**TABLE OF CONTENTS**

|  |  |
| --- | --- |
| TABLE OF CONTENT **……………………………………………………………......** | 1 |
| LIST OF SCREENSHOTS **…………………………………………………………….** | 2 |
| **3. Information of Existing Tools .………………………...………………..…………** | **3** |
| 3.1 Digital Forensic Process **…………………………………………………………...** | 3 |
| 3.1.1 Steps in Digital Forensic Process **……………………………………………..…** | 4 |
| 3.1.2 Backup and Recovery **……………………………………………………………** | 4 |
| 3.2 Existing Tools **………………..…………………………………………………….** | 4 |
| 3.2.1 Autopsy **…………………………...……………………………………………...** | 4 |
| 3.2.2 Browser History Examiner **………………………………………………………** | 5 |
| 3.2.3 NetAnalysis **………………………………………………………………………** | 6 |
| 3.2.4 Internet Evidence Finder **…..…………………………………………………......** | 7 |
| **4 Implementation Screenshot ……………………………………………………..….** | **9** |
| 4.1 Introduction **………………………………………………………………………...** | 9 |
| 4.2 Environment Setup **…………………………………………………………………** | 9 |
| 4.2.1 Hardware Requirement **…………………………………………………………..** | 9 |
| 4.2.2 Software Requirement **…………………………………………………………...** | 9 |
| 4.3 Tool information for development **…………………………………………………** | 11 |
| 4.4 Coding Language information for development **…………………………………...** | 13 |
| 4.5 Implementation Screenshot **….……………………………………………………..** | 15 |
| 4.5.1 Login Page **………….…………………….………………………………..…….** | 15 |
| 4.5.2 Main Page **………...……………………….……………………………….…….** | 16 |
| 4.5.3 Google Chrome Forensics **………………………………………………….……** | 16 |
| 4.5.4 Mozilla Firefox Forensics **….…………….………………………………………** | 17 |
| 4.5.5 Opera Browser Forensic **………………….……………………………….……..** | 17 |
| 4.5.6 Internet Explorer Browser Forensic**……..……………………………….………** | 18 |
| 4.5.7 Safari Browser Forensic **….……..………………………………………………..** | 18 |
| **5 References …………………………………………………………………………...** | **19** |

**LIST OF SCREENSHOTS**

|  |  |
| --- | --- |
| 4.5.1Login Page **…..……………………………….…………………………………** | 15 |
| 4.5.2 Main Page **….…………...………………………………………………………** | 16 |
| 4.5.3 Google Chrome Forensic **…………..…………………………………………..** | 16 |
| 4.5.4 Mozilla Firefox Forensic **…………..…………………………………………...** | 17 |
| 4.5.5 Opera Browser Forensic **……………………..…………………………………** | 17 |
| 4.5.6 Internet Explorer Browser Forensic **…..………………………………………..** | 18 |
| 4.5.7 Safari Browser Forensic **………………………………………………………..** | 18 |

**Chapter 3: Information of Existing Tools**

**3.1 Digital Forensic Process**

The digital forensic process is a recognized scientific and forensic process used in [digital forensics](https://en.wikipedia.org/wiki/Digital_forensics) investigations. Forensics process defines it as a number of steps from the original incident alert through to reporting of findings.

The process is predominantly used in [computer](https://en.wikipedia.org/wiki/Computer_forensics) and [mobile](https://en.wikipedia.org/wiki/Mobile_device_forensics) forensic investigations and consists of three steps: acquisition, analysis and reporting. Digital media seized for investigation is usually referred to as an "exhibit" in legal terminology. Investigators employ the [scientific method](https://en.wikipedia.org/wiki/Scientific_method) to recover [digital evidence](https://en.wikipedia.org/wiki/Digital_evidence) to support or disprove a hypothesis, either for a [court of law](https://en.wikipedia.org/wiki/Court_of_law) or in [civil proceedings](https://en.wikipedia.org/wiki/Civil_litigation).

Digital forensics is a branch of [forensic science](https://en.wikipedia.org/wiki/Forensic_science) encompassing the recovery and investigation of material found in digital devices, often in relation to [computer crime](https://en.wikipedia.org/wiki/Computer_crime). The term digital forensics was originally used as a synonym for [computer forensics](https://en.wikipedia.org/wiki/Computer_forensics) but has expanded to cover investigation of all devices capable of [storing digital data](https://en.wikipedia.org/wiki/Computer_data_storage).

**3.1.1 Steps in digital forensic process**

1. Assess the crime scene- To conduct an investigation, one needs to obtain proper authorization which would normally include assessing the case, asking people and documenting the results in an effort to identify crime and location of the evidence.
2. Collection phase- Here one would need to identify potential sources of data and acquire forensic data from them such as desktops, storage media, routers, cell phones,digital camera etc.. Finding the evidence, discovering their relevance, gathering the evidence, and preparing a chain of custody are the main steps in collection phase.
3. Analysis phase- Examine the collected data/files and find out the actual evidence. The computer forensic investigator must trace, filter, and extract hidden data during the process.
4. Report phase- The audience should be able to understand the evidence data which has been acquired from the evidence collection and analysis phase. The report generation phase records the evidence data found out by each analysis component. Additionally, it records the time and provides hash values of the collected evidence for the chain-of-custody.
5. Chain-of-custody and documentation phase- Documentation is essential for the investigation. For evidence to be reliable in court, integrity has to be preserved. Safe storage and tamper protection is needed. Chain of custody prevents accusation in court that the evidence has been tampered with. Evidence needs to be labeled as soon as it is collected. All actions performed by the investigator should be documented, including the reasons for doing so. This means logging all actions and integrity checks.

**3.1.2 Backup and Recovery**

**3.1.2.1 Recovery methods of browser history**

1. **Recover deleted internet history through System Restore**

The easiest method is to do a [system restore](http://windows.microsoft.com/en-GB/windows7/products/features/system-restore). If the internet history was deleted recently system restore will recover it. To get system restore up and running you can go to the ‘start’ menu and do a search for system restore which will take you to the feature. Alternatively, go to ‘Start’ click on ‘Programs’ and then ‘Accessories.’

You’ll see a ‘System Tools’ option and ‘System Restore’ will be in there. Select the date you’d like to restore your computer to and sit back and wait until it does its thing. When finished the computer will reboot and if check your browser the internet history should be in there.

## 2) See lost internet history through Desktop search programs

Sometimes though system restore options are disabled. This can happen, for example, if you have a second hand computer that’s had a previous life in a corporate environment. It’s not common but does happen. In this case you can use desktop search programs.

If you can remember a few keywords that you want to search for in the internet history, type them into the search box and they should be recovered.

## 3) Cookies show you the way

Internet cookies are also another good method to access internet history.  A cookie is a small text file that stored in your internet browser. They store your user information to for the web sites you visit. Some of us thing of them as spying tools but actually in most instances they remember your account and browsing history making it easier for you when you revisit websites.

There’s a [great wiki How page here](http://www.wikihow.com/View-Cookies) that shows in very simple terms how to access cookies on Internet Explorer, Firefox, Chrome and Safari browsers. If you can see the cookies you know what the internet history is.

**3.1.2.2 Access deleted browning history with log files**

Another method is to recover the history using log files. This method is suitable for histories that were deleted a long time ago. A word of warning though, while there is a simple step-by-step process to follow using this method some strange things can be thrown up such as warnings that you might lose other data. This isn’t common but it’s a point worth nothing. All Windows computers have a file extension that stores arbitrary data. It’s called Index.dat and is a file hidden on your computer that contains all of the web sites that you have ever visited. It lists every URL and every web page.

Before you begin navigating these steps you must set Windows to show hidden files and folders.  To do this go to ‘Start’ then ‘Settings’ then ‘Control Panel’ and finally ‘Folder Options’. When you’re in ‘Folder Options’ click the ‘View’ tab. Go to ‘Advanced settings’ and click ‘Show hidden files and folders’. Then uncheck ‘Hide Protected Operating System files’ and click OK. Once you are finished searching, don’t forget to go back and undo these changes.  
To begin your search go to My Computer and use the search tool to find all instances of index.dat in the C drive. The search should pull up multiple index.dat files. To read an index .dat file you need to know the software that created the file. However you can download index.dat reader software from the internet. [This site](http://index-dat-viewer.winsite.com/) offers such a reader though there are many more available which you’ll soon discover if you do your own search.

**3.2 Existing Tools**

**3.2.1 Autopsy**

Autopsy is a digital forensic platform for Windows and Linux. It provides the facility for data carving, timeline analysis, and web artifact analysis. The autopsy extracts the web history, cookies, bookmarks from Firefox, Chrome and IE.

Autopsy is a digital forensics platform and graphical interface to [The Sleuth Kit](https://www.sleuthkit.org/sleuthkit/index.php) and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

**Features:**

1. Easy to Use

Autopsy was designed to be intuitive out of the box. Installation is easy and wizards guide you through every step. All results are found in a single tree. See the [intuitive](https://www.sleuthkit.org/autopsy/intuitive.php) page for more details.

2) Extensible

Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from [third-parties](http://wiki.sleuthkit.org/index.php?title=Autopsy_3rd_Party_Modules). Some of the modules provide:

[Timeline Analysis](https://www.sleuthkit.org/autopsy/timeline.php) - Advanced graphical event viewing interface (video tutorial included).

Hash Filtering - Flag known bad files and ignore known good.

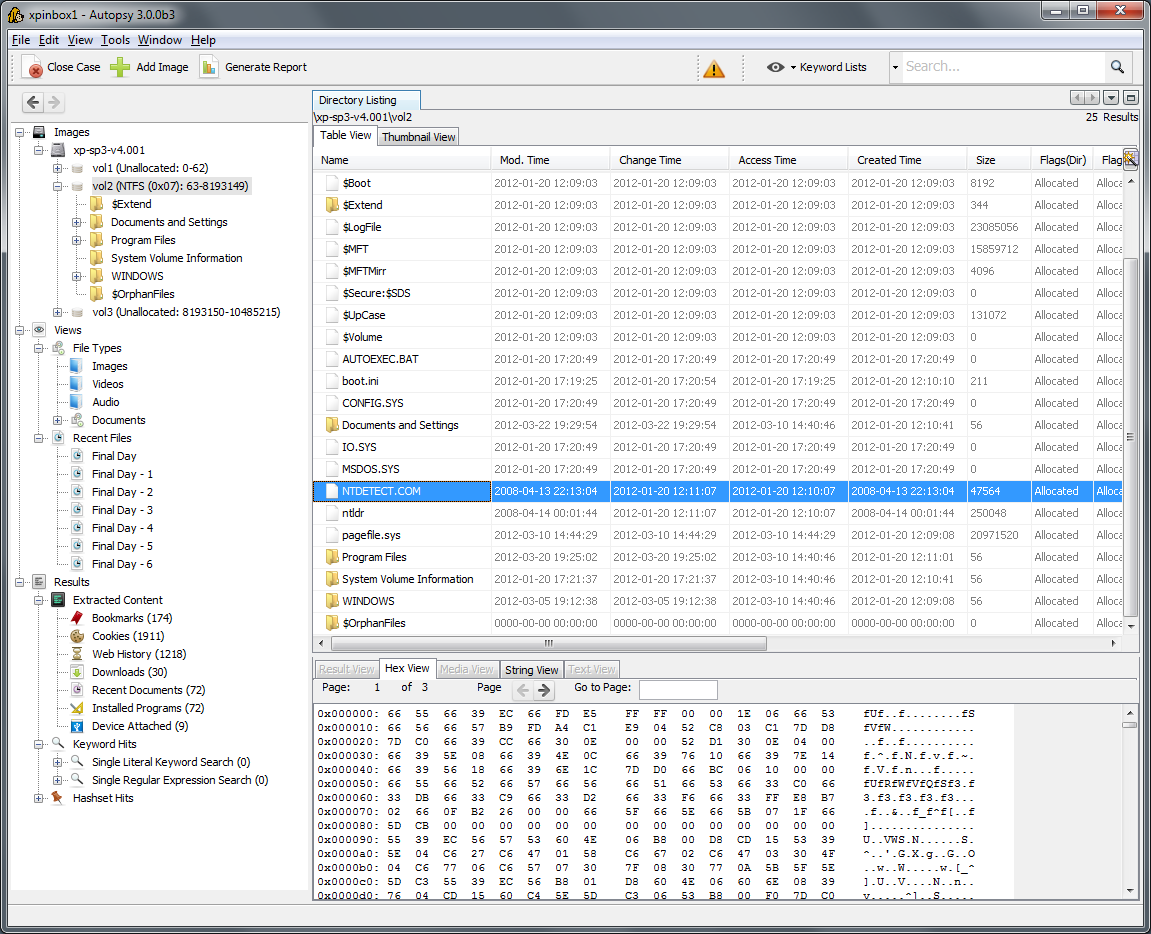
[Keyword Search](https://www.sleuthkit.org/autopsy/keyword.php) - Indexed keyword search to find files that mention relevant terms.

[Web Artifacts](https://www.sleuthkit.org/autopsy/web_artifacts.php) - Extract history, bookmarks, and cookies from Firefox, Chrome, and IE.

Data Carving - Recover deleted files from unallocated space using [PhotoRec](http://www.cgsecurity.org/wiki/PhotoRec)

Multimedia - Extract EXIF from pictures and watch videos.

Indicators of Compromise - Scan a computer using [STIX](http://stix.mitre.org/).

[](https://www.sleuthkit.org/autopsy/images/v3/overview.png)

**3.2.2 Browser History Examiner**

The Browser History Examiner analyzes web history for chrome, firefox, internet explorer web browser on the Windows platform. Browser History Examiner is a forensic software tool for capturing, extracting and analysing internet history from the main desktop web browsers. Many types of data can be analysed including website visits, searches, downloads and cached files.

**Features:**

1. **Website Activity Timeline**

Website visits are displayed alongside an interactive graph showing how many sites have been visited over a particular time period. This is useful for identifying peaks in internet activity.

**2) Cached Web Page Viewer**

Web pages stored in the browser cache are automatically reconstructed, allowing them to be easily viewed in the state that they were originally seen by a user.

**3) Internet Search History**

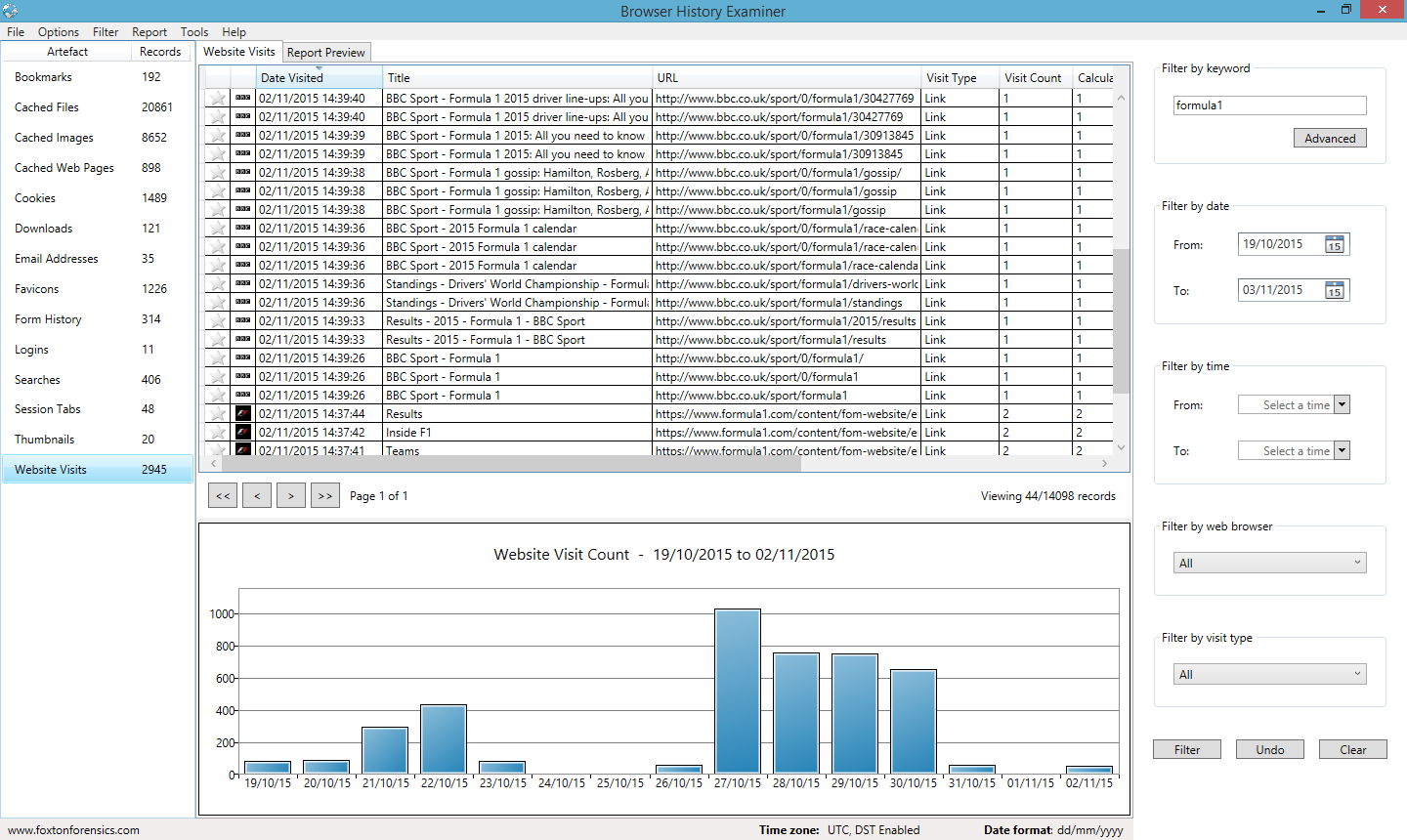
Search history is automatically extracted from multiple sources for popular sites such as Google, Bing, Yahoo, Google Maps, YouTube, Facebook, Twitter and eBay.

**4) Reporting and Data Export**

Reports can be built dynamically and saved to PDF or HTML. Records can be exported to CSV, HTML, XML or Concordance Load File.

**5) Remote Data Capture**

Web browser history can be captured from the local computer or a remote Windows computer over a network.



**3.2.3 NetAnalysis**

NetAnalysis is a state-of-the-art application for the extraction, analysis and presentation of forensic evidence relating to Internet browser and user activity on computer systems and mobile devices. Our NetAnalysis suite also includes advanced data recovery solution designed to recover deleted browser artefacts which can be imported into, and analysed in NetAnalysis. NetAnalysis is a software product that offers significant improvements over existing applications and methodologies.

#### Web Browser Forensics

#### NetAnalysis was designed specifically for web browser forensics and supports all the major desktop and mobile browsers. It supports the analysis of history, cache, cookies and other artefacts; it has powerful reporting capabilities to allow you to quickly produce evidence relating to user activity. The software also has powerful analytical tools to help you decode and understand the data.

#### Filtering And Searching

Searching, filtering and identifying items of interest/evidential value is easy with NetAnalysis. The software has a number of powerful searching and filtering features, as well as a visual filter builder to allow you to create and store powerful queries. You can also search by keywords and utilise some of the keyword lists/ready made filters we ship. To assist with rapid evidence identification, we have added a high-performance, full-featured text search engine to NetAnalysis.

**Cache Export And Page Rebuilding**

The web page rebuilding engine for NetAnalysis has been completely reengineered.  It is now considerably faster and more capable than its predecessor. We have added an offline HTML5-compliant viewer which is capable of displaying cached web pages, video, images and other content; it can also play audio files. NetAnalysis now extracts web page previews and thumbnails.

**Reporting**

The NetAnalysis reporting suite offers reporting, data analysis and visualisation. It also provides all the tools necessary, in the end-user report designer, to create virtually any report type, be it hierarchical master-detail reports, record and multi-column reports or interactive drill down and drill-through reports. The report manager provides the capability to save a report template to file and then re-use it as and when required.

**3.2.4 Internet Evidence Finder**

Internet Evidence Finder (IEF) is a computer forensics software product that can recover data from a hard drive, live RAM, or files for Internet-related evidence. IEF was designed with digital forensics examiners in mind, IEF is also used extensively by personnel in IT information security, electronic discovery, cyber security, and corporate investigations.

Features:

-Social Networking Artifacts

-Instant Messenger Chat History

-Webmail

-Full Web browser artifacts

-P2P file sharing applications

**Chapter 4: Implementation Details**

**4.1 Introduction**

This chapter deals with the setting up the environment for implementing the system. UserInterface screen shows how the user will interact with the system.

**4.2 Environment Setup**

**4.2.1 Hardware Requirement**

System: Pentium IV 2.4 GHz or more.

Processor: 2 Physical CPU Cores

Ram: 512 MB or More

Hard Disk: 20 GB (Min.)

USB Port: 2.0

Monitor: 15 VGA Color.

1 Mouse

**4.2.2 Software Requirement**

Operating system: - Windows 7 or More

Coding Language: JAVA, SQLite

Tool Used: - NetBeans 8.1

**4.3 Tool information for development**

**NetBeans IDE**

NetBeans IDE lets you quickly and easily develop Java desktop, mobile, and web applications,as well as HTML5 applications with HTML, JavaScript, and CSS. The IDE also provides a greatset of tools for PHP and C/C++ developers. It is free and open source and has a large communityof users and developers around the world.

**Best Support for Latest Java Technologies**

NetBeans IDE is the official IDE for Java 8. With its editors, code analyzers, and converters, youcan quickly and smoothly upgrade your applications to use new Java 8 language constructs, suchas lambdas, functional operations, and method references.Batch analyzers and converters are provided to search through multiple applications at the sametime, matching patterns for conversion to new Java 8 language constructs.With its constantly improving Java Editor, many rich features and an extensive range of tools,templates and samples, NetBeans IDE sets the standard for developing with cutting edgetechnologies out of the box.

**Fast & Smart Code Editing**

An IDE is much more than a text editor. The NetBeans Editor indents lines, matches words andbrackets, and highlights source code syntactically and semantically. It lets you easily refactorcode, with a range of handy and powerful tools, while it also provides code templates.The editor supports many languages from Java, C/C++, XML and HTML, to PHP, Groovy,Javadoc, JavaScript and JSP. Because the editor is extensible, you can plug in support for many other languages.

**Easy & Efficient Project Management**

Keeping a clear overview of large applications, with thousands of folders and files, and millionsof lines of code, is a daunting task. NetBeans IDE provides different views of your data, frommultiple project windows to helpful tools for setting up your applications and managing themefficiently, letting you drill down into your data quickly and easily, while giving you versioningtools via Subversion, Mercurial, and Git integration out of the box.When new developers join your project, they can understand the structure of your applicationbecause your code is well-organized.

**Rapid User Interface Development**

Design GUIs for Java SE, HTML5, Java EE, PHP, C/C++, and Java ME applications quicklyand smoothly by using editors and drag-and-drop tools in the IDE.For Java SE applications, the NetBeans GUI Builder automatically takes care of correct spacingand alignment, while supporting in-place editing, as well. The GUI builder is so easy to use andintuitive that it has been used to prototype GUIs live at customer presentations.

**Write Bug Free Code**

The cost of buggy code increases the longer it remains unfixed. NetBeans provides staticanalysis tools, especially integration with the widely used FindBugs tool, for identifying andfixing common problems in Java code. In addition, the NetBeans Debugger lets you placebreakpoints in your source code, add field watches, step through your code, run into methods,take snapshots and monitor execution as it occurs. The NetBeans Profiler provides expertassistance for optimizing your application's speed and memory usage, and makes it easier tobuild reliable and scalable Java SE, JavaFX and Java EE applications. NetBeans IDE includes avisual debugger for Java SE applications, letting you debug user interfaces without looking intosource code. Take GUI snapshots of your applications and click on user interface elements to jump back into the related source code.

**Support for Multiple Language**

NetBeans IDE offers superior support for C/C++ and PHP developers, providing comprehensiveeditors and tools for their related frameworks and technologies. In addition, the IDE has editorsand tools for XML, HTML, PHP, Groovy, Javadoc, JavaScript, and JSP.

**Cross Platform Support**

NetBeans IDE can be installed on all operating systems that support Java, from Windows toLinux to Mac OS X systems. Write Once, Run Anywhere, is as true for NetBeans IDE as it is foryour own applications... because NetBeans IDE itself is written in Java, too!

**Rich Set of Community Provided Plugins**

The NetBeans community is large and active; many users are developing new plugins all the time because NetBeans IDE is extensible and has well-documented APIs. Are you missing a feature in NetBeans IDE? Create a plugin that fills the gap and participate in making NetBeans even better than it already is!

**4.4 Coding Language information for development**

**Java Language Feature**

1. Simple

Java is easy to learn and its syntax is quite simple, clean and easy to understand. The confusing and ambiguous concepts of C++ are either left out in Java or they have been reimplemented in a cleaner way.

*Eg :* Pointers and Operator Overloading are not there in java but were an important part of C++.

2. Object-Oriented

In java everything is Object which has some data and behaviour. Java can be easily extended as it is based on Object Model.

3. Platform independent

Unlike other programming languages such as C, C++ etc which are compiled into platform specific machines. Java is guaranteed to be write-once, run-anywhere language. On compilation Java program is compiled into bytecode. This bytecode is platform independent and can be run on any machine, plus this bytecode format also provides security. Any machine with Java Runtime Environment can run Java Programs.

4. Secured

When it comes to security, Java is always the first choice. With java secure features it enable us to develop virus free, temper free system. Java program always runs in Java runtime environment with almost null interaction with system OS, hence it is more secure.

5. Robust

Java makes an effort to eliminate error prone codes by emphasizing mainly on compile time error checking and runtime checking. But the main areas which Java improved were Memory Management and mishandled Exceptions by introducing automatic **Garbage Collector** and **Exception Handling**.

6. Multithreaded

Java multithreading feature makes it possible to write program that can do many tasks simultaneously. Benefit of multithreading is that it utilizes same memory and other resources to execute multiple threads at the same time, like While typing, grammatical errors are checked along.

7. High Performance

Java is an interpreted language, so it will never be as fast as a compiled language like C or C++. But, Java enables high performance with the use of just-in-time compiler.

**4.5 Implementation Screenshot**

Implementation is the stage of the project when the theoretical design is turned out into a

working system. Thus it can be considered to be the most critical stage in achieving a successful

new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it‗s

constraints on implementation, designing of methods to achieve changeover and evaluation of

changeover methods.

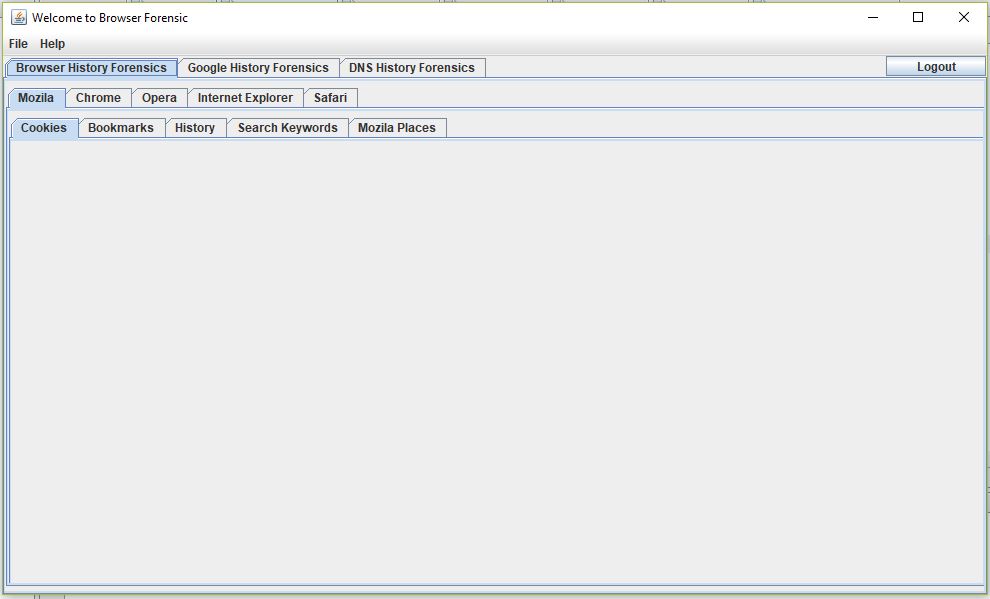
* + 1. **Login Page**

This is Login Page for the system that will use for intering into system. If you have correct credentials then and then only we can login to the system.

**** Screenshot 4.5.1 Login Page

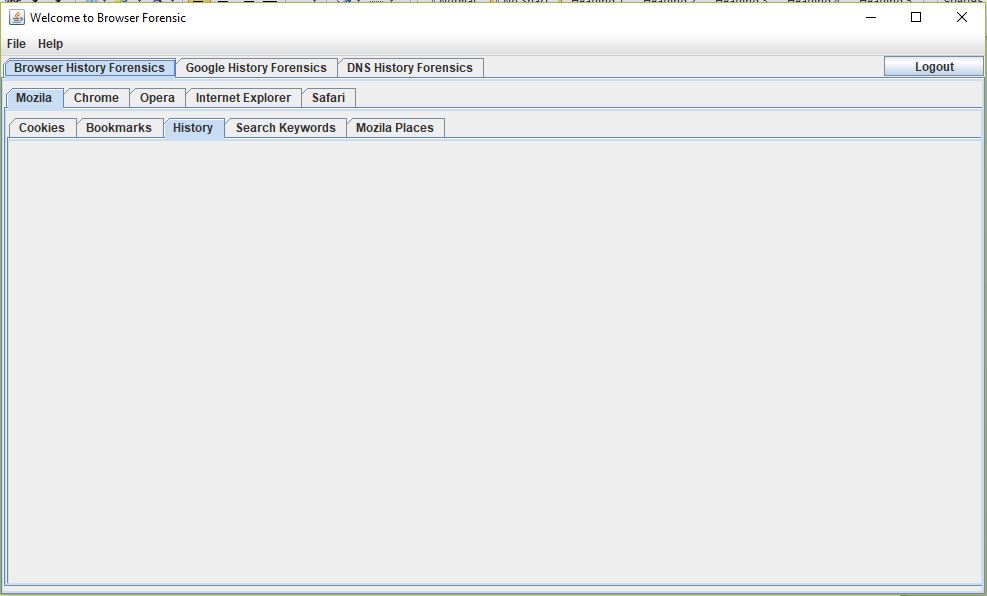
* + 1. **Home Page**

This is the main menu page or Homepage of our system. After login to the system this page is open.

**** Screenshot 4.5.2 Home Page

* + 1. **Forensic of Mozilla Browser**

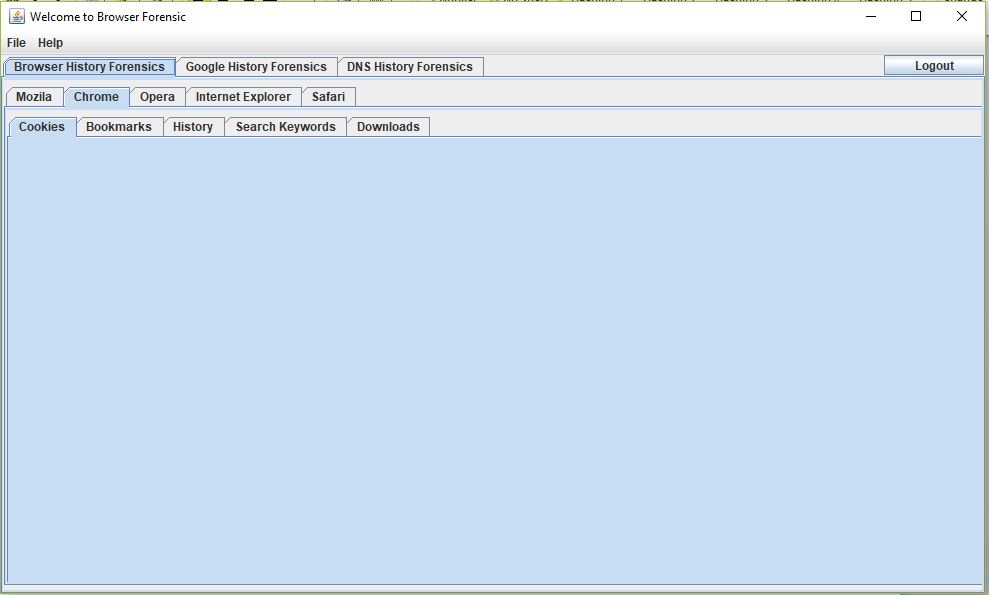
This is the for Mozilla Firefox browser forensic. This contains some more functionality tabs Cookies, Bookmarks, History, Search Keywords and Mozilla Places tab.

****

Screenshot 4.5.3 Mozilla Firefox Forensic

* + 1. **Forensic of Google Chrome**

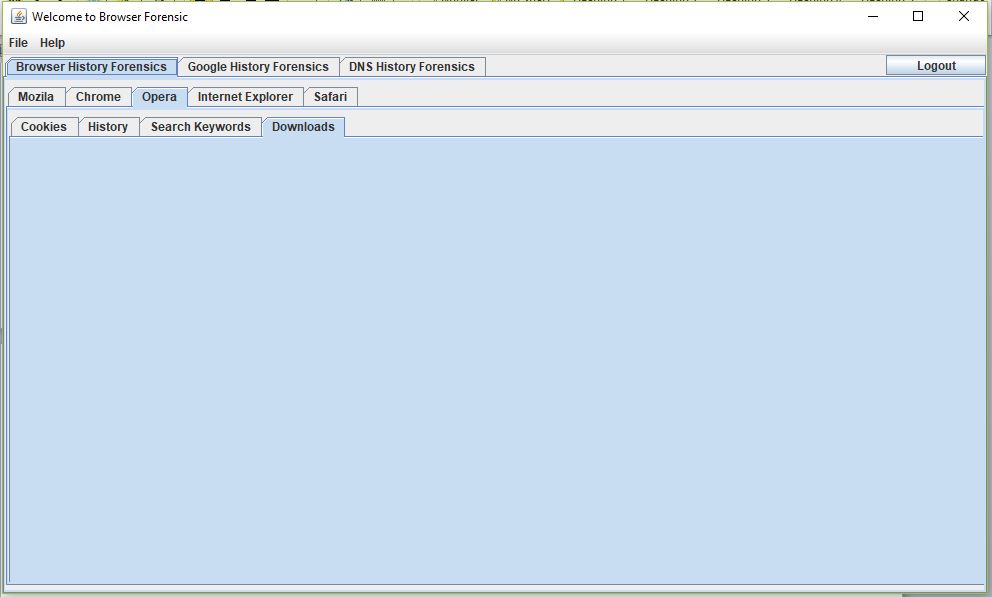
This is the for Google Chrome browser forensic. This contains some more functionality tabs Cookies, Bookmarks, History, Search Keywords and Downloads tab.

****

Screenshot 4.5.4 Google Chrome Forensic

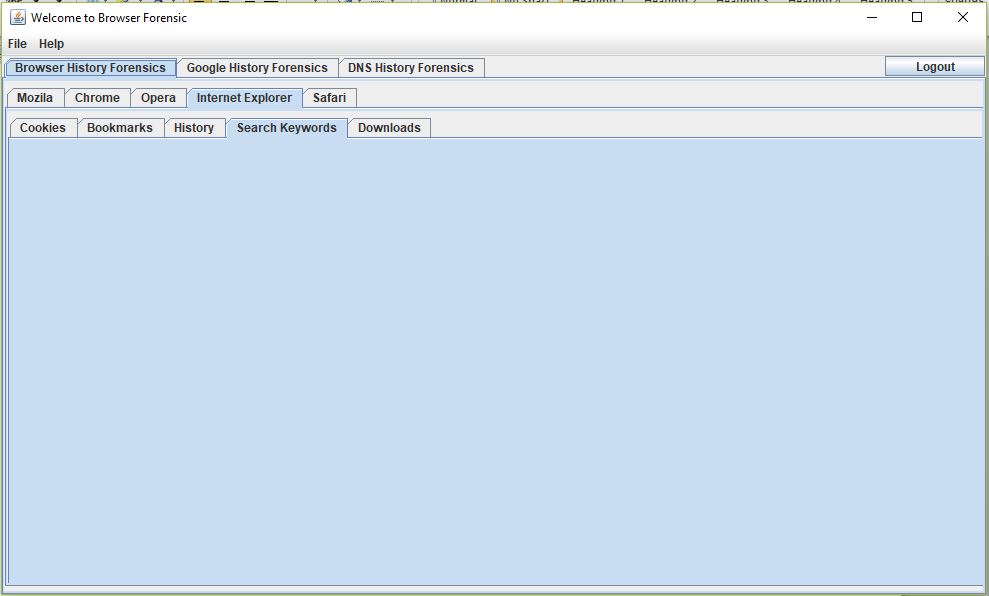
* + 1. **Forensic of Opera**

This is the for Opera browser forensic. This contains some more functionality tabs Cookies, History, Search Keywords and Downloads tab.

**** Screenshot 4.5.5 Opera Browser Forensic

* + 1. **Forensic of Internet Explorer**

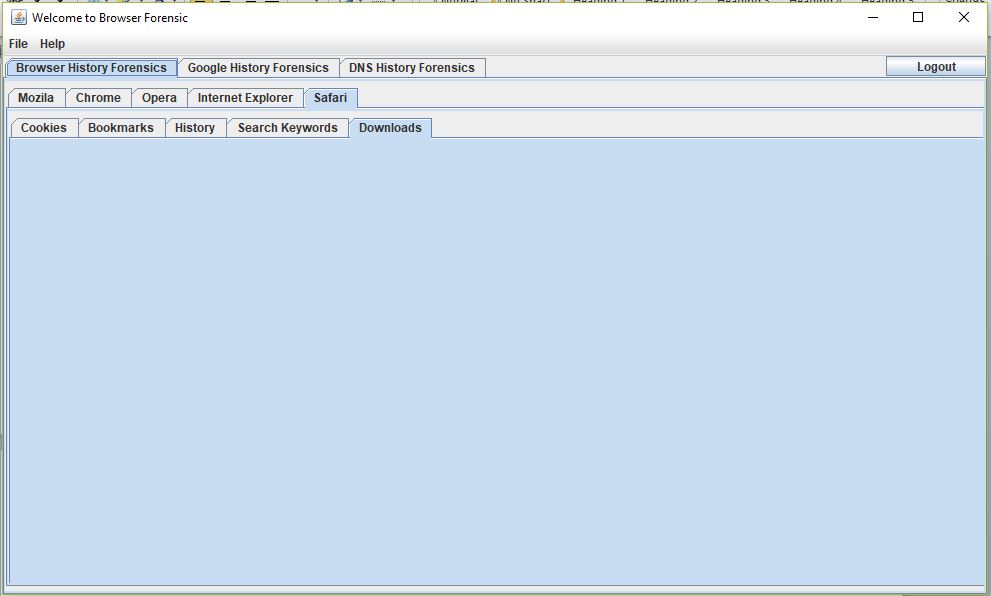
This is the for Internet Explorer browser forensic. This contains some more functionality tabs Cookies, Bookmarks, History, Search Keywords and Downloads tab.

****

Screenshot 4.5.6 Internet Explorer Forensic

* + 1. **Forensic of Safari Browser**

This is the for Mozilla Firefox browser forensic. This contains some more functionality tabs Cookies, Bookmarks, History, Search Keywords and Downloads tab.

****

Screenshot 4.5.7 Safari Browser Forensic

**Chapter 5: References**

1) Wade Alcorn,Christian Frichot ,Michele Orru ,“The Browser Hacker’s Handbook”.

2) Keith J. Jones ,”Forensic Analysis of Internet Explorer Activity Files”,International Conference on Innovations in Information Technology,2011.

3) Sherri David off Jonathan Ham, “Network Forensics Tracking Hackers through Cyberspace”,2012.

4) Andrew Marrington, Ibrahim Baggili, Talal Al Ismail, Ali Al Kaf, ”Portable Web Browser Forensics -A forensic examination of the privacy benefits of portable web browsers”,IEEE,2012.

5) Murilo Tito Pereira,”Forensic analysis of the Firefox3 internet history and recovery of

deleted SQLite records”, Sciencedirect,2009.

6) Taub, Eric A. (2006-04-05),"Deleting may be easy, but your hard drive still tells all",

New York Times. Retrieved 2009-01-11.

7) Jeff Dillon and Steve Perez, ”Prosecutor hammers away at computer forensic expert; Dad's patron describes Brenda's propositions” San Diego Union-Tribune, July 3, 2002.

8) Erhan Akbal, Fatma Guneş, Ayhan Akbal,” Digital Forensic Analyses of Web Browser Records”, Journal of Software,2016

9) “Advanced evidence collection and analysis of web browser activity”, Junghoon Oh, Korea University CIST, Republic of Korea Seungbong Lee, Sangjin Lee.2011.

10) Springer Open Journal, “Do private and portable web browsers leave incriminating

evidence?: a forensic analysis of residual artifacts from private and portable web

browsing sessions”, Donny J Ohana and Narasimha Shashidhar.

11) <http://www.linuxjournal.com/content/creating-centralized-syslog-server> - Syslog server information.

12) <http://web.iiit.ac.in/~mayank.natani/central-logging-server/> - Linux system logging mechanism that records all the system activities. These logs are very critical for system admin for troubleshooting purpose. The target is to build a central logging server which could be used automatically to save all the logs of client machines.

# 13) <http://www.toptenreviews.com/software/internet/best-internet-browser-software/> - The Best Internet Browser Software of 2017

14) <http://whatismyipaddress.com/proxy-server> -What is IP? Why it is needed? How it works?

15) <http://www.forensicfocus.com/Content/pid=97/page=1/> -IDS related information.

16) <https://www.symantec.com/connect/articles/web-browser-forensics-part-1> -Forensic tools and it’s details.

17) <https://www.symantec.com/connect/articles/web-browser-forensics-part-2> -Forensic tools and it’s details.

18) <http://www.wikihow.com/View-Cookies> –How to view cookies?

19) <https://www.easeus.com/computer-instruction/recover-browser-internet-history.html> - How to Recover Browser/Internet History?

20) “Web Browser Analysis for Detecting User Activities”, Library Journal