Forensics investigation

Jewelry store Jan Goud

Version: 1.0  
Date: <Date>

ColoPhon

|  |  |
| --- | --- |
| **NORTHWAVE BV**  **Office address:**  Marconibaan 49, 3439 MR Nieuwegein  **Postal address:**  Postbus 1305, 3430 BH Nieuwegein  **E-mail:**  info@northwave.nl | **Phone number office:**  +31 (0) 30 303 1240  **Phone number NW-CERT (24\*7):**  0800 2255 2747  **Website:**  [www.northwave.nl](http://www.northwave.nl/) |

versioning and authors

Click or tap here to enter text.

Conditions

Northwave commits to keeping all information confidential. The information provided by the client will only be used in the scope of the assignment. Northwave will ensure that all employees or third parties involved in the execution of the assignment are legally bound by this obligation. All information, trademarks, names, logos, portraits, tables or other matters where property rights apply and are used in this document are the property of their respective owner.

Disclaimer

This report is part of a fictive forensics investigation case. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Table of contents

1 Management summary 4

1.1 Introduction 4

1.2 Results And conclusions 4

2 Introduction 5

2.1 Background 5

2.2 Assignment 5

3 Findings and results 6

3.1 Main questions 6

3.1.1 Why did the installed alarm system not work? 6

3.1.2 Did the suspect have access to the vault codes and if so, how? 6

3.1.3 Where did the suspect go after the heist? 6

3.1.4 What happened to the stolen jewelry? 7

3.2 Additional questions 7

3.2.1 File system forensics 8

3.2.2 Registry Forensics 8

3.2.3 Memory Forensics 10

4 Timeline analysis 11

5 Conclusion 12

# Management summary

## Introduction

<Write a short introduction about the case>

## Results And conclusions

<Summarize the findings, conclusions and provide answer to the question if Derk was involved or not>

# Introduction

## Background

On Wednesday morning, November 11th 2015, Jan Goud’s jewelry store was robbed of all Jewelry. The vault, containing all jewelry is secured with a code only known to the main employees changed on regular intervals. Furthermore, an alarm system is installed in the store which can only be deactivated by the owner, Jan Goud. This system is managed on a web interface, reachable on the local network IP-address (<http://172.16.47.153)>.

Immediately after the heist, the newly hired intern, Derk Hekker has vanished without a trace. Derk was hired as an intern to develop a new web-shop with online payment possibilities. He was only working for a few days at the store and had a Virtual desktop to his avail.

Remarkable fact is that no physical signs of a break-in are found. Additionally, a fingerprint of Derk has been found on the inside of the vault. Combined with the sudden disappearance of Derk, he has now officially been marked as a suspect. Therefore, a forensic image of his virtual workstation has been created, including a full memory dump. These files are made available to our research team for further analysis.

## Assignment

Upon special request by the local police, we have performed a limited forensics investigation into the jewelry heist at Jewelry store Jan Goud. The main objective was to determine possible involvement of intern Derk Hekker with the jewelry heist. Our team consists of the following members:

|  |  |
| --- | --- |
| # | Name |
| 1 |  |
| 2 |  |

# Findings and results

## Main questions

### Why did the installed alarm system not work?

<Write a short introduction to the answer of this question, easy readable>

|  |  |
| --- | --- |
| **ID** | **Explanation** |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | <note down which tools you have used, for reproducibility> |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

### Did the suspect have access to the vault codes and if so, how?

<Write a short introduction to the answer of this question, easy readable>

|  |  |
| --- | --- |
| **ID** | **Explanation** |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | <note down which tools you have used, for reproducibility> |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

### Where did the suspect go after the heist?

<Write a short introduction to the answer of this question, easy readable>

|  |  |
| --- | --- |
| **ID** | **Explanation** |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | <note down which tools you have used, for reproducibility> |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

### What happened to the stolen jewelry?

<Write a short introduction to the answer of this question, easy readable>

|  |  |
| --- | --- |
| **ID** | **Explanation** |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | <note down which tools you have used, for reproducibility> |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

## Additional questions

To support the main findings, additional questions have been defined. The answers to these questions helped us to identify the relevant pieces of evidence on the system and helped us identify if Derk was indeed involved. These questions are divided in the categories File System, Registry and Memory forensics.

### File system forensics

|  |  |
| --- | --- |
| **How many shadow copies are present on the system and when were they created?** | |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | mmls, vshadowmount, vshadowinfo, dd |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

|  |  |
| --- | --- |
| **What are the differences between user’s home and desktop directory in both shadow copies** | |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | fls, vshadowmount |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

### Registry Forensics

|  |  |
| --- | --- |
| **Which users are present on the system?** | |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | Rip.pl on the SAM hive |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

|  |  |
| --- | --- |
| **How many times did each user login, and when?** | |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | Rip.pl on the SAM hive |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

|  |  |
| --- | --- |
| **Which software is installed on the system and why is that relevant?** | |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | Rip.pl on the Software hive |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

### Memory Forensics

|  |  |
| --- | --- |
| **Which suspicious processes were active on the system?** | |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | Volatility pslist, psscan, psxview |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

|  |  |
| --- | --- |
| **Which network connections were active?** | |
| Findings | <note what you found> |
| Evidence | <Include a reference to the piece(s) of evidence which supports this finding> |
| Used tools | Volatitlity netscan plugin |
| Approach | <Note down how you produced the pieces of evidence with the mentioned tools, include screenshots of the commands if possible> |
| Conclusion | <Note down which conclusion can be connected to these findings> |

# Timeline analysis

<Include a graphical timeline of the events identified during the investigation>

# Conclusion

Based on our investigation we can conclude the following facts to be true.

<include the answers to the main questions here as a short conclusion>

Appendix A: Verification of evidence files

As soon as we have received the evidence files, we have created a forensically sound copy using the FTKimager suite. This process automatically creates both an md5 and sha1 hash of the mentioned file. The information about this process is as follows:

|  |  |
| --- | --- |
| Image process started | <INSERT DATE AND TIME> |
| Image process finished | <INSERT DATE AND TIME> |
| MD5 hash | <INCLUDE HASH SCREENSHOT> |
| SHA1 hash | <INCLUDE HASH SCREENSHOT > |

After completion of our investigation we have verified both the MD5 and SHA1 hashes, the results are below:

|  |  |
| --- | --- |
| Verification started | <INSERT DATE AND TIME> |
| Verification finished | <INSERT DATE AND TIME> |
| MD5 hash comparison result | <INCLUDE HASH SCREENSHOT > |
| SHA1 hash comparison result | <INCLUDE HASH SCREENSHOT > |

For the memory file, we have performed the same exercise using the md5 tool. The results are below:

|  |  |
| --- | --- |
| MD5 hash before investigation | <INCLUDE HASH SCREENSHOT > |
| MD5 hash after completion of investigation | <INCLUDE HASH SCREENSHOT > |