Anish Adhikari

Report Writing

Component B - Individual Work - Report

Document Details

Submission ID
trn:oid:::26687:125312353

Submission Date
Dec 29, 2025, 3:06 PM GMT+5:45

Download Date
Dec 29, 2025, 3:08 PM GMT+5:45

File Name
Report Writing.docx

File Size
3.2 MB

33 Pages

2,732 Words

16,763 Characters

12% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

37 Not Cited or Quoted 12%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

1 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

2% Internet sources
0% Publications
12% Submitted works (Student Papers)

Match Groups

- **37** Not Cited or Quoted 12%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **1** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

2% Internet sources
0% Publications
12% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Student papers	
Griffth University on 2024-10-20		2%
2	Student papers	
University of Technology, Sydney on 2025-05-23		1%
3	Student papers	
University of Technology, Sydney on 2025-06-04		<1%
4	Student papers	
Kaplan International Colleges on 2021-07-23		<1%
5	Student papers	
University of Technology, Sydney on 2023-06-10		<1%
6	Student papers	
University of Technology, Sydney on 2020-06-25		<1%
7	Student papers	
University of Warwick on 2025-12-22		<1%
8	Student papers	
Edith Cowan University on 2025-09-05		<1%
9	Student papers	
University of Technology, Sydney on 2021-06-03		<1%
10	Student papers	
Murdoch University on 2025-01-07		<1%

11	Student papers	
Kaplan International Colleges on 2025-07-13		<1%
12	Student papers	
Kaplan International Colleges on 2023-04-03		<1%
13	Student papers	
Kaplan International Colleges on 2024-04-14		<1%
14	Student papers	
Pennsylvania State System of Higher Education on 2022-04-12		<1%
15	Student papers	
University of Technology, Sydney on 2025-06-04		<1%
16	Internet	
acikbilim.yok.gov.tr		<1%
17	Student papers	
Pennsylvania State System of Higher Education on 2019-10-04		<1%
18	Student papers	
Taylor's Education Group on 2013-07-04		<1%
19	Student papers	
George Mason University on 2025-07-10		<1%
20	Student papers	
Massey University on 2011-06-23		<1%
21	Student papers	
University of Technology, Sydney on 2025-06-02		<1%
22	Student papers	
Edith Cowan University on 2025-10-27		<1%
23	Student papers	
University of Technology, Sydney on 2025-05-31		<1%
24	Student papers	
Dundee and Angus College on 2023-05-10		<1%

25 Student papers

University of Technology, Sydney on 2024-05-31 <1%

26 Student papers

uwe on 2022-07-26 <1%

Cyber Crime and Digital Evidence

Report Writing

Submitted by:

Full Name: Anish Adhikari

Orbund ID : 11147

Student ID : 24071101

Kathmandu, Nepal

TABLE OF CONTENTS

1. Introduction

1.1 Case Overview and Request

21

This report summarizes the conclusion of a forensic analysis on case evidence of Bob Hunter, user of Hunter XP disk image. As per the request of University of the West of England (UWE), I examined the suspect's computer looking for the signs of criminal activities or any misconduct.

The evidential media in this case was Hunter XP disk image which possibly consisted of digital footprints confirming the usage of the system. The goal was to confirm the offences via the system based on the digital artifacts.

1.2 Analyst's Relevant Experience

The report along with the examination was prepared by Anish Adhikari, studying for a bachelor's degree in Cybersecurity and Digital Forensics. Despite being part of academic coursework, this analysis strictly followed the procedure of digital forensics with standard reporting.

Furthermore, the analyst has formal training in evidence handling, file system analysis, timeline reconstruction, as well as handling professional forensics tools.

2. Evidence Summary

2.1 Description of Digital Evidence Items

11 The digital evidence examined in this case consisted of a forensic disk image named “Hunter XP for Dongled v6.E01”. The image represents a system running the Microsoft Windows XP operating system and was provided in EnCase Evidence File (.E01) format.

Fig 2.1.1 : Hunter Xp Image file

2.2 Unique Identifiers

In the initial phase of investigation, cryptographic hash verification was practiced so that the investigation evidence remained authentic. After generating the MD5 hash value of evidence file it got verified in Autopsy before any analysis then after completion of analysis, the value was recalculated reusing the same tool and comparing with original hash value.

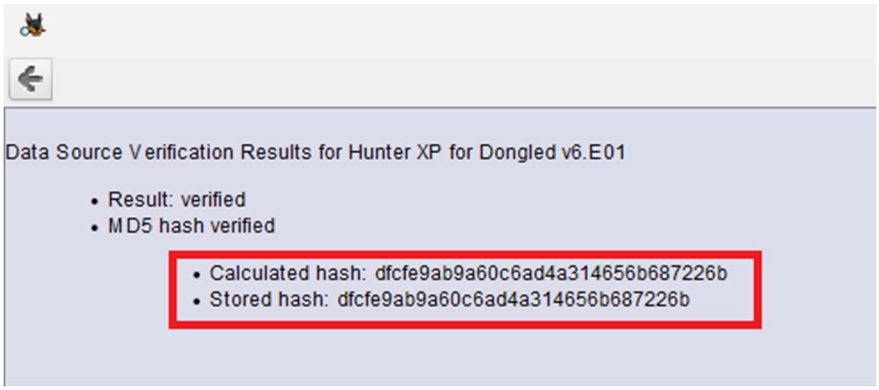

Fig 2.2.1: MD5 verified Hash Value

26 MD5 hash value: **dfcfe9ab9a60c6ad4a314656b687226b**

MD5 verified hash value: **dfcfe9ab9a60c6ad4a314656b687226b**

The matching hash values obtained before and after the investigation confirmed that the evidence file remained unaltered throughout the examination process.

2.3 Evidence Provenance and Condition

The reported image was intact with integrity hence no sign of manipulation and inconvenience was discovered. To ensure the accuracy of the analysis, the image was directly loaded into Autopsy as it was automated in read-only manner.

All the recorded data during examination were stored safely on the analyst's personal computer and the protocol of examination was strictly followed in accordance with forensic guidelines to qualify it for academic investigation.

3. Examination Summary

3.1 Overview of Critical Findings and Conclusions

This report outlines the investigation conducted on a Microsoft Windows XP disk image named “Hunter XP" which belonged to the suspect Bob Hunter who was accused of stalking, blackmailing and manipulation. The main objective of this finding was to identify, retrieve and record the relevant details of the crime and to verify the usage of the system in that offence.

During the procedure, email artifacts were recovered which directly linked Bob to the crime. The extortion related communication with metadata, search engines with blackmail tactics, methods of stalking and ways to fabricate the evidence strongly corresponded the forethought planning of the accused committing the sin.

Multiple photographs were discovered confirming secret spying and stalking acts. The blackmailed text messages with bank details further suggested the extortion of money from the victims' families. During investigation, an individual named Billy was identified as an accomplice of Bob. The exchanged messages and emails revealed cooperation and coordination between them to execute the crime.

Additionally, forensic analysis detected signs of CD burning software with data erasing tools that suggested attempts to tamper the evidence. The files showed irregular signatures which corroborated the possible manipulation. Furthermore, the system data and profile information verified that the system was frequently employed even during the relevant period.

Therefore, based on the resources , Bob Hunter is expected to be guilty. He along with his helper Billy misused the system to stalk, conspire and extort the victims. Hence, the acquired details matched the charges against him.

3.2 Tools Used

The following table outlines the forensic tools used during the examination, along with their respective versions and purposes.

Tool Name	Version	Purpose
Autopsy	4.22.1	Open-source tool used to analyze the disc image.
Exterro FTK Imager	7.7.3.81	Tool used to analyze the disc image.
AccessData Registry Viewer	2.0.0.7	Used to examine content of the Registry File.
RegRipper	3.0	Used to examine content of the Registry File.

Event Log Explorer	5.7	Used to analyze Windows system, security, and application event logs.
Parrot OS	6.4	Operating System used to run Ophcrack.
Ophcrack	3.8.0	Used to recover password hashes to identify weak or reused passwords.
PECmd	1.5.0.0	Used to read the content of prefetch file

3.3 Elimination of Irrelevant Data

During investigation, various data were retrieved from which irrelevant data were identified and later excluded. Default Windows XP system files, background operating system processes, and built-in accounts that were not associated with the crime were disregarded to increase the efficiency of investigation. Duplicated and repetitive data were reviewed and were reduced to single one to reduce cognitive overload. Eliminating outdated files logs and data unrelated to the crime assured accuracy by recording only substantial information to testify direct evidence.

4. Forensic Analysis and Findings

4.1 System Profiling and User Information

17 The user's Operating System appeared to be Microsoft Windows XP. It was installed on February 28, 2002, at 22:02:39 GMT. Additional information about the system is listed on the table below.

Operating System Information	
Name	PC-V770KUX75EHT
Program Name	Microsoft Windows XP
Processor Architecture	x86
Product ID	55277-005-6418583-21673
Owner	PC User
Organization	PC User Company

3 3

Key Properties	
Last Written Time	6/4/2002 23:01:57 UTC
OS Install Date (UTC)	Thu Feb 28 22:02:39 2002

Fig 4.1.1 : Operating System Installation Date

The system operated under Central Daylight Time during daylight saving periods and Central Standard Time during standard periods. The time zone bias was set to 360 minutes (6 hours), with an active time bias of 300 minutes (5 hours) when daylight saving time was in effect.

```
----------------------------------------
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2002-04-18 14:33:31Z
  DaylightName   -> Central Daylight Time
  StandardName   -> Central Standard Time
  Bias           -> 360 (6 hours)
  ActiveTimeBias -> 300 (5 hours)
----------------------------------------
```

Fig 4.1.2: Time zone Information

The system was last shut down on **June 4, 2002**, at **22:58:42Z**.

```
----------------------------------------
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2002-06-04 22:58:42Z
ShutdownTime  : 2002-06-04 22:58:42Z
----------------------------------------
source_os v.20200511
(System) Parse Source OS subkey values

----------------------------------------
```

Fig 4.1.3: Last Shutdown Time

The Operating System was found to have 5 user accounts in total, including both built-in and user-created accounts. Most of the activity was performed by the user Bob Hunter, with RID 1004.

```
Username        : Administrator [500]
SID             : S-1-5-21-1229272821-1580818891-854245398-500
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Thu Feb 28 15:22:36 2002 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account
```

Fig 4.1.4: Account information associated with RID 500

```
Username        : Guest [501]
SID             : S-1-5-21-1229272821-1580818891-854245398-501
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Thu Feb 28 15:22:36 2002 Z
Name            :
Last Login Date : Mon Jun  3 16:49:37 2002 Z
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

Fig 4.1.5 : Account information associated with RID 501

```
Username        : HelpAssistant [1000]
SID             : S-1-5-21-1229272821-1580818891-854245398-1000
Full Name       : Remote Desktop Help Assistant Account
User Comment    : Account for Providing Remote Assistance
Account Type    : Custom Limited Acct
Account Created : Thu Feb 28 21:47:33 2002 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Thu Feb 28 21:47:33 2002 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account
```

Fig 4.1.6 : Account information associated with RID 1000

```
Username         : SUPPORT_388945a0 [1002]
SID              : S-1-5-21-1229272821-1580818891-854245398-1002
Full Name        : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
User Comment     : This is a vendor's account for the Help and Support Service
Account Type     : Custom Limited Acct
Account Created : Thu Feb 28 21:56:13 2002 Z
Name             :
Last Login Date : Never
Pwd Reset Date   : Thu Feb 28 21:56:13 2002 Z
Pwd Fail Date    : Never
Login Count      : 0
  --> Password does not expire
  --> Account Disabled
  --> Normal user account
```

Fig 4.1.7: Account information associated with RID 1002

```
Username         : Bob Hunter [1004]
SID              : S-1-5-21-1229272821-1580818891-854245398-1004
Full Name        :
User Comment     :
Account Type     : Default Admin User
Account Created : Thu Feb 28 22:22:17 2002 Z
Name             :
Last Login Date : Tue Jun  4 23:01:54 2002 Z
Pwd Reset Date   : Thu Feb 28 22:22:17 2002 Z
Pwd Fail Date    : Never
Login Count      : 37
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

Fig 4.1.8: Account information associated with RID 1004

The user account with RID 1003 was missing. The **SecEvent.Evt** file showed that the user account with the username "Owner" and RID 1003 had been deleted.

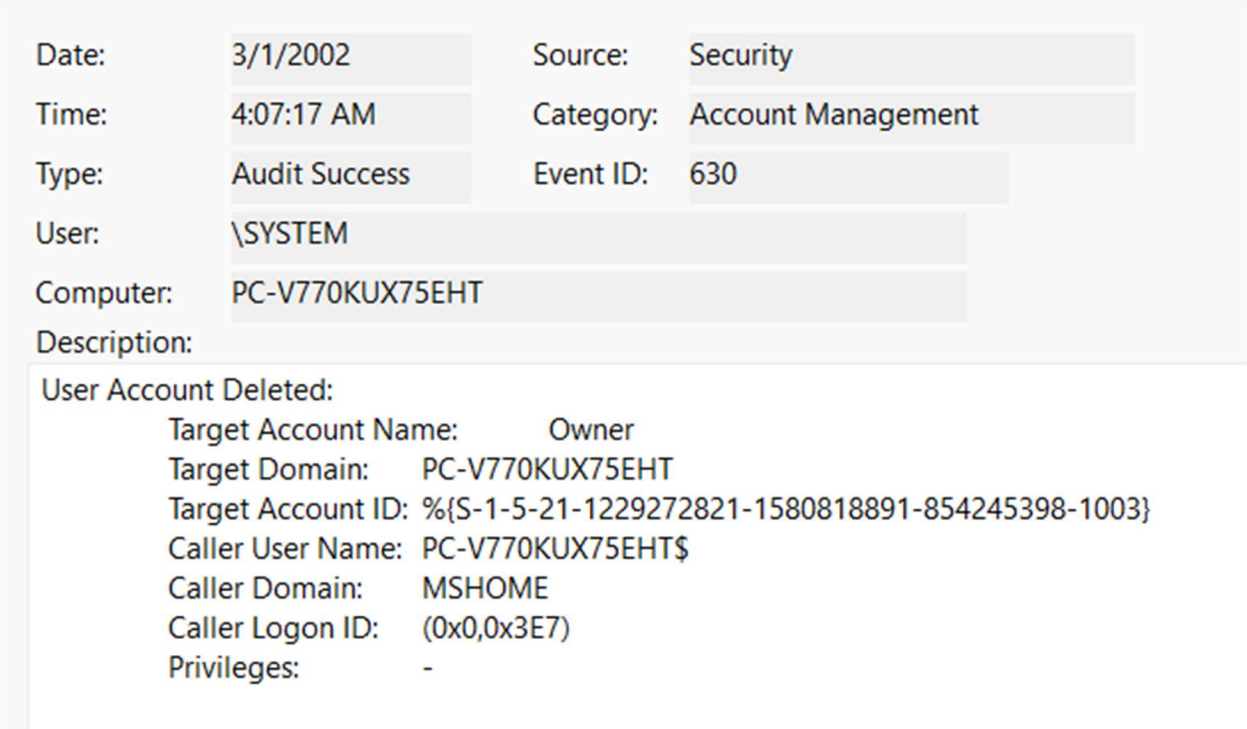

Fig 4.1.9: Deletion of the User Account name "Owner" with RID 1003

4.2 File System and File Signature Analysis

The file system of the examined volume (vol2) was identified as **NTFS**, as confirmed by volume metadata and the presence of NTFS system files.

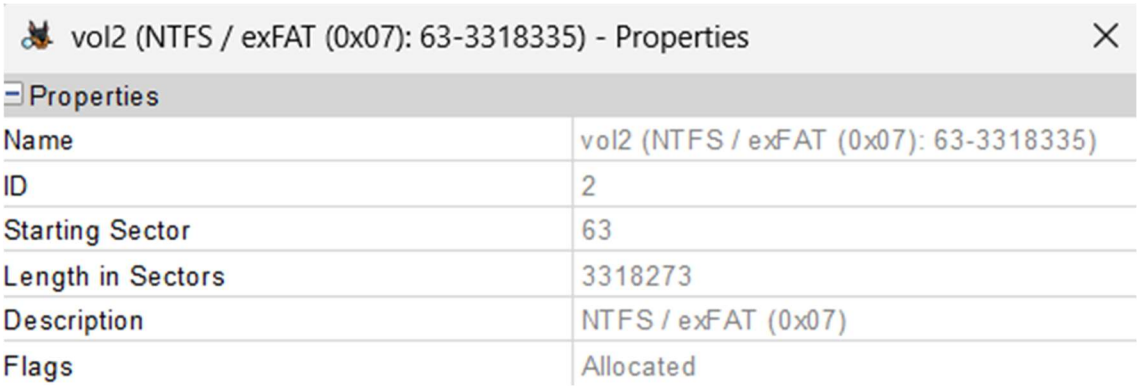

Fig 4.2.1 : Properties of vol2

There are total of 58 files with extension mismatch detected.

There were multiple files with different extensions, for instance there is a file named **"wbkC1.tmp"** with .tmp extension but is a jpeg file.

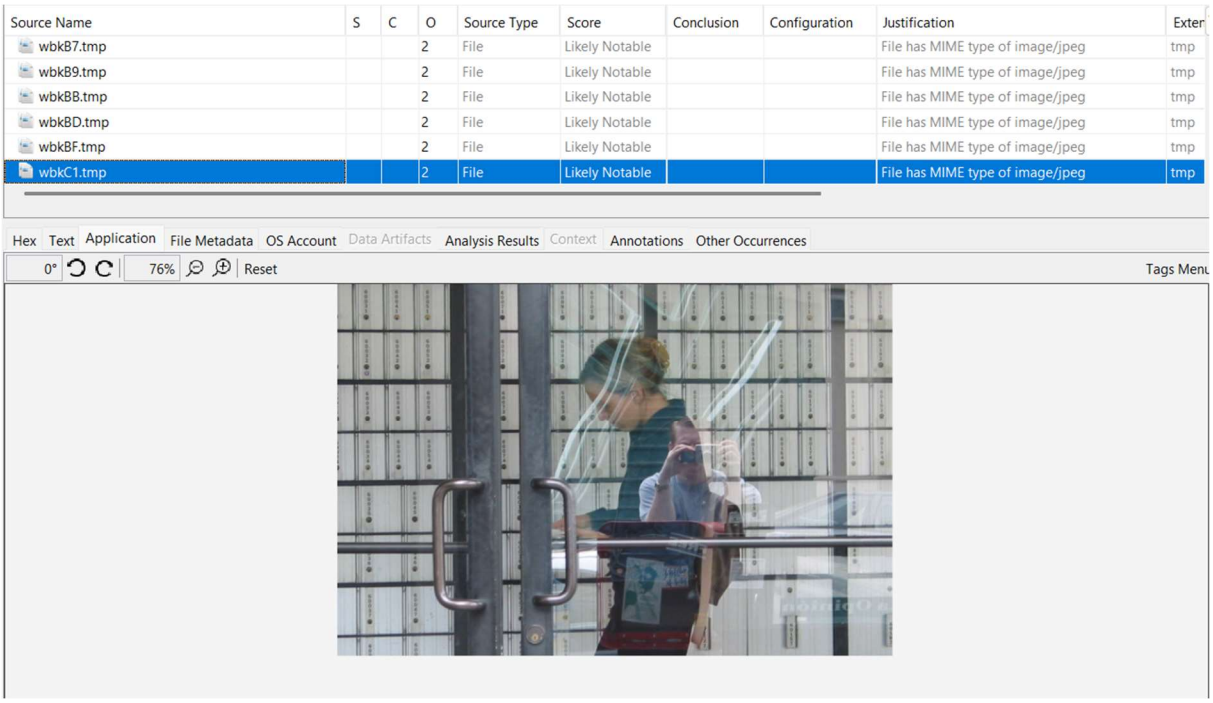

Fig 4.2.2: JPEG file with .tmp extension

Upon viewing the Hexadecimal value, we can see that it starts with header **FF D8 FF** which indicates it is a jpeg file.

```
0x00000000: FF D8 FF E1  1B FE 45 78   69 66 00 00   49 49 2A 00
0x00000010: 08 00 00 00  09 00 0F 01   02 00 06 00   00 00 7A 00
0x00000020: 00 00 10 01  02 00 13 00   00 00 80 00   00 00 12 01
0x00000030: 03 00 01 00  00 00 01 00   00 00 1A 01   05 00 01 00
0x00000040: 00 00 A0 00  00 00 1B 01   05 00 01 00   00 00 A8 00
0x00000050: 00 00 28 01  03 00 01 00   00 00 02 00   00 00 32 01
0x00000060: 02 00 14 00  00 00 B0 00   00 00 13 02   03 00 01 00
0x00000070: 00 00 01 00  00 00 69 87   04 00 01 00   00 00 C4 00
0x00000080: 00 00 8E 05  00 00 43 61   6E 6F 6E 00   43 61 6E 6F
0x00000090: 6E 20 50 6F  77 65 72 53   68 6F 74 20   47 32 00 00
0x000000a0: 00 00 00 00  00 00 00 00   00 00 00 00   B4 00 00 00
0x000000b0: 01 00 00 00  B4 00 00 00   01 00 00 00   32 30 30 32
0x000000c0: 3A 30 34 3A  32 34 20 30   31 3A 31 30   3A 33 35 00
0x000000d0: 1B 00 9A 82  05 00 01 00   00 00 56 03   00 00 9D 82
0x000000e0: 05 00 01 00  00 00 5E 03   00 00 00 90   07 00 04 00
0x000000f0: 00 00 30 32  31 30 03 90   02 00 14 00   00 00 0E 02
0x00000100: 00 00 04 90  02 00 14 00   00 00 22 02   00 00 01 91
0x00000110: 07 00 04 00  00 00 01 02   03 00 02 91   05 00 01 00
0x00000120: 00 00 3E 03  00 00 01 92   0A 00 01 00   00 00 46 03
0x00000130: 00 00 02 92  05 00 01 00   00 00 4E 03   00 00 04 92
0x00000140: 0A 00 01 00  00 00 66 03   00 00 05 92   05 00 01 00
0x00000150: 00 00 6E 03  00 00 06 92   05 00 01 00   00 00 76 03
0x00000160: 00 00 07 92  03 00 01 00   00 00 05 00   00 00 09 92
0x00000170: 03 00 01 00  00 00 00 00   00 00 0A 92   05 00 01 00
0x00000180: 00 00 7E 03  00 00 7C 92   07 00 C2 01   00 00 86 03
0x00000190: 00 00 86 92  07 00 08 01   00 00 36 02   00 00 00 A0
0x000001a0: 07 00 04 00  00 00 30 31   30 30 01 A0   03 00 01 00
0x000001b0: 00 00 01 00  00 00 02 A0   03 00 01 00   00 00 80 02
```

Fig 4.2.3 : Hexadecimal output of wbkC1.tmp file

4.3 Image Analysis

The images were in the directory**:**

4 **/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application Data/Microsoft/Cd Burning/Hunter Pics/**

Inside this directory, the images were sorted into three separate subfolders according to their respective names:

- **Christina Detsiwt –** held images associated with the victim Christina Dewist
- **Sabrina Dewercs –** held images associated with the victim Sabrina Dewercs
- **Sabrina and Christina –** held images featuring both victims together

The collection included 115 images of Christina Detsiwt stored in her respective folder, 49 images of Sabrina Dewercs in her folder, and 11 photographs showing both Sabrina and Christina together in their combined folder.

Listing
/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application Data/Microsoft/CD Burning/Hunter Pics 6 Results
Table Thumbnail Summary
Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2002-06-05 00:40:00 GMT	2002-06-05 00:40:00 GMT	2002-06-05 00:40:00 GMT	2002-06-05 00:39:52 GMT	56	Allocated	Allocated	unknown
[parent folder]				2002-06-05 00:39:52 GMT	2002-06-05 00:39:52 GMT	2002-06-05 00:39:52 GMT	2002-02-28 22:24:03 GMT	256	Allocated	Allocated	unknown
Christina Detsiwt				2002-06-05 00:39:57 GMT	2002-06-05 00:39:57 GMT	2002-06-05 00:39:57 GMT	2002-06-05 00:39:52 GMT	56	Allocated	Allocated	unknown
Sabrina and Christina				2002-06-05 00:39:58 GMT	2002-06-05 00:39:58 GMT	2002-06-05 00:39:58 GMT	2002-06-05 00:39:57 GMT	56	Allocated	Allocated	unknown
Sabrina Dewercs				2002-06-05 00:40:00 GMT	2002-06-05 00:40:00 GMT	2002-06-05 00:40:00 GMT	2002-06-05 00:39:58 GMT	184	Allocated	Allocated	unknown
Thumbs.db			2	2002-06-04 23:28:22 GMT	2002-06-05 00:40:00 GMT	2002-06-04 23:59:16 GMT	2002-06-04 23:28:20 GMT	28672	Allocated	Allocated	unknown

Fig 4.3.1 : Folder with the name of Victim's

The following photographs were from the above-mentioned folders:

Fig 4.3.2 : Picture of Christina Detsiwt

The above-mentioned photograph is from the Folder **Christina Detsiwt** and consists total of 115 images of Christina.

Fig 4.3.3: Picture of Sabrina and Christina

The above-mentioned photograph is from the folder **Sabrina and Christina** and is part of a collection of 11 images of both of them together.

The below-mentioned photograph is from the folder **Sabrina Dewercs** and is part of a collection of 49 images of Sabrina.

Fig 4.3.4: Picture of Sabrina Dewercs

The images included photographs showing the victim's daily activities and other content relevant to the stalking allegations. The images show that the photo was taken without the victim's consent.

Deleted and Recovered Images:
A significant number of images were deleted by the user, as evidenced by their recovery from the Recycler. Forensic recovery techniques allowed retrieval of these deleted files from both the Recycler and unallocated space, indicating that the suspect attempted to remove incriminating evidence.

12 Location of **RECYCLER:** /img_Hunter XP for Dongled v6.E01/vol_vol2/**RECYCLER**

20 **Fig 4.3.5:** Image from RECYCLER

Fig 4.3.6: Image from RECYCLER

The camera that was used to capture these images was **Canon PowerShot G2** as the photos were analyzed, all had same analysis result.

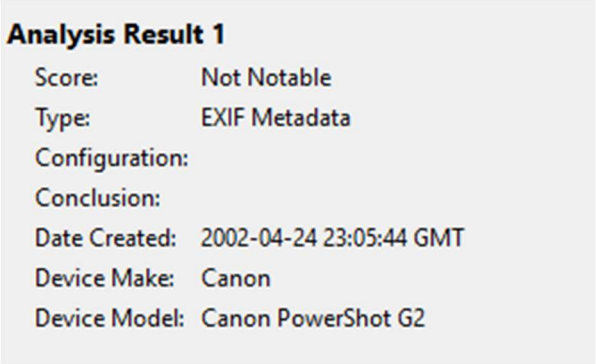

Fig 4.3.7 : Analysis Result

4.4 Internet Activity

The Web Browsers Installed on the suspect's PC were:

1. Internet Explorer
2. Microsoft Edge

The suspect primarily used Internet Explorer for web browsing. Although Microsoft Edge was installed on the system, there was little to no evidence indicating regular use.

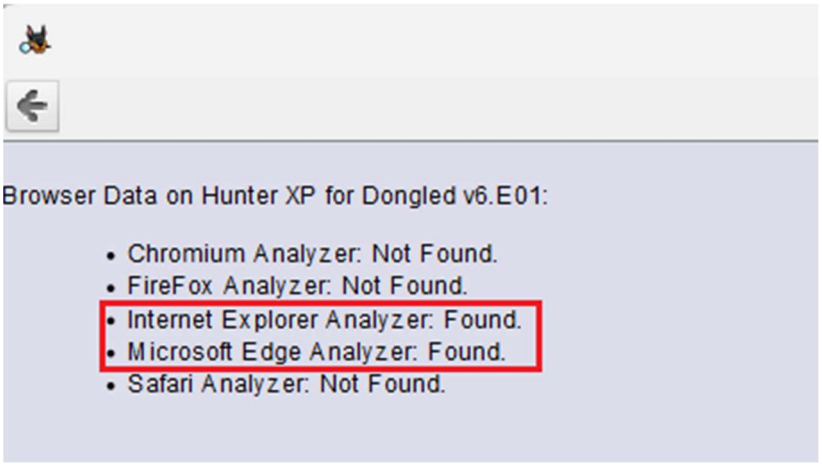

Fig 4.4.1 : Proof of Installation of Internet Explorer and Microsoft Edge

The suspect had bookmarked a total of 16 websites, suggesting regular use of these sites as part of daily internet activity.

Source Name	...	...	...	URL	Title	Date Created	Program Name
Free Hotmail.url			2	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=hotmail	Free Hotmail.url	2002-02-28 22:24:03 GMT	Internet Explorer Analyzer
Windows.url			2	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windows	Windows.url	2002-02-28 22:24:03 GMT	Internet Explorer Analyzer
RealPlayer.url			2	http://www.real.com	RealPlayer.url	2002-03-01 15:10:08 GMT	Internet Explorer Analyzer
RealPlayer Home Page.url			2	http://www.real.com	RealPlayer Home Page.url	2002-03-01 15:10:08 GMT	Internet Explorer Analyzer
Windows Media.url			2	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=windows...	Windows Media.url	2002-02-28 22:24:03 GMT	Internet Explorer Analyzer
Customize Links.url			2	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=...	Customize Links.url	2002-02-28 22:24:03 GMT	Internet Explorer Analyzer
MSN.com.url			2	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=l..	MSN.com.url	2002-02-28 22:24:02 GMT	Internet Explorer Analyzer
Get $$$ - Refer a friend!.url				aol://1391:44-65063/	Get $$$ - Refer a friend!.url	2002-03-01 15:58:49 GMT	Internet Explorer Analyzer
Get $$$ - Refer a friend!.url				aol://1391:44-65063/	Get $$$ - Refer a friend!.url	2002-03-01 15:58:49 GMT	Internet Explorer Analyzer
Here you go Dad.url			2	http://www.guidancesw.com/	Here you go Dad.url	2002-06-03 18:51:30 GMT	Internet Explorer Analyzer
Real.com Radio Tuner.url			2	http://realguide.real.com/stations/	Real.com Radio Tuner.url	2002-03-01 15:10:08 GMT	Internet Explorer Analyzer
Welcome to Xdrive Plus login.url			2	http://plus.xdrive.com/XDRequestDispatcher?action=OpenLogi..	Welcome to Xdrive Plus login.url	2002-03-31 16:23:21 GMT	Internet Explorer Analyzer
Radio Station Guide.url			2	http://www.microsoft.com/isapi/redir.dll?prd=windows&sbp=...	Radio Station Guide.url	2002-02-28 22:24:02 GMT	Internet Explorer Analyzer
AnyWho Internet Directory Assistance; Yellow Page			2	http://www.anywho.com/cgi-bin/htwpq	AnyWho Internet Directory Assist..	2002-03-31 14:44:11 GMT	Internet Explorer Analyzer
Hotmail Home.url			2	http://lw14fd.law14.hotmail.msn.com/cgi-bin/hmhome?curmbo	Hotmail Home.url	2002-03-31 14:23:08 GMT	Internet Explorer Analyzer
http--plus.xdrive.com-XDRequestDispatcheraction=			2	http://plus.xdrive.com/XDRequestDispatcher?action=FolderVie..	http--plus.xdrive.com-XDRequest..	2002-06-04 23:21:26 GMT	Internet Explorer Analyzer

Fig 4.4.2 : Suspect web bookmarks

6

The suspect utilized the website **http://www.guidancesw.com** to blackmail the father of Christina and Sabrina. The webpage used for this blackmailing activity is presented below.

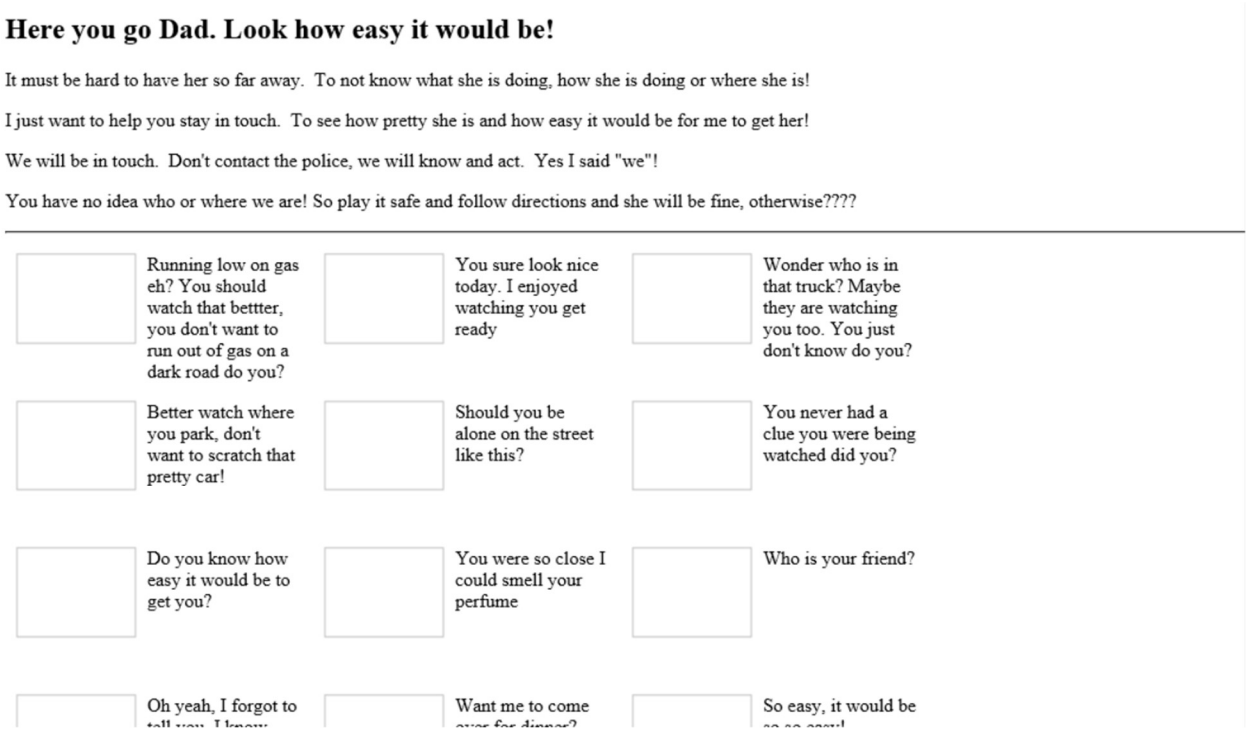

Fig 4.4.3 : Interface of the blackmailing website

Xdrive is an online storage platform. The user bookmarked the website xdrive.com and visited it repeatedly over several days, which suggested that data may have been stored on the service.

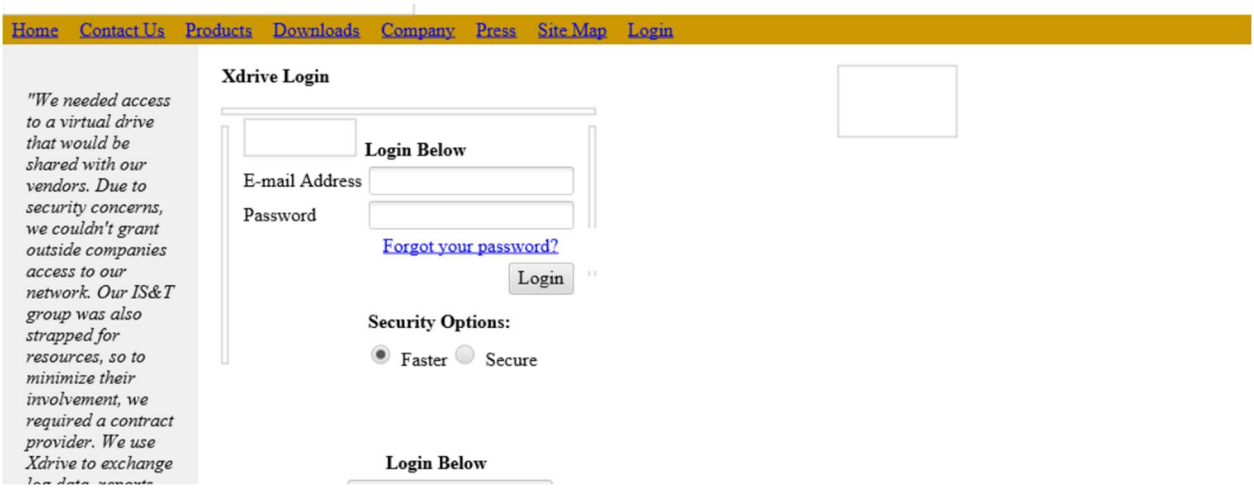

Fig 4.4.4 : Login page of Xdrive

A review of the user's web activity revealed that the user had searched for Criminal Defense Lawyers.

Fig 4.4.5 : Criminal Defense Lawyers website

4.5 Messaging and Email Activity

There was extensive messaging interaction between the user Bob Hunter and a partner named Billy. Initially, the exchanges between Bob and Billy revealed that Bob informed Billy he had been following two girls and knew where they lived.

Chaser1191 = Bob Hunter

billy ray 0001 = Billy Ray

[hunter.log, Chaser1191: I followed the two girls last week, I know where they both live
billy ray 0001: very good, I think it is time we think about hitting up the family for cash
Chaser1191: I agree
Chaser1191: I followed them to Florida, well Kims family anyway
Chaser1191: I think that we can really scare up some good $$$$
Chaser1191: how much should we ask for
Chaser1191: what do you think their security is worth
billy ray 0001: I was thinking about 500,000 to start
billy ray 0001: they have it
billy ray 0001: we just need to convince them that its worth it
Chaser1191: I am flying out to LA this next Monday the 20th I will finalize the stuff then
Chaser1191: plus I will get a few more facts on them to really convince them
Chaser1191: we will hold it back as our trump card
billy ray 0001: sounds like a good idea
Chaser1191: whats Kim's work address
billy ray 0001: I think it is 572 green street in pasadena but she may have just been visiting the other one.
Chaser1191: i will check that when I am there
Chaser1191: its not too far away
billy ray 0001: ok
billy ray 0001: if i learn differently i will let you know
billy ray 0001: can you be reached out there
Chaser1191: yes, either on yahoo, aim or aol, not sure about hotmail anymore
Chaser1191: they cancelled the acount for awhile, did not use it
Chaser1191: but i reactivated it today
billy ray 0001: ok
billy ray 0001: gotta go
Chaser1191: ok, I will call you later]

Fig 4.5.1 : Conversation between Bob and Billy

High levels of communication were observed between two email addresses: **chaser1191@hotmail.com** and **billyray150@hotmail.com**. The address chaser1191@hotmail.com was identified as belonging to the primary suspect, Bob Hunter, while billyray150@hotmail.com was believed to belong to his associate or accomplice.

In the content below, it was evident that the accomplice Billy Ray had identified the email addresses of the father of Sabrina and Christina.

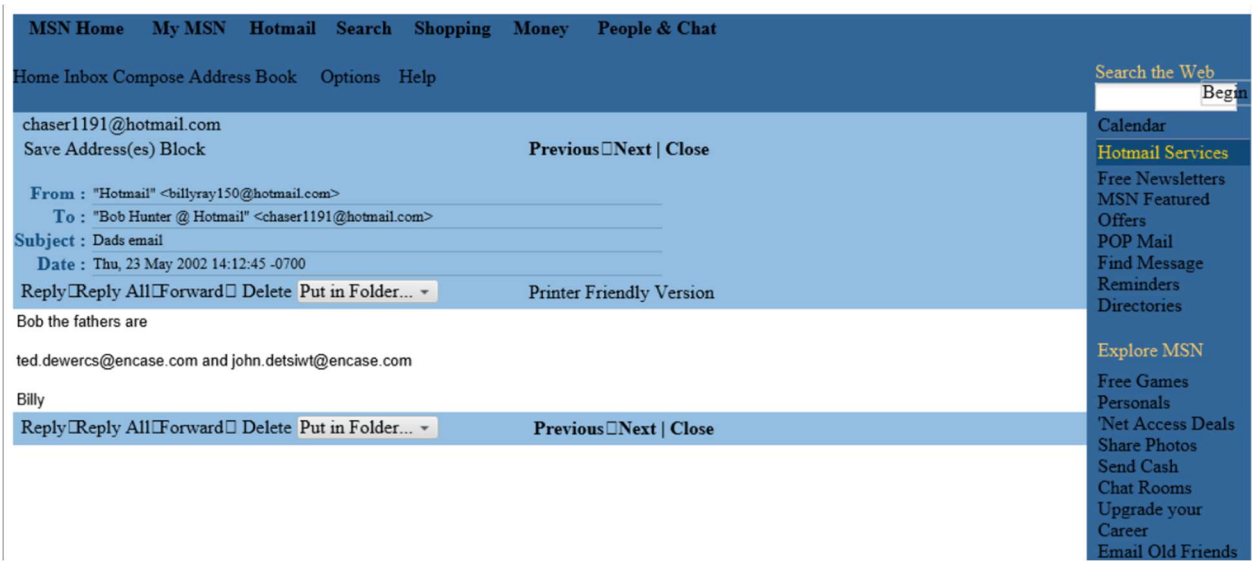

Fig 4.5.2: Email addresses of victim's father

Below is the threatening message that appeared to have been sent to the respective fathers.

Fig 4.5.3: Threating message sent to the victim's father

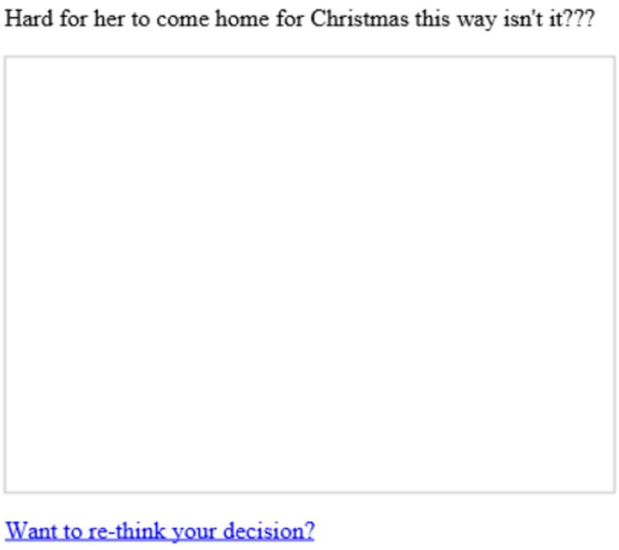

Fig 4.5.4 : Blackmailing

The ransom demand total of 1 million dollars each, and information about the bank routing number and account number was required to ensure the girls' safety.

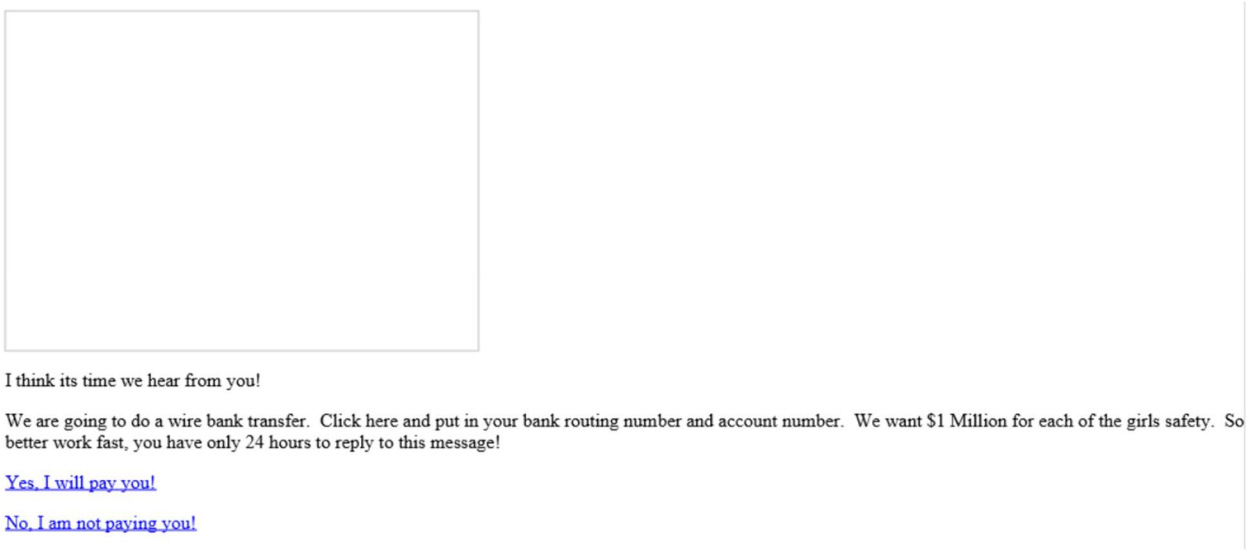

Fig 4.5.5 : Bank information asked by the Bob Hunter to victim's father

Ted Dewercs replied by saying that they were joking but John Detsiwt provided his bank routing number and account number.

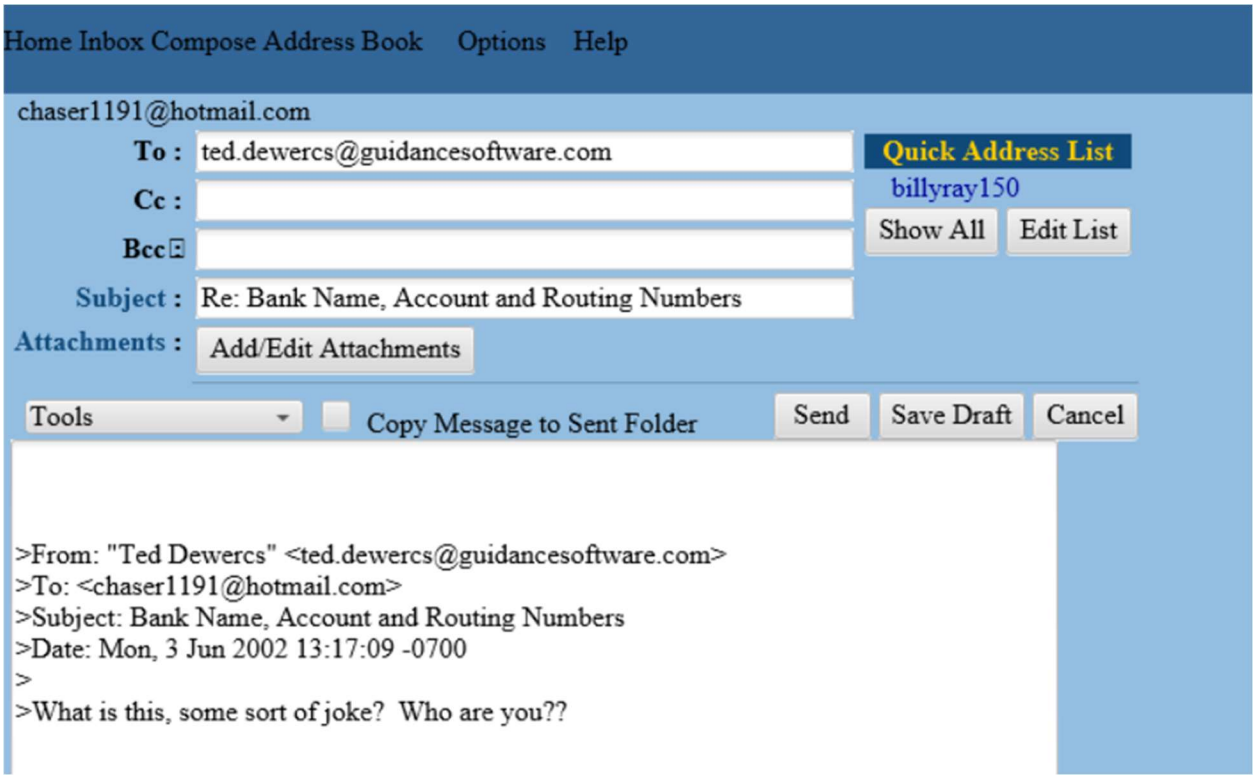

Fig 4.5.6 : Reply of Ted Dewercs

Fig 4.5.7 : Reply of John Detsiwt

4.6 Disc Wiping Activities

The executable **CLEANMGR.EXE** was used to free up disk space by locating and deleting unnecessary files from the system. It was last run on June 3, 2002, at 17:08:40 GMT.

```
Executable name: CLEANMGR.EXE
Hash: 1F86EA8E
File size (bytes): 45,730
Version: Windows XP or Windows Server 2003

Run count: 5
Last run: 2002-06-03 17:08:40

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME1 Serial: B0837BF8 Created: 2002-02-28 15:13:36
```

Fig 4.6.1: Content of **CLEANMGR.EXE-1F86EA8E.pf** with PECMD

IMAPI.EXE enabled applications to write data and audio onto optical media like CDs and DVDs. Since IMAPI.EXE was the last program run on the PC, this indicated that the suspect was likely attempting to tamper with data and destroy evidence. It was last run on 2002-06-05 00:40:01 GMT.

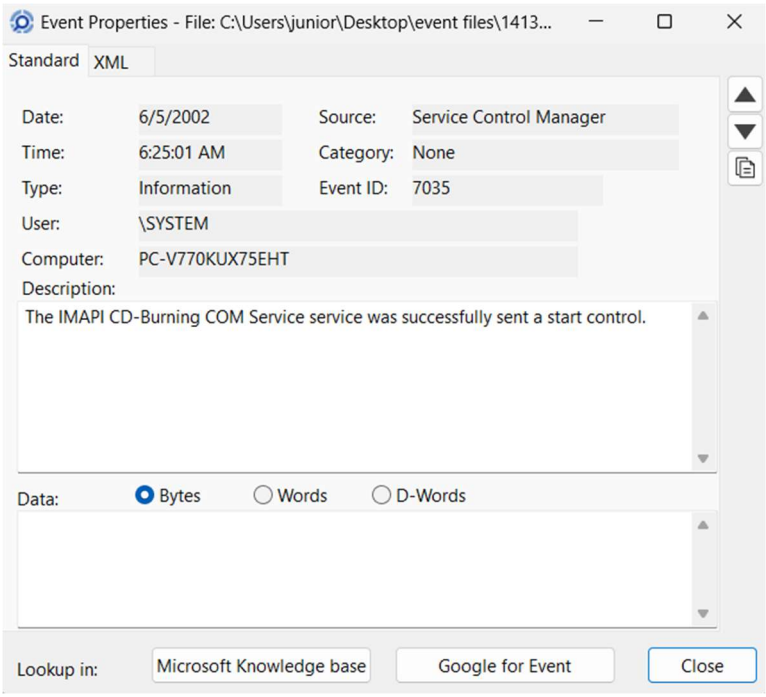

Fig 4.6.2: log content showing running of IMAPI.EXE

```
Executable name: IMAPI.EXE
Hash: BF740A4
File size (bytes): 9,900
Version: Windows XP or Windows Server 2003

Run count: 22
Last run: 2002-06-05 00:40:01

Volume information:

#0: Name: \DEVICE\HARDDISKVOLUME1 Serial: B0837BF8 Created: 2002-02-28 15:13:36 Directories: 8 File references: 36
```

Fig 4.6.3: Content of **IMAPI.EXE-0BF740A4.pf** with PECmd

4.7 External Devices and Removable Media

13 There were total of 11 USB devices that were attached to the device to the devices. The system was attached to 2 printers, 1 mouse, 1 video capture device, 1 PDA, 2 storage devices, and 4 root/USB hubs.

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
system			1	2002-06-04 23:01:36 GMT		ROOT_HUB	4&15736a3f&0	Hunter XP for Dongled v6.E01
system			1	2002-03-01 15:35:47 GMT		ROOT_HUB	4&19dea8de&0	Hunter XP for Dongled v6.E01
system			1	2002-06-04 23:01:38 GMT	HP, Inc	LaserJet 2200	00CNDRF03485	Hunter XP for Dongled v6.E01
system			1	2002-06-03 15:43:46 GMT	HP, Inc	Jornada 548 / iPAQ HW6515 Pocket PC	6&215733eb&0&4	Hunter XP for Dongled v6.E01
system			1	2002-03-01 15:35:53 GMT	Lexmark International, Inc.	Z52 Printer	6&215733eb&0&1	Hunter XP for Dongled v6.E01
system			1	2002-06-04 23:01:37 GMT	Texas Instruments, Inc.	TUSB2040/2070 Hub	5&b114931&0&2	Hunter XP for Dongled v6.E01
system			1	2002-03-01 15:35:48 GMT	Texas Instruments, Inc.	TUSB2040/2070 Hub	5&e03868c&0&1	Hunter XP for Dongled v6.E01
system			1	2002-06-04 23:01:37 GMT	Microsoft Corp.	IntelliMouse Explorer	5&b114931&0&1	Hunter XP for Dongled v6.E01
system			1	2002-06-04 23:01:38 GMT	Dazzle	Global Village VideoFX Grabber	6&215733eb&0&3	Hunter XP for Dongled v6.E01
system			1	2002-06-05 00:06:06 GMT	Trek Technology (S) PTE, Ltd	Trek2000 TD-G2	6&215733eb&0&2	Hunter XP for Dongled v6.E01
system			1	2002-06-03 20:05:14 GMT	Netac Technology Co., Ltd	Product: 0003	6&215733eb&0&2	Hunter XP for Dongled v6.E01

Fig 4.7.1 : Attached USB Devices

I found evidence of a primary hard drive, a floppy disk drive, and two different optical disc drives. I also discovered that several removable storage devices were plugged into the system between February and June 2002.

```
mountdev2 v.20200517
(System) Return contents of System hive MountedDevices key

MountedDevices
LastWrite time = 2002-06-05 00:06:07Z

Volume                                          Disk Sig                        Offset
-------                                         --------                       --------
\??\Volume{b5234b45-2c5c-11d6-b170-806d6172696f}    d1 1b d1 1b                       0
\??\Volume{fb859ea0-780e-11d6-b759-806d6172696f}    2e 00 98 f0                       0
\DosDevices\C:                                      2e 00 98 f0                       0
\DosDevices\F:                                      d1 1b d1 1b                       0

\??\Volume{b5234b45-2c5c-11d6-b170-806d6172696f}
  Thu Feb 28 15:06:14 2002
\??\Volume{fb859ea0-780e-11d6-b759-806d6172696f}
  Tue Jun  4 23:01:19 2002

Device: \??\FDC#GENERIC_FLOPPY_DRIVE#5&29337118&0&0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{b5234b40-2c5c-11d6-b170-806d6172696f}
  \DosDevices\A:

Device: \??\IDE#CdRomCREATIVE_DVD-ROM_DVD2240E_____________1.5A____#5&35c6ca11&0&0.1.0#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{b5234b41-2c5c-11d6-b170-806d6172696f}
  \DosDevices\D:

Device: \??\SCSI#CdRom&Ven_YAMAHA&Prod_CRW4260&Rev_1.0h#4&2c1afece&0&000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{b5234b42-2c5c-11d6-b170-806d6172696f}
  \DosDevices\E:

Device: \??\STORAGE#RemovableMedia#5&373eb979&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{b5234b43-2c5c-11d6-b170-806d6172696f}
```

```
Device: \??\STORAGE#RemovableMedia#5&373eb979&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{b5234b43-2c5c-11d6-b170-806d6172696f}

Device: \??\STORAGE#RemovableMedia#8&1076ba65&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{82ac0d71-6752-11d6-b639-00038a000015}

Device: \??\STORAGE#RemovableMedia#8&358be6a6&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{fb859ea6-780e-11d6-b759-00038a000015}
  \DosDevices\G:


Unique MAC Addresses:
80:6D:61:72:69:6F
00:03:8A:00:00:15
----------------------------------------
```

Fig 4.7.2 : Mounted Devices

5. Conclusion

This forensic examination was carried out to identify any unauthorized or criminal activity performed using the examined computer system. Based on the analysis of the available digital evidence, several significant findings were identified.

The recovered artefacts show that the suspect actively used the system to carry out repeated actions related to stalking, harassment, blackmail, and attempts to interfere with or conceal evidence. These findings were supported by user account activity, file system data, image files, internet usage records, and system artefacts recovered during the examination.

2 All analysis was conducted using accepted digital forensic tools and methods. The integrity of the evidence was maintained throughout the examination process, and hash values were used to ensure that the data was not altered during analysis.

2 Based on the totality of the digital forensic evidence examined, in my professional opinion, to a reasonable degree of forensic certainty, that the suspect knowingly and intentionally engaged in the identified activities using the examined system. This conclusion is based solely on the evidence that was provided for analysis.

6. Glossary of Terms

1. **Autopsy:** An open-source digital forensic platform used for analyzing and investigating data.
2. **EnCase Evidence File:** A forensic file format used to store an exact, verified copy of digital evidence.
3. **Cryptographic Hash Verification:** The process of confirming that digital data has not been altered by comparing hash values.
4. **Extortion:** The act of obtaining money or advantage through threats.
5. **Metadata:** Data that provides information about other data, such as time, date, and file details.
6. **CD Burning:** The process of writing or copying data onto a CD.
7. **NTFS (New Technology File System):** A file system used by Windows to store and organize files on a hard drive.
8. **Unallocated Space:** Areas of a storage device that are not currently assigned to any file or folder.
9. **CLEANMGR.EXE:** A Windows utility that frees up disk space by removing unnecessary files.
10. **IMAPI.EXE:** A Windows process that handles CD/DVD burning.
11. **Mounted Device:** A storage device that has been connected and made accessible by the operating system.

7. APPENDIX

Metadata of the Images:

1. **Fig 4.3.2:** Picture of Christina Detsiwt

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application Data/Microsoft/CD Burning/Hunter Pics/Christina Detsiwt/102-0218_IMG.JPG
Type:	File System
MIME Type:	image/jpeg
Size:	130566
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-04-24 20:53:00 GMT
Accessed:	2002-06-05 00:04:17 GMT
Created:	2002-05-14 18:02:14 GMT
Changed:	2002-06-05 00:49:59 GMT
MD5:	77c7b4d99f47bfb137639a1c6426f965
SHA-256:	5d42034c2b43c3323437c882b4391248e7ee824a1315f13a746a8a082ca9a8a4
Hash Lookup Results:	UNKNOWN
Internal ID:	670

2. **Fig 4.3.3:** Picture of Sabrina and Christina

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application Data/Microsoft/CD Burning/Hunter Pics/Sabrina and Christina/103-0331_IMG.JPG
Type:	File System
MIME Type:	image/jpeg
Size:	136891
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-04-25 23:02:00 GMT
Accessed:	2002-06-04 23:33:26 GMT
Created:	2002-05-14 18:02:20 GMT
Changed:	2002-06-05 00:49:28 GMT
MD5:	ff738483d65d244e8f09c845267de75f
SHA-256:	b75190921a4b9d6670e4676199aa277513340a1f9248bf98fe8775213d6b9b4e
Hash Lookup Results:	UNKNOWN
Internal ID:	867

3. **Fig 4.3.4:** Picture of Sabrina Dewercs

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Application Data/Microsoft/CD Burning/Hunter Pics/Sabrina Dewercs/103-0361_IMG.JPG
Type:	File System
MIME Type:	image/jpeg
Size:	147655
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-04-25 23:03:00 GMT
Accessed:	2002-06-05 00:02:48 GMT
Created:	2002-05-14 18:02:22 GMT
Changed:	2002-06-05 00:50:00 GMT
MD5:	afd5ce89161be8beecfc34b1507d1fb7
SHA-256:	ca6e1c44fc9e5b5a9cc065d4143029900aba90e3449009985d999b3983e24037
Hash Lookup Results:	UNKNOWN
Internal ID:	929

4. **Fig 4.3.5:** Image from RECYCLER

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df590.JPG
Type:	File System
MIME Type:	image/jpeg
Size:	114243
File Name Allocation:	Unallocated
Metadata Allocation:	Allocated
Modified:	2002-04-29 22:17:00 GMT
Accessed:	2002-06-05 00:04:35 GMT
Created:	2002-05-14 18:01:51 GMT
Changed:	2002-06-05 00:50:00 GMT
MD5:	22e50503e059fdc3be13d171424c74c5
SHA-256:	df5cc18ca75773468c3f15941acb7ca429bb9446619688ae79e5a7087140fc17
Hash Lookup Results:	UNKNOWN
Internal ID:	9549

5. **Fig:4.3.6:** Image from RECYCLER

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df553.JPG
Type:	File System
MIME Type:	image/jpeg
Size:	89526
File Name Allocation:	Unallocated
Metadata Allocation:	Allocated
Modified:	2002-04-29 22:15:00 GMT
Accessed:	2002-06-05 00:02:49 GMT
Created:	2002-05-14 18:01:48 GMT
Changed:	2002-06-05 00:50:00 GMT
MD5:	a57e0eef461d35d81936c601c1682687
SHA-256:	c2a96c36bce56bea08e1831b913e5d113af6358ed23184ad27fa2de78e3a8070
Hash Lookup Results:	UNKNOWN
Internal ID:	9511

6. **Fig:4.4.3 :** Login page of Xdrive

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/UFK38B83/page[1].htm
Type:	File System
MIME Type:	text/html
Size:	12916
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-05-14 16:57:08 GMT
Accessed:	2002-05-14 16:57:08 GMT
Created:	2002-05-14 16:57:08 GMT
Changed:	2002-05-14 16:57:08 GMT
MD5:	c469b2b2178e8d31fa81692714779f6b
SHA-256:	cdc0f6fa0e060402dcf9461086e68fa59ae48eeb31061d50eee092bd8da016d7
Hash Lookup Results:	UNKNOWN
Internal ID:	4049

7. **Fig:4.4.4 :** Criminal Defense Lawyers website

Metadata

Name:	/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
Type:	File System
MIME Type:	text/html
Size:	26239
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-06-03 18:08:29 GMT
Accessed:	2002-06-03 18:08:29 GMT
Created:	2002-06-03 18:08:28 GMT
Changed:	2002-06-03 18:08:29 GMT
MD5:	0a03ec269fc46dc104a4575704344574
SHA-256:	9e38fe0e2623993dfd961082f67603cfa9c4b6728415db8230b94b08758feb47
Hash Lookup Results:	UNKNOWN
Internal ID:	3292

8. **Fig:4.5.1 :** Conversation between Bob and Billy

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Program Files/America Online 7.0/download/Hunter.log
Type:	File System
MIME Type:	text/x-log
Size:	1490
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-05-14 17:27:03 GMT
Accessed:	2002-05-14 17:27:03 GMT
Created:	2002-05-14 17:12:59 GMT
Changed:	2002-05-14 17:27:03 GMT
MD5:	550fc78db36baa1de1a2d2ddf1fa671b
SHA-256:	7f799c31d091106c31f48f5f9c50dd182c4e274b9e9d2cd1a64d5fcbb2efd269
Hash Lookup Results:	UNKNOWN
Internal ID:	6607

9. **Fig:4.5.2:** Email addresses of victim's father

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/8XGPQD6L/getmsg[2].58
Type:	File System
MIME Type:	text/html
Size:	24840
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-06-03 18:33:27 GMT
Accessed:	2002-06-03 18:33:27 GMT
Created:	2002-06-03 18:33:27 GMT
Changed:	2002-06-03 18:33:27 GMT
MD5:	cdd4cdcbdcddce2ba26af2084f7da47f
SHA-256:	f6c1c109b05b5c6f621a7839afd0b4df25356e7d4eb9e56c0b26da6fa45c4ac6
Hash Lookup Results:	UNKNOWN
Internal ID:	3704

10. **Fig:4.5.3:** Threating message sent to the victim's father

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/6ZSJ6T6D/getmsg[8].htm
Type:	File System
MIME Type:	text/html
Size:	21113
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-06-04 23:42:28 GMT
Accessed:	2002-06-04 23:42:28 GMT
Created:	2002-06-04 23:42:27 GMT
Changed:	2002-06-04 23:42:28 GMT
MD5:	a659cb24ee6f9b3a8d9ff3e7259344f9
SHA-256:	32057cea35f1fa032250187e572a0d161532a761ff374f5250c1dbb9171c054e
Hash Lookup Results:	UNKNOWN
Internal ID:	2693

11. **Fig:4.5.4:** Blackmailing

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/042WFPGU/results[4].htm
Type:	File System
MIME Type:	text/html
Size:	560
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-06-03 19:08:18 GMT
Accessed:	2002-06-03 19:08:18 GMT
Created:	2002-06-03 19:08:18 GMT
Changed:	2002-06-03 19:08:18 GMT
MD5:	51fdd6bad05cb016b6faa8f9ee224acd
SHA-256:	d87902f49bf01a231f8ba018ca41ace8d946f0805ea08e30a1773cda1dd8adbb
Hash Lookup Results:	UNKNOWN
Internal ID:	1224

12. **Fig:4.5.5 :** Bank information asked by the Bob Hunter to victim's father

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/6ZSJ6T6D/or_else[1].htm
Type:	File System
MIME Type:	text/html
Size:	874
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-06-03 19:08:12 GMT
Accessed:	2002-06-03 19:08:12 GMT
Created:	2002-06-03 19:08:12 GMT
Changed:	2002-06-03 19:08:12 GMT
MD5:	2d2eb087cfb1e20d41b35cd2f48c597a
SHA-256:	2918c163bc582e88764220311afea929777b15ceb72a3efd9e4a942436af5632
Hash Lookup Results:	UNKNOWN
Internal ID:	2628

13. **Fig:4.5.6 :** Reply of Ted Dewercs

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/UFK38B83/compose[1].htm
Type:	File System
MIME Type:	text/html
Size:	21607
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-06-03 20:22:44 GMT
Accessed:	2002-06-03 20:22:44 GMT
Created:	2002-06-03 20:22:42 GMT
Changed:	2002-06-03 20:22:44 GMT
MD5:	95e716e0e841baa2725a1ac6a04caea8
SHA-256:	7857b185b0b9304a70adfa1505361d17086063d222ffa8cf1a154dbea69e1a16
Hash Lookup Results:	UNKNOWN
Internal ID:	4248

14. **Fig:4.5.7 :** Reply of John Detsiwt

Metadata

Name:	/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/UFK38B83/getmsg[5].htm
Type:	File System
MIME Type:	text/html
Size:	21099
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2002-06-03 20:17:19 GMT
Accessed:	2002-06-03 20:17:51 GMT
Created:	2002-06-03 20:17:18 GMT
Changed:	2002-06-03 20:17:19 GMT
MD5:	f8469b56117e447ba0c218e13a859b6a
SHA-256:	360452ced6363195e8b2bbcdcc034358e8b5221e74d51c371b1f9c0be632d6e9
Hash Lookup Results:	UNKNOWN
Internal ID:	4530