**🧪 Experiment 5: Forensic Investigation of Web Browser Logs to Detect Evidence**

**✅ Step-by-Step Procedure (As Per PDF)**

**🔹 Step 1: Install Browser History Examiner**

Go to the official download page: 🔗 https://www.foxtonforensics.com/browser-history-examiner/download

**Note:** Browser History Examiner is a **Windows-based tool**. So to use it on Kali Linux, you have 2 options:

* Use **Wine** to run the .exe tool.
* Or install it on a **Windows VM**.

**👉 Option A: Run using Wine on Kali**

If you're on Kali Linux and want to run it with Wine:

bash

CopyEdit

sudo apt update

sudo apt install wine -y

Download the .exe from the website, then run it:

bash

CopyEdit

wine BrowserHistoryExaminerSetup.exe

**🔹 Step 2: Launch Browser History Examiner**

After installation:

* Open **Browser History Examiner**.
* Click on **"Start New Case"**.
* Select the **user profile or browser cache/history files** you want to examine (Chrome, Firefox, IE, etc.).
* The tool will scan and show:
  + Visited sites
  + Timestamps
  + Downloaded files
  + Cached content

**🔹 Step 3: Analyze the Extracted Evidence**

* Use the **interface tabs** to view:
  + History
  + Cookies
  + Downloads
  + Cache
* Export reports if needed for documentation.

🧠 Examples of evidence you can find:

* **Visited websites**
* **Search queries**
* **Login timestamps**
* **Webmail artifacts**
* **Cached images/emails**

**🧾 Output:**

* Screenshot of:
  + Visited websites
  + Cookie timeline
  + Page titles and URLs
* Exported CSV or HTML report (optional)