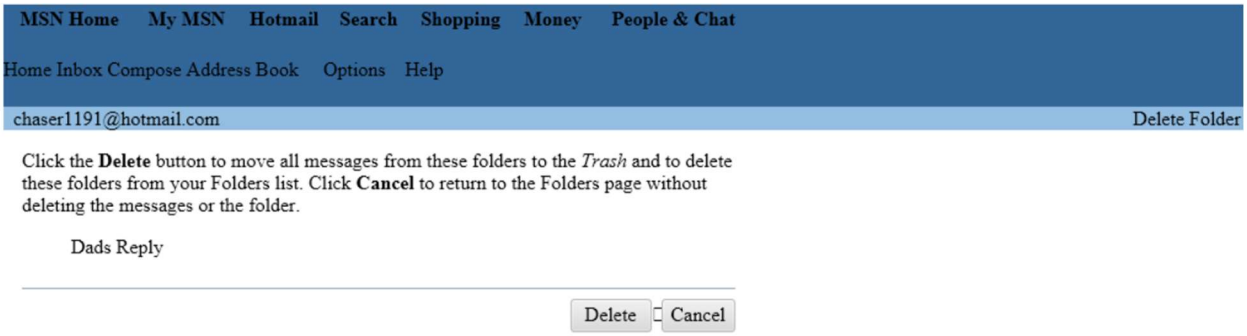
Run Count: 2

Path: /img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/Prefetch/IMAPI.EXE-0BF740A4.pf

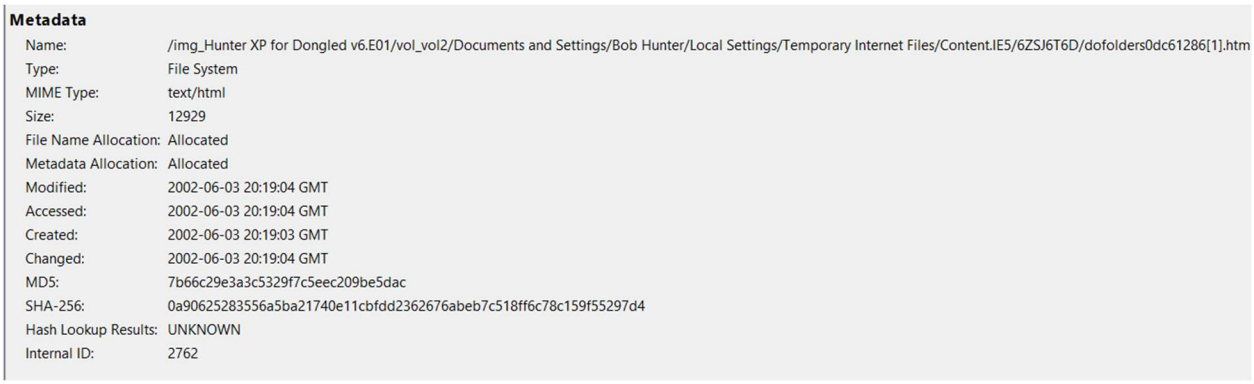
Created On	**2002-02-28 22:24:19 GMT**
Modified On	**2002-06-05 00:40:07 GMT**
SHA-256	**7337b08f811c3ecea35ae870d5fb7353f714c753806a4863854b9e59991be5b4**
MD-5	**0b4a4eb2c3ae3bf4c6503d0d52185b91**
Size	**9900**

5.More Relevant Evidences

1. dofolders0dc61286[1].htm



We can clearly see that, Bob Hunter tried erasing the fathers mail from the Hotmail.



2. memopad.bak

PM#F:\Palm\HunterB\memopad\memopad.dat
0 6 0 0 1 OOOOOOX
Business
Business
Personal
Personal@
+AOL
s/name: chaser1191@aol
p/w: bigjake
Billy
I followed Kim and her friend. I think her friends name is Sabrina. We need to decide how to proceed. We need to be careful. We don't need the police involved
.Hotmail
chaser1191@hotmail.com
p/w: bigjake
-Yahoo information
bob_hunter1191 p/w bigjake
)AIM Information
chaser1191 p/w bigjake
bX Drive
chaser1191@hotmail.com
1191
http://plus.xdrive.com/XDRequestDispatcher?action=OpenLogin
Bill
I am leaving soon so I thought I would jot this note down to send later. I will be flying to LA to confirm the work address and find and confirm the friends name. I want to be able to send the information to the family so on. I agree that 500,000 is a good amount to start out with.
I think the daughters safety is worth that don't you?
I can't believe that they did not even know that it was us taking the photos. She even talked to me once.
I will let you know as soon as I learn anything.

Here, we can see that Bob Hunter is threating and talking about ransom. Billy Ray and Bob Hunter also had conversations about their plan.

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/memopad/memopad.bak
Type:	File System
MIME Type:	application/octet-stream
Size:	1467
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2002-05-14 19:13:29 GMT
Accessed:	2002-05-14 19:13:29 GMT
Created:	2002-05-14 19:02:46 GMT
Changed:	2002-05-14 19:13:29 GMT
MD5:	09b75ffa6b31fb769431832e03af82f8
SHA-256:	eefe64b6da96e52c0a24505330085885e1b48f5edcfac4a3799bba649a248f6f
Hash Lookup Results:	UNKNOWN
Internal ID:	10215

3. todo.bak

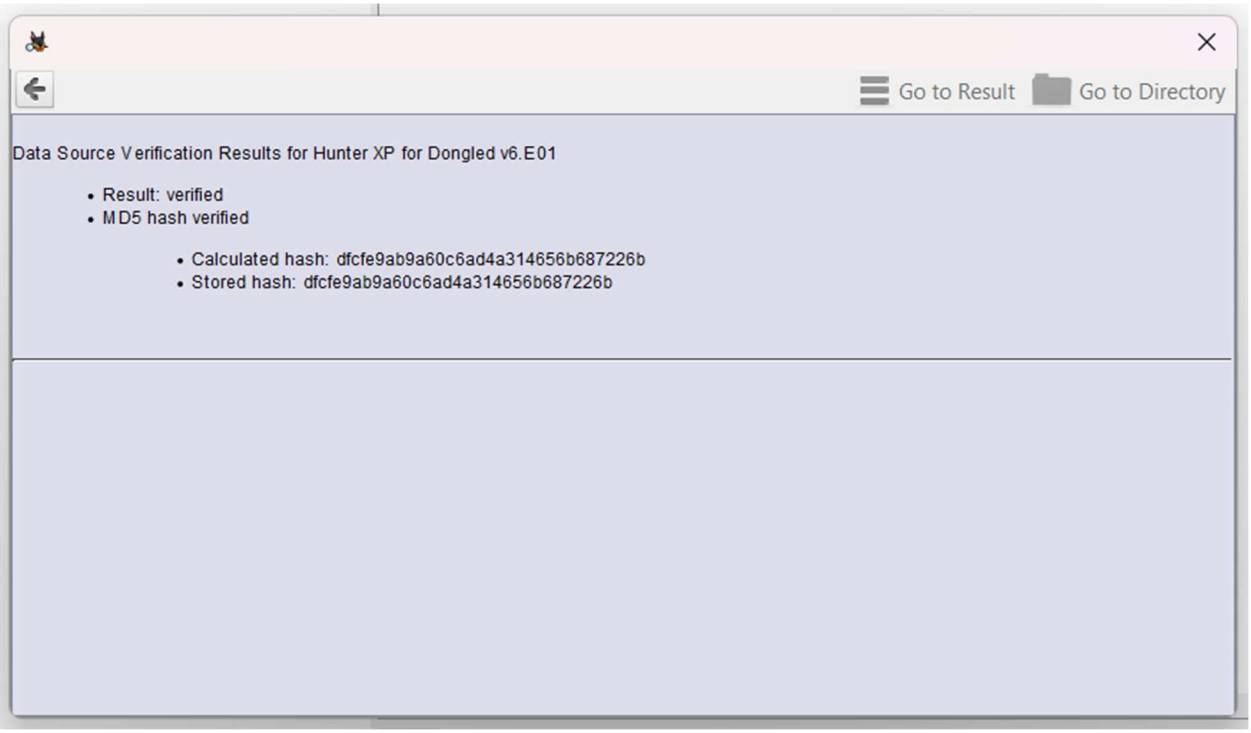
```
F:\Palm\HunterB\todo\todo.dat
16 0 0 1 1 0 0 0 0 0 0 XOO
Business
Business
Personal
Personal,
"Send Kim's information to Billyray
Setup bank accout
'Check the green street address billy
```

Here, we can see that Bob Hunter is talking about Kim's information and banking details also.

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/todo/todo.bak
Type:	File System
MIME Type:	application/octet-stream
Size:	511
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2002-05-14 19:13:29 GMT
Accessed:	2002-05-14 19:13:29 GMT
Created:	2002-05-14 19:02:45 GMT
Changed:	2002-05-14 19:13:29 GMT
MD5:	2f8c56df2f43687a58beefad17423dd9
SHA-256:	2630fec95f40181afdb2007e46bf131dcbe423d01196756878e1386ee93ae59d
Hash Lookup Results:	UNKNOWN
Internal ID:	10227

Hash Analysis through Autopsy



Here, as you can see no data has been tempered.

6.Conclusion

The forensic examination revealed the following key findings:

The evidence points to this being a case of stalking and extortion. The criminals of these crimes were identified as Bob Hunter and Billy Ray, while the victims include Sabrina Dewercs, Christina Detsiwt, Teddy Dewercs, and John Detsiwt.

Hunter and Ray engaged in stalking Sabrina and Christina, covertly photographing them without consent using a Canon PowerShot G2 digital camera. These photographs were used to threaten their fathers, John Detsiwt and Ted Dewercs, as part of an extortion scheme.

Further investigation revealed that Hunter and Ray had been researching legal professionals and gathering stalking-related information. Their computer also contained anti-forensic tools, encryption software, and digital data-wiping utilities, underscoring their intent to conceal evidence.

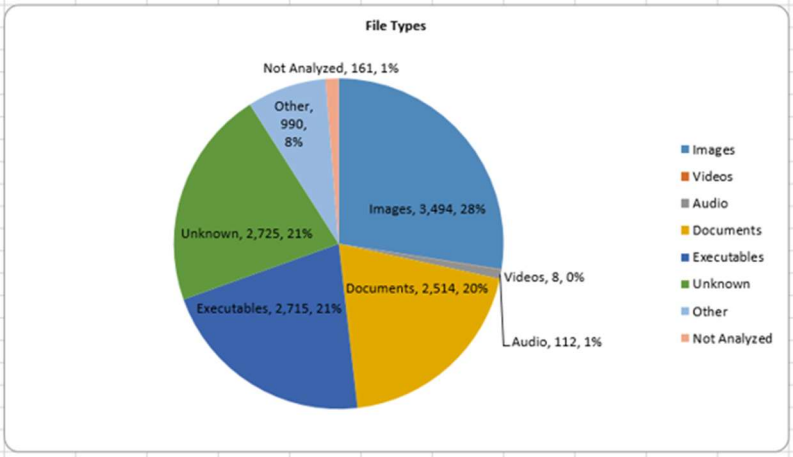
All findings are based on evidence analyzed and validated using industry-standard forensic tools. Conclusions are objective and do not infer guilt or innocence.

7.Appendix of Supporting Exhibits

Using Autopsy we have appendix data source summary.

Usage	OS Drive (Microsoft Windows XP)
OS	Microsoft Windows XP
Size	4.10 GB

File Types	**Count**
Images	3,494
Videos	8
Audio	112
Documents	2,514
Executables	2,715
Unknown	2,725
Other	990
Not Analyzed	161



Allocated Files	11,806
Unallocated Files	913
Slack Files	8,366
Directories	2,405