# Module 11: Dark Web Forensics Report

Lara Alofi

2110886

Y

Computer Hacking Forensic Investigator (CHFI)

Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/645b10cc-3250-4230-8f7d-862784ac31bf>

Username on EC-Council System

1. 2110886@uj.edu.sa

A white rectangle with black and blue arrows

Description automatically generated

**Lab 01:**

This lab focuses on identifying Tor Browser activity on a suspect's Windows machine during a forensic investigation. Investigators analyze prefetch files to uncover traces of the Tor Browser, even if it has been uninstalled or deleted. The lab introduces tools like **WinPrefetchView** to extract metadata, including execution timestamps and run counters, and demonstrates how network connections associated with Tor can be monitored using the netstat command. By analyzing these artifacts, forensic investigators can establish a timeline and confirm potential dark web activity linked to the case.

**Lab 02:**

This lab demonstrates the process of analyzing RAM dumps to uncover artifacts related to Tor Browser activities on a suspect's machine. Using **Bulk Extractor**, investigators analyze memory dumps to retrieve valuable forensic evidence, such as website domains, email addresses, URLs, and search queries associated with Tor Browser usage. By examining files like domain.txt, email.txt, json.txt, url.txt, and url\_searches.txt, investigators can extract artifacts, reconstruct email communications, and trace online activity even when the browser is closed. This method provides critical insights into suspect behavior and aids in building a case with substantial evidence.