Lab – Analyzing the Windows Registry for Evidence

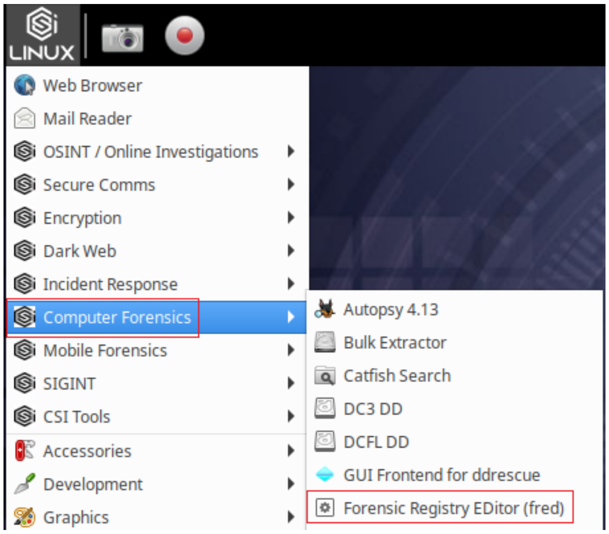
Overview

In this lab, you will learn how to perform a forensics analysis of the Windows registry for finding forensic information relevant to a criminal investigation. On any Windows system, the registry is a source of evidence against the cybercriminal as it maintains the details of the activity on the system.

Lab Requirements

- Completion of the following lab
  - Lab – Acquiring a Forensic Copy of the Windows Registry
- An installation of VirtualBox
- One virtual install of CSI Linux

In our previous lab, **Acquiring a Forensic Copy of the Windows Registry**, we used a USB install of FTK Imager to create for forensic copy of a live Windows 10 registry. We saved the registry files to the same USB drive and then mounted the USB drive inside our virtual install of CSI Linux to give us access to the saved files for analysis using the free registry analysis tool, Forensic Registry Editor (fred)


LINUX
Web Browser
Mail Reader
OSINT / Online Investigations
Secure Comms
Encryption
Dark Web
Incident Response
Computer Forensics
Mobile Forensics
SIGINT
CSI Tools
Accessories
Development
Graphics
Autopsy 4.13
Bulk Extractor
Catfish Search
DC3 DD
DCFL DD
GUI Frontend for ddrescue
Forensic Registry EDitor (fred)