**Project Requirement and Specification**

On

**Performance analysis of Web Browser Forensic Tools :**

(CSE Semester IV Mini Project)



**Submitted to:                                                                    Submitted by:**

Dr. Vikas Tripathi Yadeesh Bhagnal

(Mini Project Incharge) B.Tech CSE-SE / 74

                                                                                                               Roll No.  2015117

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**GRAPHIC ERA DEEMED UNIVERSITY DEHRADUN**

1. **About Project**

The mini project that I selected is Performance analysis of Web Browser Forensic Tools. This project is based on the demonstration of performance of some web forensic tools as well as its implementation to analyze the activity logs of a Browser.

**Web Browser Forensic Tools** helps to analyze evidence like history, cache, cookies, downloads list, entering URL addresses, access time of visit, frequency of visits from the user's computer etc. It can be very useful for tracing a criminal in case any sort of crime occurs.

1. **Performance analysis of Web Browser Forensic Tools**

The Web Browser Forensic Tools which have been used are as follows:

* EnCase Forensic
* Forensic Toolkit (FTK)
* X-Ways Forensic (XWF)

**2.1 EnCase Forensic**

The software comes in several product designed for forensic, cyber security, security analysis and e-discovery use. EnCase is generally used to recover evidence from seized hard drives.  Encase allows the investigator to conduct in depth analysis of user files to collect evidence such as documents, pictures, internet history and Windows Registry information.

* + 1. **Pros:**
* EnCase is a very user-friendly forensic tool. It provides the analyst to work with a user-friendly interface.
* This tool also has good reporting functionalities built into it, in terms of processing and analysis feature.
* It also has a free version that can be used for evidence acquisition and is easy to use.
* EnCase has built in support for almost all types of encryption including Bitlocker, MacAfee, Symantec etc.
* Good keyword searching capabilities and scripting features are available.
  + 1. **Cons:**
* This is a very expensive tool ( approx. 3600 $).
* Encase processing can take a lot of time in case of very large compound files and mails.
* The latest versions of Encase sometimes are not compatible with other forensic based tools.
  1. **Forensic Toolkit (FTK)**

Forensic Toolkit or FTK is a computer forensics software made by AccessData. It scans a hard drive looking for various information. It can potentially locate deleted emails and scan a disk for text strings to use them as password dictionary to crack encryption.

* + 1. **Pros:**
* It has a simpler user interface and advanced search capabilities.
* FTK supports Encrypting File System (EFS) decryption.
* It produces a case log file.
* It has significant bookmarking and salient reporting features.
  + 1. **Cons:**
* FTK does not support scripting features.
* It also does not have a timeline view.
* It does not have multi-tasking capabilities.
* There is no progress bar to estimate the time remaining.
  1. **X-Ways Forensic**

X-ways Forensic is a powerful, commercial computer forensic tool. It is windows based licensed software which offers many functionalities pertaining to computer forensics.

* + 1. **Pros:**
* Evidence processing options can be customized as per the requirement of the case .
* It has a very flexible filtering options as well as highly customized search functions.
* It is portable in nature and it checks for new feature on a regular basis.
  + 1. **Cons:**
* The user interface is complex.
* It is a dongle-based software and does not work without it.
* There is no support for Bitlocker

1. **Analyzing the activity logs of web browser using forensic tools.**

Our task is to analyze the activity logs of a web browser using forensic tools. We will be analyzing the logs of **Google Chrome** using **Browser History Examiner** forensic tool

* 1. **Steps for using the Forensic Tool.**
* To check the activity logs, first we need to capture history from the computer.

Graphical user interface, application

Description automatically generated

* Select browser and the type of data that you want to analyze.
* Select the destination folder where you want information to be stored.
* Click on **Capture**.

Graphical user interface, text, application

Description automatically generated

* The Browser history examiner will begin to capture data from the machine.

Graphical user interface, text, application

Description automatically generated

* A pop up will appear saying that capture is complete and whether the user wants to load captured history now.
* Click yes to view the history.

Graphical user interface, text, application, email

Description automatically generated

* Data extraction process will be started.

Graphical user interface

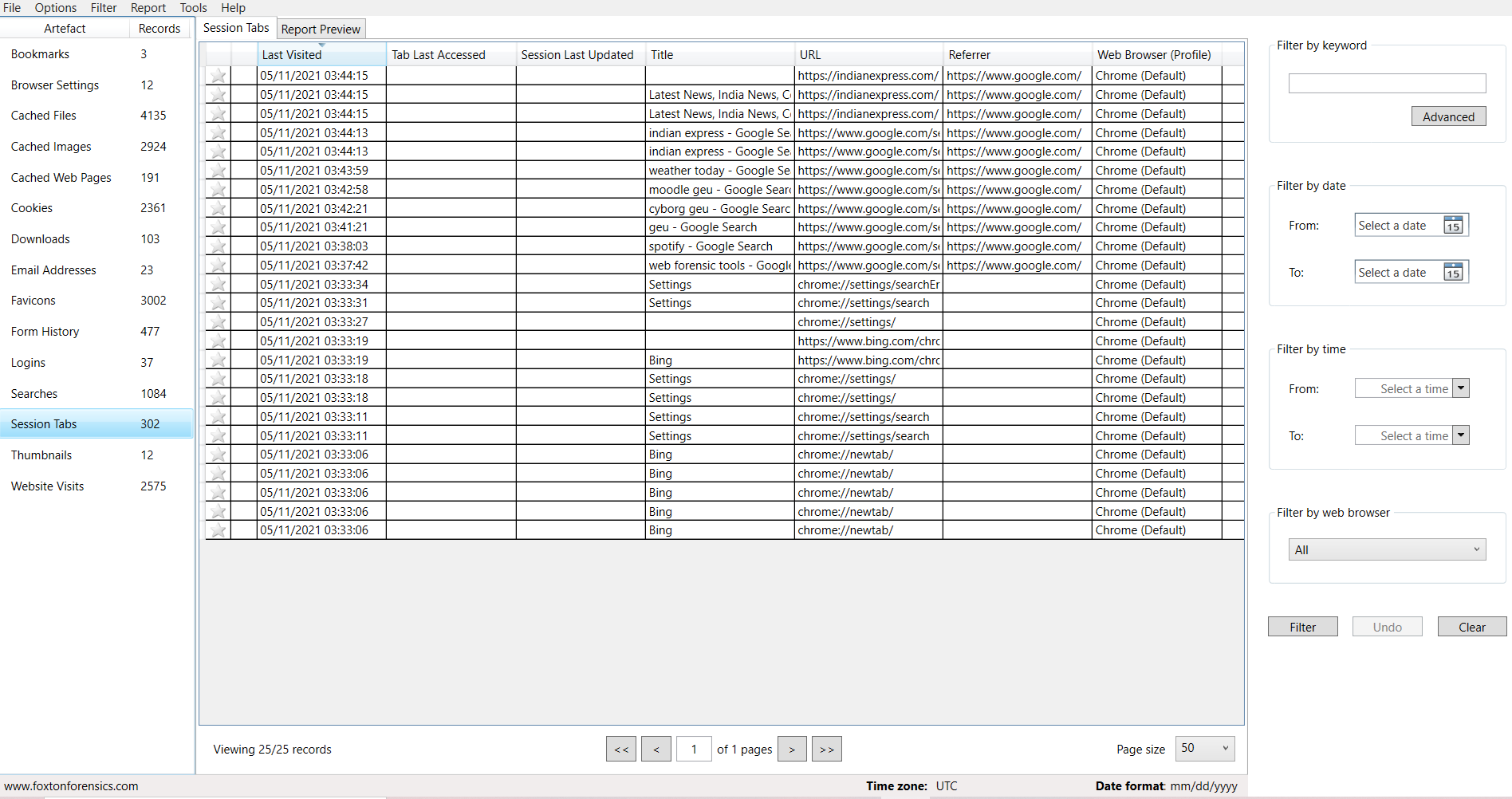
Description automatically generated

* After completion of the process the user can check information like visited websites, recent tabs, searches, logins, downloads etc.

Graphical user interface, application, table

Description automatically generated

Viewing the **websites visited.**



Viewing the **session tabs.**

Graphical user interface, table

Description automatically generated

Viewing the **search history**.

REFERENCE :

* <https://accessdata.com/products-services/forensic-toolkit-ftk>
* <https://security.opentext.com/encase-forensic>
* <https://www.x-ways.net/forensics/index-m.html>
* <https://www.youtube.com/watch?v=sfYWMtO3SdU&t=378s>
* <https://nasbench.medium.com/web-browsers-forensics-7e99940c579a>