Lab Assignment

Cybersecurity Professional Program

Digital Forensics &
Incident Response

Windows Live Analysis

DFIR-05-L3
Prefetch Investigation

Lab Objectives

Learn how to identify previously executed programs on the machine, even after their removal.

Lab Mission

Perform an installation and uninstallation of software to investigate the evidence of its existence.

Lab Duration

10–20 minutes

Requirements

- Basic knowledge of Windows
- Basic knowledge of process forensics

Resources

- Environment & Tools
    - VirtualBox
        - Windows 10
- Extra Lab Files
    - ***AnyDesk.exe***
    - ***Winprefetchview.zip***

Textbook References

- Chapter 5: Windows Live Analysis
    - Section 6: Process Forensics

Lab Task

In this task, you will identify evidence that a deleted program was previously executed on the computer.

1. Use the provided **AnyDesk** executable to install the software in the Windows 10 VM.

2. Uninstall **AnyDesk**.

3. Find evidence of prefetch files that indicate that **AnyDesk** software was executed in the system by typing **C:\windows\Prefetch** in the search.

4. Investigate the prefetch file using the provided **WinPrefetchView** software to find additional evidence of **AnyDesk** usage.