Forensics Examination Report

Cyber Crime and Digital Evidence

Submitted by

Name: Sidhant Kumar Chaurasiya

Student ID:10487

Cyber Security and digital forensics

Kathmandu, Nepal

Details of forensics analyst

- **Report title**:-Forensics Examination of " Hunter XP " Image
- **Examiner**:-Sidhant Kumar Chaurasiya
- **Tools Used:**
  →FTK Imager 4.7.12
  →Autopsy 4.19.2
  →Registry Viewer 1.8.0.5
  →Event Log Explorer 4.8
  →Reg ripper 3.0

Executive Summary

The forensics investigation of the "Hunter XP" disk image uncovered significant evidence of illicit activity, including stalking, extortion, conspiracy, evidence tempering, and ransomware threats. Artifacts such as user activity logs, internet browsing history, email communication, deleted files, and manipulated data were identified during the examination. The investigation utilized multiple forensic tools to ensure data integrity, thorough analysis, and dual verification of the findings.

Methodology

The investigation began with image verification of the image given to us using an FTK imager to load the picture and confirm hash values, ensuring integrity. Dual verification was performed using autopsy which validated metadata consistency. Artifacts recovery, including NTFS data craving, was conducted with photoRec in the /vol_vol2/RECYCLER directory. Registry and system analysis using Reg-Ripper extracted OS details, time zones, and account data. Internet history (index.dat) and email communication stored in temporary files were analyzed to uncover user activity. Entropy and encryption analysis, alongside file signature analysis, revealed a mismatch file extension indicative of tempering. Manual extraction of connected USB and network logs provides further insight into external device usage and network activity.

File System Examination

There are many files and directories in the evidence image that have a lot of important information

- **Memopad.dat**
  It is a files that store information relevant to the program that created it like PDFs, email attachments, etc. Here in this, there is a discussion between Billy and chaser1191@hotmail.com here they discuss Kim and her friend Sabrina also about how much amount to ask for Ransomware
- **SAM registry file:**
  The SAM (security account manager) register file in the location "/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config/" was extracted and analyzed

using the Reg-Ripper tool. Through the analysis, it was found that there is only one user named Bob Hunter.

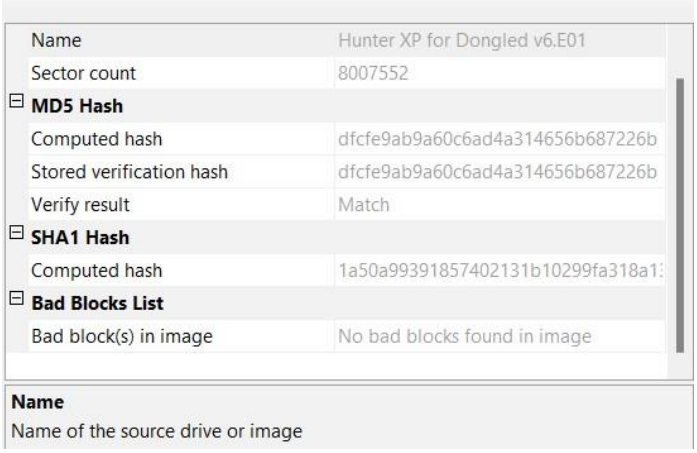
- **E-mail Messages**
  This folder lists all the email addresses present in the evidence image. This is obtained through a forensics examination of the evidence using the autopsy tool. The email message has shed light on the actual occurrence of the evidence of the event that has progressed on the days of May 14 to 20. The email ID used in the conversation threads and ransomware discussion between chaser1191@hotmail.com and friend@bemine.com ted.dewercs@encase.com and john.detsiwt@encase.com

Finding

1. **verify evidence integrity**

   ➢ To verify the image integrity of Hunter XP. I analyze the image file using an autopsy and FTK imager and check the hash value.

From FTK imager



from autopsy

The data sources verification result of hunter XP hash value is the same so the integrity of data wasn't compromised

2. **User Activity Analysis**

- **Active user account**: Bob Hunter
- **Last login activity:** Tue Jan 4 2002, 23:01:54 2002 UTC(from SAM file analysis)
- **Browsing history**: located in the index.dat file

Browsing history screenshot

```
Client UrlCache MMF Ver 5.2
HASH
z6#]
URL
Cookie:bob hunter@hotmail.msn.com/
bob hunter@hotmail.msn[1].txt
URL
Cookie:bob hunter@google.com/
bob hunter@google[1].txt
URL
Cookie:bob hunter@mediaplex.com/
bob hunter@mediaplex[1].txt
URL
Cookie:bob hunter@trafficmp.com/
bob hunter@trafficmp[2].txt
URL
Cookie:bob hunter@msn.com/
bob hunter@msn[2].txt
URL
~2tt
Cookie:bob hunter@doubleclick.net/
bob hunter@doubleclick[1].txt
URL
Cookie:bob hunter@7search.com/scripts
bob hunter@scripts[1].txt
URL
Cookie:bob hunter@clickbank.net/
bob hunter@clickbank[1].txt
URL
Cookie:bob hunter@www.addfreestats.com/cgi-bin
bob hunter@cgi-bin[1].txt
URL
Cookie:bob hunter@www.commission-junction.com/
bob hunter@www.commission-junction[1].txt
URL
Cookie:bob hunter@bfast.com/
bob hunter@bfast[2].txt
URL
Cookie:bob hunter@www.ci.mil.wi.us/bob hunter@www.ci.mil.wi[1].txt
URL
Cookie:bob hunter@statse.webtrendslive.com/S000-00-4-11-124357-1816bob hunter@S000-00-4-11-124357-1816[1].txt
URL
Cookie:bob hunter@mapquest.com/bob hunter@mapquest[1].txt
URL
Cookie:bob hunter@yahoo.com/
bob hunter@yahoo[1].txt
URL
Cookie:bob hunter@microsoft.com/
bob hunter@microsoft[1].txt
URL
Cookie:bob hunter@64.225.152.215/
bob hunter@64.225.152[1].txt
URL
Cookie:bob hunter@www.techdepot.com/
```

Hash Value:

MD5	8188afdda0fcf41d0b4da45737a9841d
SHA-256	2a0f41adb8d9275fc26cfd552205a6cc0fad46c67941c659fbefe2e598d69178

Login Details:-find by analysis the SAM file in Reg Ripper which is exported from "/img_Hunter XP for Dongled v6.E01/vol_vol2/WINDOWS/system32/config/

```
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
```

3. **Deleted and Recovered Files**

- Recovered images:
  File: Df826.JPG (suspected evidence found in /RECYCLER).

Fig:1 fig:2

The hash value of the Fig:1

MD5	3428d550b20e4c39df0b99c8425807d6
SHA-256	db1fb3f9fc2b6a68a782de901321d609a7e7b743a3b860cd6c21b0417359f5c9

The hash value of the Fig:2

MD5	fa64b24f10df62fb7c22241e75aa7929
SHA-256	3a6c800af7f807864a8f58b48f2d6a187d9bbf1b420e80c0fdc8fdd4a933e761

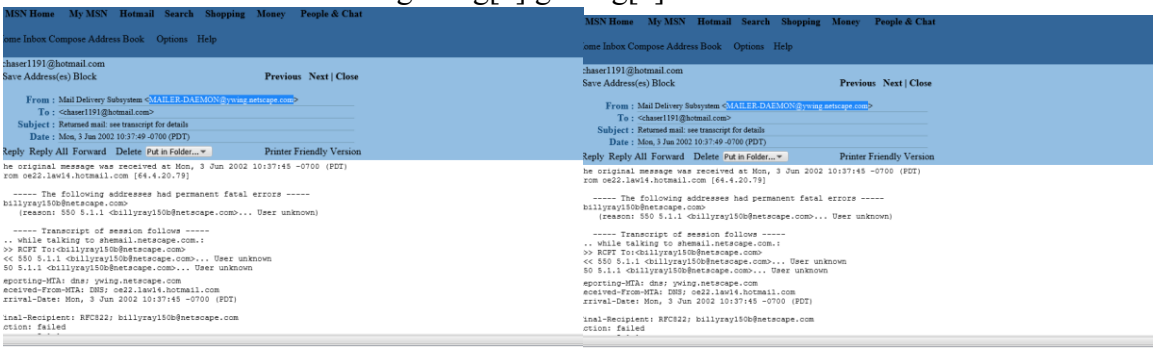
- Tampered Files:
  Example: aim10.tmp(GIF files with mismatch extension)

The hash value of tempered files:

MD5	632496573a1a699deb31707bca9dfea5
SHA-256	aee7bd1040e223dae10b3eb06651b00e86fcb77fa9bd3581ee700b750fa0cd14

4. **Email communication:**

- Emails showing involvement in ransomware discussions
- Emails IDs: friend@bemine.com, chaser1191@hotmail.com, billyray150b@netscape.com, MAILER-DAEMON@ywing.netscape.com,
- File path:/img_Hunter XP for Dongled v6.E01/vol_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/UFK38B83/getmsg[1]/getmsg[1]/0



Img1 img2

The hash value of the email img1

MD5	45e6ec03366c6c6a7973ab56fc4ce0a4
SHA-256	57dcc0927a31c0691b8093b6bebeedad43a927187f77bfd62d5b044257522d84

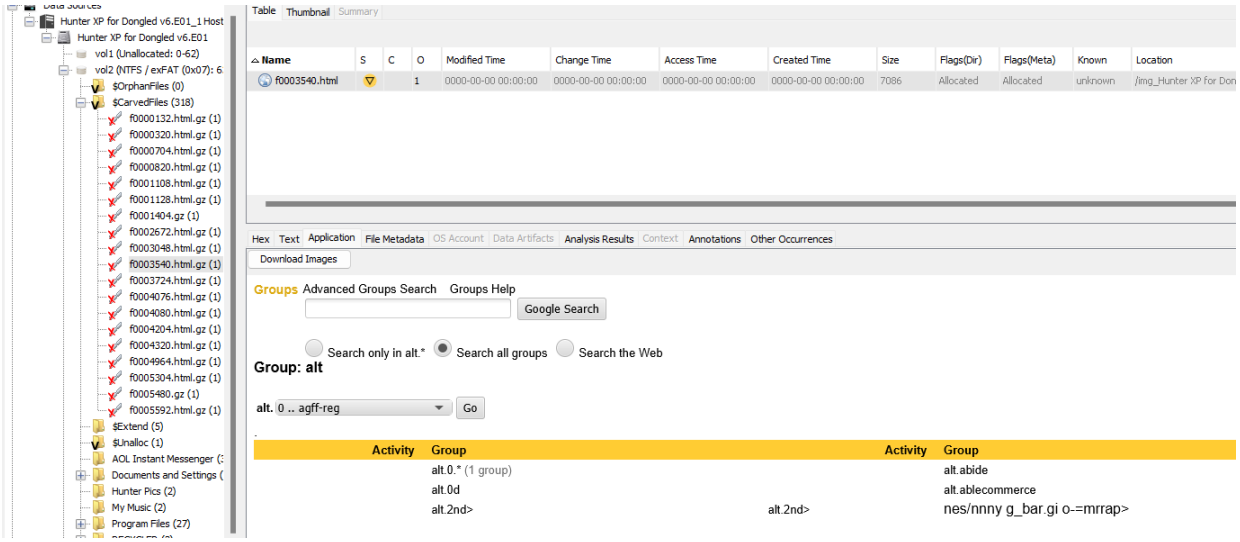
The hash value of the email img2

MD5	0cf2484e952ebee3fa1f2d1c2b556284
SHA-256	**949250ed2b519a25d03d7960cdf386b721e1b6db381941ee176117c5b08d38b2**

5. Encryption and wiping tools

- Tools Found: BCWipe, BestCrypt(it's a tool used to erase data from a computer)
- Location: /img_Hunter XP for Dongled v6.E01/vol_vol2//$CarvedFiles/

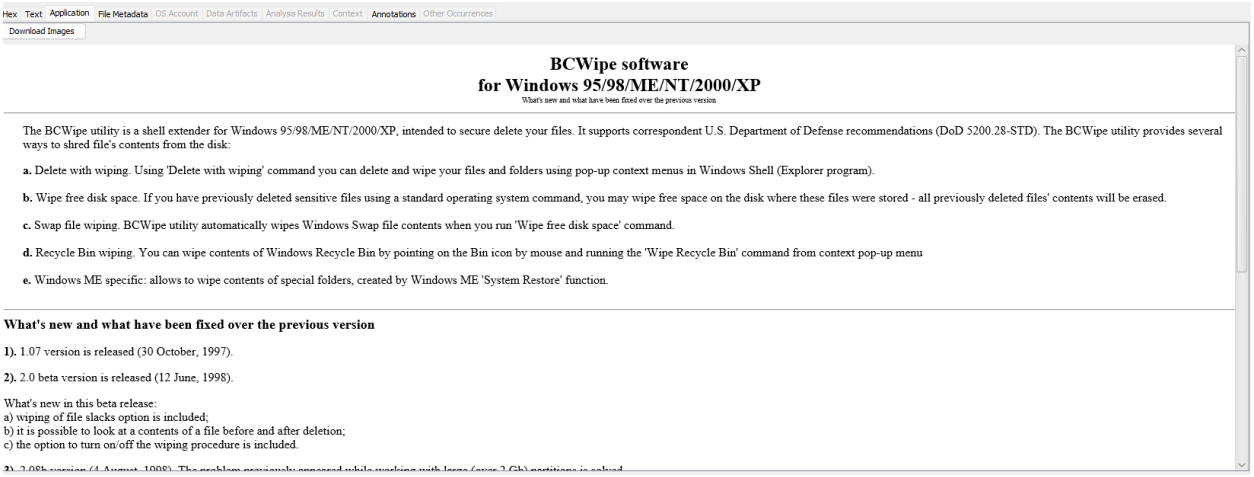
Encryption files



The hash value of encryption file

MD5	f45d4517ffd78bdaf63770bf77f4e97d
SHA-256	**2c83df69ef7fccd0f1748aeb4f32a24c52a3691c75afdf5ceeabd337c0538ee3**

Wiping tools



Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Download Images

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.

Hash value

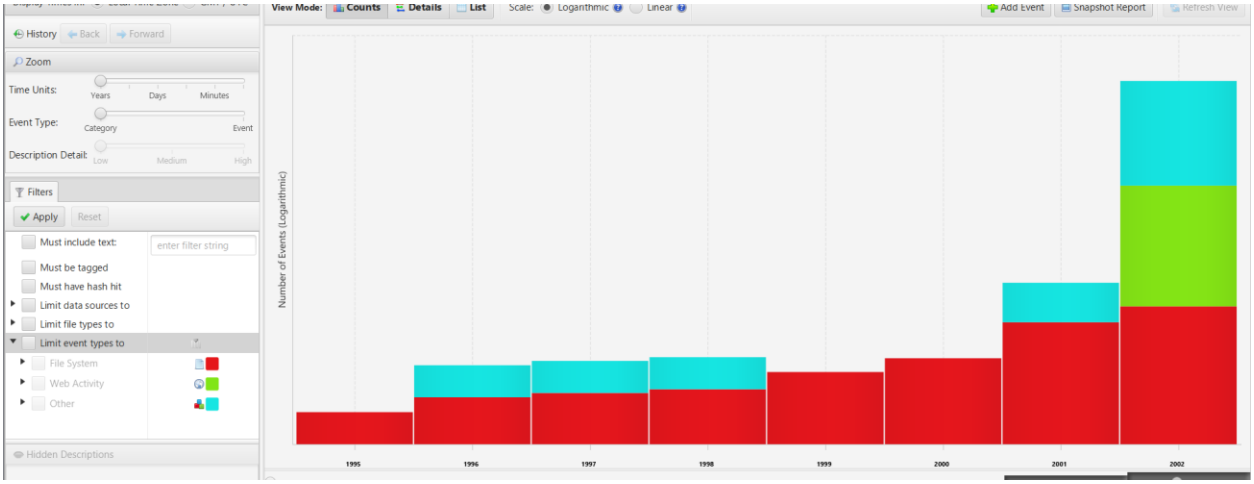
MD5	7bd4d1650d2b527c6f98cfd370b4062a
SHA-256	**9f2a1b4eb2331b47761387e37c438ac34830336bdc2617605dc579e926dab19d**

6. **External Devices and Network Logs:**

Connected devices like the USB IntelliMouse Explorer and CD-ROM drives were identified in `/system32/control2set/enum/`. Network connection details were located in `/etc/networks`. showing attempts to transfer or exfiltrate data, which strengthens the case timeline.

7. **Timeline Analysis:**

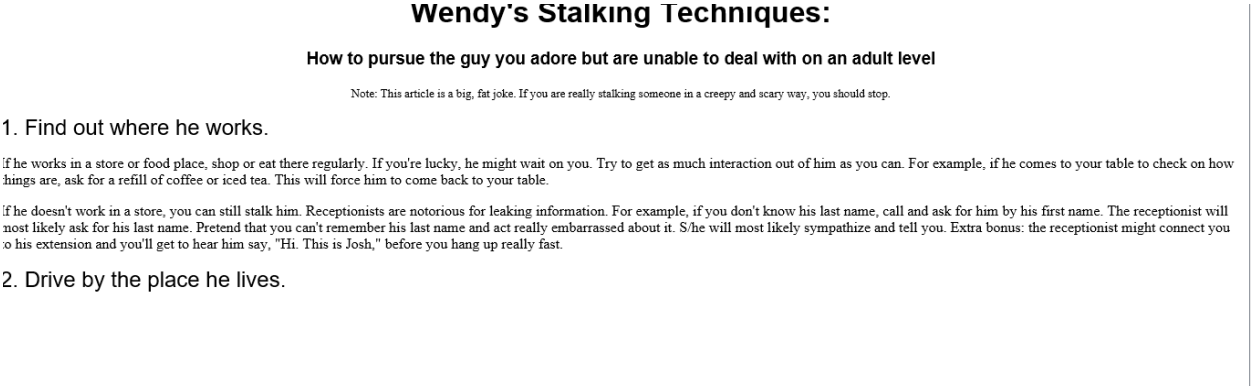
The SAM file and Plaso tool provided a detailed timeline of user activity, including logins, file system interactions, and web activity. Screenshots of these logs demonstrated a clear cause-and-effect sequence, linking key actions to the suspect's activities and establishing the incident's timeline.



8. **Staking:** - here in this screenshot I can find that the user has researched stalking

- Location: /img_Hunter XP for Dongled v6.E01/vol_vol2//$CarvedFiles/f0000000_The_Stalker_s_Home_Page_No_More_Privacy_As_Seen_on_the_LEEZA_ShowIs_Big_Brother_Watching.html

MD5:	ca2308cae91a8d9fd7a180420b02ab6f
SHA-256:	7865a22837b4f6112ee18dbd99cc9e8e70a37472d449442598d8d10e0e2681fe



Wendy's Stalking Techniques:

How to pursue the guy you adore but are unable to deal with on an adult level

Note: This article is a big, fat joke. If you are really stalking someone in a creepy and scary way, you should stop.

1. Find out where he works.

If he works in a store or food place, shop or eat there regularly. If you're lucky, he might wait on you. Try to get as much interaction out of him as you can. For example, if he comes to your table to check on how things are, ask for a refill of coffee or iced tea. This will force him to come back to your table.

If he doesn't work in a store, you can still stalk him. Receptionists are notorious for leaking information. For example, if you don't know his last name, call and ask for him by his first name. The receptionist will most likely ask for his last name. Pretend that you can't remember his last name and act really embarrassed about it. S/he will most likely sympathize and tell you. Extra bonus: the receptionist might connect you to his extension and you'll get to hear him say, "Hi. This is Josh," before you hang up really fast.

2. Drive by the place he lives.

- Location:-/img_Hunter XP for Dongled v6.E01/vol_vol2//$CarvedFiles/f0001512_Wendy_Stalking_Techniques.html

MD5:	73bb54bc655a671c02be60fc13472916
SHA-256:	06ad8bcf7f384f44917d690b3663e2012fdc2115b545ac9ca6b80227cb702e44

8. Others: -

- File name: or_else[1].thm (This message seems to be part of a ransom or phishing attempt. It could involve kidnapping, or a scam designed to extract sensitive banking details under duress)

I think its time we hear from you!

We are going to do a wire bank transfer. Click here and put in your bank routing number and account number. We want $1 Million for each of the girls safety. So better work fast, you have only 24 hours to reply to this message!

Yes, I will pay you!

No, I am not paying you!

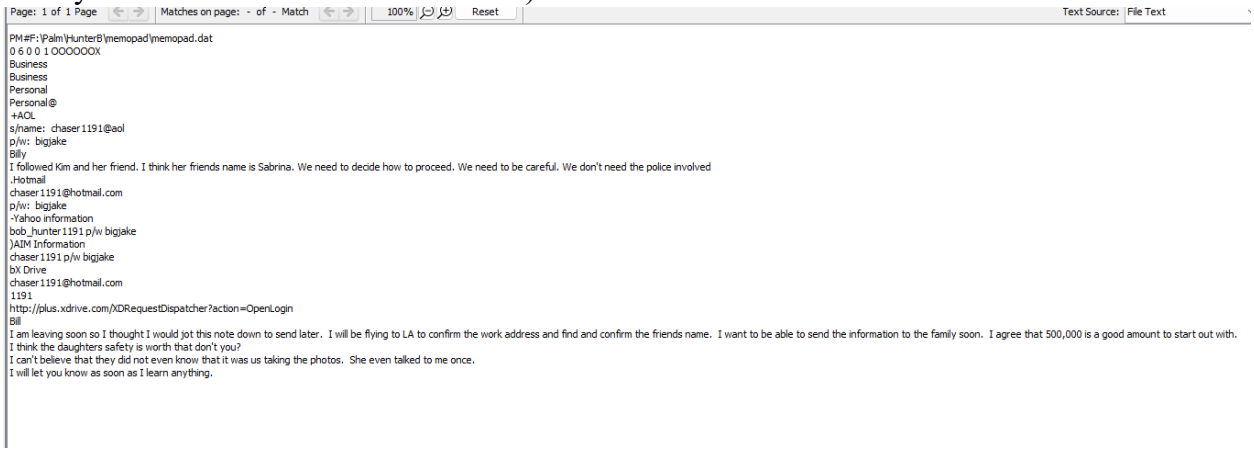
MD5:

2d2eb087cfb1e20d41b35cd2f48c597a

SHA-256:

2918c163bc582e88764220311afea929777b15ceb72a3efd9e4a942436af5632

- File name: Memopad.dat (This file involves private or potentially sensitive information, possibly related to surveillance, tracking, or negotiations. The reference to a large sum of money could indicate a serious situation.)



MD5:

09b75ffa6b31fb769431832e03af82f8

SHA-256:

eefe64b6da96e52c0a24505330085885e1b48f5edcfac4a3799bba649a248f6f

- **Summary Table of Evidence**

Here's a concise table you can add to highlight your findings:

Evidence Type	Details	Location	Tools Used
Integrity Verification	Hash values match	FTK Imager and Autopsy	FTK Imager and Autopsy
Internet History	Visited suspicious websites	index.dat	Manual, Event Log Viewer
Active User	Bob Hunter, last login: Jun 4, 2002	SAM file	RegRipper
Emails	Ransomware discussions	/Temporary Internet Files	Manual analysis
Deleted Files	Recovered Df826.JPG	/RECYCLER	PhotoRec, Autopsy
File Signature Tampering	aim10.tmp (GIF file)	/vol_vol2	Autopsy
Encryption/Wiping Tools	BCWipe, BestCrypt	/CarvedFiles	Manual extraction
External Devices	USB devices, CD-ROM drives	/control2set/enum/	Manual analysis

Conclusion:

The forensic investigation of the "Hunter XP" disk image has provided compelling evidence linking Bob Hunter to serious criminal activities, including ransomware deployment, extortion, data manipulation, and conspiracy. The examination revealed a coordinated effort to execute and conceal these crimes, as demonstrated by the following findings:

- User Activity and Identity: Analysis of system files confirmed "Bob Hunter" as the active user, with documented login details and browsing history consistent with the timeline of the offenses.
- Incriminating Email Evidence: Email communications recovered from the disk show explicit discussions of ransom demands and negotiations, implicating the user in extortion activities.
- Manipulated and Deleted Files: Evidence of file tampering and recovered deleted files supports attempts to cover tracks and hide illicit activities.
- Use of Concealment Tools: Tools such as BCWipe and BestCrypt were found, indicating a deliberate effort to encrypt sensitive information and erase evidence.
- External Devices and Data Transfers: Logs of external device usage and network connections suggest unlawful attempts to transfer or exfiltrate data.
- Timeline Validation: Comprehensive timeline reconstruction corroborates the sequence of events, linking user actions to criminal outcomes.

The integrity of the evidence was confirmed through hash value verification, ensuring the reliability of the digital artifacts. The recovered data, combined with an analysis of network and device activity, demonstrates clear intent and direct involvement in these unlawful actions.

This evidence constitutes a solid and irrefutable basis to pursue legal actions against Bob Hunter, with findings that establish culpability beyond reasonable doubt.

Appendix: