A novel approach for threat detection in Windows using cache memory forensics

MSc Industry Internship
MSCCYB1

Pushkar Yewalekar
Student ID: X21194254

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Pushkar Yewalekar ……………………………………………………………………………………

Student ID: X21194254……………………………………………………………………………………………

Programme: MSCCYB1 ………………………………………………… **Year:** 2022-2023 ..

Module: MSc Industry Internship ..……………………………………………………………

Supervisor: Prof Vikas Sahni ………………………………………………………………………………

Submission Due Date: 04 September 2023 ……………………………………………………………………………………………………

Project Title: A novel approach for threat detection in Windows using cache memory forensics ……………………………………………………………………………………………

Word Count: 616 ………………………… **Page Count:** 9………………………………………………..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Pushkar Yewalekar …………………………………………………………………

Date: 04 Sept 2023 ……………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A novel approach for threat detection in Windows using cache memory forensics

Pushkar Yewalekar
X21194254

1 Introduction

This document is as a reference for the industry internship research which aims to provide complete overview of working details that are mentioned in the research project report. The industry research project is built to enhance the digital forensic methodology by focusing on the cache memory part of asset identification and examination. The cache memory is a highly evident & valuable artefacts that significantly helps in rebuilding the attack vectors. These artefacts are found in cache memory and this configuration manual aims to recreate the incident using open-source tools.

2 Requirements

2.1 Hardware

Processor	AMD Ryzen 5
Memory	16GB
Architecture	64bits

2.2 Software

Operating System	Windows11 (v10.0.22621.2215)
Acquisition	FTK Imager 4.7.1.2
Analysis	Volatility 2
Programming	Python 2.7

3 Implementation

3.1 Lab Setup - Memory Acquisition Tool – FTK Imager

Step1: Download FTK Imager:

- Visit the official AccessData[1] (Now known as Exterro) website to download the FTK Imager installation file. This ensures that the downloaded file is in its latest version of the software.

Step 2: Install FTK Imager on Windows:

- Locate the downloaded FTK Imager setup file (usually named something like "FTK_Imager_x64.exe" for 64-bit Windows.
- Run the installer. Follow the on-screen instructions provided by the installer. You may be prompted to accept the software's terms and conditions, specify an installation directory, and create shortcuts.

[1] https://go.exterro.com/l/43312/ccessData-FTK-Imager-4-7-1-exe/fdxwv8

- Once the installation is complete, you can launch FTK Imager by finding it in your Start Menu or using the desktop shortcut (if created).

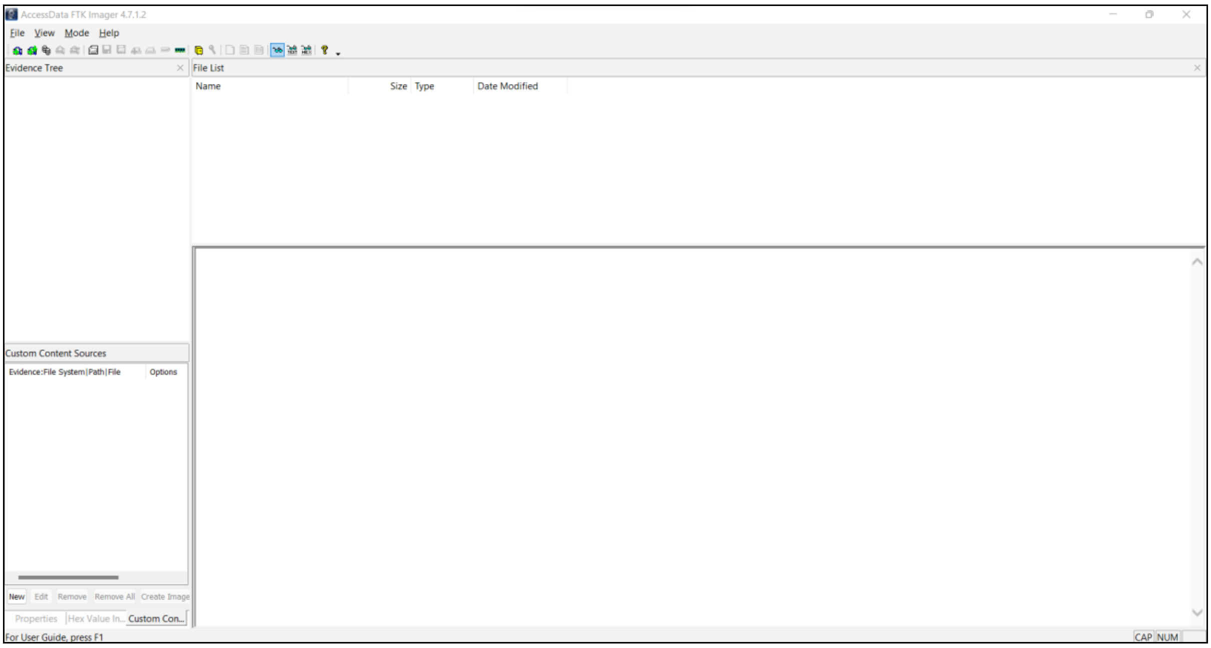


Fig 2. FTK Imager

- This tool helps in creating disk image (bit by bit) along with other several functionalities of acquisition and analysis.

3.2 Use of memory analysis tools

Step 1: Installing Prerequisites:

It is necessary ensure that Python2.7 is installed on the system, as Volatility is a Python-based tool. Python to be installed from the official website. Additionally, it is important to have pip (Python package manager) installed.

Step 2: Downloading Volatility:

Next step is to proceed to download Volatility[2]

Step 3: Installing Volatility:

After downloading the Volatility source code, navigate to the Volatility folder within the terminal and install it using pip:

```
cd volatility
```

Step 4: Verifying Installation:

To ensure that Volatility has been successfully installed, execute the following command in the terminal:

```
.\volatility --version
```

[2] http://downloads.volatilityfoundation.org/releases/2.6/volatility_2.6_win64_standalone.zip

Step 5: Obtaining a Memory Dump:

To use Volatility effectively, it needs a memory dump from the system to analyse. Memory dumps can be acquired using various tools and methods, such as using FTK Imager on Windows as discussed above.

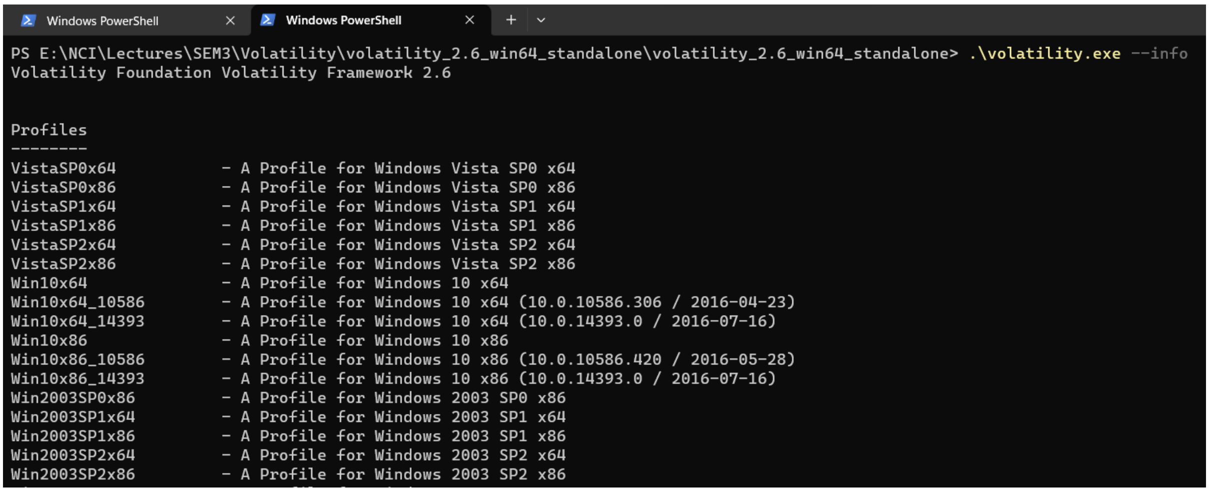
Step 6: Analysing the Memory Dump:

Once a memory dump is obtained, next step is analyse it using Volatility. The following basic command should be used:

.\volatility.exe -f path/to/memory_dump.img <plugin_name>

Replace the path/to/memory_dump.img with the actual path to the memory dump and <plugin_name> with the name of the desired Volatility plugin. Volatility has various plugins for various tasks, including process analysis, network connection extraction, and more. One such command to view volatility plugins is

.\volatility.exe --info



```
PS E:\NCI\Lectures\SEM3\Volatility\volatility_2.6_win64_standalone\volatility_2.6_win64_standalone> .\volatility.exe --info
Volatility Foundation Volatility Framework 2.6


Profiles
--------
VistaSP0x64           - A Profile for Windows Vista SP0 x64
VistaSP0x86           - A Profile for Windows Vista SP0 x86
VistaSP1x64           - A Profile for Windows Vista SP1 x64
VistaSP1x86           - A Profile for Windows Vista SP1 x86
VistaSP2x64           - A Profile for Windows Vista SP2 x64
VistaSP2x86           - A Profile for Windows Vista SP2 x86
Win10x64              - A Profile for Windows 10 x64
Win10x64_10586        - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
Win10x64_14393        - A Profile for Windows 10 x64 (10.0.14393.0 / 2016-07-16)
Win10x86              - A Profile for Windows 10 x86
Win10x86_10586        - A Profile for Windows 10 x86 (10.0.10586.420 / 2016-05-28)
Win10x86_14393        - A Profile for Windows 10 x86 (10.0.14393.0 / 2016-07-16)
Win2003SP0x86         - A Profile for Windows 2003 SP0 x86
Win2003SP1x64         - A Profile for Windows 2003 SP1 x64
Win2003SP1x86         - A Profile for Windows 2003 SP1 x86
Win2003SP2x64         - A Profile for Windows 2003 SP2 x64
Win2003SP2x86         - A Profile for Windows 2003 SP2 x86
```

4 Conclusion

Using the above tools FTK Imager and Volatility, and following the proposed methodology for digital forensic process, using cache memory, several artefacts is extracted which proves to contain high evidential value in forensic investigations. However, this is not limited to only tools proposed in the paper, use of low-level language like Python and C/C++, which have capabilities to reach kernel level and read data, can be very useful in terms of digital forensic as all the activities within a system has to be present in the cache, till its last footprint. Use of such crucial information, however, volatile, will reduce efforts in investigation process and save a lot of resources including time.

5 Bibliography

Fidelis, N. (2022, September 9). *OSINT Tools - Accessdata FTK Imager. how to install and get started with drive imaging*. Waldo’s Page. https://cybernetacks.hashnode.dev/osint-tools-accessdata-ftk-imager-how-to-install-and-get-started-with-drive-imaging

Cpuu. (2023, April 27). *An introduction to volatility 3 and installation guide*. cpuu. https://cpuu.hashnode.dev/an-introduction-to-volatility-3

Cary, M. (2018, October 29). *Installing volatility on windows*. DFIR on the Mountain. https://dfironthemountain.wordpress.com/2018/10/29/installing-volatility-on-windows/

Volatilityfoundation. (n.d.). *Volatilityfoundation/volatility: An advanced memory forensics framework*. GitHub. https://github.com/volatilityfoundation/volatility

FTK® Imager. Exterro. (n.d.). https://www.exterro.com/ftk-imager

Wire1ess. Hacking, Pentesting and IT Security. (n.d.). https://exitno.de/memory/

French, N. (2022, September 24). *FLARE Script Series: Automating Obfuscated String Decoding*. Twitter. https://twitter.com/NancyAFrench/status/1573702602386284548

Monthly Internship Report

This report consists of monthly activities performed during the internship.

Name: Pushkar Yewalekar
Student Number: x21194254
Company: Cybermate Forensics & Data Security Solutions Pvt. Ltd.
Duration: 05th June 2023 – 18th Aug 2023

Month - June
During start of my internship, I was assigned tasks to overview current practices of acquisition of source assets and to research on how the current approach can be improved. I was also assigned to create list of limitations in the current methodology of performing forensic activities and scope of improvement in the same. From this part I learnt the topic of my research topic supported by my mentor. This also helped me in literature review as I was tasked with several research readings during this time.

Activities Performed:

- Reviewing previous reports
- Reporting of issues in the current practice
- Exploring possible factors helping the company in facilitating the projects faster and efficiently

Employer comments:
Pushkar has completed assigned tasks well within time. He has been reporting to the management timely. Management team is happy with his performance.

Student Sign: Pushkar

Date: 02/09/2023

Employer Sign:

Date: 02.09.23

Monthly Internship Report

This report consists of monthly activities performed during the internship.

Name: Pushkar Yewalekar
Student Number: x21194254
Company: Cybermate Forensics & Data Security Solutions Pvt. Ltd.
Duration: 05th June 2023 – 18th Aug 2023

Month - July
Further, around mid-term of my internship, I was assigned to do extensive technical research on new approaches that could enhance threat detection and prove as a preliminary example of cache acquisition techniques that prove to be evidential in forensics as well as acceptable in the court of law. Alongside I was given live cases to handle and implement new approaches that support the research. This part helped my building the design specification and research methodology and how can the approach be implemented.

Activities performed:

- Research on improving forensic investigation efficiency
- Research on open source tools
- Study of cyber law
- Academic research

Employer comments:
Pushkar has shown exceptional skills on research and helped the technical team by assisting them in cases. He has also given his inputs on live cases that has given better outcomes in terms of performance indicators.

Student Sign: Pushkar

Date: 02/09/2023

Employer Sign:

Date: 02.09.23

Monthly Internship Report

This report consists of monthly activities performed during the internship.

Name: Pushkar Yewalekar
Student Number: x21194254
Company: Cybermate Forensics & Data Security Solutions Pvt. Ltd.
Duration: 05th June 2023 – 18th Aug 2023

Month - Aug
Towards the end, I was asked to present findings of my research and learning outcomes from the case studies given to me. From these case studies, I practically worked on my research and finally pivoting to the final stage of research that successfully ended in positive outcome of thesis.

Activities performed:

- Performed analysis of forensic case studies
- Used enhanced approach to achieve better efficiency in investigation
- Report writing
- Academic research

Employer comments:
Pushkar has completed his internship with Cybermate forensics solutions pvt ltd. He has successfully completed all the tasks given to him along with his research. He is hard working professional and I highly appreciate his efforts put for the company and his research. Please feel free to contact me regarding his employment with us as intern. Thanks.

Student Sign: Pushkar

Date: 02/09/2023

Employer Sign:

Date: 02.09.23