Analyzing a registry using Reg Ripper

Authors: Khushi Gupta, Ishan Perera. Email: *{kxg095, wdp006}@shsu.edu*

Mentor Name: Kendall Faichtinger Mentee Name: Illya Hamadov

Contents

1 Introduction

The Windows registry is a critical component of Windows operating systems, yet it is likely the least understood component of a Windows system when it comes to digital analysis.

The Windows registry stores a great deal of configuration information, including settings for various functions within the system. Additionally, the registry also maintains historical information about the user activity, details about the applications installed and accessed, and much more. All this data can be incredibly useful to a forensic examiner, especially when trying to piece together a timeline of the system and/or user activity.

The registry is divided into Hives. A hive in the Windows Registry is the name given to a major section of the registry that contains registry keys, registry subkeys, and registry values. Hives hold information about *user profiles, applications, configurations, network connections, printers*, etc [1]. RegRipper works by pulling information from the supporting files of the Windows registry hive.

The registry is divided into five hives namely:

HKEY_CLASSES_ROOT: This hive contains information about registered applications and file associations.

HKEY_CURRENT_USER: This hive stores settings that are specific to the currently logged-in user such as mapped network drives, keyboard layout etc.

HKEY_LOCAL_MACHINE: This hive stores settings that are specific to the local computer. It has five subkeys which are commonly used for extracting evidence.

> *SAM:* This is used to reference the Security Accounts Manager databases for all domains into which the local system has been administratively authorized or configured.
>
> *Security:* This key is linked to the security database of the domain into which the current is logged on such as security policies.
>
> *System:* This key contains information about the Windows system setup such as mounted devices, filesystem-related information, etc.
>
> *Software:* This key contains software and windows settings. It is mostly modified by application and system installers.

HKEY_USERS: This hive contains user-specific configuration for all currently active users on the computer.

HKEY_CURRENT_CONFIG: This hive acts as a pointer to the registry key that keeps the information about the hardware profile currently being used.

In this lab, we will use the tool RegRipper to extract information from the registry.

2 Overview

RegRipper was created and maintained by Harlan Carvey. RegRipper, written in Perl, is the fastest, easiest, and best tool for registry analysis in forensics examinations. It is an open-source tool, written in Perl, for extracting/parsing information (key, values, data) from the registry and presenting it for analysis. RegRipper consists of two basic tools, both of which provide similar capabilities. The RegRipper GUI allows the analyst to select a hive to parse, an output file for the results, and a profile (list of plugins) to run against the hive. RegRipper also includes a command-line (CLI) tool called rip. Rip can be pointed against a hive and can run either a profile (a list of plugins) or an individual plugin against that hive.

This lab focuses on locating inculpatory or exculpatory evidence on a Windows registry so that it may be presented in a court of law.

You are a forensic analyst and you have been assigned a case. A first responding officer seized the hard drive of the computer and a crime scene evidence technician skilled in data acquisition made an image of the hard drive and the protected areas (registry) with FTK imager. You are given the registry hives and are expected to examine them for any evidentiary artifacts that might relate to this case using RegRipper.

This lab makes use of RegRipper version 2.8 due to the variety of plugins it offers.

If interested, you can check out the latest version of RegRipper (RegRipper 3.0) which is available on the website given below. This version also offers a GUI interface for easy usage.

https://github.com/keydet89/RegRipper3.0 [2]

While the required installer files and manuals are available in the repository, we would recommend you browse through the website and familiarize yourself with the tool.

3 Learning Objectives

After completing the lab, a student should be able to:

1. Understand the Windows registry and its role for digital forensic analysts
2. Understand how the Windows registry can be used to track activities on suspect systems
3. Using RegRipper to analyze Windows registry hives for the purpose of extracting evidence
4. Comprehending the different ‘plugins’ available for RegRipper and the purpose that they serve
5. Using RegRipper in command-line mode and grasping the available options

4 Background Knowledge

This lab is intended for undergraduate digital forensic classes.

The background knowledge required by the student, prior to starting the lab are:

1. Understanding of what a Windows registry is
2. Knowledge on the structure of the Windows registry
3. Basic knowledge on how to use the Windows command line
4. Follow the instructions to utilize the software to conduct a forensic investigation.

5 Lab Environment

Before doing the activity, the students are expected to download and install RegRipper on their windows device keeping in mind the minimum system requirements needed for the application.

6 Tools Required

1. RegRipper 2.8 (Older or newer versions may also suffice)

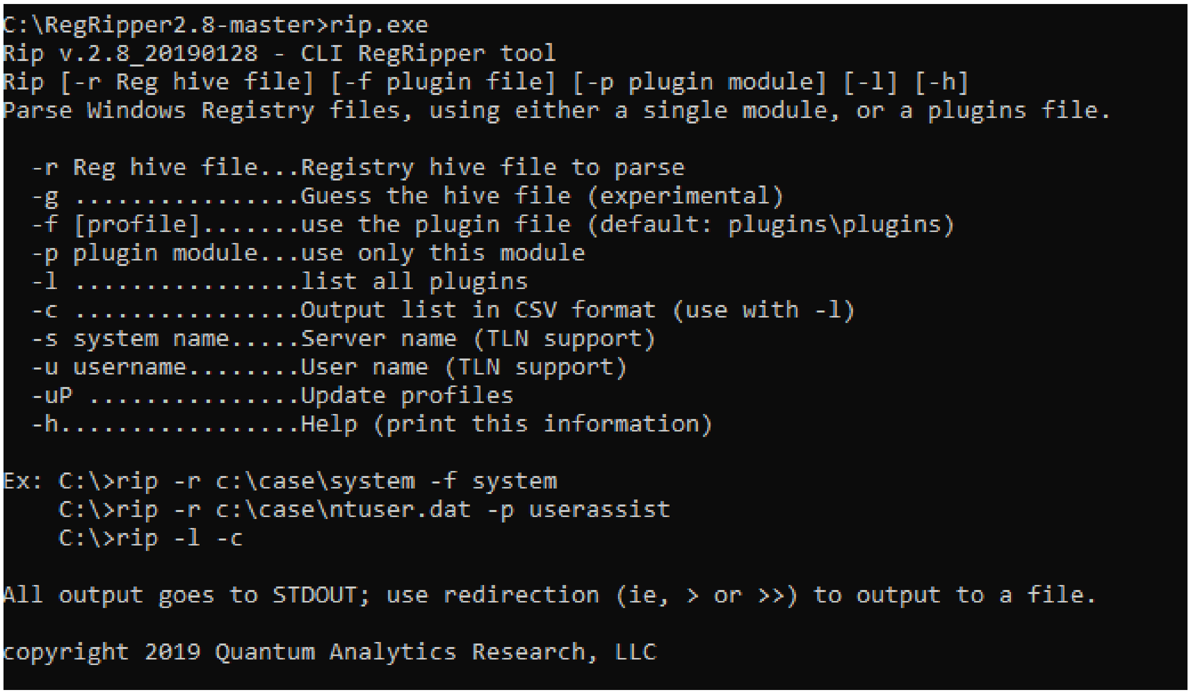
7 Lab Tasks

1) Uncompress the "***RegistryForensicsLab.rar***" file given with this lab to get the lab materials.
2) Unzip the "RegRipper2.8.rar" file
3) Place the lab materials in a folder comfortable for you to use them. We would recommend putting in your "**C:"** drive.
4) For ease of use, you can also copy the path and put it in the environment variables of the system to avoid writing the path repeatedly.
5) Place the registry hives in a suitable handy folder for ease of use. We recommend placing the registry hives inside the RegRipper folder. Note: The NTUSER.dat file might be hidden by default. Ensure that you are viewing hidden files to locate that file.
6) Have a look at the csv file attached in the folder for the different plugins that RegRipper offers. This will come in handy during the lab.

8 Brief Overview of the Interface

We will start with the command line interface of RegRipper for our analysis.

Execution of the main executable file (rip.exe) shows you the different options it has.

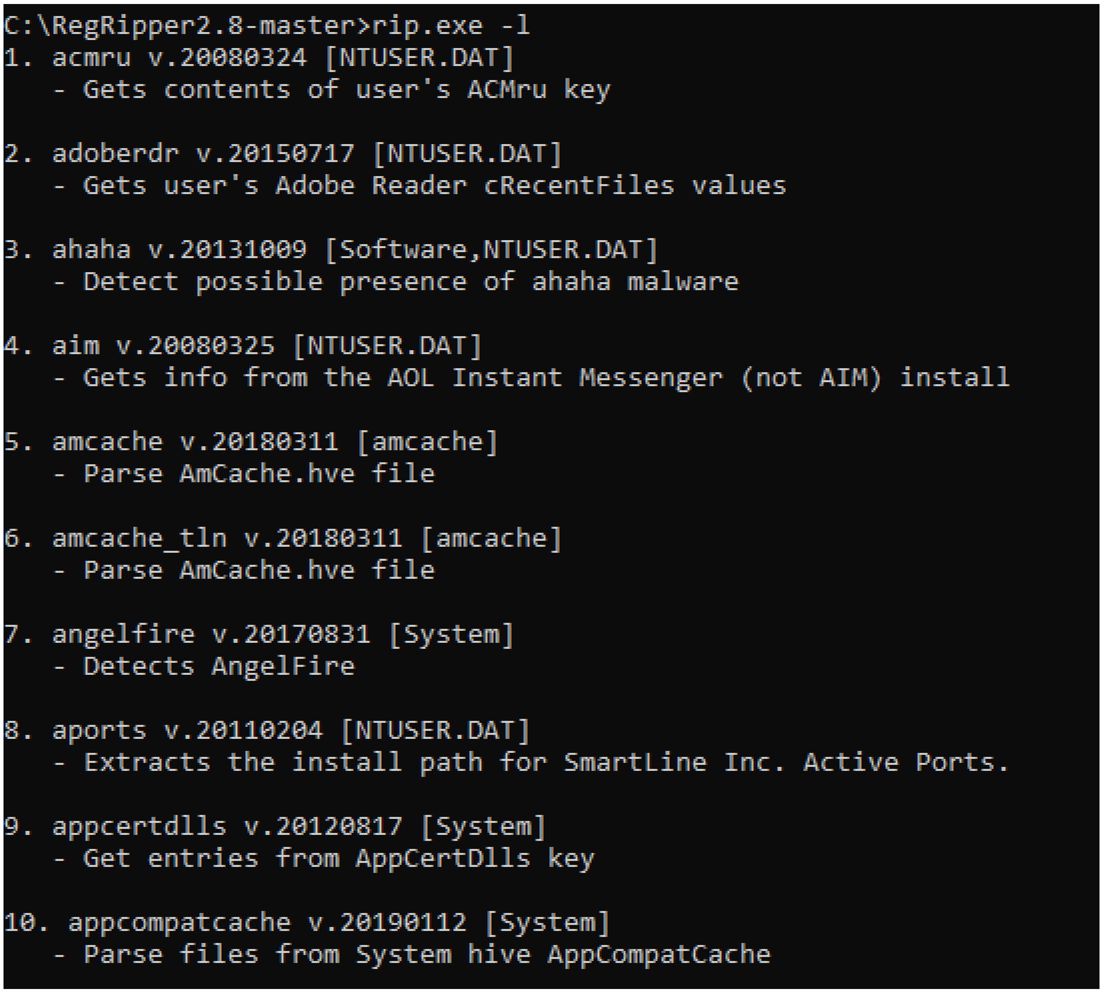


```
C:\RegRipper2.8-master>rip.exe
Rip v.2.8_20190128 - CLI RegRipper tool
Rip [-r Reg hive file] [-f plugin file] [-p plugin module] [-l] [-h]
Parse Windows Registry files, using either a single module, or a plugins file.

  -r Reg hive file...Registry hive file to parse
  -g ................Guess the hive file (experimental)
  -f [profile].......use the plugin file (default: plugins\plugins)
  -p plugin module...use only this module
  -l ................list all plugins
  -c ................Output list in CSV format (use with -l)
  -s system name.....Server name (TLN support)
  -u username........User name (TLN support)
  -uP ...............Update profiles
  -h.................Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
    C:\>rip -r c:\case\ntuser.dat -p userassist
    C:\>rip -l -c

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.

copyright 2019 Quantum Analytics Research, LLC
```

Figure 1: Different options used in RegRipper

Notice that -r is used to load a registry hive file, while -p is used to load a specific plugin module. These are the most used options that will be used in the lab.

RegRipper has a lot of different plugins for various tasks. You can use the command **“rip.exe -l”** to view all the plugins.



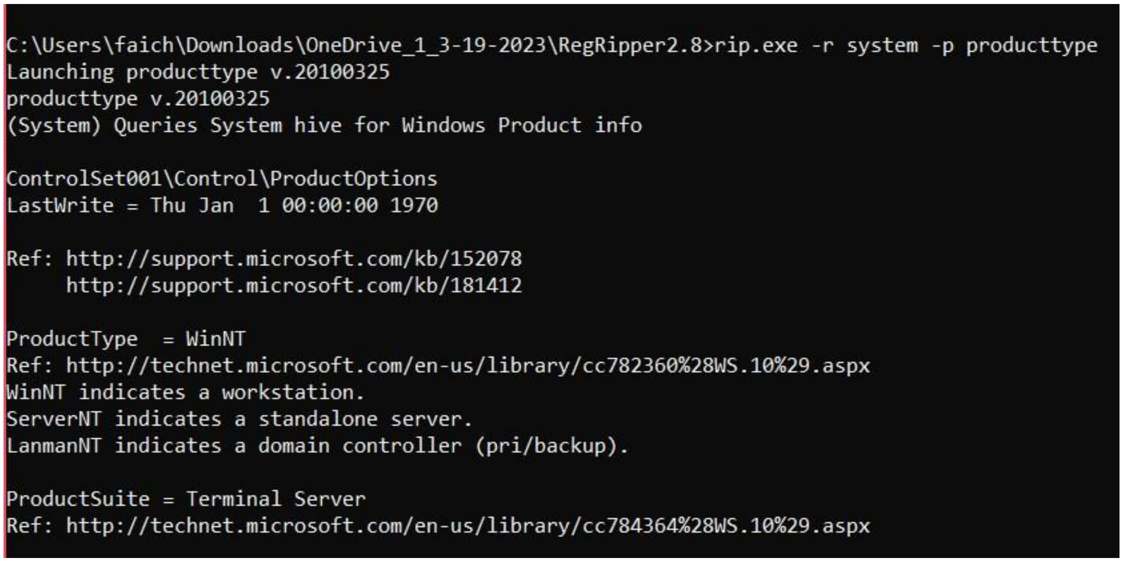
```
C:\RegRipper2.8-master>rip.exe -l
1. acmru v.20080324 [NTUSER.DAT]
   - Gets contents of user's ACMru key

2. adoberdr v.20150717 [NTUSER.DAT]
   - Gets user's Adobe Reader cRecentFiles values

3. ahaha v.20131009 [Software,NTUSER.DAT]
   - Detect possible presence of ahaha malware

4. aim v.20080325 [NTUSER.DAT]
   - Gets info from the AOL Instant Messenger (not AIM) install

5. amcache v.20180311 [amcache]
   - Parse AmCache.hve file

6. amcache_tln v.20180311 [amcache]
   - Parse AmCache.hve file

7. angelfire v.20170831 [System]
   - Detects AngelFire

8. aports v.20110204 [NTUSER.DAT]
   - Extracts the install path for SmartLine Inc. Active Ports.

9. appcertdlls v.20120817 [System]
   - Get entries from AppCertDlls key

10. appcompatcache v.20190112 [System]
   - Parse files from System hive AppCompatCache
```

Figure 2: Different plugins used in RegRipper

9 Lab Challenges and Deliverables/Lab Questions

1. The suspect’s computer could be a workstation, a server, or a domain controller. Determine the type of system it is. Hint: System hive file

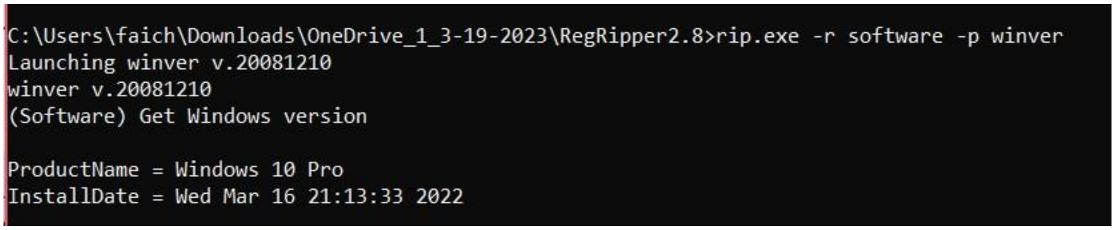
By using the plugin “producttype” and the system hive file, I was given the output of WinNT which indicates that the suspect’s computer was a workstation.



```
C:\Users\faich\Downloads\OneDrive_1_3-19-2023\RegRipper2.8>rip.exe -r system -p producttype
Launching producttype v.20100325
producttype v.20100325
(System) Queries System hive for Windows Product info

ControlSet001\Control\ProductOptions
LastWrite = Thu Jan  1 00:00:00 1970

Ref: http://support.microsoft.com/kb/152078
     http://support.microsoft.com/kb/181412

ProductType  = WinNT
Ref: http://technet.microsoft.com/en-us/library/cc782360%28WS.10%29.aspx
WinNT indicates a workstation.
ServerNT indicates a standalone server.
LanmanNT indicates a domain controller (pri/backup).

ProductSuite = Terminal Server
Ref: http://technet.microsoft.com/en-us/library/cc784364%28WS.10%29.aspx
```

2. What is the operating system and its version? When was it installed? Hint: Software hive file

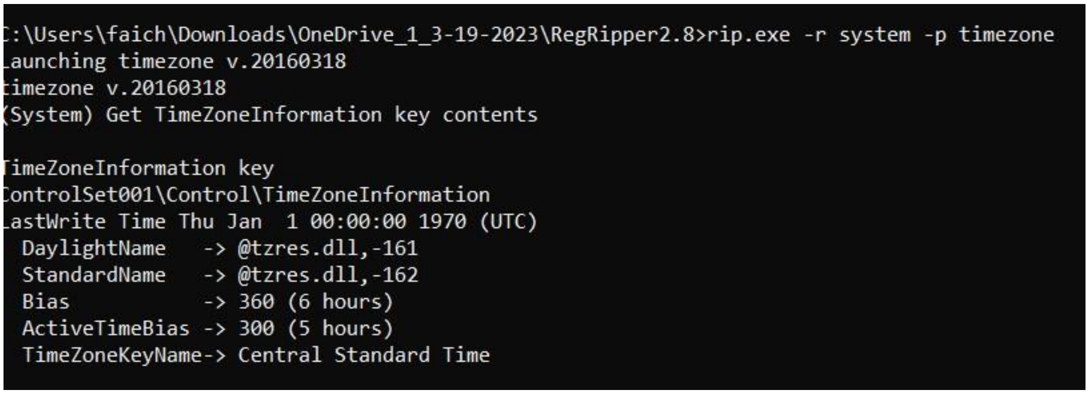
   By using the “winver” plugin and the software hive file, I was able to determine that the operating system was Windows and the version was Windows 10 Pro.



```
C:\Users\faich\Downloads\OneDrive_1_3-19-2023\RegRipper2.8>rip.exe -r software -p winver
Launching winver v.20081210
winver v.20081210
(Software) Get Windows version

ProductName = Windows 10 Pro
InstallDate = Wed Mar 16 21:13:33 2022
```

3. What time zone is used by the computer? Hint: System hive file

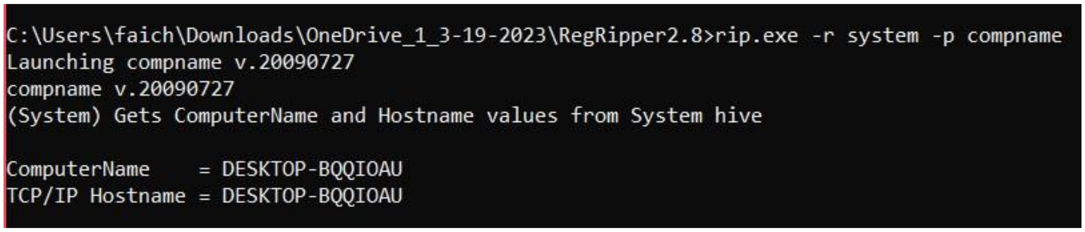
By using the “timezone” plugin and the system hive file I was able to determine that the time zone used by the computer was Central Standard Time.



```
:\Users\faich\Downloads\OneDrive_1_3-19-2023\RegRipper2.8>rip.exe -r system -p timezone
aunching timezone v.20160318
imezone v.20160318
(System) Get TimeZoneInformation key contents

imeZoneInformation key
ontrolSet001\Control\TimeZoneInformation
astWrite Time Thu Jan  1 00:00:00 1970 (UTC)
  DaylightName   -> @tzres.dll,-161
  StandardName   -> @tzres.dll,-162
  Bias           -> 360 (6 hours)
  ActiveTimeBias -> 300 (5 hours)
  TimeZoneKeyName-> Central Standard Time
```

4. What is the name of the computer being investigated? Hint: System hive file

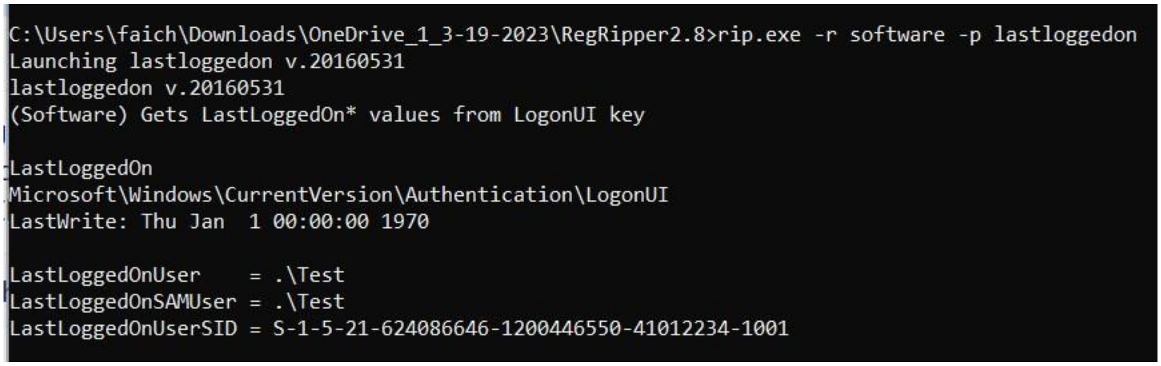
By using the "compname" plugin and the system hive file, I was able to determine that the computer's name was DESKTOP-BQQIOUA.



```
C:\Users\faich\Downloads\OneDrive_1_3-19-2023\RegRipper2.8>rip.exe -r system -p compname
Launching compname v.20090727
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = DESKTOP-BQQIOAU
TCP/IP Hostname = DESKTOP-BQQIOAU
```

5. Which user logged on last and when? Hint: Software hive file

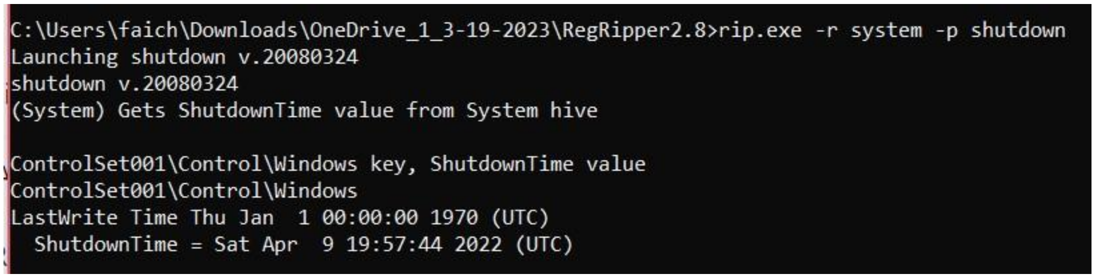
   By using the plugin "lastloggedon" and the software hive file I was able to determine that the last logged on user was .\Test and they last logged on Thursday January 1, 1970 at 00:00:00.



```
C:\Users\faich\Downloads\OneDrive_1_3-19-2023\RegRipper2.8>rip.exe -r software -p lastloggedon
Launching lastloggedon v.20160531
lastloggedon v.20160531
(Software) Gets LastLoggedOn* values from LogonUI key

LastLoggedOn
Microsoft\Windows\CurrentVersion\Authentication\LogonUI
LastWrite: Thu Jan  1 00:00:00 1970

LastLoggedOnUser    = .\Test
LastLoggedOnSAMUser = .\Test
LastLoggedOnUserSID = S-1-5-21-624086646-1200446550-41012234-1001
```

6. When was the system last shut down? Hint: System hive file

   By using the "shutdown" plugin and the system hive file I was able to determine that the last shut down occurred on Saturday August 9, 2022 at 19:57:44.



```
C:\Users\faich\Downloads\OneDrive_1_3-19-2023\RegRipper2.8>rip.exe -r system -p shutdown
Launching shutdown v.20080324
shutdown v.20080324
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
ControlSet001\Control\Windows
LastWrite Time Thu Jan  1 00:00:00 1970 (UTC)
  ShutdownTime = Sat Apr  9 19:57:44 2022 (UTC)
```

Great Job! After the successful completion of this lab, we gathered some key pieces of evidence that are of great value to the investigation. We got the product type of the machine, the operating system it was running on, the time zone it used, the different users on the system, the installed applications, and much more.

9.1 Estimated Completion Time

The total estimated time to complete this lab is about two hours.

9.1.1 Validation/Evaluation Criteria

The grade for this lab is based on the correctness and exposition quality of the answers to the above questions.

10 Lab Submission Guidelines

Please turn in the deliverables, including the solutions to the questions and the approach taken to arrive at these conclusions to the learning management system as directed by your instructor.

11 Notes for Instructors (and learners)

Instructors and students, this lab aims to develop a fundamental skill in using a seminal digital forensic software, Regripper.

12 References

[1] stevewhims, “Registry Hives - Win32 apps.” https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives (accessed Apr. 28, 2022).

[2] H. Carvey, *RegRipper3.0*. 2022. Accessed: Apr. 28, 2022. [Online]. Available: https://github.com/keydet89/RegRipper3.0

13 Feedback

After completing the lab, please critique the lab in an effort to improve my work. Some of the questions you can ask yourself in the process include the following:

- Were the instructions/documentation as thorough as it could have been?
- Did you learn new techniques while solving the case?

Please reach out to me via email (kxg095@shsu.edu) in case of any feedback.