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](mailto: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**

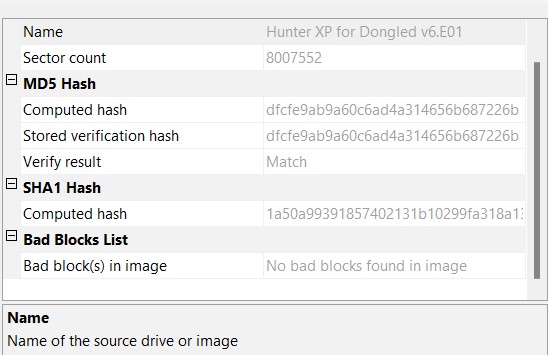
This folder lists all the email addresses present in the evidence image. This is obtained through a forensics examination of the evidence using the autopsy tool. The email message has shed light on the actual occurrence of the evidence of the event that has progressed on the days of May 14 to 20. The email ID used in the conversation threads and ransomware discussion between [chaser1191@hotmail.com](mailto:chaser1191@hotmail.com) and [friend@bemine.com](mailto: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



A close up of a computer screen

Description automatically generated from autopsy

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

A screenshot of a computer

Description automatically generated

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

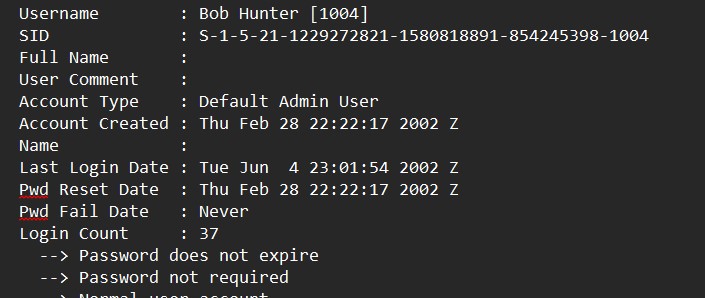
A screenshot of a computer

Description automatically generated

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/



3. **Deleted and Recovered Files**

* Recovered images:

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

A couple of women walking on a beach

Description automatically generated

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)

A blue square with a white letter u and a square hat with red text

Description automatically generated

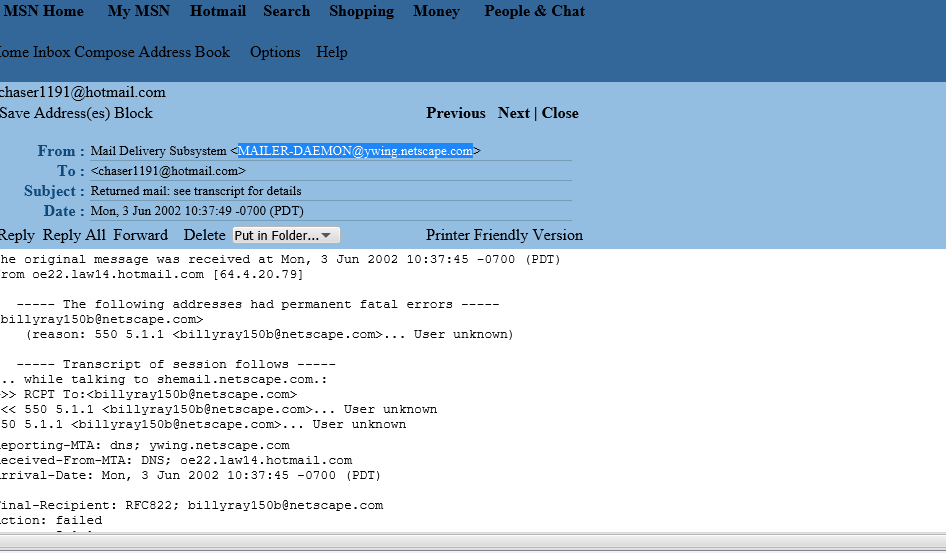
The hash value of tempered files:

|  |  |  |
| --- | --- | --- |
| MD5 | |  | | --- | | 632496573a1a699deb31707bca9dfea5 | |
| SHA-256 | aee7bd1040e223dae10b3eb06651b00e86fcb77fa9bd3581ee700b750fa0cd14 |

4. **Email communication:**

* Emails showing involvement in ransomware discussions
* Emails IDs: [friend@bemine.com](mailto:friend@bemine.com), [chaser1191@hotmail.com](mailto:chaser1191@hotmail.com), [billyray150b@netscape.com](mailto:billyray150b@netscape.com), [MAILER-DAEMON@ywing.netscape.com](mailto: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

A screenshot of a computer

Description automatically generated

Img1 img2

The hash value of the email img1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MD5 | |  |  |  | | --- | --- | --- | | |  |  | | --- | --- | |  | 45e6ec03366c6c6a7973ab56fc4ce0a4 | | |
| SHA-256 | |  | | --- | | 57dcc0927a31c0691b8093b6bebeedad43a927187f77bfd62d5b044257522d84 | |

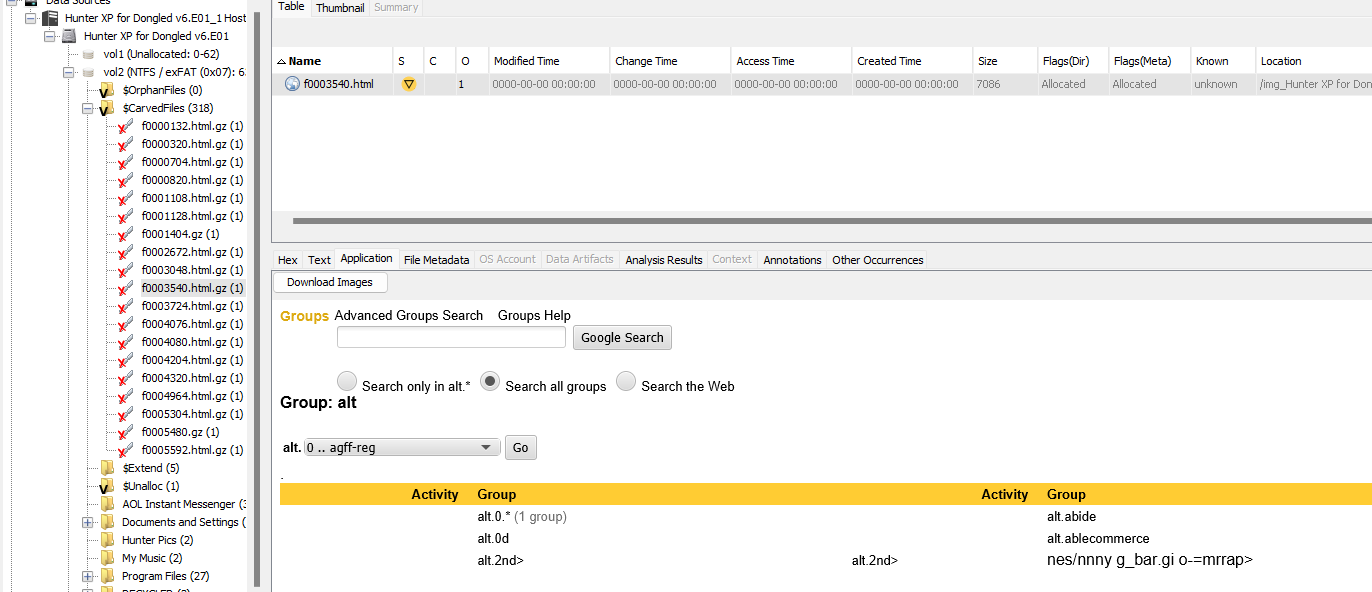
The hash value of the email img2

|  |  |  |  |
| --- | --- | --- | --- |
| 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

A screenshot of a computer

Description automatically generated

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.

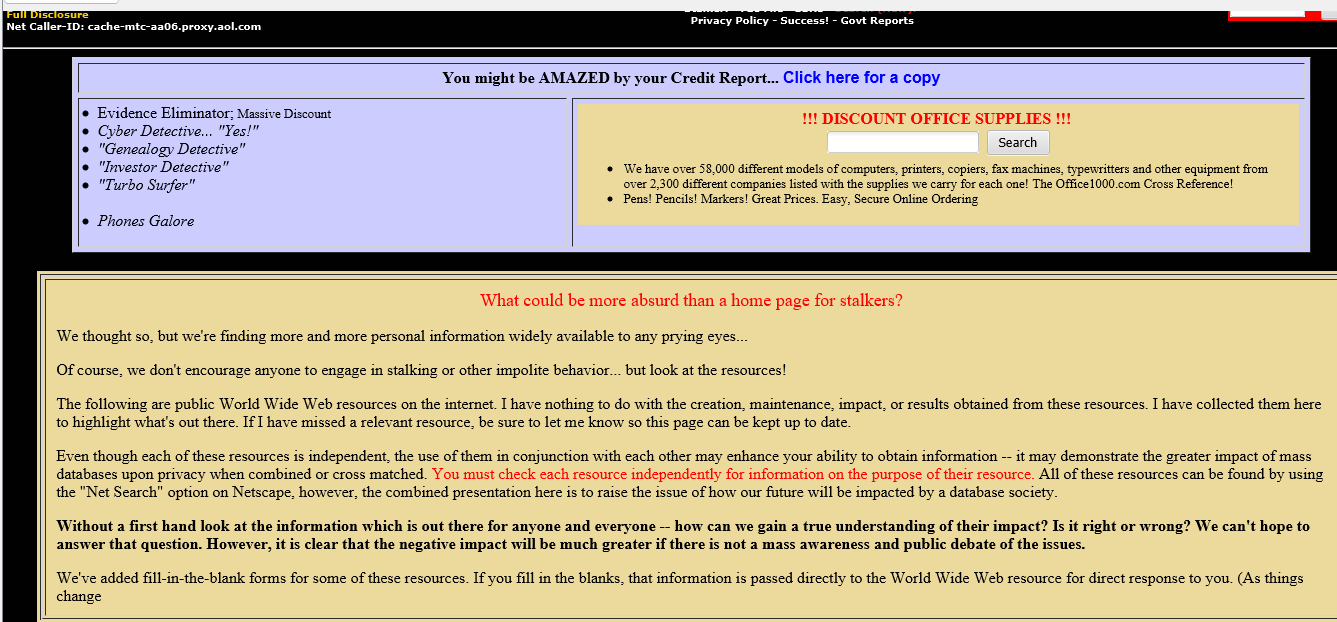
7. **Timeline Analysis:**

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.

A screen shot of a graph

Description automatically generated

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 |

A white paper with black text

Description automatically generated

* 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)

A close-up of a computer screen

Description automatically generated

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.)A screenshot of a computer

  Description automatically generated

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:**

A pie chart with text and numbers

Description automatically generated

A screenshot of a computer

Description automatically generated