# MODULE 06 Defeating Anti-forensics Techniques

Lara Alofi

2110886

Y

Computer Hacking Forensic Investigator (CHFI)

Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/05f267f3-33e5-46ee-848e-3dce0e06eaa1>

Username on EC-Council System

1. 2110886@uj.edu.sa

A screenshot of a computer

Description automatically generated

**Lab 01:**

In this lab, I explored the acquisition of volatile information from a live Windows system for digital forensics investigations. Using both Windows Server 2022 and Windows 11 virtual machines, I gathered data including system time, network information, logged-on users, and active processes using various tools such as PsTools, LogonSessions, and NetworkOpenedFiles. Additionally, I ran commands like netstat and created a Python script to monitor network duration and bandwidth usage. This exercise provided hands-on experience in capturing volatile data, which is crucial for effective forensic analysis in live systems.

**Lab 02:**

In this lab, we investigated a Windows RAM image using Redline to examine active processes, identify anomalies, and analyze network connections. Our primary objective was to locate and extract forensic information, such as the PID of a specific process (U10Detect.exe), to understand the process hierarchy and determine any potential security concerns. This lab emphasized using Redline’s capabilities for memory analysis, allowing us to gather valuable insights into system activities and uncover potential signs of compromise within the forensic image.

**Lab 03:**   
In this lab, we explored the process of extracting and analyzing artifacts from a Windows RAM dump file using MemProcFS. The scenario involved forensic investigator David, who needed to mount and examine the memory dump for forensic evidence. Using a virtual file system, MemProcFS allowed us to parse and view memory artifacts as organized text files, making it easier to detect hidden rootkits, analyze suspicious processes, and uncover hidden objects. By successfully mounting the memory dump on a virtual M: drive, we accessed and examined critical artifacts, enhancing our skills in Windows RAM forensics.

**Lab 04:**

In this lab, we learned to capture and examine Windows registry files on a live system using AccessData FTK Imager and Hex Workshop. The scenario emphasized the importance of analyzing the Windows registry to extract forensic artifacts such as user activity, recent files, and USB usage. We began by installing FTK Imager to capture registry files from a live Windows Server environment and saved these files in a designated folder. Afterward, we used Hex Workshop to open and view the contents of the captured registry files, allowing us to analyze specific details related to system activity and installed applications. This exercise reinforced our skills in live registry file acquisition and analysis.

**Lab 05:**

In Lab 5, we explored methods for examining web browser artifacts to detect suspicious online activities. Using tools like ChromeCacheView, ChromeCookiesView, and ChromeHistoryView for Google Chrome, along with MZCacheView, MZCookiesView, and MZHistoryView for Mozilla Firefox, we extracted browsing history, cache, and cookies. These tools provided valuable details, such as URLs, file paths, access dates, and server information, which help investigators identify unusual behavior patterns or unauthorized site access. This process is crucial in forensic investigations for gathering evidence of potential cyber misconduct.

**Lab 06:**

In Lab 6, we focused on recovering InPrivate browsing data, a common challenge in forensic investigations involving hidden browsing activities. Through AccessData FTK Imager, we examined a logical disk image and specifically analyzed the pagefile.sys, which stores data on inactive processes and recent file interactions. By searching for “SystemUpdate.exe,” the malicious file the attacker downloaded in Incognito mode, we identified details, including the IP address (10.10.1.8) of the Ubuntu server from which it was accessed. This lab emphasized the importance of deep artifact searches to uncover evidence from private browsing sessions.

**Lab 07:**   
In Lab 7, we explored carving and analyzing browser SQLite3 database files to uncover web activity for forensic investigation. Using AccessData FTK Imager, we extracted the Chrome browser’s History and Web Data SQLite files from a disk image, then examined them with SysTools SQLite Viewer. This allowed us to analyze downloaded files, visited URLs, and search terms, as well as view account information saved in the browser. This exercise demonstrated how to extract and analyze browser artifacts, a key step in uncovering hidden or suspicious user activity on compromised systems.

**Lab 08:**  
In Lab 8, we focused on extracting and reconstructing cached web pages from Google Chrome to investigate a cyber incident involving a malicious file download. Using AccessData FTK Imager, we extracted the cached data from the browser's cache directory. We then utilized the Browser History Examiner tool to analyze the cached web pages, viewing them as they appeared to the user. This included examining cached images, web pages, and file sizes for different content types, essential for understanding the user's online activities during the investigation. This lab emphasized the importance of accessing and interpreting cached data in digital forensic investigations.

**Lab 09:**   
will work with OSForensics to enhance your digital forensics skills. The lab focuses on creating a forensic case, where you'll input relevant details such as case name and investigator information. You'll perform file searches to identify potential evidence, utilizing keywords and advanced search options. Additionally, the lab involves gathering and analyzing user activities, as well as recovering deleted files to verify their integrity. This hands-on experience will provide a comprehensive understanding of OSForensics and its application in digital investigations.

**Lab 10:**

will focus on extracting information about loaded processes on a computer using the Process Explorer tool. The lab emphasizes the importance of understanding processes as instances of executing programs, which is crucial for identifying malicious activities during forensic investigations. You will navigate to the Process Explorer executable, accept the license agreement, and explore its graphical user interface (GUI) to view and analyze running processes. Tasks include examining process details such as CPU usage, viewing associated DLLs, and analyzing their properties. The lab also covers saving string data and searching online for additional information about specific DLLs. By the end of this lab, you will gain practical skills in using Process Explorer to investigate loaded processes, enhancing your expertise in digital forensics.

**Lab 11:**

In Lab 11, you used Event Log Explorer to analyze Windows event logs related to a cyber-crime incident at a technology company. The lab focused on examining the **Brute Force.evtx** file to identify **Audit Failure** and **Audit Success** events indicative of brute force attacks. Key tasks included installing the application, filtering events to isolate relevant entries, and saving the analyzed logs for further investigation. This lab highlighted the significance of event log analysis in digital forensics for uncovering malicious activities and constructing timelines of security breaches.

A screenshot of a computer

Description automatically generated