Summary Digital Forensic Report

Prepared for CLIENT XYZ

Case Number: 0010

**John Doe**

Case Name

Digital Forensic Analyst

C5W Cybercrime Unit

## Table of Contents

Cover Page ……………………………………………………………………………………………….1

Table of Contents ………………………………………………………………………………………...2

Executive Summary ……………………………………………………………………………………..3

Investigation Details ……………………………………………………………………………………..4

Acquisition and Handling of Evidence ………………………………………………………...4

Investigation Environment ……………………………………………………………………...4

Tools Used in Analysis ………………………………………………………………………….4

Investigation Scope ……………………………………………………………………………..4

Evidence Overview ………………………………………………………………………………………5

Analysis Overview ……………………………………………………………………………………….7

## Executive Summary

## Investigation Details

### 2.1 Acquisition and Handling of Evidence

How the evidence was handled and copied to workstation

### 2,2 Investigation Environment

OS Name: Microsoft Windows 10 Enterprise 2016 LTSB

Version: 10.0.14393 Build 14393

OS Manufacturer: Microsoft Corporation

System Name: FORENSICVDI-047

System Manufacturer: VMWare, Inc.

System Model: VMWare Virtual Platform

System Type: x64-based PC

### 2.3 Tools Used in Analysis

HashMyFiles (version number not available)

Magnet AXIOM Examine (version number not available)

Magnet AXIOM Process v3.9.0.18130

| Name | Version | Hashes | Notes |
| --- | --- | --- | --- |
| [AXIOM](http://www.magnetforensics.com) |  |  |  |
|  |  |  |  |

### 2.4 Investigation Scope

Scope of work done, this will help you avoid Scope creep.

## Evidence Overview

Table 3-1: Disk Image and Case File

| File | MD5 Hash | SHA1 Hash | File Size (Bytes) |
| --- | --- | --- | --- |
| ForensicImage.E01 | 1234567890aed57b217737585a999ddd | 123456789073c5b755cef7932b4e8f9fe211b363 | 6,308,012,554 |
| files.db | 1234567890aed57b217737585a999ddd | 123456789073c5b755cef7932b4e8f9fe211b363 | 2,058,278,218 |
| Memory.dmp | 1234567890aed57b217737585a999AAA |  | 40000096 |

Table 3-2: Extracted Image Files

| Original File URL | Extracted File | MD5 Hash | SHA1 Hash | File Size (Bytes) | Evidence Figure |
| --- | --- | --- | --- | --- | --- |
|  | 1\_Carved.jpeg | 1234567890aed57b217737585a999ddd | 123456789073c5b755cef7932b4e8f9fe211b363 | 116011 | 3.1 |
|  | 2\_Carved.jpeg | 1234567890aed57b217737585a999ddd | 123456789073c5b755cef7932b4e8f9fe211b363 | 171858 | 3.2 |
|  | 3\_Carved.jpeg | 1234567890aed57b217737585a999ddd | 123456789073c5b755cef7932b4e8f9fe211b363 | 117713 | 3.3 |

## Analysis Overview

### 4.1 Processing Evidence:

### 4.2 Examining Processed Evidence to Answer Questions

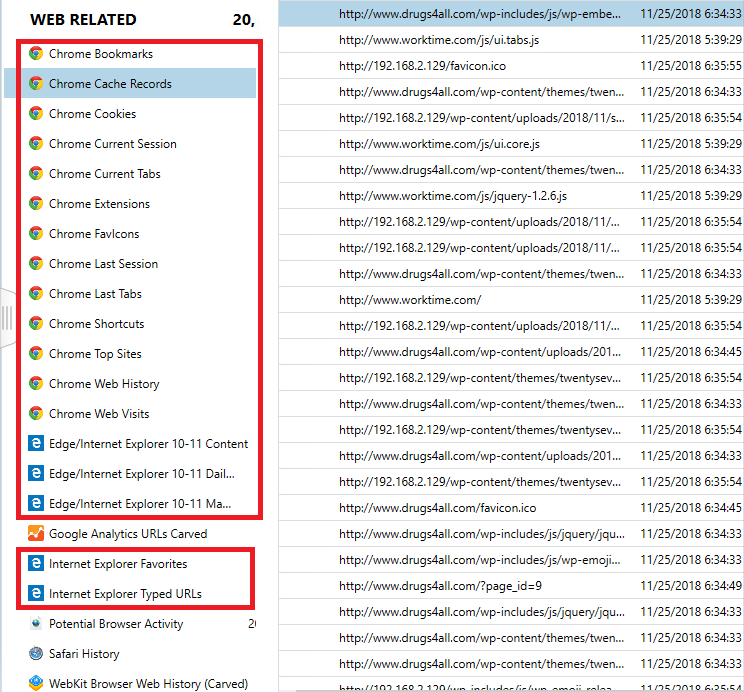
1. What web browsers did the employee use on his/her system?  
     
   By viewing the sections under “Web Related” in the case file with Magnet AXIOM Examine, I found three unique web browsers: Google Chrome, Internet Explorer, and Safari (See figure 4.3). However, because Safari is not a web browser used on Windows operating systems, it would not be included in this count. I was left with two web browsers that the employee used on their system: Google Chrome and Internet Explorer.  
     
     
   Figure 4.3: Web related artifacts. Highlighted: Valid web browsers used by the employee.
2. What are the websites (in terms of URLs) that the user visited?  
     
   From examining the contents of the “Chrome Web Visits” and “Edge/Internet Explorer 10-11 Main History”, I found the information about the employee website visits that I’ve outlined in Table 4-1.

Table 4-1 Web Visit Information

| Website URL | # of Visits | Website Title | Date/Time Range |
| --- | --- | --- | --- |
| worktime.com | 6 | Welcome to WorkTime | 11/25/2018 5:39:29PM-6:34:06PM |
| yahoo.com | 7 | N/A | 11/25/2018 6:01:40PM |
| go.microsoft.com | 2 | N/A | 11/25/2018 5:41:43PM |
| msn.com | 2 | N/A | 11/25/2018 5:41:48PM |
| drugs4all.com | 4 | support you! | 11/25/2018 6:34:33PM-6:37:21PM |
| google.com | 3 | N/A | 11/25/2018 6:01:43PM |

## Conclusion

## 

## Appendix

### Appendix A : Execution OS Artifacts

### 

### Appendix B : Terms