UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**REPORT**

Subject: Digital Forensics

Semester II (2022 – 2023)

**REGISTRY SPY AND OPEN EDR**

Student: Võ Anh Kiệt

Student ID Number: 20520605

Student: Nguyễn Bùi Kim Ngân

Student ID Number: 20520648

Student: Nguyễn Bình Thục Trâm

Student ID Number: 20520815

Class: NT334.N21.ANTN

University of Information Technology

Lecturer: Nguyễn Tấn Cầm

**Hồ Chí Minh City, June 2023**

UNIVERSITY OF INFORMATION TECHNOLOGY

FACULTY OF COMPUTER NETWORK AND COMMUNICATION

Logo, company name

Description automatically generated

**REPORT**

Subject: Digital Forensics

Semester II (2022 – 2023)

**REGISTRY SPY AND OPEN EDR**

Student: Võ Anh Kiệt

Student ID Number: 20520605

Student: Nguyễn Bùi Kim Ngân

Student ID Number: 20520648

Student: Nguyễn Bình Thục Trâm

Student ID Number: 20520815

Class: NT334.N21.ANTN

University of Information Technology

Lecturer: Nguyễn Tấn Cầm

**Hồ Chí Minh City, June 2023**

Acknowledgement

To begin, we would like to thank our advisor, PhD Nguyễn Tấn Cầm, for his direction and consistent monitoring, as well as for providing important project information and for their help in finishing the research.

My gratitude and appreciation also extend to our colleagues and lecturers who assisted us in the development of the project, as well as to those who have volunteered their time and skills to assist us.

Võ Anh Kiệt – 20520605 – ANTN.2020

Nguyễn Bùi Kim Ngân – 20520648 – ANTN.2020

Nguyễn Bình Thục Trâm – 20520815 – ANTN.2020

Contents

[Acknowledgement 3](#_Toc105666586)

[Part 1: Introduction 6](#_Toc105666587)

[1.1. Overview 6](#_Toc105666588)

[1.2. Problem Statement 7](#_Toc105666589)

[1.3. Scope 8](#_Toc105666590)

[1.4. Objective 8](#_Toc105666591)

[Part 2: Background 9](#_Toc105666592)

[2.1. Fundamental of face recognize 9](#_Toc105666593)

[2.2. OpenCV 10](#_Toc105666594)

[2.3. OpenCV – HaarCascade Classification 10](#_Toc105666595)

[2.4. OpenCV – Single Shot Detector base ResNet network – Caffe Model 11](#_Toc105666596)

[Part 3: Design and Code 13](#_Toc105666597)

[3.1. Design 13](#_Toc105666598)

[3.1.1. Register 13](#_Toc105666599)

[3.1.2. Recognize and verify 14](#_Toc105666600)

[3.2. HaarCascade 15](#_Toc105666601)

[3.2.1. Register 15](#_Toc105666602)

[3.2.2. Recognize and Verify 16](#_Toc105666603)

[3.3. Caffe 18](#_Toc105666604)

[3.3.1. Register 18](#_Toc105666605)

[3.3.2. Recognize and Verify 20](#_Toc105666606)

[Part 4: Implement and Test 22](#_Toc105666607)

[4.1. Implemet 22](#_Toc105666608)

[4.1.1. HaarCascade 22](#_Toc105666609)

[4.1.2. Caffe 23](#_Toc105666610)

[4.2. Test 25](#_Toc105666611)

[4.3. Review 25](#_Toc105666612)

[Part 5: Conclusion and Future Work 26](#_Toc105666613)

[5.1. Conclusion 26](#_Toc105666614)

[5.2. Future work 26](#_Toc105666615)

[Reference 27](#_Toc105666616)

Part 1: Introduction

* 1. Overview Registry Spy

In today's digital landscape, where vast amounts of data are generated and stored, the management and organization of information have become paramount. One crucial aspect of data management revolves around the utilization of registry tools, which serve as centralized repositories for storing and accessing important information. These tools play a vital role in various domains, including healthcare, finance, logistics, and more.

The Registry Tool Analysis is an in-depth examination of the functionalities, benefits, and challenges associated with registry tools. This comprehensive report aims to provide an insightful overview of these tools, their significance, and the impact they have on businesses and organizations.

The analysis will delve into the fundamental principles behind registry tools, shedding light on how they facilitate the efficient handling of data through structured hierarchies and standardized formats. By capturing, organizing, and maintaining essential information in a central location, registry tools offer unparalleled convenience and accessibility, streamlining critical processes within an organization.

Moreover, the report will explore the diverse applications of registry tools across industries. It will delve into the healthcare sector, where patient registries enable the collection and analysis of data for medical research, epidemiological studies, and personalized patient care. Additionally, registry tools are widely adopted in financial institutions for customer relationship management, compliance monitoring, and fraud detection, providing an integrated approach to managing client data.

While the benefits of registry tools are significant, the analysis will also address the challenges that organizations face when implementing and maintaining these tools. This includes considerations such as data security, privacy concerns, scalability, and interoperability, which require careful attention to ensure the optimal performance and integrity of registry systems.

Ultimately, this Registry Tool Analysis aims to equip organizations, decision-makers, and professionals with a comprehensive understanding of the role and potential of registry tools in modern data management. By exploring their capabilities, benefits, and challenges, this report will serve as a valuable resource for anyone seeking to leverage the power of registry tools to enhance their data management practices and drive operational efficiency.

* 1. Overview EDR

In the realm of cybersecurity, the ever-evolving threat landscape calls for innovative approaches to protect digital assets. Endpoint Detection and Response (EDR) has emerged as a crucial component in the defense against advanced cyber threats. EDR solutions provide organizations with the ability to detect, investigate, and respond to malicious activities at the endpoint level.

This analysis aims to provide an in-depth examination of EDR, its functionalities, and the significance it holds in safeguarding modern digital environments. By focusing on the intersection of endpoint security, threat detection, and incident response, this report will shed light on the pivotal role that EDR plays in mitigating cyber risks.

The analysis will delve into the fundamental principles behind EDR, exploring how it leverages advanced technologies such as behavioral analytics, machine learning, and artificial intelligence to identify suspicious activities, detect malware, and respond to security incidents. With real-time visibility into endpoints, EDR solutions enable security teams to proactively defend against sophisticated threats, including zero-day exploits, advanced persistent threats (APTs), and fileless attacks.

Furthermore, the report will discuss the key features and capabilities of EDR solutions, including continuous monitoring, forensic investigation, threat intelligence integration, and automated response. By providing granular visibility into endpoint activities and establishing comprehensive defense mechanisms, EDR empowers organizations to swiftly identify and neutralize threats, minimizing the potential impact of cyber incidents.

However, alongside the benefits, the analysis will also address the challenges associated with implementing and managing EDR solutions. This includes considerations such as system complexity, resource requirements, false positives, and ensuring compatibility with existing security infrastructure. Organizations must carefully evaluate these factors to maximize the effectiveness of their EDR implementations.

Ultimately, this EDR analysis aims to equip organizations, security professionals, and decision-makers with a comprehensive understanding of the value and potential of EDR in the face of evolving cyber threats. By exploring its functionalities, benefits, and challenges, this report will serve as a valuable resource for anyone seeking to enhance their cybersecurity posture and protect their digital assets through the adoption of robust EDR solutions.

* 1. Problem Statement

In today's interconnected world, where digital devices are pervasive and play a crucial role in our personal and professional lives, the threat of malware infiltration poses a significant challenge. Malicious software, commonly known as malware, continues to evolve and adapt, finding new and innovative ways to breach the security defenses of devices, including computers, smartphones, tablets, and Internet of Things (IoT) devices.

The problem lies in the ever-increasing sophistication and diversity of malware, which can infiltrate devices through various attack vectors, such as malicious email attachments, infected websites, software vulnerabilities, social engineering techniques, and unauthorized app downloads. Once inside a device, malware can wreak havoc by stealing sensitive information, compromising user privacy, conducting unauthorized activities, and even rendering the device inoperable.

The consequences of malware infiltration are far-reaching and impactful. Individuals and organizations face the risk of financial loss, identity theft, data breaches, system disruptions, and reputational damage. Moreover, as technology continues to advance and more devices become interconnected through the Internet of Things, the potential for widespread malware outbreaks and cascading effects becomes a pressing concern.

Addressing the problem of malware infiltration requires a multi-faceted approach that encompasses robust cybersecurity measures, user education, proactive threat detection, and effective incident response. It is crucial for individuals, enterprises, and security professionals to stay vigilant, continuously update their defenses, and employ security solutions that can detect and mitigate emerging malware threats.

Furthermore, as the boundaries between personal and professional device usage blur, the problem becomes even more complex. Enterprises must grapple with the challenge of securing a diverse range of devices, including those owned by employees (Bring Your Own Device - BYOD), which introduces additional risks and potential vulnerabilities to corporate networks.

In summary, the problem of malware infiltration into devices represents an ongoing and ever-evolving challenge in today's digital landscape. As the threat landscape continues to evolve, it is imperative for individuals, organizations, and the security community as a whole to remain vigilant, adapt to emerging threats, and implement robust security measures to safeguard against the infiltration and impact of malware on devices.

Malware, malificious file,…

Users The endpoint device

* 1. Scope

Deploy the EDR

Deploy the Registry Spy

Analysis the endpoint device

Detect malware

* 1. Objective

Using the EDR sponsor by OpenEDR to analysis the machine and detect malware.

Using the Registry spy to detect the DAT file

Part 2: Background

* 1. Registry spy

Registry Spy is a free, open-source cross-platform Windows Registry viewer. It is a fast, modern, and versatile explorer for raw registry files.

Features include:

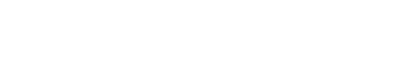
* Windows, macOS, and Linux support
* Fast, on-the-fly parsing means no upfront overhead
* Open multiple hives at a time
* Searching
* Hex viewer
* Modification timestamps

A green text on a black background

Description automatically generated with medium confidence

* 1. EDR – OpenEDR

Open EDR is a sophisticated, free, open-source endpoint detection and response solution. It provides analytic detection with Mitre ATT&CK visibility for event correlation and root cause analysis of adversarial threat activity and behaviors in real time. This world-class endpoint telemetry platform is available to all cyber-security professionals, and every sized organization, to defend against threat actors and cyber criminals.



Capability:

* Visibility and coverage: Open EDR solutions provide visibility into all activity and can cover both physical and virtualized environments.
* Detection: It provides an effective solution on detecting potential threats.
* Response: It reacts quickly and helps you contain and remediate incidents.
* Management and reporting: It is easy to manage and provide comprehensive reports that can help you improve your security posture.

Part 3: Design and Code

3.1. Design

3.1.1. Register

Diagram

Description automatically generated

3.1.2. Recognize and verify

Diagram

Description automatically generated

3.2. HaarCascade

3.2.1. Register

Get the data of the users from Images

Graphical user interface, text, application

Description automatically generated

Process the image

Text

Description automatically generated

Save the data to pickle file

Text

Description automatically generated

3.2.2. Recognize and Verify

Load the model and pickle file

Text

Description automatically generated

Load the video stream, start recognizing and verifying

Text

Description automatically generated

Text

Description automatically generated

3.3. Caffe

3.3.1. Register

Load the model, database and declare variable

Text

Description automatically generated

Process the image

Text

Description automatically generated

Save the data to pickle file

Text

Description automatically generated

3.3.2. Recognize and Verify

Load the model and data

Text

Description automatically generated

Start recognizing and verify

Text

Description automatically generated

Text

Description automatically generated

Part 4: Implement and Test

4.1. Implemet

4.1.1. HaarCascade

Before registering

A picture containing person

Description automatically generated

Register

Text

Description automatically generated

Recognize and verify

A picture containing person, indoor, hair

Description automatically generated

4.1.2. Caffe

Before registering

A person taking a selfie

Description automatically generated

Register

Text

Description automatically generated

Recognize and verify

A picture containing text, person

Description automatically generated

4.2. Test

|  |  |  |  |
| --- | --- | --- | --- |
|  | HaarCascade | Caffe | Paper1 |
| Recognize in normal light | Pass | Pass | Pass |
| Recognize a part of face | Pass | Pass | Not mentioned |
| Detect fake face | Not Pass | Not Pass | Pass |
| Recognize in low light | Not Pass | Not Pass | Not mentioned |
| Respone time counter | 2.0052 second | 2.2138 second | 0.3496 second |
| Accuracy | 46.8547% | 71.8954% | 99.95% |

4.3. Review

This project provides the simple functions and features to register and verify the people with ficial recognition. In this project, people can regist with the pictures and verify with the video stream. Despite the verified testcase, it still faces a security problem and user experience.

Part 5: Conclusion and Future Work

5.1. Conclusion

In this project, we demonstrated another authentication method using facial recognition and authentication with HaarCascade and Caffe (powered by ResNet). The program works well with a basic function for users to register and verify.

Due to the latest technology, we faced many problems due to our lack of knowledge about face recognition as well as multithreaded programming in Python. Besides, facing difficulties in developing and deploying Azure Function is also a challenge for us.

Although our project is not excellent enough for real-world application because of security issues with facial recognition, it is the foundation for development in the next steps. So, we will continue to develop it after this project.

During the implementation of this project, we had the opportunity to review and update the knowledge that we had acquired during our 2 years of study at the university. Furthermore, we have also gained valuable insights into new technology trends.

5.2. Future work

Various adaptations, test, and experiments were left for the future due to lack of time. Future work issues extend to more advanced features

* Develop the mobile app and web app allowing user to have more methods in registering and verifying
* Implement the program in the IOT device such as Raspberry Pi
* Build the training data system using the larger data to improve the register and verify system
* Improve the register and verify system algorithm to pop up the accuracy of the system

Reference

1. Jong-Hyuk Im , Seong-Yun Jeon, & Mun-Kyu Lee (2020). Practical Privacy-Preserving Face Authentication for Smartphones Secure Against Malicious Clients. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 15, 2020 (2386-2401)
2. Adrian Rosebrock, Face detection with OpenCV and deep learning, 2018, <https://www.pyimagesearch.com/2018/02/26/face-detection-with-opencv-and-deep-learning/>
3. Chi-Feng Wang, What’s the Difference Between Haar-Feature Classifiers and Convolutional Neural Networks? 2018, <https://towardsdatascience.com/whats-the-difference-between-haar-feature-classifiers-and-convolutional-neural-networks-ce6828343aeb>
4. OpenCV library documentation, <https://opencv.org/>
5. Ramiz Raja, Face Detection Using Opencv And Python: A Beginner’s Guide, 2017 <https://www.superdatascience.com/opencv-face-detection/>
6. Renan Dias, The 5 Factors of Authentication, 2017, <https://medium.com/@renansdias/the-5-factors-of-authentication-bcb79d354c13>