Name:

Semester:

Year: 2024

Section Number:



Lab 1WorksheetDigital Forensics Technology and Practices

Table of Contents

Introduction 3

Screenshot 1 – Your First Name Computer Name 4

Screenshot 2 – Create a YOURNAME User account 4

Screenshot 3 – Create a YOURNAME Service 4

Screenshot 4 – Add Yourname.EXE to the Startup Folder for Administrator 5

Screenshot 5 – Your First Folder with the Registry Files with Date Modified 5

Screenshot 6– Windows Computer Name Date Pulled from the Registry 6

Screenshot 7– Yourname Service Pulled from the Registry 6

Screenshot 8 – SAM (Security Accounts Manager) with Yourname 7

Screenshot 9 – Autoruns with Yourname. EXE running at Startup 7

Screenshot 10 – Autoruns with Yourname Service Running 8

Take a screenshot of the Yourname Service Runningwithin the Autoruns program. 8

Conclusion 8

APA References 10

Alghamdi, M. I. (2021). Digital forensics in cyber security—recent trends, threats, and opportunities. Cybersecurity Threats with New Perspectives. 10

Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., ... & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access, 10, 25464-25493. 10

Ferguson, R. I., Renaud, K., Wilford, S., & Irons, A. (2020). PRECEPT: a framework for ethical digital forensics investigations. Journal of Intellectual Capital, 21(2), 257-290. 10

Montasari, R., & Hill, R. (2019, January). Next-generation digital forensics: Challenges and future paradigms. In 2019 IEEE 12th International conference on global security, safety and sustainability (ICGS3) (pp. 205-212). IEEE. 10

Singh, A., Venter, H. S., & Ikuesan, A. R. (2020). Windows registry harnesser for incident response and digital forensic analysis. Australian Journal of Forensic Sciences, 52(3), 337-353. 10

# Introduction

**Students:** In the box below, please explain the purpose of using the Windows Registry and explain how it is relevant to Digital Forensics Technology and Practices.

|  |
| --- |
| Introduction |
| The Windows Registry serves as a central repository for storing configuration settings and system information for the Windows operating system. It plays a crucial role in managing various aspects of system behavior, including user preferences, installed software, hardware configurations, and system security settings. Essentially, it acts as a hierarchical database that organizes data into keys and values, making it easier for the operating system and applications to access and modify settings efficiently.  In the realm of Digital Forensics Technology and Practices, the Windows Registry holds significant importance. During forensic investigations, analysts often rely on the Registry to uncover valuable evidence related to system activities, user actions, and potential security breaches. By analyzing Registry entries, forensic experts can reconstruct a timeline of events, track user interactions, identify installed software and its usage patterns, detect malicious activities such as malware infections or unauthorized system modifications, and gather valuable intelligence for investigative purposes.  Moreover, the Windows Registry can provide crucial insights into system configurations, network settings, user accounts, installed applications, and recent activities, aiding forensic investigators in understanding the context of a digital incident and piecing together the sequence of events leading to a security breach or other digital crimes. Additionally, Registry artifacts can serve as digital fingerprints, helping forensic analysts establish links between digital evidence and specific individuals, devices, or actions, thereby strengthening the integrity of forensic investigations and supporting legal proceedings. Overall, the Windows Registry is a fundamental component of Digital Forensics Technology, enabling investigators to extract actionable intelligence and uncover critical evidence essential for attributing cyber incidents, securing systems, and prosecuting offenders. |

# Screenshot 1 – Your First Name Computer Name

1. Your First Name in the Computer Name Box. The Name of the computer should be your first name. The use of anyone else’s name may result in an academic integrity review by your professor. Please label your screenshot to receive full credit.

**Take a screenshot of the Yourname being used in the computer name.**

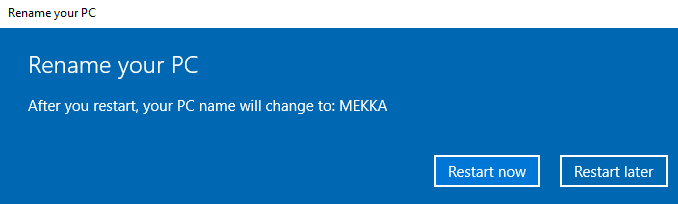


Figure 1: Renaming computer to First name

# Screenshot 2 – Create a YOURNAME User account

1. The Name of the User created should match your first name. The use of anyone else’s name may result in an academic integrity review by your professor. Please label your screenshot to receive full credit.

**Take a screenshot of the Yourname user account being create at the command line.**

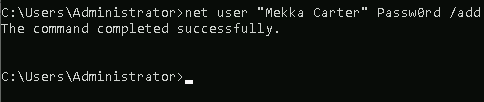
****

Figure 2: creating user account with my name

# Screenshot 3 – Create a YOURNAME Service

1. The Name of the Service created should match your first name. The use of anyone else’s name may result in an academic integrity review by your professor. Please label your screenshot to receive full credit.

**Take a screenshot of the Yourname being used in the Service being Created on Windows.**

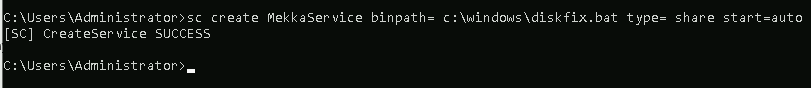


Figure 3: My name being used in a service

# Screenshot 4 – Add Yourname.EXE to the Startup Folder for Administrator

1. The Name of the file should be your first name. The use of anyone else’s name may result in an academic integrity review by your professor. Please label your screenshot to receive full credit.

**Take a screenshot of the Yourname being used in the startup folder for the administrator**

# Picture 10

Figure 4: My name being used at start up

# Screenshot 5 – Your First Folder with the Registry Files with Date Modified

1. **The Name of the Folder should match your first and last name. The use of anyone else’s name may result in an academic integrity review by your professor.** Timestamps from a previous semester may also result in an academic integrity review by your professor. Please label your screenshot to receive full credit.

**Take a screenshot of the Yourname folder with the collected registry files.**

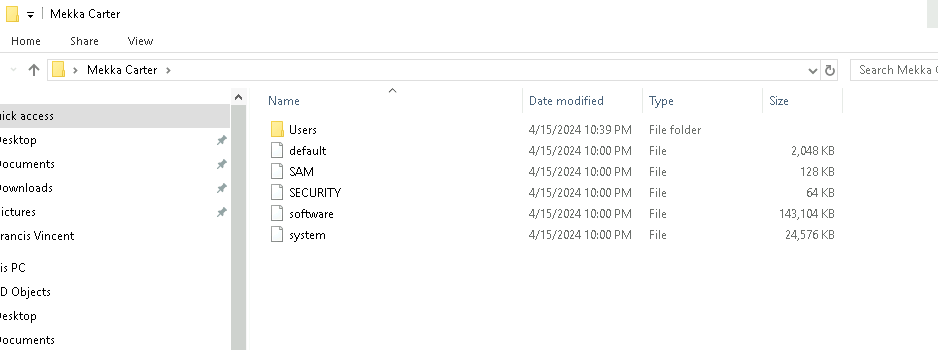
****

Figure 5: My folder, under my name with collected registry entries

# Screenshot 6– Windows Computer Name Date Pulled from the Registry

1. Show the system hive of the registry with the Computer Name of your Windows operating system. Label your screenshot.

**Take a screenshot of Yourname in the system registry under machine name.**

# Picture 25

Figure 6: Computer name pulled out of Registry

# Screenshot 7– Yourname Service Pulled from the Registry

1. Show the system hive of the registry with the Yourname Service. Label your screenshot.

**Take a screenshot of the Yourname Service in the system registry under services**

# Picture 19

Figure 7: Service pulled out of Registry

# Screenshot 8 – SAM (Security Accounts Manager) with Yourname

1. The Name of the User listed in the SAM file created during should match your first name. The use of anyone else’s name may result in an academic integrity review by your professor. Please label your screenshot to receive full credit.

**Take a screenshot of the Yourname user in the SAM file from the Windows Registry.**

# Picture 16

Figure 8: SAM Security with my name

# Screenshot 9 – Autoruns with Yourname. EXE running at Startup

1. The Name of the executable file should match your first name. The use of anyone else’s name may result in an academic integrity review by your professor. Please label your screenshot to receive full credit.

**Take a screenshot of the Yourname file in Startupwithin the Autoruns program.**

# Picture 28

Figure 9: myname file running in autorun program

# Screenshot 10 – Autoruns with Yourname Service Running

1. The Name of the Servicelisted in Autoruns should match your first name. The use of anyone else’s name may result in an academic integrity review by your professor. Please label your screenshot to receive full credit.

# Take a screenshot of the Yourname Service Runningwithin the Autoruns program.

# Picture 31

Figure 10: Mekka Service running within the Autoruns program

# Conclusion

**Students:** In the box below, please explain the purpose of doing this lab below and explain how it is relevant to Digital Forensics Technology and Practices. Highlight any new learning that occurred while doing this lab.

**Hint: Discuss tools and commands used in the lab.**

|  |
| --- |
| Conclusion |
| The purpose of conducting the lab described above is to gain practical experience in utilizing various tools and commands related to Windows system administration and registry analysis. This hands-on activity allows us as students to familiarize ourselves with essential concepts such as renaming the computer, creating user accounts and services, modifying startup items, and extracting information from the Windows Registry.  This lab is highly relevant to Digital Forensics Technology and Practices for several reasons. First and foremost, it provides students with insight into the inner workings of the Windows operating system, including how system configurations, user accounts, and services are managed and stored within the Windows Registry. Understanding these components is crucial for forensic investigators when analyzing digital evidence extracted from Windows-based systems.  Secondly, by performing tasks such as creating user accounts and services, modifying startup items, and examining registry entries, we learn how to identify potential indicators of compromise or suspicious activity on a system. For example, abnormal changes to startup items or the creation of unauthorized user accounts or services could indicate malicious intent which could prompt further investigation by forensic analysts.  Moreover, this lab introduces us to various tools and commands commonly used in digital forensics investigations. For instance, tools like Command Prompt, Registry Editor, and Autoruns are utilized to carry out tasks such as creating user accounts, modifying registry entries, and analyzing startup items. By becoming proficient in using these tools, we should be able to develop essential skills required for conducting effective forensic examinations of Windows-based systems.  In terms of new learning, there are several key takeaways from this lab. For instance, so far we’ve learned about the structure of the Windows Registry, including its hierarchical organization into keys and values, and how to navigate and manipulate registry entries using tools like the Registry Editor. Additionally, we’ve gained insight into how various system components interact with each other, such as how startup items are configured and executed during system boot-up.  Overall, this lab provides valuable hands-on experience and practical knowledge that is directly applicable to the field of Digital forensics. By mastering the tools and techniques demonstrated in this lab, we should be able to enhance our investigative skills and effectively analyze digital evidence extracted from Windows-based systems, ultimately contributing to the successful resolution of digital forensic cases. |

# APA References

# Alghamdi, M. I. (2021). Digital forensics in cyber security—recent trends, threats, and opportunities. *Cybersecurity Threats with New Perspectives*.

# Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., ... & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access*, *10*, 25464-25493.

# Ferguson, R. I., Renaud, K., Wilford, S., & Irons, A. (2020). PRECEPT: a framework for ethical digital forensics investigations. *Journal of Intellectual Capital*, *21*(2), 257-290.

# Montasari, R., & Hill, R. (2019, January). Next-generation digital forensics: Challenges and future paradigms. In *2019 IEEE 12th International conference on global security, safety and sustainability (ICGS3)* (pp. 205-212). IEEE.

# Singh, A., Venter, H. S., & Ikuesan, A. R. (2020). Windows registry harnesser for incident response and digital forensic analysis. *Australian Journal of Forensic Sciences*, *52*(3), 337-353.