**Ass 9 - CCleaner**

**🧽 What is CCleaner?**

**CCleaner** is a **popular system optimization and privacy cleaning tool** developed by Piriform. It helps users **clean junk files**, **erase digital footprints**, and **optimize their system performance**.

It’s often used in **anti-forensics** to remove **digital traces** (logs, histories, temp files) that could otherwise be used to investigate or reconstruct user activity.

**🧠 In Simple Words:**

Think of CCleaner as a **digital eraser**. It wipes out the evidence of your actions on a computer — like:

* Web history
* Recently opened files
* Cache and cookies
* Temporary system files
* Application usage logs

So, if someone were trying to track what you did on the system, they would find very little if CCleaner had cleaned it up.

**🔍 Key Features Relevant to Anti-Forensics:**

| **Feature** | **Purpose** |
| --- | --- |
| **Cleaner** | Removes browser cache, cookies, and history. Cleans system temp files, clipboard data, recent documents, etc. |
| **Registry Cleaner** | Deletes unused or broken Windows registry entries (not very forensic-focused, but useful for stealth). |
| **Drive Wiper** | Overwrites free disk space to ensure deleted files **can’t be recovered** (very important for anti-forensics). |
| **Uninstall/Startup Manager** | Helps remove software and manage what runs on boot (can remove forensic tools). |
| **Scheduled Cleaning** | Can be set to run automatically to ensure consistent trace removal. |

**🔐 Anti-Forensics Use Case (Within Legal Context):**

| **Action** | **CCleaner Feature** |
| --- | --- |
| Remove web browsing traces | Browser Cleaner |
| Delete temp files that store activity | System Cleaner |
| Prevent recovery of deleted files | Drive Wiper (with secure erase method) |
| Remove app usage traces (like MRU – Most Recently Used) | Application Cleaner |

**NOTE**: Using CCleaner to hide malicious or unauthorized activities is illegal. It’s okay to use it for **privacy** and **learning purposes**, not for **tampering with digital evidence**.

**🧪 How to Do the Assignment**

**🔹 Objective:**

Study how CCleaner hides or removes digital traces and how it can be used in anti-forensic scenarios.

**✅ Step-by-Step for Assignment:**

**1. Install and Open CCleaner**

* Download from <https://www.ccleaner.com>
* Install it on a test (non-critical) system.

**2. Explore Key Modules:**

* Go to the **Custom Clean** tab — run a scan and note what it finds (browser history, system files, etc.).
* Use **Drive Wiper** under “Tools” → “Drive Wiper” to securely erase free space.
* Use the **Registry Cleaner** to clean registry logs.
* Optionally explore **Startup Manager** and **Uninstall** features.

**3. Perform Tasks and Capture Screenshots**

* Before cleaning: Browse a few websites, open documents, etc.
* Run CCleaner and clean everything.
* Use a forensic tool (like Recuva or Windows Event Viewer) to try finding traces.
* Report what was deleted or hidden.

**📄 Sample Report Format**

diff

CopyEdit

🔧 Tool Studied: CCleaner

📌 Features Used:

- Custom Clean (deleted temp files, web history)

- Drive Wiper (securely wiped free space)

- Registry Cleaner

📝 Observations:

- After cleaning, browser history and temp files were gone.

- Recuva couldn’t recover files from free space.

- Most Recently Used (MRU) lists were cleared.

🔐 Anti-Forensic Insight:

CCleaner can effectively erase digital footprints and prevent data recovery using its secure wipe and system clean features.

⚠️ Note: This activity was done on a test machine for educational purposes only.