Digital Forensic Analysis Report Using Autopsy

This forensic investigation report focuses on the analysis of a seized hard drive, referred to as “image washer.” The aim is to uncover and document digital evidence related to suspected criminal activity, with a forensic methodology that ensures legal admissibility.

The report sets the foundation for the forensic analysis, emphasizing the recovery of digital evidence in a legally sound manner. The primary tool used for investigation is Autopsy 4.21.0. Details the use of Autopsy to examine the hard disk, extract data, and analyze user profiles, emails, and web activities. The emails link to a fraudulent operation involving stolen credit cards, password theft, and website spoofing.

**Table of Contents**

1. **Introduction…………………………………………………………………………………………………………………….**
2. **Software Information………………………………………………………………………………………………………**
3. **Main Body……………………………………………………………………………………………………………………….**

3.1 Forensics Analysis of the Case………………………………………………………………………………….

3.2 Time Zone Analysis……………………………………………………………………………………………………………

3.3 Operating System Information……………………………………………………………………………………………

3.4 Software programs and its installations……………………………………………………………………….

3.5 Documents, media, pictures……………………………………………………………………………………….

3.6 User Information……………………………………………………………………………………….

3.7 USB Device Attached ………………………………………………………….

3.8 Internet Activity ………………………………………………………….

3.8.1 Web Bookmark……………………………………………………

3.8.2 Web Cookies………………………………………………………………………………..

1. **Conclusion……………………………………………………………………………………………………………………….…**
2. **Appendices……………………………………………………………………………………………………………………...**

**1 Introduction**

This report's objective is to perform a digital forensic analysis on an image washer, a hard drive that was seized. Its main objective is to locate and obtain data using forensic techniques. The study is to follow information trails to rebuild the timeline and offer a thorough comprehension. The report carefully records processes in accordance with legal requirements, guaranteeing its admissibility in court.

**2 Software Information**

For the inquiry, Autopsy 4.21.0 was used, which provides a structured report format with subcategories. The primary section centers on the information retrieved from the HDD and hardware components connected to the system. Profiles explore the personal lives of those who use this device. The goal of email forensics is to offer digital evidence that can be admitted in court by carefully examining emails to confirm authenticity, identify sender, recipients, source, and timestamps in a way that is compliant with the law. The relevance of the website is found in the extensive log of actions exchanged by a group engaged in fraudulent activities, including the use of fictitious credit cards and techniques for password theft via agent installation. An essential component of investigations, timeline analysis helps create event and computer usage sequences. For this, Autopsy's sophisticated timeline interface is utilized.

**3 Main Body**

**3.1 Forensic Analysis of the Case:**

These report sections provide critical analyses of the key suspects and evidence in the case. They provide in-depth insights regarding every suspicious document, file, and folder that they painstakingly describe. After a careful inspection, the hard drive displays a variety of dubious components from the picture that have been painstakingly dissected and examined for certain results. The email part, for example, reveals the sophisticated plan used by the skimmers to steal credit card numbers, PINs, and create fictitious cards that are verified by Luhn's Algorithm.

The study reveals the strategies used by the skimmer organization, such as inserting an XRAY trap film inside ATMs to capture card and PIN information. Significantly, the identification of files such as validateCard.jar reveals techniques for verifying credit card data and an effective HTTrack utility for website replication and abuse.

Some documents, such as "How to Steal Credit Numbers.doc" and "AllStateCreditCardAgency.doc," contain important information that has been mentioned in emails but cannot be accessed because they are password protected. These documents' contents, which are thought to include information on credit card theft, are still secret.

**3.2 Time Zone Analysis**

The Time zone is  Europe/London BST and GMT. From the installation of the operating system (Fig 2) on Mon Mar 10 23:44:32 2008 BST to Mon Mar 10 23:44:32 2008 GMT. (Fig 1).

**3.3 Operating System Information**

| **Program Name** | Microsoft Windows XP |
| --- | --- |
| **Name** | WASHER1 |
| **Product ID** | 55274-338-5471047-22865 |
| **Artifact ID** | 9223372036854775469 |
| **Owner** | John Washer |
| **Acquisition Details** | Description: Drive from Office Computer  Case Number: 08-12345  Evidence Number: AD-08-98  Examiner Name: Nick Drehel  Acquiry Software Version: FTKI2.5.3.14 |
| **Device ID** | c5bff3ba-520f-4cbe-acf5-a9f694de0aa3 |
| **Date/Time of Installation:** | 2007-07-25 06:16:06 BTS |
| **Processor Architecture:** | x86 |
| **Program Name:** | Microsoft Windows XP |
| **File System Type:** | NTFS |

**3.4 Software Program Installation**

The hardware devices detected within the hard disk are listed in the subsequent table. A total of 23 installed programs are identified and thoroughly outlined in the table below.

| WinZip 11.1 v.11.1.7466 | 2008-02-13 01:17:01 GMT |
| --- | --- |
| WebFldrs XP v.9.50.5318 | 2007-08-04 21:19:51 BST |
| Microsoft NetShow Player 2.0 | 2007-08-04 21:19:49 BST |
| MPlayer2 | 2007-08-04 21:19:49 BST |
| Viewpoint Media Player | 2007-07-25 13:52:43 BST |
| Adobe Flash Player 9 ActiveX v.9 | 2007-07-25 21:38:30 BST |
| AOL Instant Messenger | 2007-07-25 21:14:06 BST |
| Branding | 2007-07-25 21:13:05 BST |
| PCHealth | 2007-07-25 21:13:01 BST |
| AddressBook | 2007-07-25 21:13:01 BST |
| DirectAnimation | 2007-07-25 21:13:01 BST |
| ICW | 2007-07-25 21:13:01 BST |
| NetMeeting | 2007-07-25 21:13:01 BST |
| OutlookExpress | 2007-07-25 21:12:58 BST |
| DirectDrawEx | 2007-07-25 01:12:58 BST |
| Fontcore | 2007-07-25 01:12:58 BST |
| IE40 | 2007-07-25 01:12:58 BST |
| IE4Data | 2007-07-25 01:12:58 BST |
| IE5BAKEX | 2007-07-25 01:12:58 BST |
| IEData | 2007-07-25 01:12:58 BST |
| MobileOptionPack | 2007-07-25 01:12:58 BST |
| SchedulingAgent | 2007-07-25 01:12:58 BST |
| Connection Manager | * + 1. 01:07:57 BST |

**3.5 Documents, media, pictures**

1. Found a document

| **Buy peanut butter**  **· Call mom**  **· Kill Familiars**  **· Burry Wes’s enemies**  **· Confess to the police**  **Click here for something funny!**  **------------------------------METADATA------------------------------**  **Application-Name: Microsoft Office Word**  **Author: John Washer**  **Character Count: 157**  **Comments: If you are reading this then you are snooping and I know where you live!**  **Company:**  **Content-Type: application/msword**  **Creation-Date: 2008-02-12T00:46:00Z**  **Edit-Time: 5400000000**  **Keywords:**  **Last-Author: John Washer**  **Last-Modified: 2008-02-12T00:55:00Z**  **Last-Save-Date: 2008-02-12T00:55:00Z**  **Page-Count: 1**  **Revision-Number: 2**  **Template: Normal**  **Word-Count: 39**  **X-Parsed-By: org.apache.tika.parser.DefaultParser**  **comment: If you are reading this then you are snooping and I know where you live!**  **cp:revision: 2**  **cp:subject: Things I have to do before I turn**  **creator: John Washer**  **custom:Owner: true**  **custom:Telephone number: 555-555-1212**  **date: 2008-02-12T00:55:00Z**  **dc:creator: John Washer**  **dc:subject:**  **dc:title: To Do List**  **dcterms:created: 2008-02-12T00:46:00Z**  **dcterms:modified: 2008-02-12T00:55:00Z**  **extended-properties:Application: Microsoft Office Word**  **extended-properties:Company:**  **extended-properties:Template: Normal**  **meta:author: John Washer**  **meta:character-count: 157**  **meta:creation-date: 2008-02-12T00:46:00Z**  **meta:keyword:**  **meta:last-author: John Washer**  **meta:page-count: 1**  **meta:save-date: 2008-02-12T00:55:00Z**  **meta:word-count: 39**  **modified: 2008-02-12T00:55:00Z**  **subject: Things I have to do before I turn**  **title: To Do List**  **w:comments: If you are reading this then you are snooping and I know where you live!**  **xmpTPg:NPages: 1** |
| --- |

2 I found a picture with the name of bad day Appendix (Fig 6). In this picture we can clearly see a crashed plane on the shore of sea.

3 I have found two pictures of men holding a fish in their hands in the ship. The pictures captured in the year of 2007. Appendix (Fig 7,8).

4 Found a picture of plane while launching some missiles. Appendix (Fig 9)

5 A horrible cat Appendix (Fig 10).

6 Kangaro Appendix (Fig 11)

7 Found a text file having sensitive information like username and password in encrypted form, Its written in it. (Fig 12).

| HTTrack3.42+htsswf+htsjava launched on Wed, 13 Feb 2008 08:34:11 at http://www.kli.org/ +\*.png +\*.gif +\*.jpg +\*.css +\*.js -ad.doubleclick.net/\* -mime:application/foobar  (winhttrack -qwr2%e0C2%Ps2u1%s%uN0%I0p3DaK0H0%kf2A25000%f#f -F "Mozilla/4.5 (compatible; HTTrack 3.0x; Windows 98)" -%F "<!-- Mirrored from %s%s by HTTrack Website Copier/3.x [XR&CO'2007], %s -->" -%l "en, en, \*" http://www.kli.org/ -O1 "C:\My Web Sites\Klingon Lang Site" +\*.png +\*.gif +\*.jpg +\*.css +\*.js -ad.doubleclick.net/\* -mime:application/foobar )  Information, Warnings and Errors reported for this mirror:  note: the hts-log.txt file, and hts-cache folder, may contain sensitive information,  such as username/password authentication for websites mirrored in this project  do not share these files/folders if you want these information to remain private  08:34:12 Info: Note: due to www.kli.org remote robots.txt rules, links begining with these path will be forbidden: /tlhIngan-Hol/, /ftppub/, /kli/membermails.html (see in the options to disable this)  HTTrack Website Copier/3.42 mirror complete in 54 seconds : 116 links scanned, 115 files written (726091 bytes overall) [765299 bytes received at 14172 bytes/sec], 16.5 requests per connection  (No errors, 0 warnings, 1 messages)  ------------------------------METADATA------------------------------ |
| --- |

8 Found some document having sensitive information about All state credit agency and How to steal credit numbers but it is password protected. (Fig 13)

**3.6 Users Information**

Information about users and profiles will be presented in the upcoming table. This includes default users as well as those specifically created by the hard disk owner. The goal is to provide a comprehensive overview of the entire user base by elaborating on each of these entries. (Fig 3).

| **Login Name** | **Host** | **Creation Time** |
| --- | --- | --- |
| HelpAssistant | Washer.E01\_1 Host | 2007-07-25 02:11:56 BST |
| Billy Bob Brubeck | Washer.E01\_1 Host | 2007-08-04 02:14:13 BST |
| SUPPORT\_388945a0 | Washer.E01\_1 Host | 2007-07-25 02:13:42 BST |
| Mr Smee | Washer.E01\_1 Host | 2007-08-04 02:18:00 BST |
| The Wolf | Washer.E01\_1 Host | 2007-08-04 02:15:03 BST |
| Captian Hook | Washer.E01\_1 Host | 2007-08-04 02:18:11 BST |
| Artimus | Washer.E01\_1 Host | 2008-02-13 01:13:46 GMT |
| Guest | Washer.E01\_1 Host | 2007-07-24 19:57:36 BST |
| Administrator | Washer.E01\_1 Host | 2007-07-24 19:57:36 BST |
| SYSTEM | Washer.E01\_1 Host |  |
| LOCAL SERVICE | Washer.E01\_1 Host |  |
| NETWORK SERVICE | Washer.E01\_1 Host |  |

**3.7 USB Device Attached**

The table below showcases the hardware devices detected on the hard disk. (Fig 15).

| Date/Time | Device Make | Device Model |
| --- | --- | --- |
| 2008-03-10 08:11:21 GMT |  | ROOT\_HUB |
| 2008-03-10 08:11:25 GMT |  | ROOT\_HUB |
| 2008-03-10 08:11:25 GMT |  | ROOT\_HUB |
| 2008-03-10 08:11:25 GMT |  | ROOT\_HUB |
| 2008-02-13 05:33:30 GMT | Silicon Integrated Systems Corp. | Super Flash 1GB / GXT 64MB Flash Drive |
| 2008-02-13 02:16:24 GMT | Apple, Inc. | iPod Video |
| 2008-02-13 05:22:08 GMT | SanDisk Corp. | SDCZ2 Cruzer Mini Flash Drive (thin) |
| 2008-03-10 08:39:49 GMT | SanDisk Corp. | SDCZ2 Cruzer Mini Flash Drive (thin) |
| 2007-07-25 19:22:29 BST | SanDisk Corp. | SDCZ2 Cruzer Mini Flash Drive (thin) |
| 2008-03-10 08:07:30 GMT | Trek Technology (S) PTE, Ltd | Product: 9005 |
| 2008-03-10 08:11:22 GMT | Linksys | WUSB54G v4 802.11g Adapter [Ralink RT2500USB] |

**3.8 Internet activity**

**3.8.1 Web Bookmark:**

| **Domain** | **Title** | **Data Source** | **Date created** | **Program Name** |
| --- | --- | --- | --- | --- |
| microsoft.com/ | Customize Links.url | Washer.E01 | 2007-08-04 02:18:34 BST | Internet Explorer Analyzer |
| microsoft.com/ | Free Hotmail.url  Windows | Washer.E01 | 2007-08-04 02:18:34 BST | Internet Explorer Analyzer |
| microsoft.com/ | Media.url | Washer.E01 | 2007-08-04 02:18:34 BST | Internet Explorer Analyzer |
| microsoft.com/ | Windows.url | Washer.E01 | 2007-08-04 02:18:34 BST | Internet Explorer Analyzer |
| microsoft.com/ | MSN.com.url | Washer.E01 | 2007-08-04 02:18:34 BST | Internet Explorer Analyzer |
| microsoft.com/ | Radio Station Guide.url | Washer.E01 | 2007-08-04 02:18:34 BST | Internet Explorer Analyzer |

(Fig 4)

# **3.8.2 Web Cookies:**

| **Date Created** | **Domain** | **Description** | **Name** |
| --- | --- | --- | --- |
| 2007-07-25 20:10:09 BST | atwola.com/ | Flagged as distributes malware or unwanted file download. | badsrfi |
| 2007-07-25 02:35:28 BST | aol.com | online service provider ,Email Services | RSP\_COOKIE |
| 2007-07-25 02:37:45 BST | aim.com | IMAP access to your *Aim.com* (AOL Mail | s\_p\_s\_prop14 |
| 2007-07-25 19:23:52 BST | Ads.pointroll.com | Business name generator | PRID |
| 2007-07-25 20:10:33 BST | advertising.com | *Advertising.com*, now a part of ONE by AOL, enables marketers to reach consumers via programmatic buying and performance-driven campaign | ACID |
| 2007-07-25 18:51:32 BST | partner2profit.com | *Reported as spyware* <https://github.com/dyne/dowse/blob/master/conf/blocklists/spyware.p2p> | Ccode |
| 2007-07-25 02:35:29 BST | *edge.ru4.com* | *RU4.com* operates as an advertising company that is part of a network of sites, | ru4.uid |
| 2007-07-25 02:43:45 BST | atdmt.com | *ATDMT* is a tracking cookie served by Facebook | *AA002* |

(Fig 5)

**4. Conclusion**

A thorough analysis of all the evidence acquired will be done in the report's last part. Through an examination of the important questions of What, How, Why, and When, this research seeks to shed light on the suspects' motivations. The report will carefully review the information gathered to address the problems indicated above by utilising a timeline analysis.

The discovered hard drives have a lifespan ranging from 2000 to 2008. Interestingly, the evidence found fits the period from July 2007 to February 2008.

In order to solve the enigma of the Washer Use case, this section methodically examines the What, How, Why, and When factors. A targeted analysis is carried via applying autopsy's Timeline filter, which filters file kinds and events to extract crucial information that makes the connections. Although the hard disc was manufactured between 2000 and 2008, crucial incidents that are crucial to the case happened between 2007 and 2008.A screenshot of a computer

Description automatically generated

(Fig 16)

A screenshot of a computer

Description automatically generated

(Fig 17)

**5 Appendices**  
A screenshot of a computer

Description automatically generated

Fig 1

A screenshot of a computer

Description automatically generated

Fig 2

A screenshot of a computer

Description automatically generated

Fig 3

A screenshot of a computer

Description automatically generated

Fig 4

A screenshot of a computer

Description automatically generated

Fig 5

A screenshot of a computer

Description automatically generated

Fig 6

A screenshot of a computer

Description automatically generated

Fig 7

A screenshot of a computer

Description automatically generated

Fig 8

A screenshot of a computer

Description automatically generated

Fig 9

A screenshot of a computer

Description automatically generated

Fig 10

A screenshot of a computer

Description automatically generated

Fig 11

A screenshot of a computer

Description automatically generated

Fig 12

A screenshot of a computer

Description automatically generated

Fig 13

A screenshot of a computer

Description automatically generated

Fig 14

A screenshot of a computer

Description automatically generated

Fig 15