**TABLE OF CONTENTS**

|  |  |
| --- | --- |
| TABLE OF CONTENT **……………………………………………………………......** | 1 |
| LIST OF FIGURE **…………………………………………………………………......** | 3 |
| LIST OF SCREENSHOTS **…………………………………………………………….** | 4 |
| LIST OF TABLES **…………………………………………………………………......** | 6 |
| **1. Introduction ………………………………...………………………………………** | **6** |
| 1.1 Background and Motivation **……………………………………………………….** | 6 |
| 1.1.1 Computer Forensics Background **………………………………………………...** | 6 |
| 1.1.2 Motivation and Challenges **………………………………………………………** | 7 |
| 1.1.2.1 Cyber Challenges **………………………………………………………………** | 8 |
| 1.2 Statement of the problem **………………………………………………………......** | 11 |
| 1.3 Block Diagram **……………………………………………………………………..** | 11 |
| 1.4 Operational Workflow **……………………………………………………………..** | 12 |
| 1.5 Conclusion **…………………………………………………………………………** | 12 |
| **2 Literature Survey ………………………………………………………………..….** | **13** |
| 2.1 Introduction **…………………………………………………………………..…….** | 13 |
| 2.1.1 Browser Forensics **………………………………………………………….…….** | 13 |
| 2.2 Digital Forensics Process **…………………………………………………..………** | 13 |
| 2.2.1 Types of Digital Forensics **………………………………………………………** | 15 |
| 2.3 Digital Forensics for Browser **……………………………………………….……..** | 16 |
| 2.3.1 Top Nine Web Browser **………………………………………………….………** | 16 |
| 2.3.2 Sources of Browser Evidences **…………………………………………………..** | 17 |
| 2.3.3 Browsers used for forensics **……………………………………………………..** | 18 |
| 2.4 Backup and Recovery **……………….…………………………………….……….** | 21 |
| 2.4.1 Recovery method for deleted information in Web browsers **……………………** | 21 |
| 2.4.2 Access deleted browning history with log files **…………………………………** | 22 |
| 2.4.3 Locations of Internet Browser Artifacts **………………………………………...** | 24 |
| 2.4.4 How to Recover Browser/Internet History **……..……………………………….** | 25 |
| 2.5 Existing Tools **………………..…………………………………………………….** | 44 |
| 2.5.1 Autospy **…………………………...……………………………………………...** | 44 |
| 2.5.2 Browser History Examiner **………………………………………………………** | 45 |
| 2.5.3 NetAnalysis **………………………………………………………………………** | 46 |
| 2.5.4 Internet Evidence Finder **…..…………………………………………………......** | 47 |
| **3 Implementation Screenshot ……………………………………………………..….** | **48** |
| 3.1 Login Page **…………….……………………………………………………..…….** | 53 |
| 3.2 Main Page **…………...……………………………………………………….…….** | 54 |
| 3.3 Google Chrome Forensics **…………………………………………………….……** | 54 |
| 3.4 Mozilla Firefox Forensics **…….……………………………………………………** | 55 |
| 3.5 Opera Browser Forensic **…………………………………………………….……..** | 55 |
| 3.6 Internet Explorer Browser Forensic**…..…………………………………….………** | 56 |
| 3.7 Safari Browser Forensic **…………..………………………………………………..** | 56 |
| **4 References …………………………………………………………………………...** | **57** |

**LIST OF FIGURES**

|  |  |
| --- | --- |
| 1.1 Block Diagram **…………………………………………………………………....** | 11 |

**LIST OF SCREENSHOTS**

|  |  |
| --- | --- |
| 2.1DNS Cache to view deleted browsing history **……………………………………** | 26 |
| 2.2 Deleted browsing history **…………………………………………………………** | 26 |
| 2.3 Chrome History in User File System **……………………………………………..** | 27 |
| 2.4 Firefox History in User File System **……………………………………………...** | 27 |
| 2.5 Internet Explorer History in User File System **……………………………………** | 28 |
| 2.6 Microsoft Edge in User File System **……………………………………………..** | 28 |
| 2.7 Safari in User File System **………………………………………………………..** | 29 |
| 2.8.1 Chrome History using Cookies Step 1 **………………………………………….** | 29 |
| 2.8.2 Chrome History using Cookies Step 2 **………………………………………….** | 30 |
| 2.8.3 Chrome History using Cookies Step 3 **………………………………………….** | 30 |
| 2.8.4 Chrome History using Cookies Step 4 **………………………………………….** | 31 |
| 2.8.5 Chrome History using Cookies Step 5 **………………………………………….** | 31 |
| 2.9.1 Firefox History using Cookies Step 1 **…………………………………………..** | 32 |
| 2.9.2 Firefox History using Cookies Step 2 **…………………………………………..** | 32 |
| 2.9.3 Firefox History using Cookies Step 3 **…………………………………………..** | 33 |
| 2.9.4 Firefox History using Cookies Step 4 **…………………………………………..** | 33 |
| 2.10.1 IE History using Cookies Step 1 **………………………………………………** | 34 |
| 2.10.2 IE History using Cookies Step 2 **………………………………………………** | 34 |
| 2.10.3 IE History using Cookies Step 3 **……………………………………………..** | 35 |
| 2.10.4 IE History using Cookies Step 4 **……………………………………………..** | 35 |
| 2.10.5 IE History using Cookies Step 5 **……………………………………………..** | 36 |
| 2.11.1 MS Edge History using Cookies Step 1 **……………………………………...** | 36 |
| 2.11.2 MS Edge History using Cookies Step 2 **……………………………………...** | 37 |
| 2.11.3 MS Edge History using Cookies Step 3 **……………………………………...** | 37 |
| 2.11.4 MS Edge History using Cookies Step 4.1 **……………………………………** | 38 |
| 2.11.5 MS Edge History using Cookies Step 4.2 **……………………………………** | 38 |
| 2.11.6 MS Edge History using Cookies Step 5 **……………………………………...** | 39 |
| 2.12.1 Safari History using Cookies Step 1 **…………………………………………..** | 39 |
| 2.12.2 Safari History using Cookies Step 2 **…………………………………………..** | 40 |
| 2.12.3 Safari History using Cookies Step 3 **…………………………………………..** | 40 |
| 2.12.4 Safari History using Cookies Step 4 **…………………………………………..** | 41 |
| 2.13.1 Recover deleted browsing history from Google History Step 1 **………………** | 42 |
| 2.13.2 Recover deleted browsing history from Google History Step 2 **……………...** | 42 |
| 3.5.1 Login Page **……………………………………………………………………** | 53 |
| 3.5.2 Homepage **…………………………………………………………………….** | 54 |
| 3.5.3 Forensic of Mozilla Firefox **………………………………………………….** | 54 |
| 3.5.4 Forensic of Google Chrome **………………………………………………….** | 55 |
| 3.5.5 Forensic of Opera Browser **…………………………………………………..** | 55 |
| 3.5.6 Forensic of Internet Explorer **………………………………………………..** | 56 |
| 3.5.7 Forensic of Safari Browser **…………………………………………………..** | 56 |
|  |  |
|  |  |

**LIST OF TABLES**

|  |  |
| --- | --- |
| 2.1 Top Nine Browser Rating chart **…………………………………………………..** | 17 |
| 2.2 Evidence sources of Browser **…………………………………………………….** | 17 |
| 2.3 Private browsing effect on Evidence Source Mozilla **…………………………...** | 19 |

**Chapter 1: Introduction**

Browser forensic is mainly used for analyzing things like browsing history and general web activity of a pc to check for suspicious usage or content that has been accessed. This also refers to monitoring traffic on a webpage and analysis of LOG files from server to get actual information about targeted machine. Computers and their storage media is the object of investigative analysis, known as Computer Forensics, aimed at characterizing and interpreting the digital evidences present on the devices.

The internet is used by almost everyone, including suspects under investigation. A suspect may use a web browser to collect information, to hide his/her crime, or to search for a new crime method. Searching for evidence left by web browsing activity is typically crucial component of digital forensic investigations. Almost every movement of a suspect performed by using a web browser thus would leave a trace on a computer. Thus when an investigator analyzes the suspect’s computer, this evidence can provide useful information. After retrieving data such as cookies, cache, history and download list from a suspect’s computer, it is possible to analyze this evidence for web sites visited, time and frequency of access, and search engine keywords used by the suspect.

Following can be the different sources where an investigator can find evidences in browser.

1. Surfing history
2. Bookmarks
3. Download
4. Cookies
5. Cache
   1. **Background and Motivation**

**1.1.1 Computer Forensics Background**

Computer forensics involves the investigation of digital sources to acquire evidence that can be used in a court of law. It can also be used to identify and respond to threats to hosts and systems. We use computer forensics to investigate computer crime or misuse, theft of trade secrets, theft of or destruction of intellectual property, and fraud. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it. Traditional cyber forensics have focused on dead-box analysis [1], but there is an emerging methodology for live-box analysis a technique that preserves and harvests vital evidence from a computer‘s physical memory, also referred to as random-access memory (RAM) or volatile memory. Cookies from various browsers contain important information about evidences. Try to recovering deleted cookies and other temporal file from system to get more evidences.

**1.1.2 Motivation and Challenges**

Forensics is changing in the digital age, and the legal system is still catching up when it comes to properly employing digital evidence broadly speaking, digital evidence is information found on a wide range of electronic devices that is useful in court because of its probative value. It's like the digital equivalent of a fingerprint or a muddy boot. However, digital evidence tendered in court often fails to meet the same high standards expected of more established forensics practices, particularly in ensuring the evidence is what it purports to be. This is not the first time that technology has impacted the way evidence is gathered and presented in courts. And it's not the first time that there have been problems in the way new evidence is used [2]. You might remember the case of the death of Azaria Chamberlain at Ayers Rock (Uluru) more than 30 years ago. Forensics played a key role in the conviction of Lindy Chamberlain in 1982. However, her conviction was later reversed in 1988 following closer scrutiny of the evidence. Subsequent coronial inquests, a court case featuring controversial DNA forensic evidence, and the subsequent Australian Royal Commission into Azaria's death, resulted in a fundamental reconsideration of Australian forensic practices.

There is still a vigorous debate in the legal world over the usage and reliability of DNA evidence, for example. This is now being mirrored in more recent court challenges over the use of digital evidence. The special properties and technical complexity of digital evidence makes it even more challenging, as courts find it difficult to understand the true nature and value of that evidence. In fact, my first role as a digital forensics consultant is typically to act as an interpreter, explaining what the evidence means in a legal context.

Leveraging Internet browser artifacts can be complex, but the value of the information available makes it worth the effort. The basics of Internet browser forensics revolve around artifacts such as Web sites visited, timestamps and counts of access, search histories, download activity, communications and the potential to rebuild Web pages viewed from cached files. However, locating and leveraging this information can be challenging without the needed prerequisite knowledge. The main challenges include:

* **Multiple browsers:** Investigators will likely encounter [**numerous mainstream browsers**](http://www.netmarketshare.com/). There may even be multiple browsers in use on the same machine.
* **Varied storage schemes:** Once investigators determine which browser(s) are being used, they must realize that each browser may store different types of artifacts, differently and in different locations. This is very important because different browsers often require different tools and approaches.
* **New/updated architectures:** Browser developers may even completely change the architecture between versions, as Mozilla Firefox and Internet Explorer (IE) have done in the past. For example, many tools that supported IE through Version 9 became useless with the release of IE 10 due to the significant changes made.
* **Non-standard browsers:** To further frustrate investigators, attackers may actually install a non-standard browser in an effort to obfuscate their activities.

**1.1.2.1 Cyber Challenges**

It is increasingly common for criminal trials to rely on digital evidence. And regrettably, it is not uncommon for innocents to be convicted and guilty people acquitted because of digital evidence.

There are several reasons for this. Firstly, the evidence might be compelling at first glance, but it could be misleading. The defendant may also have limited financial resources to rebut the evidence. The defense lawyers might also misread the evidence. Plea-bargaining offers can also lessen sentences. Conversely, other investigations may not get to trial because of the complexity or incompleteness of the evidence. Worryingly, some defendants are pleading guilty based on what appears to be overwhelming hearsay digital evidence without robust defense rebuttal. In these cases, the defense lawyer – whose job it is to analyze the evidence – may simply not understand it. This is why external digital forensics consultants can be so important. However, the high cost of mounting a defense using forensic practitioners is often beyond the financial reach of many. For those qualified to receive legal aid, it is increasingly hard to obtain sufficient funding because of stringent budgeting regimes in various Australian jurisdictions. Other factors can affect the validity of the evidence, including: failure of the prosecution or a plaintiff to report exculpatory data; evidence taken out of context and misinterpreted; failure to identify relevant evidence; system and application processing errors; and so forth. Investigators undertaking these important but tedious tasks are often under resourced over-burdened with complex cases, increasingly large and complex datasets, etc.

Forensic analyses and evidence presentations are sometimes confounded by inexperienced investigators and communicators, which is further exacerbated by faulty case management. Another problem issue is the paucity of reliable forensic tools and processes that meet the needs of investigators and the expectations of the courts. However, I also suspect some courts in Australia and elsewhere may be unaware of these undercurrents, or what standards they should expect of the evidence.

Digital forensics is still in its infancy, and it is more of an art form lacking broad scientific standards to supports its use as evidence. There is a call among researchers to test and trial better forensic practices and forensic tools. This is especially important due to the increasing size of data storage on some personal computing devices, let alone cloud and network storage, which presents greater recovery and jurisdictional challenges to practitioners.

We also need new tools and processes capable of locating and recovering sufficient evidence from larger data sets quickly, efficiently and thoroughly. Forensic tools are often commercial products, thus profit-driven rather than science-based, and do not fulfill real forensic needs. They increasingly fail to identify all evidence from larger datasets in a timely manner. The processes used by law enforcement tend to be agency-centric with little consensus on practice, standards and processes and sharing of case knowledge.

Cyber security threats to governments, businesses and individuals highlight our vulnerability to malicious attacks on our information assets and networks. Prevention and threat mitigation is topical, but we often overlook the simple act of bringing miscreants to justice and proving the innocence of those framed by their actions [3].

There is an old adage in forensics (thanks to Arthur Conan Doyle's fictional detective Sherlock Holmes): "There is nothing more deceptive than an obvious fact." This also applies to digital forensics, where I have all too often encountered cases of investigator bias and laziness when seeking the truth. Encouragingly, sounder tools and processes are emerging that I expect will rejuvenate this emerging discipline.

Some of challenges are:

* Increase in numbers of devices per person
* Larger storage devices
* Increased turnaround time
* Case backlogs
* Pressure to accelerate reporting time
* Technology changes
* New apps
* Cloud forensics

**Aim**

Find out all the evidences present in Communication Devices and Browsers and apply the forensics on that evidences and show the criminals information.

**1.2 Statement of the problem**

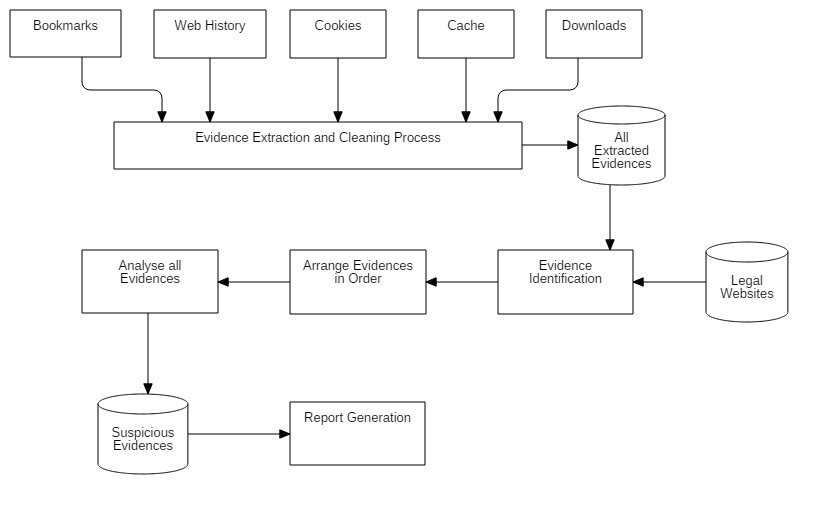
a. Study forensics on communication devices

Collect all possible evidences which are present on all Network communication devices and collect all LOG files present in that devices and apply forensics on those devices.

b. Forensics of browser to collect all local and server based evidences

Browser contain most of the information about user so collect and find all evidences present in Browser History, Cookies, and LOG files and present it properly.

**1.3 Block Diagram**

****

**Figure 1.1 Block Diagram**

Information ofabove block diagram is as follows.

Sources: Bookmarks, Web History, Cookies, cache, Downloads.

Evidence Extraction and cleaning process: Here all compressed data extracted in normal data.

All Extracted Evidences: All Extracted Evidences stored in database.

Legal Websites: This is the authorized websites by proxy server.

Evidence Identification: Find the illegal websites,evidences.

Arrange Evidences in Order: arrange all evidences in proper manner.

Analyze all evidences: Apply forensics process.

Suspicious Evidences: finding the suspicious data.

Report Generation: Generates the criminal’s information.

**1.4 Operational Workflow**

1) Select the source and get all possible evidences present in device.

2) Collect all evidences from communication devices and study the LOG files apply the forensics on that file.

3) Apply forensics on browser to find evidences.

4) Display the analysis reports and results.

**1.5 Conclusion**

We collect basic information about Digital Forensics their parameter and find various areas where we can do our research work to find, search, collect, recover various evidences which is useful to further investigation and proposed some module for Web Forensics.

**Chapter 2: Literature Survey**

**2.1 Introduction**

**2.1.1Browser Forensics**

The Internet is used by almost everyone, including suspects under investigation. A suspect may use a Web browser to collect information, to hide his/her crime, or to search for a new crime method. Searching for evidence left by Web browsing activity is typically crucial component of digital forensic investigations. Almost every movement a suspect performs while using a Web browser leaves a trace on the computer, even searching for information using a Web browser. Therefore, when an investigator analyzes the suspect‘s computer, this evidence can provide useful information. After retrieving data such as cache, history, cookies, and download list from a suspect‘s computer, it is possible to analyze this evidence for Web sites visited, time and frequency of access, and search engine keywords used by the suspect [2][18-19].

Research studies and tools related to analysis of Web browser log files exist, and a number of them share common characteristics. First, these studies and tools are targeted to a specific Web browser or a specific log file from a certain Web browser. Many kinds of Web browser provide Internet services today, so that a single user can use and compare different kinds of Web browser at the same time. For this reason, performing a different analysis for each Web browser is not an appropriate way to detect evidence of a user‘s criminal activity using the Internet. Moreover, it is not sufficient to investigate a single log file from a single browser because the evidence may be spread over several log files

**2.2 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 researcher [Eoghan Casey](https://en.wikipedia.org/wiki/Eoghan_Casey) 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).

**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.

**2.2.1 Types of Digital Forensics-**

**a. Network Forensics-**

Network forensics is a sub-branch of [digital forensics](https://en.wikipedia.org/wiki/Digital_forensics) relating to the monitoring and analysis of [computer network](https://en.wikipedia.org/wiki/Computer_network) traffic for the purposes of information gathering, legal evidence, or [intrusion detection](https://en.wikipedia.org/wiki/Intrusion_detection). Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

Network forensics is a comparatively new field of forensic science. The growing popularity of the Internet in homes means that computing has become network-centric and data is now available outside of disk-based [digital evidence](https://en.wikipedia.org/wiki/Digital_evidence). Network forensics can be performed as a standalone investigation or alongside a [computer forensics](https://en.wikipedia.org/wiki/Computer_forensics) analysis (where it is often used to reveal links between digital devices or reconstruct how a crime was committed).

Compared to computer forensics, where evidence is usually preserved on disk, network data is more volatile and unpredictable. Investigators often only have material to examine if packet filters, firewalls, and intrusion detection systems were set up to anticipate breaches of security.

**The Internet**

The internet can be a rich source of digital evidence including web browsing, email, [newsgroup](https://en.wikipedia.org/wiki/Newsgroup), synchronous chat and [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) traffic. For example, web server logs can be used to show when a suspect accessed information related to criminal activity. Email accounts can often contain useful evidence; but email headers are easily faked and, so, network forensics may be used to prove the exact origin of incriminating material. Network forensics can also be used in order to find out who is using a particular computerby extracting user account information from the network traffic.

**b. Database Forensics-**

Database forensics is a branch of [digital forensic science](https://en.wikipedia.org/wiki/Digital_forensics) relating to the forensic study of [databases](https://en.wikipedia.org/wiki/Databases) and their related metadata. The discipline is similar to [computer forensics](https://en.wikipedia.org/wiki/Computer_forensics), following the normal forensic process and applying investigative techniques to database contents and metadata. Cached information may also exist in servers [RAM](https://en.wikipedia.org/wiki/RAM) requiring [live analysis](https://en.wikipedia.org/wiki/Digital_forensics#live_analysis) techniques.

A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity in order to verify the actions of a database user. Alternatively, a forensic examination may focus on identifying transactions within a database system or application that indicate evidence of wrongdoing, such as fraud.

Software tools can be used to manipulate and analyse data. These tools also provide audit logging capabilities which provide documented proof of what tasks or analysis a forensic examiner performed on the database.

**c. Browser Forensics-**

Web forensic is mainly used for analyzing things like browsing history and general web activity of a pc to check for suspicious usage or content that has been accessed. This also refers to monitoring traffic on a webpage and analysis of LOG files from server to get actual information about targeted machine.

The internet is used by almost everyone, including suspects under investigation. A suspect may use a web browser to collect information, to hide his/her crime, or to search for a new crime method. Searching for evidence left by web browsing activity is typically crucial component of digital forensic investigations. Almost every movement of a suspect performed by using a web browser thus would leave a trace on a computer. Thus when an investigator analyzes the suspect’s computer, this evidence can provide useful information. After retrieving data such as cookies, cache, history and download list from a suspect’s computer, it is possible to analyze this evidence for web sites visited, time and frequency of access, and search engine keywords used by the suspect

**2.3 Digital Forensics for Browser**

**2.3.1 Top Nine Web Browser**

|  |  |  |
| --- | --- | --- |
| **Rank** | **Browser Name** | **Ratings** |
| 1 | Mozilla Firefox | 9.85 |
| 2 | Google Chrome | 9.72 |
| 3 | Opera | 9.30 |
| 4 | Safari | 9.00 |
| 5 | Internet Explorer | 8.63 |
| 6 | Torch | 8.28 |
| 7 | Maxthon | 8.22 |
| 8 | SeaMonkey | 7.75 |
| 9 | Avant Browser | 6.47 |

Table 2.1 Top Nine Browser Rating chart [15]

**2.3.2 Sources of Browser Evidences**

|  |  |  |
| --- | --- | --- |
| Sr. No. | Sources | Possible Evidences |
| 1 | Surfing History | Contain typed URLs, redirects and also the number of visits to a  Particular site. |
| 2 | Bookmarks | This would mainly contain shortcuts or bookmarks created to  Specific Websites by the user. |
| 3 | Download | An investigator would mainly need to check for downloaded file in  the default locations, also in the user defined locations or sometimes  files are downloaded to default locations and then are moved or  copied to user Defined locations. |
| 4 | Cookies | These are files that contain a wealth of information about the user. It  would contain information like usernames, passwords and web  Session information. |
| 5 | Cache | It is a temporary area on the disk which is used tostore most recently  Visited web sites. |

Table 2.2 Evidence sources of Browser

**2.3.3 Browsers used for forensics**

**1. Microsoft Internet Explorer-**

Microsoft Internet Explorer is one of the most commonly used web browsers on Windows. A list of areas from where most IE browsing artifacts are located could be as follows

* 1. Cookies(index.dat)
  2. History(index.dat)
  3. Registry(typed URLs, search queries, auto-complete, protected storage)
  4. Downloads
  5. Temporary Internet files and index.dat entries

It also offers users private browsing features called In Private Browsing. In Private Browsing allows the users to surf through internet without possibly leaving a trace on their computer. But still, while using in Private Browsing, some information such as cookies and temporary files are temporarily stored so that web pages work correctly. After the browsing session ends, all that data is discarded. Following is a list of areas affected by In Private Browsing.

1. Evidence Source from temporary internet files- In private browsing, it is stored on disk but is deleted after session.
2. Evidence from webpage history is not stored in Private Browsing.
3. Evidence from form data and password is also not stored in private browsing.
4. Evidence from anti-phishing cache- In Private Browsing, temporary information is encrypted and stored.
5. Evidence from automatic cache restore- In Private browsing, store is successful only if tab crashes and not entire session.
6. Evidence from document object model storage- This evidence is also discarded after session in Private browsing.

**2. Mozilla Firefox-**

Mozilla Firefox is another popular web browser which can be found on multiple platforms. [4,5 from doc]. Browsers like Mozilla and Chrome can also be found on mobile device working on platforms like Android, iPads etc.. Following could be the common areas where Firefox web browsing artifacts can be found and located:

1. Sqlite database structure
2. Prefs.js(user preference)
3. Signons.txt(encrypted data for website authentication)
4. Form history(Sqlite)
5. Cookies(Sqlite)
6. Firefox cache
7. Places(bookmarks and history)
8. Downloads

**Private Browsing features of Mozilla-**

Private browsing mode allows users to surf the Internet without saving any information about visited sites or pages. Mozilla makes it clear that private browsing mode does not make users anonymous from web sites, ISPs, and networks. So private browsing is merely affected in the application layer recognized in the OS. Aside from other privacy features, there is an option to enable the Dot-Not-Track feature in Firefox which requests that web sites do not track user browsing behavior.

|  |  |
| --- | --- |
| **Evidence Source** | **Private browsing affects Evidence Source** |
| Visited Pages | Will not be added in History menu, Library history, or other bar list. |
| Form and search bar entries | Nothing entered will be saved for Form Auto-complete |
| Passwords | No new passwords will be saved |
| Download list entries | No downloaded files will be listed under Downloads |
| Cookies | Cookies not saved |
| Cached web content | Cached web content not saved |
| Flash Cookies | Latest version of flash must be used to prevent saving |
| Offline web content and user data | This data is not saved |

Table 2.3 Private browsing effect on Evidence Source Mozilla

**3. Google Chrome-**

Google Chrome is another very popular web browser that can be found on both Windows and Mac OS [4]. Evidences from Chrome can be located in:

1. JSON(Javascript Object Notation) structure- this is a text based open standard design for human readable data
2. Downloads
3. Bookmarks
4. Web data
5. Keyword search terms
6. Keywords
7. URL database
8. History index
9. Current and last sessions
10. Top sites database
11. Media cache

Chrome offers Incognito mode for users to browse the internet in a private setting. Incognito mode does not save or record any browsing or download histories, ad all created cookies will be removed when exiting a session completely. Additionally, if users are working in Chrome OS, surfing the internet under guest browsing also does the same thing. Once the guest session is closed, all browsing information is completely erased.

**4. Safari**

The Apple Safari web browser is mainly used on Mac/iOS operating system but is also available for Windows. A list of common areas where evidences from Safari can be located are:

1. .plist(Proper List) Structure
2. Cookies(plist)
3. Bookmarks(plist)
4. History(plist)
5. WebPageIcons(plist)
6. Keychains(plist)
7. Downloads(plist)

Current version of Apple’s Safari is 6.0 which is not updated in Windows. In Safari, private browsing ensures that web pages are not added to the history list, cookie changes are discarded, searched are not added to search fields, and websites cannot modify information stored on computer.

**5. Microsoft Edge**

The Microsoft Edge browser is fast, simple and safe way to get around on the web. Almost millions of people chose Opera to surf the web on their computers. We can find evidences in following sources in Opera Browser

1. cookies4.dat(binary)- Stored cookies
2. contacts.adr(text)-Stored contacts used for e-mail and chat
3. global.dat(text)- Stored global history
4. vlink.dat(binary)- Stored visited links

**2.4 Backup and Recovery**

**2.4.1 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.

**2.4.2 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.

**Possible evidences from these could include:**

1. Surfing History could include typed URLs, redirects and also the number of visits to a particular site.
2. Bookmarks would mainly contain shortcuts or bookmarks created to specific websites by user.
3. For downloads, an investigator would mainly need to check for downloaded file in the default locations which can also include user defined locations or sometimes files that are downloaded to default locations and are then moved or copied to user defined locations.
4. Cookies are the files that contain a wealth of information about the user, It may contain information like usernames, passwords and web session information.
5. Cache is a temporary area on the disk which is used to store most recently visited web sites.

A suspect or an attacker can use different web browsers for committing the crime or an attack. So an investigator must know the different methods for recovery of deleted information from various web browsers. Following would give recovery methods for different browsers from different sources as mentioned above:

**Internet Explorer-** From Internet Explorer, an investigator can extract information from various sources like cache, history, cookies and download. Recovery method for cache would be to recover temporary internet files. For recovering deleted information from history, investigator must do recovery of weekly or daily index.dat files through craving method. Recovery of cookies files would give the information in cookies Internet Explorer does not have a download information.

**Mozilla Firefox-** Mozilla firefox can give information only through history for which an investigator must do recovery of session files through craving method.

**Opera Mini-** Just like Mozilla firefox, opera mini would contain information through history only for which investigator must recover session files.

**Google Chrome-** Google Chrome would contain information from cache and history.

From cache, an investigator can retrieve cache files which are temporary internet files while from history he/she can recover monthly history files for the purpose of investigation.

**Safari-** From Safari web browser, recovery from history and cookies files is possible for which an investigator must recover session files and cookies files respectively.

**2.4.3 Locations of Internet Browser Artifacts**

Below is a list of major browsers and the locations they use to store their information for the applicable operating systems.

**Internet Explorer**

Cache: C:\Users\SYSTEM\_USER\AppData\Local\Microsoft\Windows\Caches

Session:C:\Users\SYSTEM\_USER\AppData\Roaming\Mozilla\Firefox\Profiles\l7ohums2.default-1429948445160

Icon Cache: C:\Users\SYSTEM\_USER\AppData\Local\Microsoft\Windows\Explorer

Thumb Cache: C:\Users\SYSTEM\_USER\AppData\Local\Microsoft\Windows\Explorer

Layout: C:\Users\SYSTEM\_USER\AppData\Local\Microsoft\Windows\Shell

Themes: C:\Users\SYSTEM\_USER\AppData\Local\Microsoft\Windows\Themes

Notifications: C:\Users\SYSTEM\_USER\AppData\Local\Microsoft\Windows\Notifications

**Mozilla Firefox**

History:C:\Users\SYSTEM\_USER\AppData\Roaming\Mozilla\Firefox\Profiles\ l7ohums2.default-1429948445160

Bookmarks:C:\Users\SYSTEM\_USER\AppData\Roaming\Mozilla\Firefox\Profiles\l7ohums2.default-1429948445160\bookmarkbackups

Plugins:C:\Users\SYSTEM\_USER\AppData\Roaming\Mozilla\Firefox\Profiles\l7ohums2.default-1429948445160\searchplugins

Sessions:C:\Users\SYSTEM\_USER\AppData\Roaming\Mozilla\Firefox\Profiles\l7ohums2.default-1429948445160\sessionstore-backups

Cookies:C:\Users\SYSTEM\_USER\AppData\Roaming\Mozilla\Firefox\Profiles\l7ohums2.default-1429948445160

**Google Chrome**

History: C:\Users\SYSTEM\_USER\AppData\Local\Google\Chrome\User Data\Default\

Cookie: C:\Users\SYSTEM\_USER\AppData\Local\Google\Chrome\User Data\Default

Visited Links: C:\Users\SYSTEM\_USER\AppData\Local\Google\Chrome\User Data\Default

Login Data: C:\Users\SYSTEM\_USER\AppData\Local\Google\Chrome\User Data\Default

Session: C:\Users\SYSTEM\_USER\AppData\Local\Google\Chrome\User Data\Default\Session Storage

File System: C:\Users\SYSTEM\_USER\AppData\Local\Google\Chrome\User Data\Default\File System\Origins

Extensions:C:\Users\SYSTEM\_USER\AppData\Local\Google\Chrome\User Data\Default\Extensions

**Safari**

Windows 10: C:\Users\SYSTEM\_USER\AppData\Roaming\Apple Computer\Safari

Cookies: C:\Users\SYSTEM\_USER\AppData\Roaming\Apple Computer\Safari\Cookies

Bookmarks: C:\Users\SYSTEM\_USER\AppData\Roaming\Apple Computer\Safari

History: C:\Users\SYSTEM\_USER\AppData\Roaming\Apple Computer\Safari

Session: C:\Users\SYSTEM\_USER\AppData\Roaming\Apple Computer\Safari

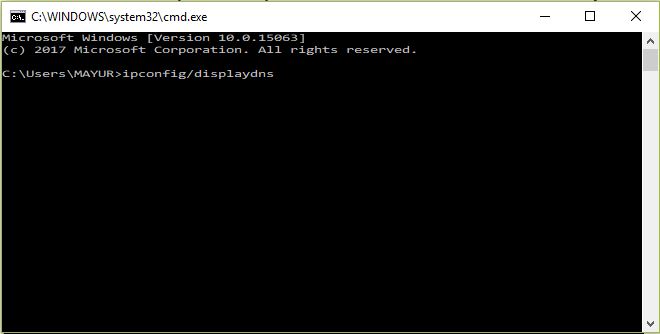
Top Sites: C:\Users\SYSTEM\_USER\AppData\Roaming\Apple Computer\Safari

# 2.4.4 How to Recover Browser History

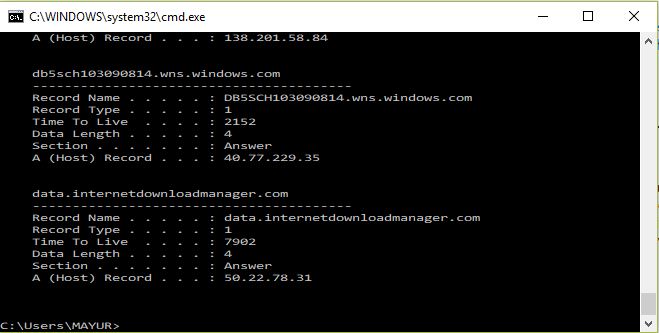
We offer you three major methods to **recover browser/internet history** files: use DNS Cache to find deleted browsing history, use data recovery software to recover lost browsing history files or to recover deleted history by using Google history. And all these three methods can be applied for browsing internet history recovery on all browsers such as Chrome, Firefox, IE Edge etc. Let's see how to recover lost or deleted browser internet history now.

**1) Method 1: Use DNS Cache to find and view deleted browsing history**

DNS, which is known as Domain Name System, can work as a fast method to restore searches or history for you. But when computer is restarted, it will not be able to help you find browsing history then. DNS cache can only work when almost everything is connected to the internet. Therefore, if you need to restore deleted browsing history for an app or video game, please do not shut down or restart the computer. You may still have a chance to view the deleted internet history: Open **Command Prompt**, type **ipcongif/displaydns** and click **Enter**.



Screenshot 2.1DNS Cache to view deleted browsing history



Screenshot 2.2 Deleted browsing history

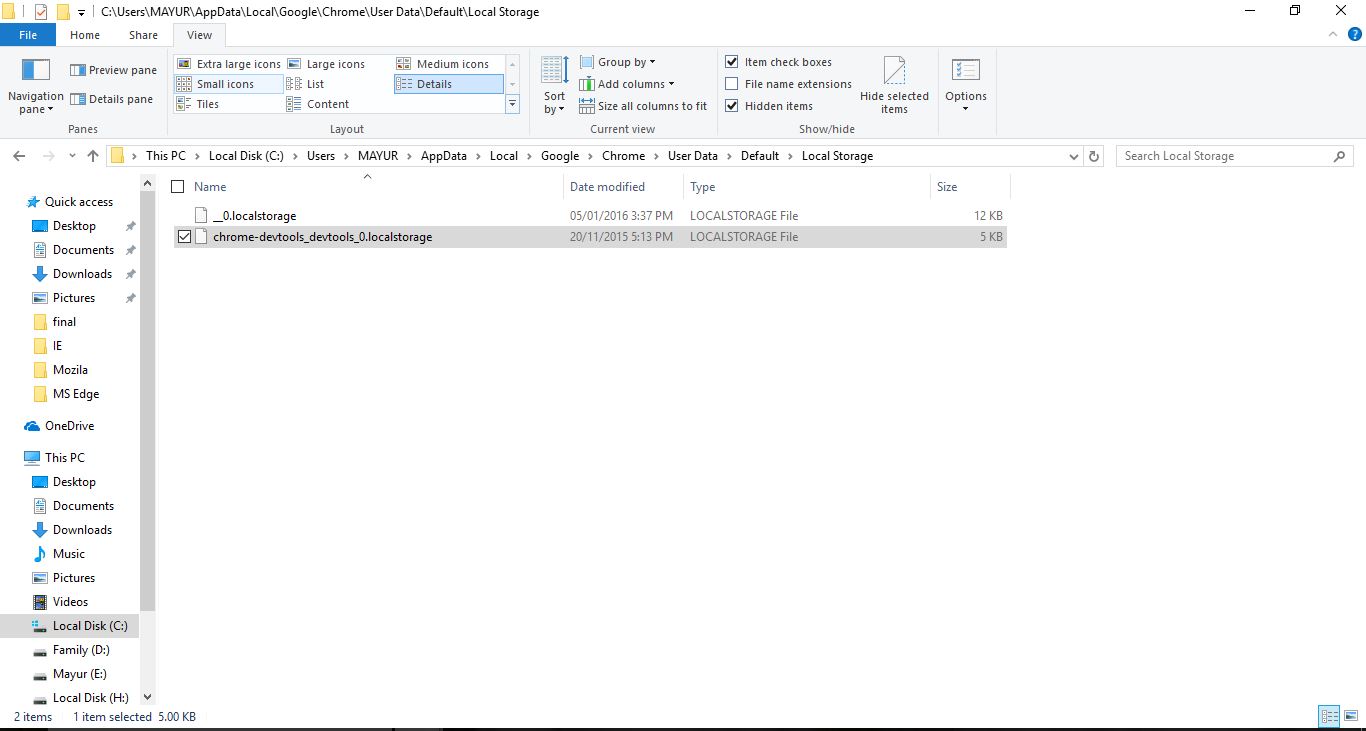
While someone may be able to delete their browsing history, the DNS Cache stores this information. It should be noted that this method may be confusing because it saves history from everything connected to the internet, such as apps, and not just your browser

**2) Method 2: Use data recovery software to recover lost browsing history files**

**Type I: Using User File System**

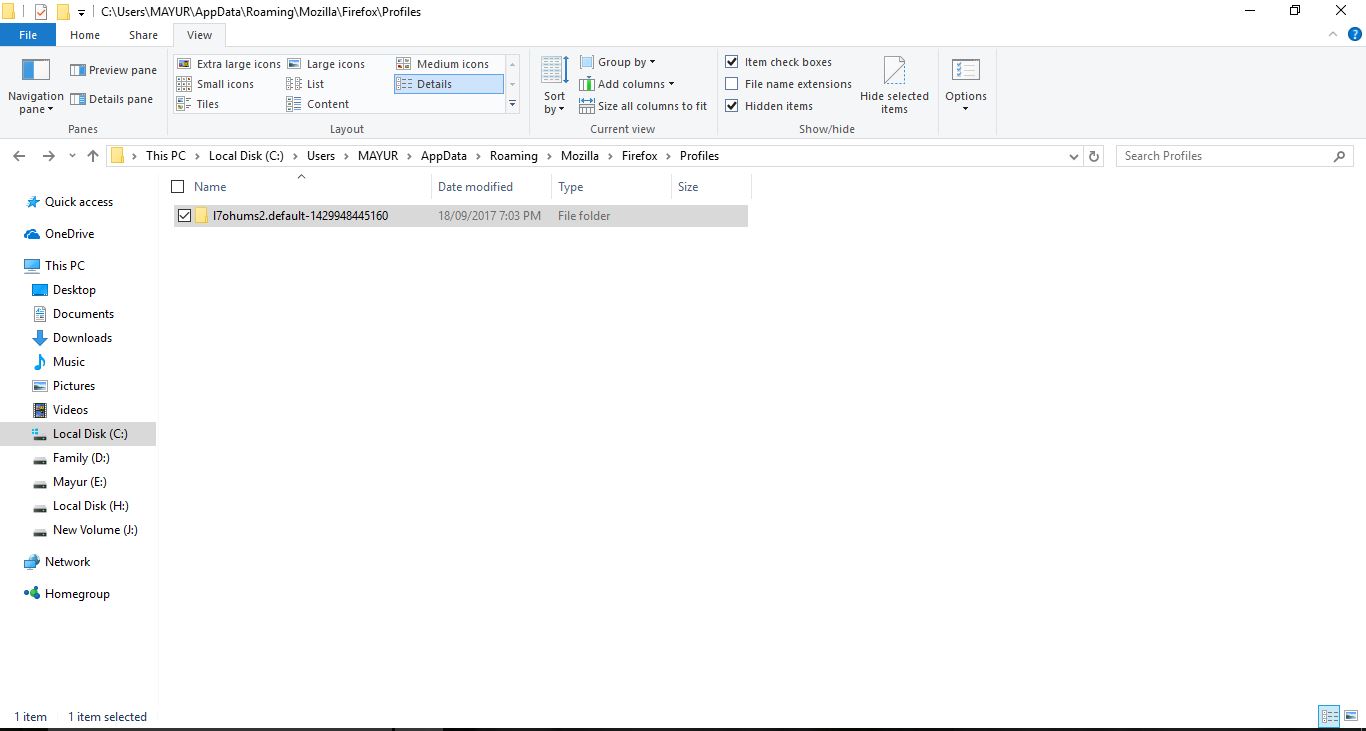
If you don’t know where to find your saved computer browsing history, please follow next path to see whether the history files are deleted or not now:

**Google Chrome**: C:\Users\SYSTEM\_USER\AppData\Local\Google\Chrome\User Data\Default\local storage

**

Screenshot 2.3 Chrome History in User File System

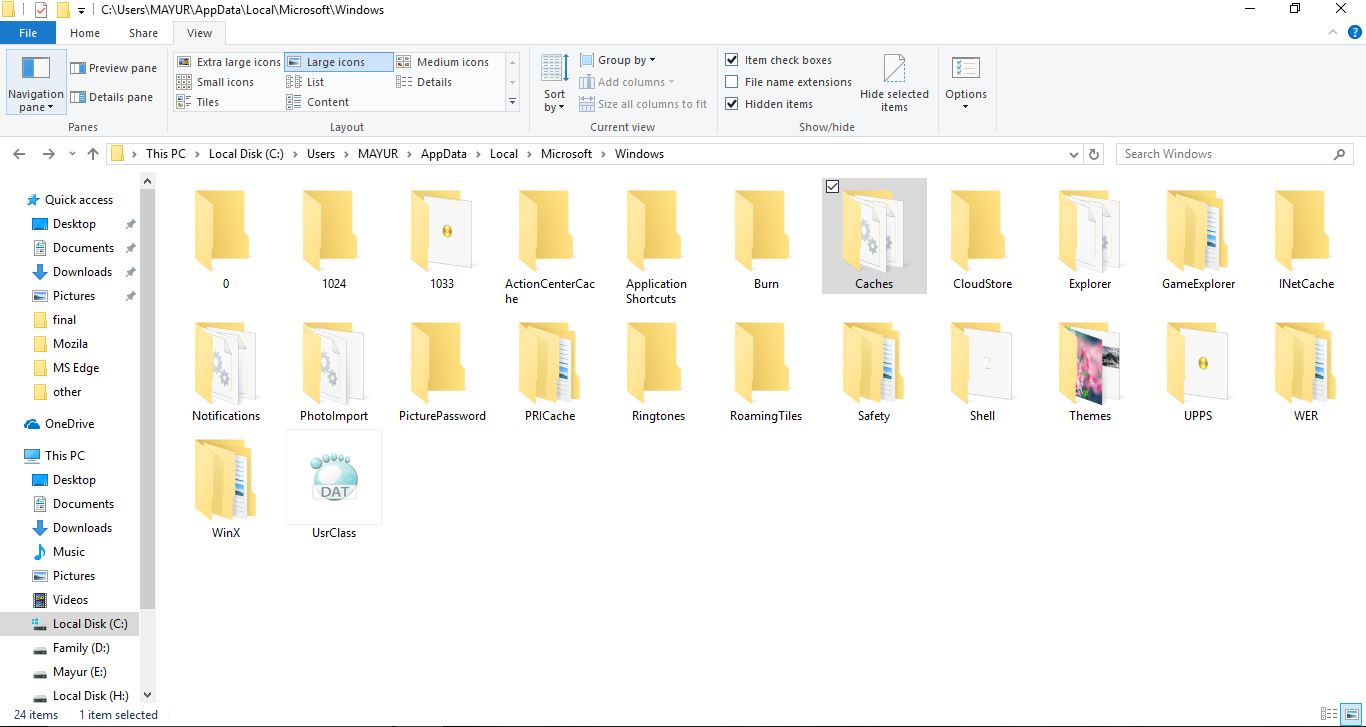
**Mozilla Firefox**: C:\Users\ SYSTEM\_USER\AppData\Roaming\Mozilla\Firefox\Profiles\

**

Screenshot 2.4 Firefox History in User File System

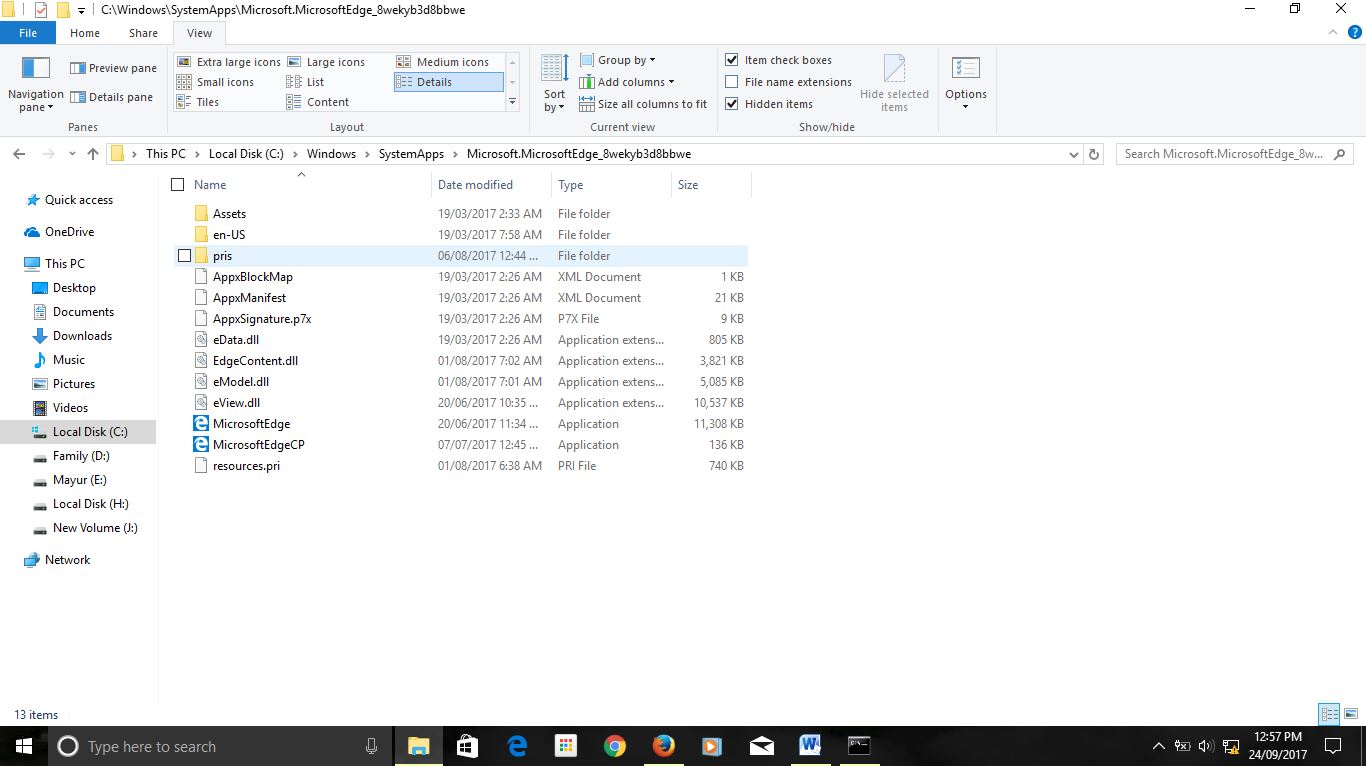
**Internet Explorer**: C:\Users\SYSTEM\_USER\AppData\Local\Microsoft\Windows\History

If you like to save all browser history in your computer like other files, when you deleted the browsing history from the browser, you’ll delete the history files from your computer. You still have a chance to restore the deleted browsing history files by using professional [data recovery software.](https://www.easeus.com/data-recovery-software/)

Screenshot 2.5 Internet Explorer History in User File System

**Microsoft Edge:** **C:\Windows\SystemApps\Microsoft.MicrosoftEdge\_8wekyb3d8bbwe**

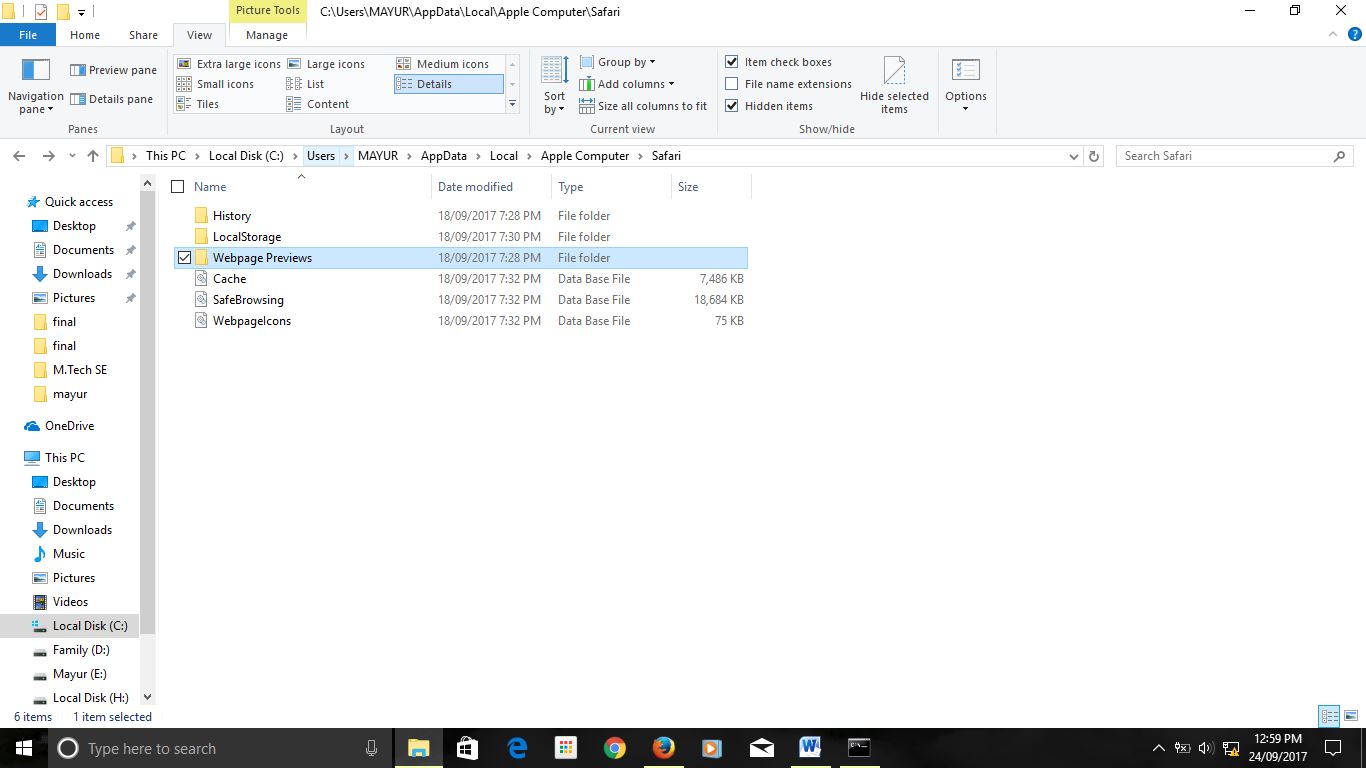
Microsoft Edge files location in user file system.

****

Screenshot 2.6 Microsoft Edge History in User File System

**Apple Safari: C:\Users\SYSTEM\_USER\AppData\Local\Apple Computer\Safari**

Apple Safari files location in user file system.

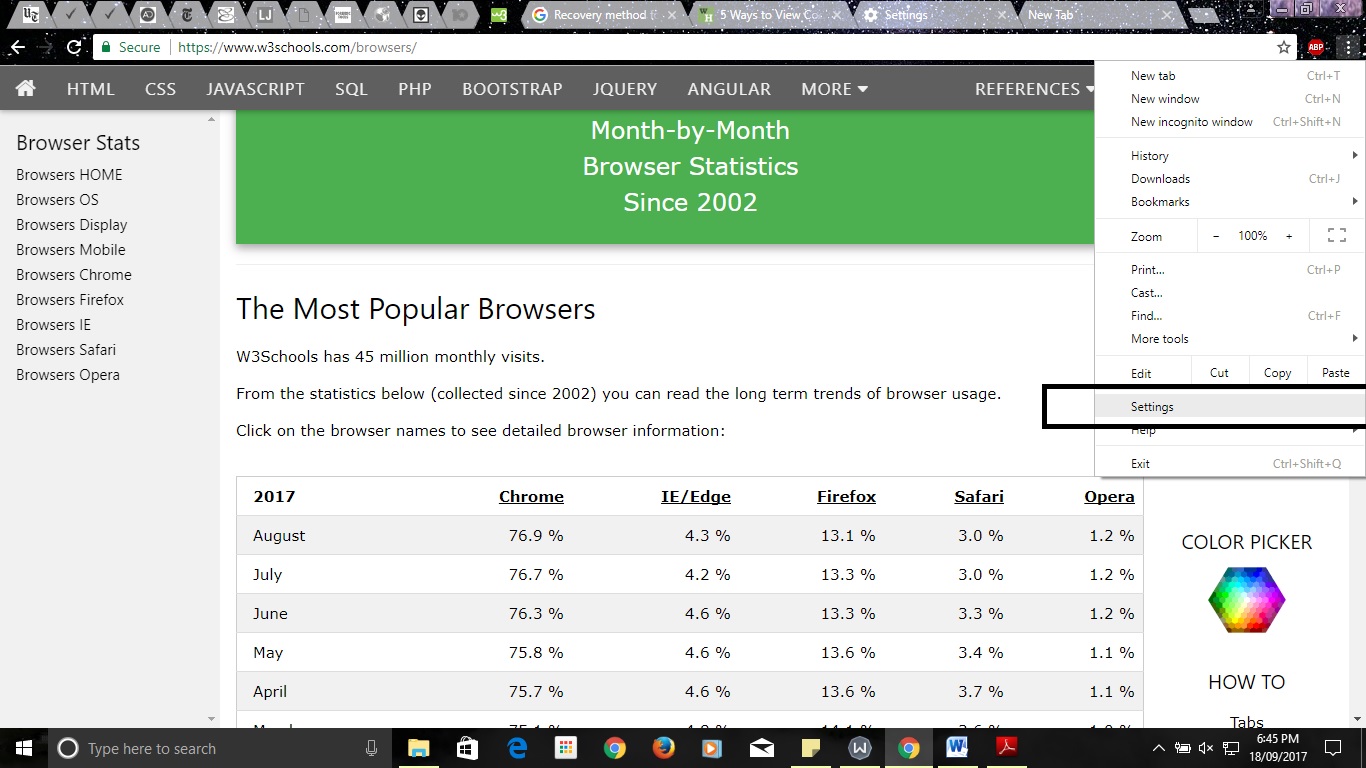
****

Screenshot 2.7 Safari History in User File System

**Type II- Using Browser Cookies**

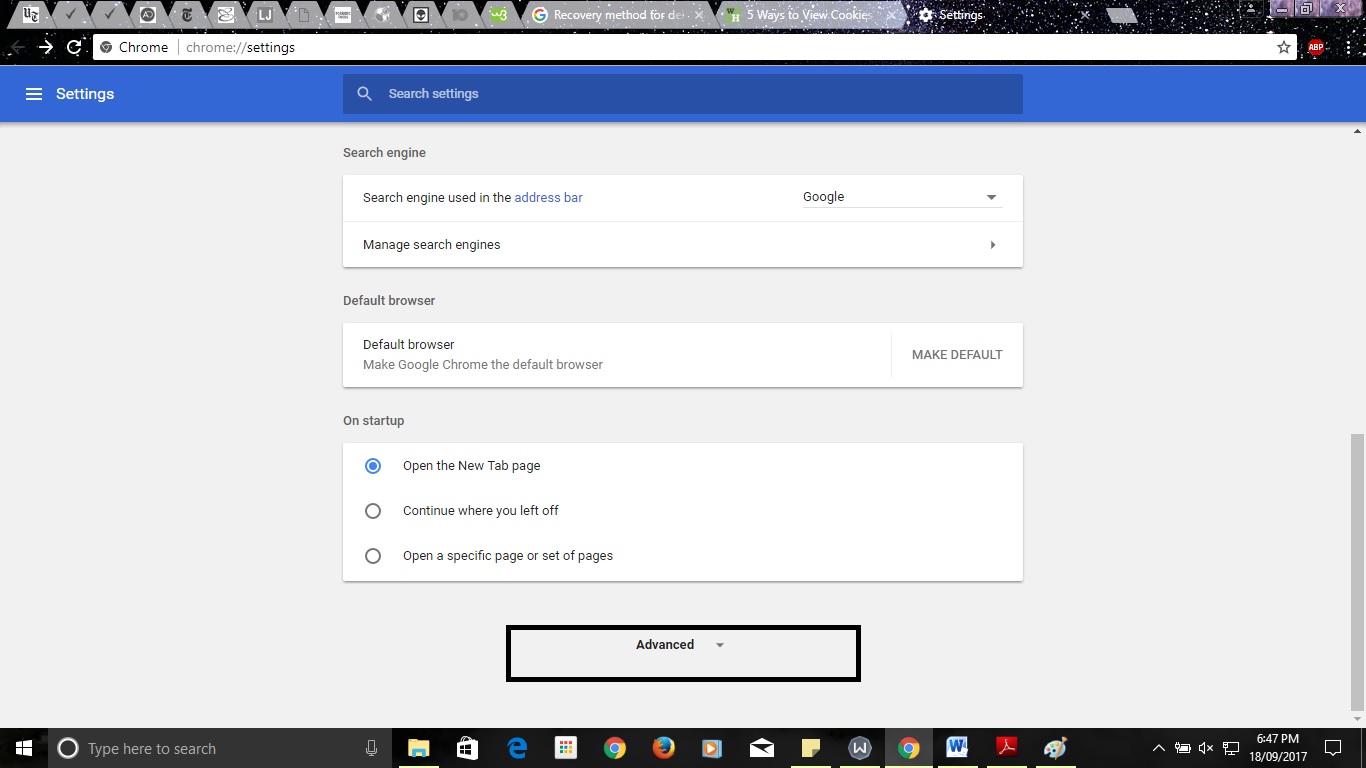
**Google Chrome:**

Step 1) Open Google Chrome. Click Settings This icon is in the top-right corner of the Chrome window.

****

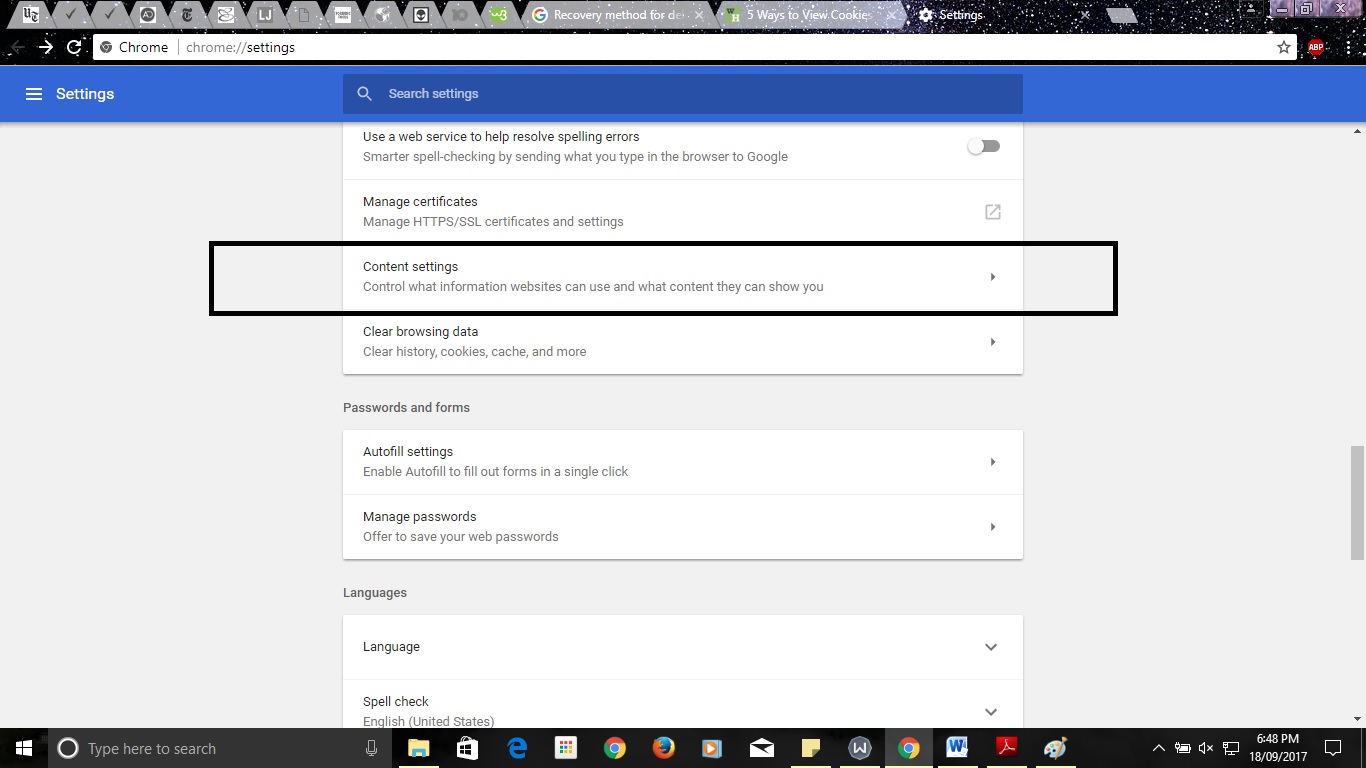
Screenshot 2.8.1 Chrome History using Cookies Step 1

STEP 2) Click Advanced. It's toward the bottom of the drop-down menu.



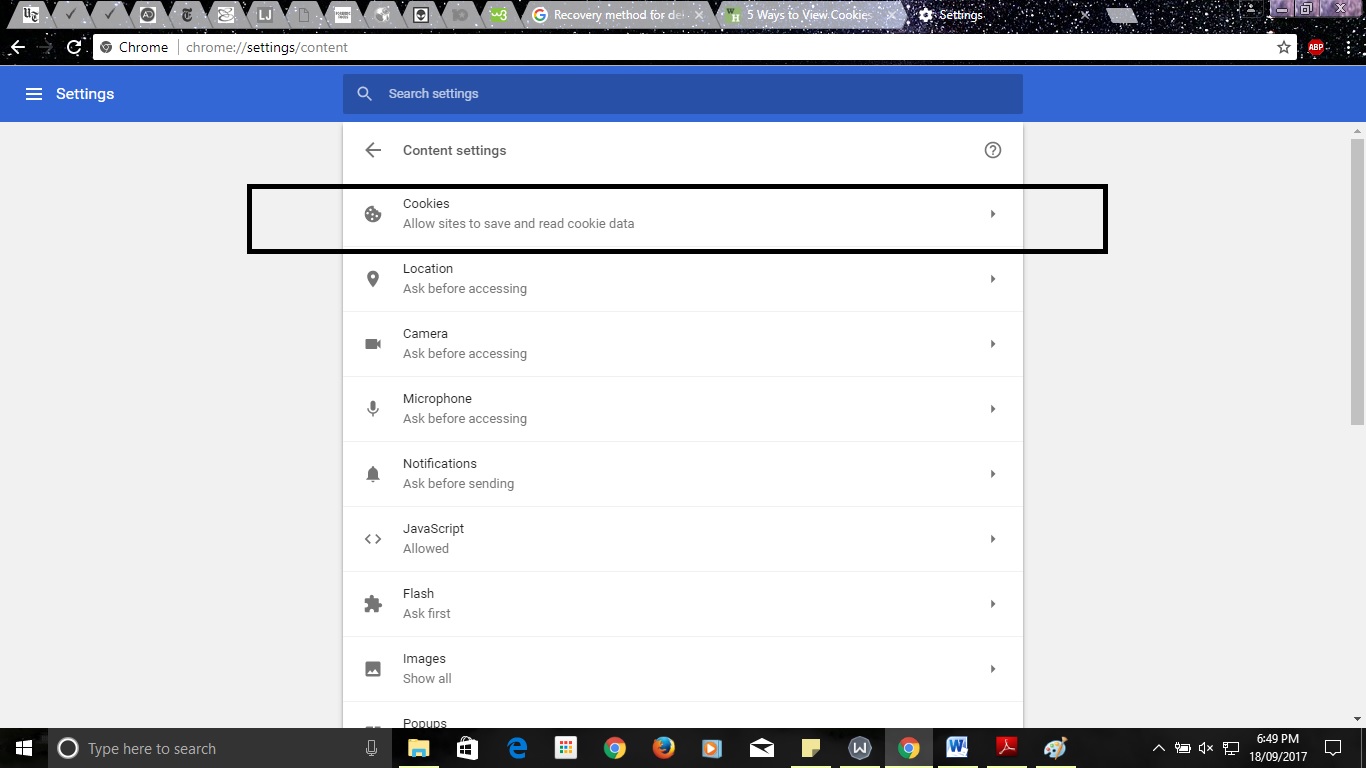
Screenshot 2.8.2 Chrome History using Cookies Step 2

STEP 3) Click Content settings. It's toward the bottom of the "Privacy" group of options.



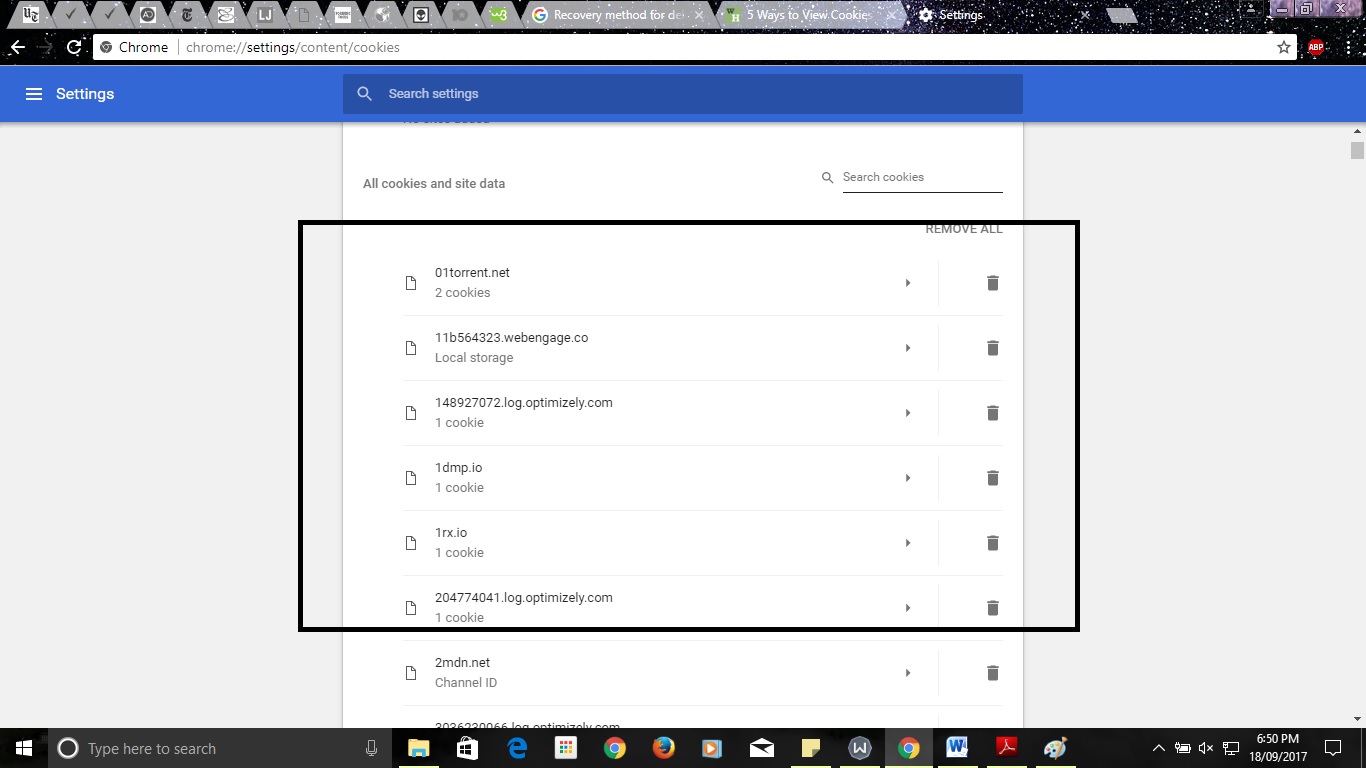
Screenshot 2.8.3 Chrome History using Cookies Step 3

STEP 4) Click Cookies. This option is at the top of the page. Doing so will bring up a list of your Chrome browser's cookies and other temporary files.

****

Screenshot 2.8.4 Chrome History using Cookies Step 4

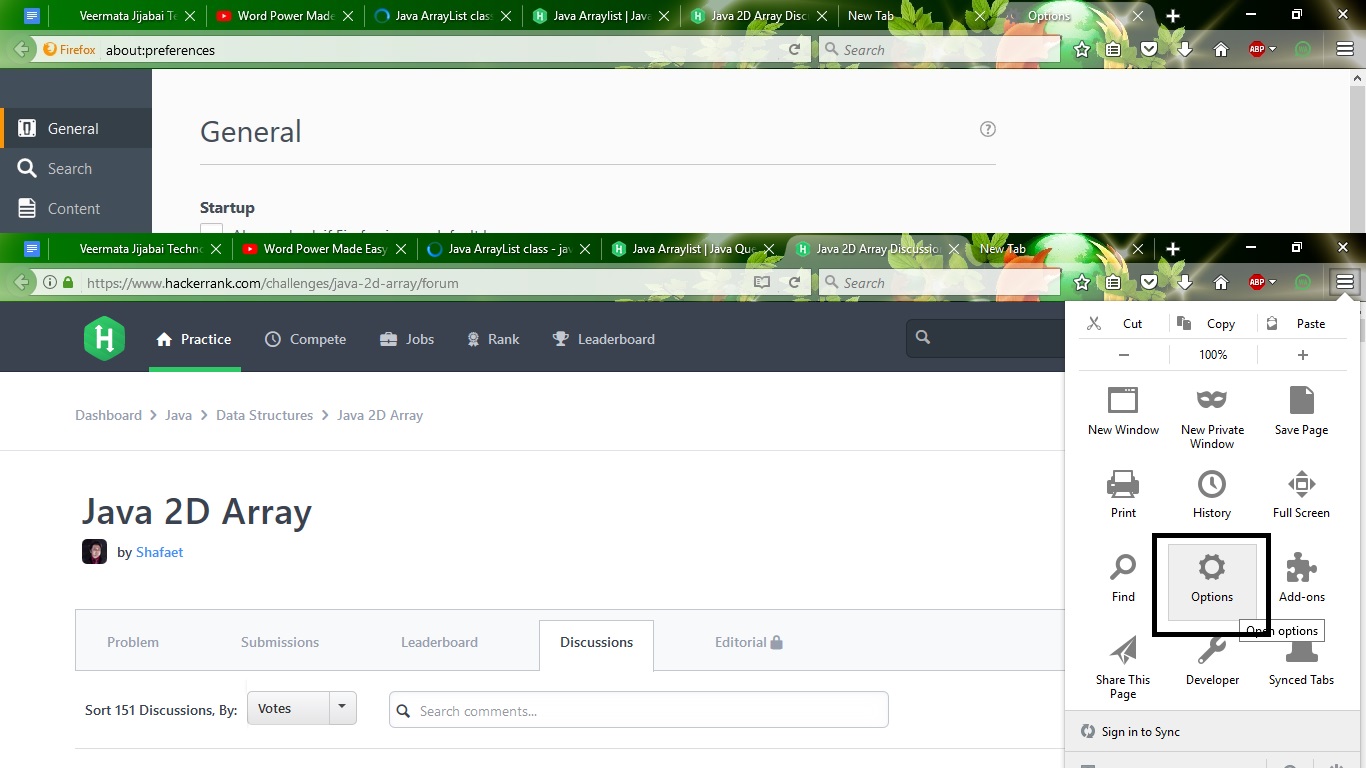
STEP 5) Review your browser's cookies. They're beneath the "All cookies and site data" heading near the bottom of the page. Any item with "[number] cookie(s)" next to it is a cookie. You can click an item to view a list of the cookies' names, and you can click an individual cookie within an item's list to view its attributes.

****

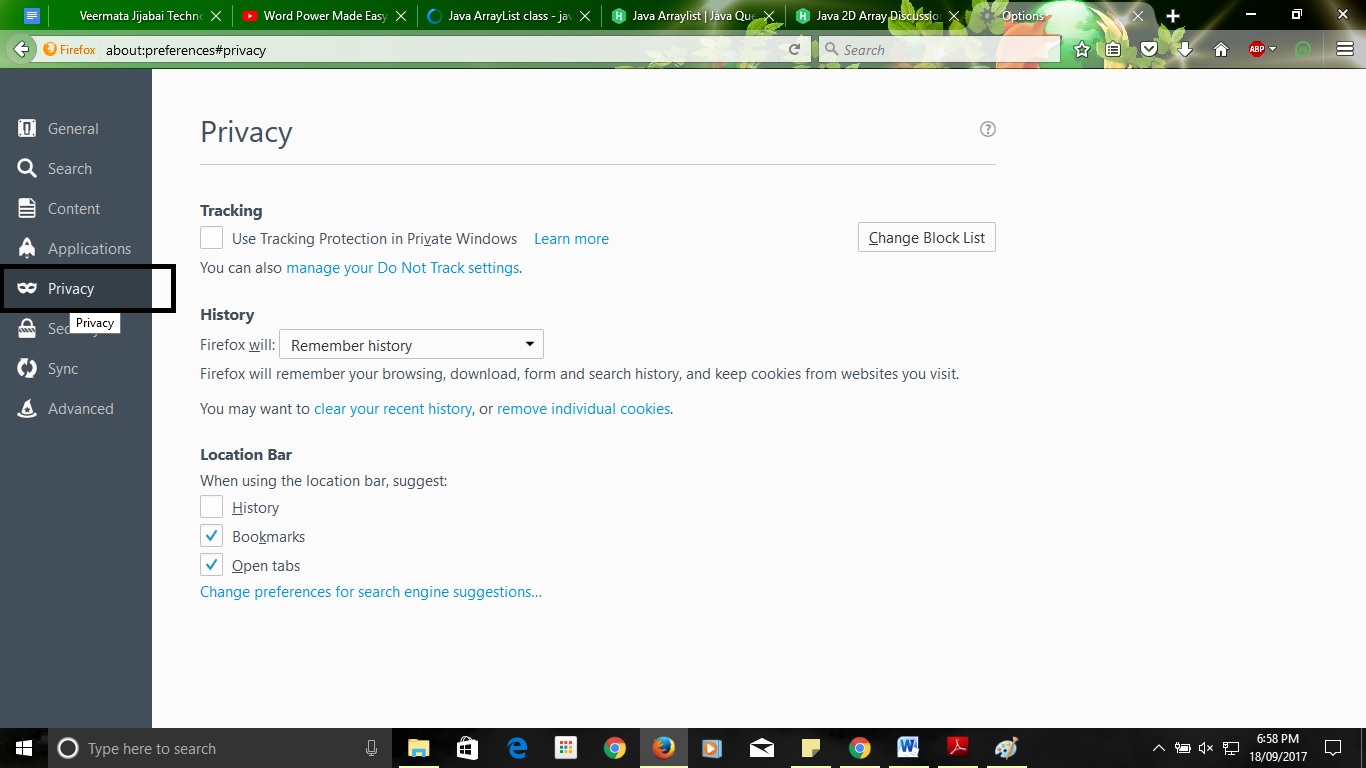
Screenshot 2.8.5 Chrome History using Cookies Step 5

**Mozilla Firefox:**

Step 1) Click Open Menu. This icon is in the top-right corner of the browser window. Click Option. It's a gear-shaped icon in the drop-down menu.

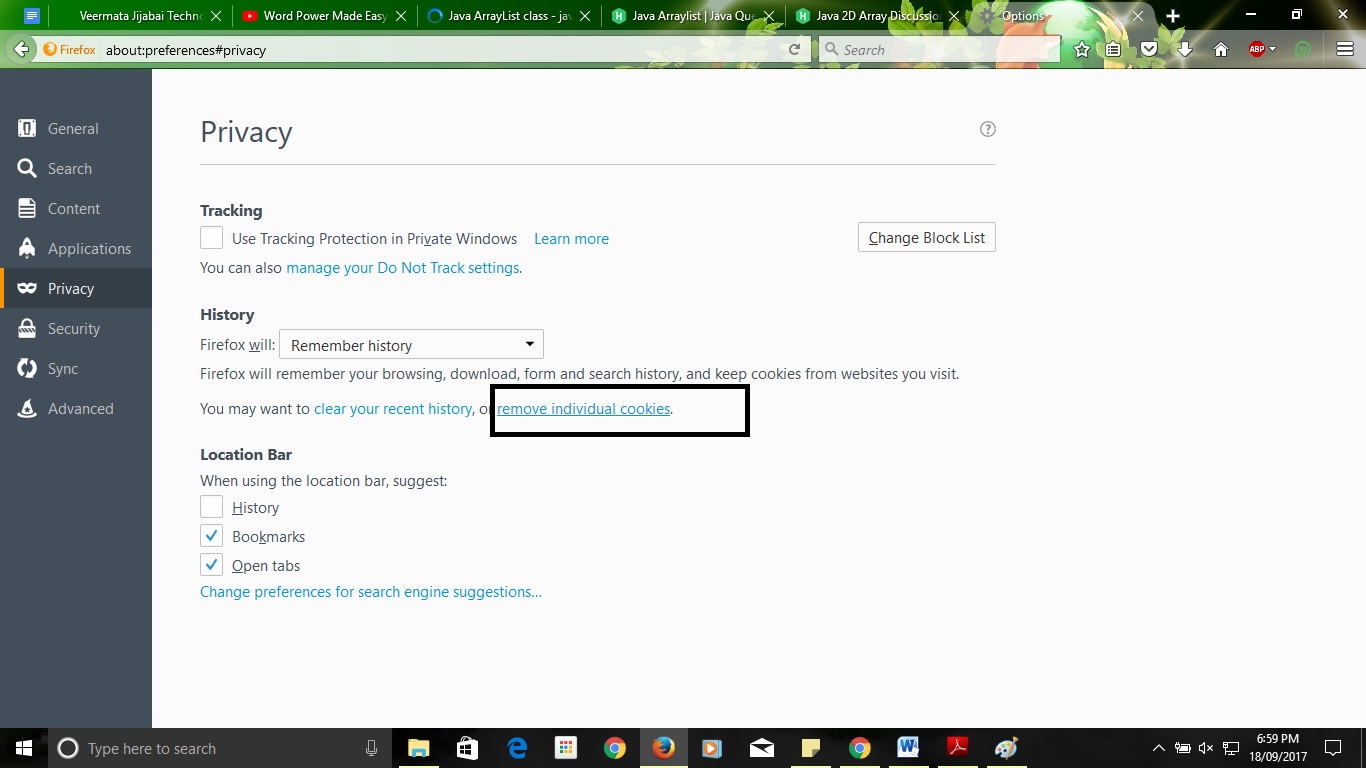
Screenshot 2.9.1 Firefox History using Cookies Step 1

Step 2) Click Privacy. This tab is on the left side of the page.



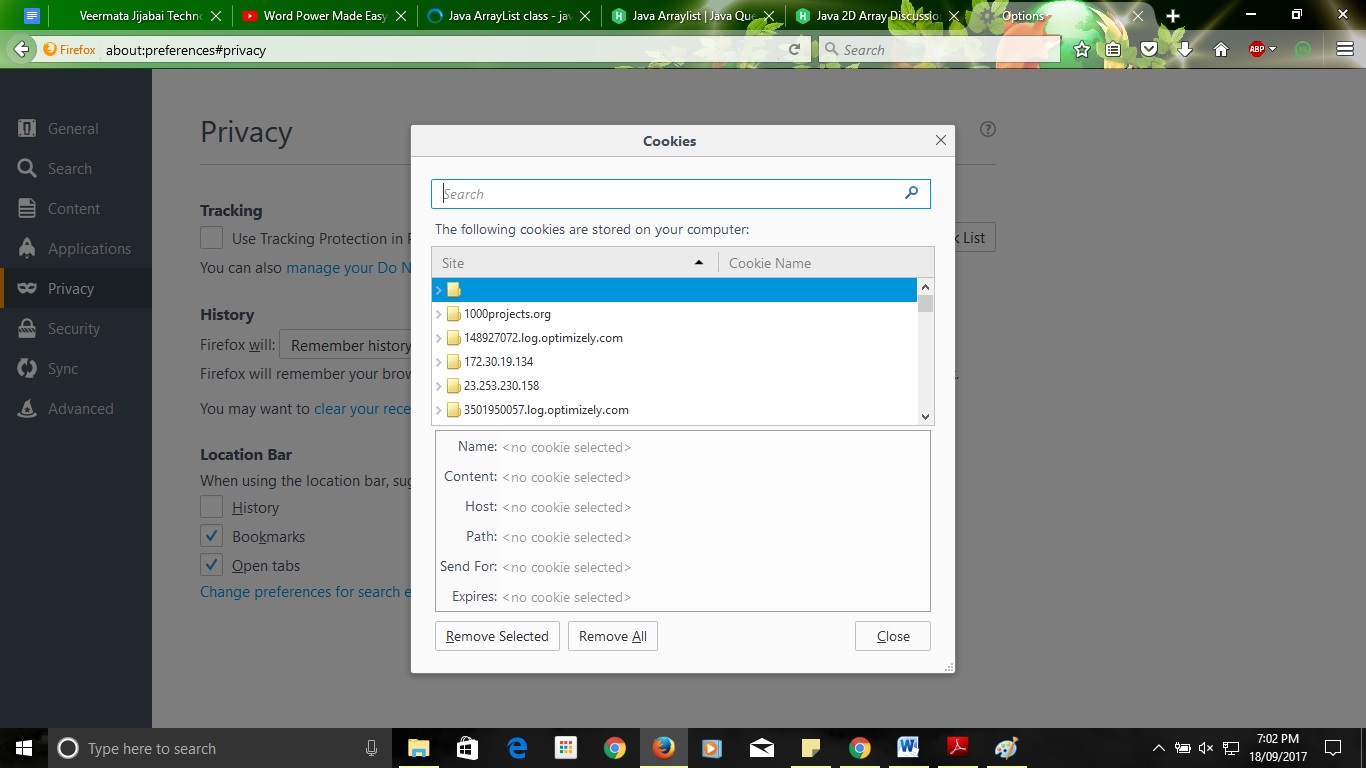
Screenshot 2.9.2 Firefox History using Cookies Step 2

Step 3) Click remove individual cookies. It's a link in the middle of the page. Doing so will bring up a list of your Firefox browser's cookies. If you're using custom settings for your Firefox history, you won't have the remove individual cookies option; instead, click the Show Cookies button on the right side of the page.



Screenshot 2.9.3 Firefox History using Cookies Step 3

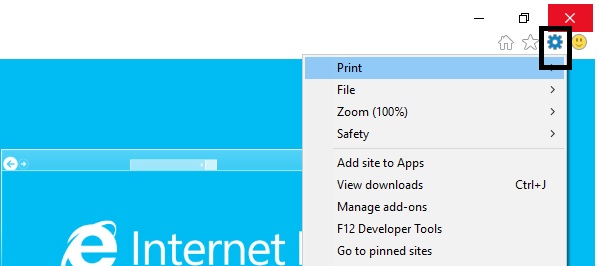
Step 4) Review your browser's cookies. Firefox cookies are organized by site. Double-clicking a site's folder will display its cookies, and clicking a cookie will display its specific attributes.



Screenshot 2.9.4 Firefox History using Cookies Step 4

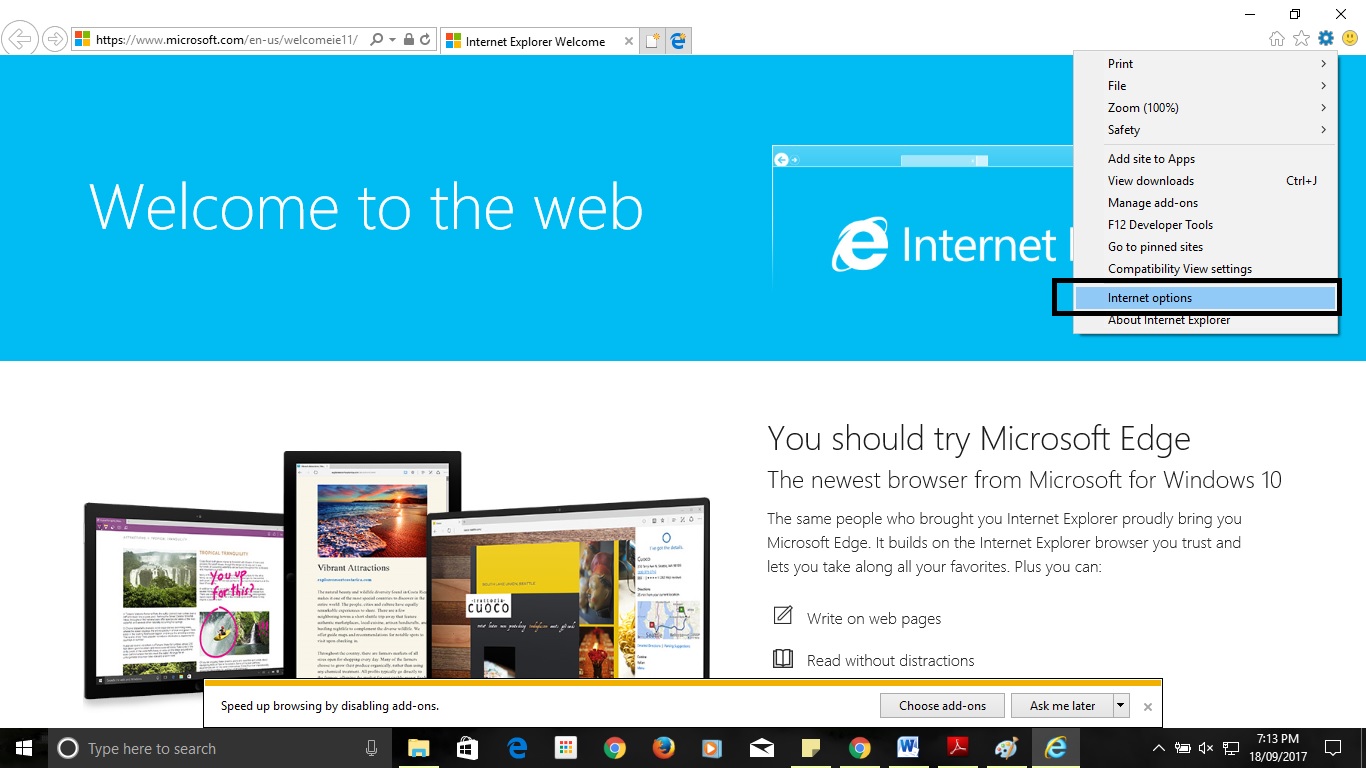
**Internet Explorer:**

Step 1)Open Internet Explorer. It's a light-blue "e" icon with a yellow stripe. Click Settings. It's in the top-right corner of the Internet Explorer window.



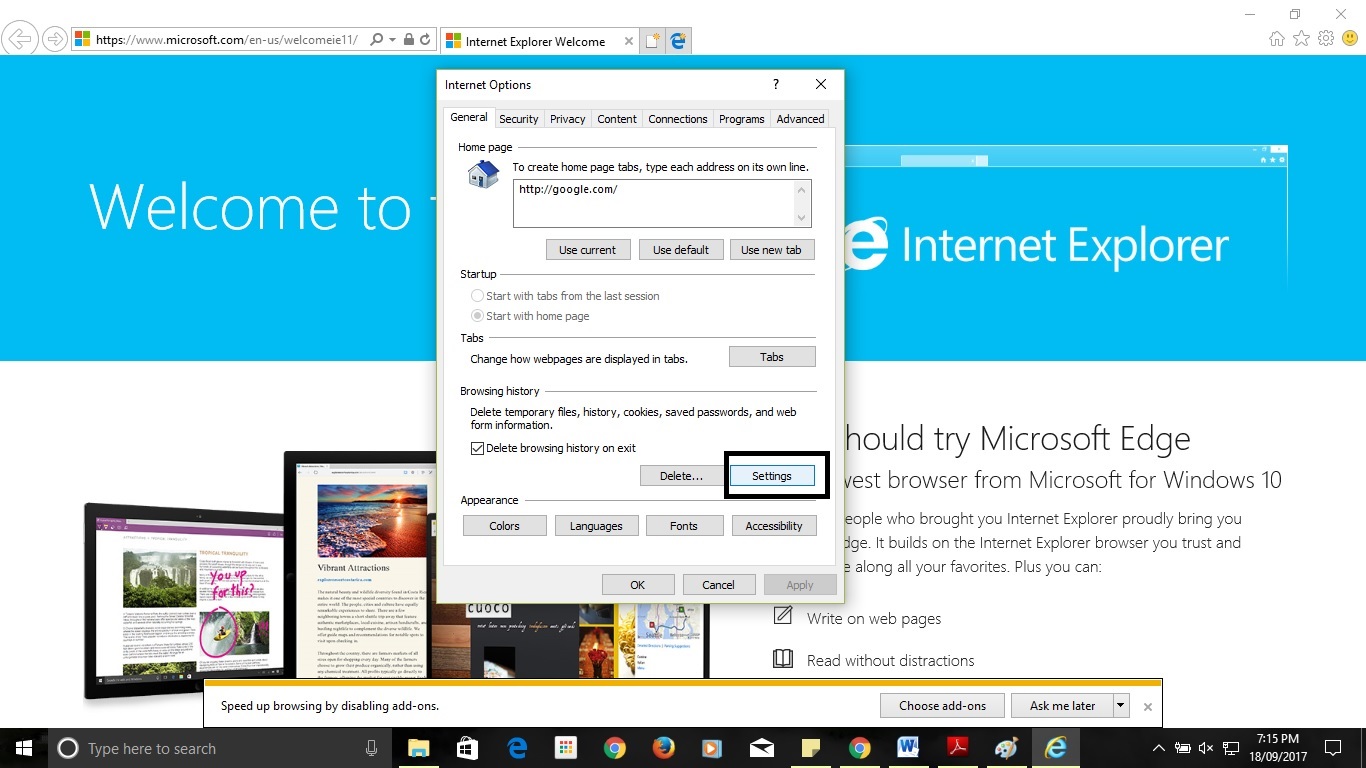
Screenshot 2.10.1 IE History using Cookies Step 1

Step 2) Click Internet Options This option is near the bottom of the screen.



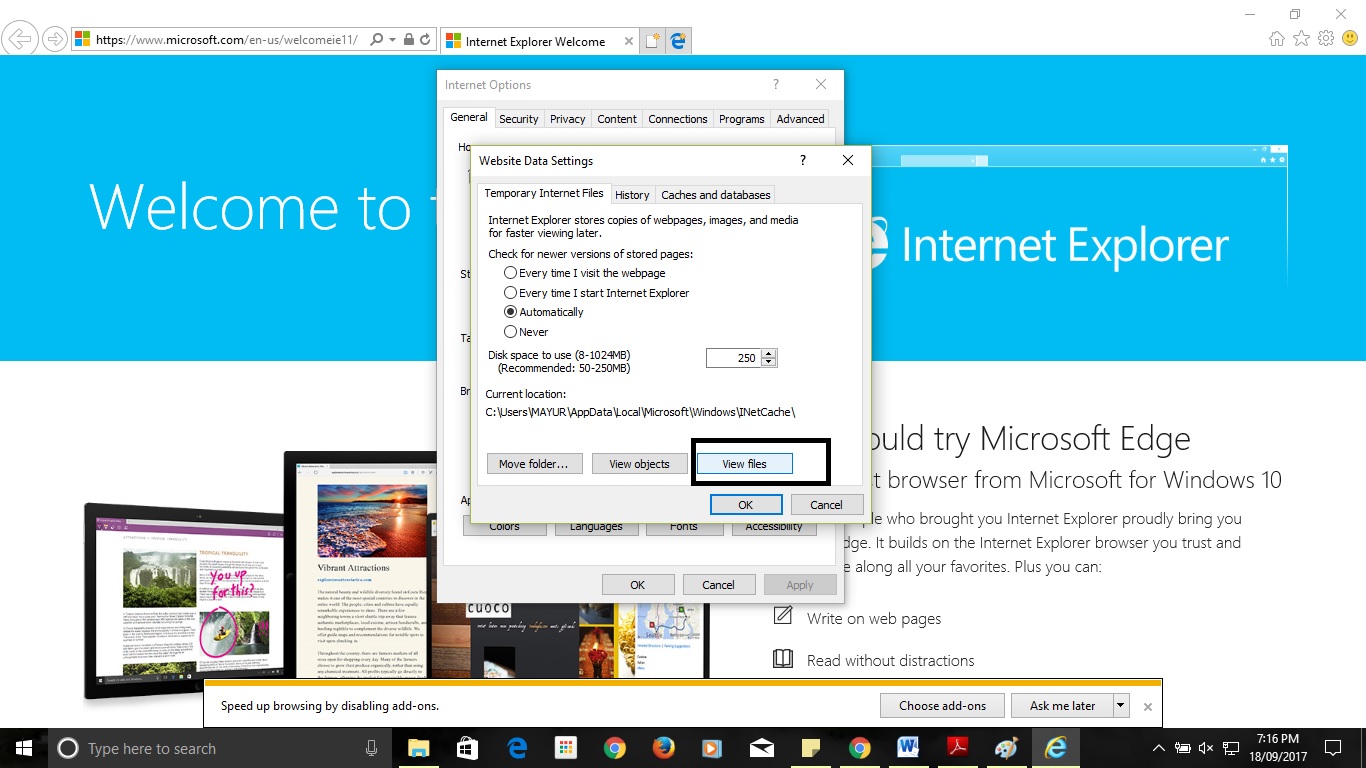
Screenshot 2.10.2 IE History using Cookies Step 2

Step 3) Click Settings. It's in the lower-right side of the "Browsing history" section. If you don't see Settings, first click the General tab at the top of the Internet Options window.



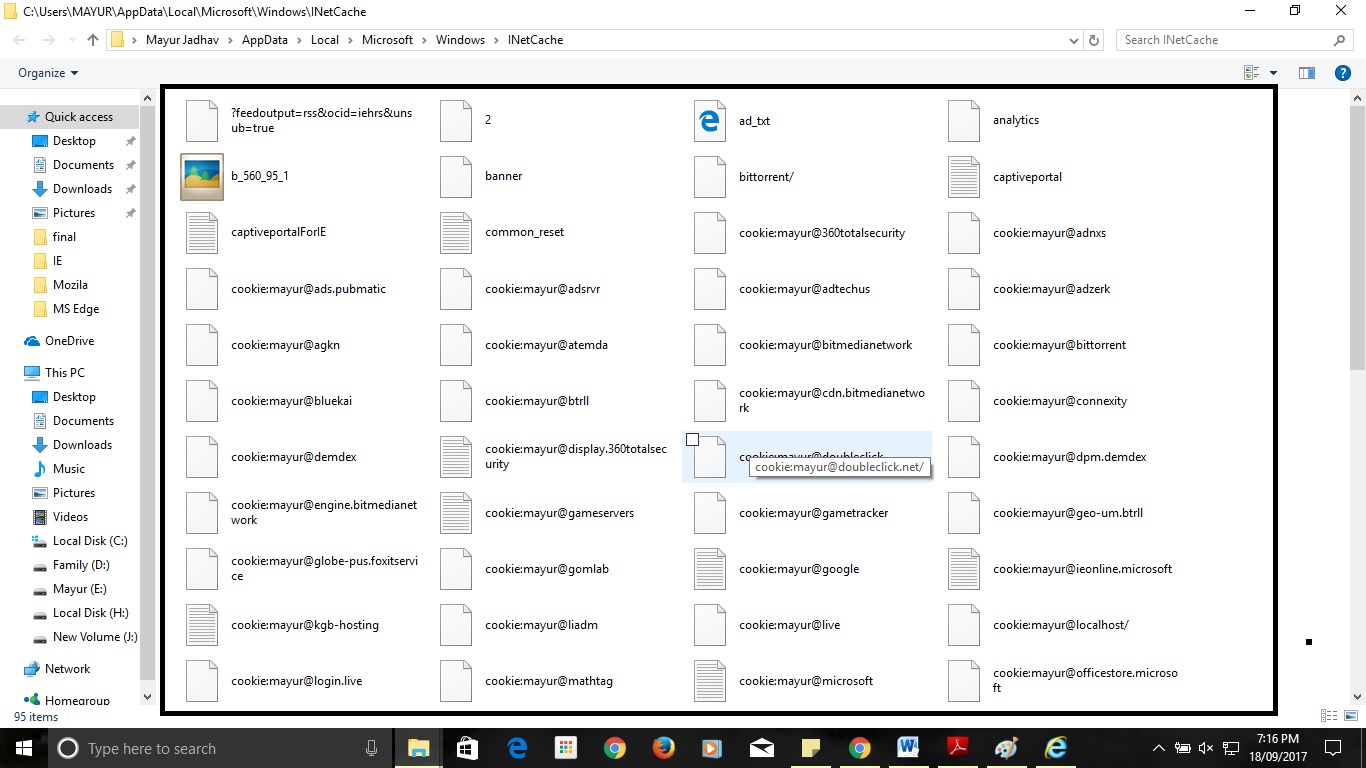
Screenshot 2.10.3 IE History using Cookies Step 3

Step 4)Click View Files. You'll see this option near the bottom of the Settings pop-up window.



Screenshot 2.10.4 IE History using Cookies Step 4

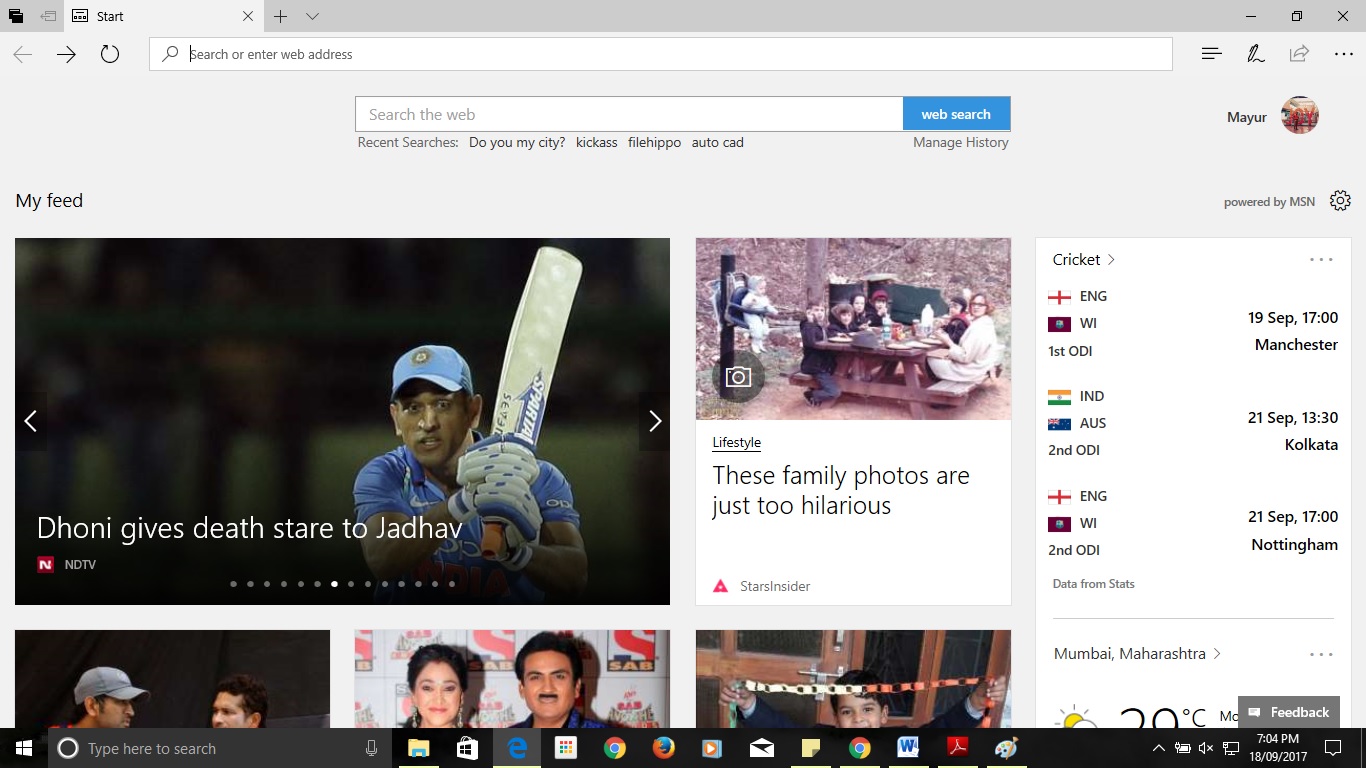
Step 5) Review Internet Explorer's cookies. The files in this folder are all temporary files from browsing, but any file with "cookie:[your username]" in its name is a cookie. Unlike most browsers, you cannot view an Internet Explorer cookie's specific attributes.



Screenshot 2.10.5 IE History using Cookies Step 5

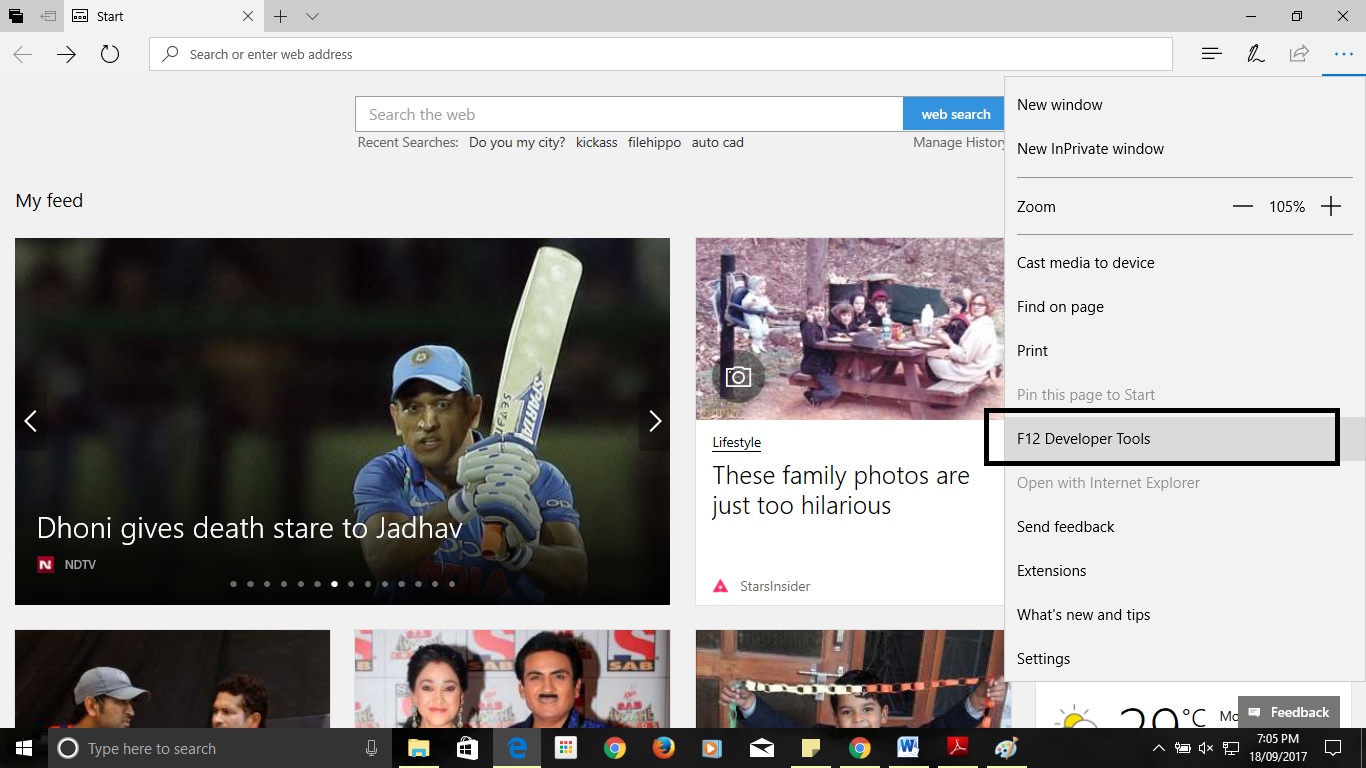
**Microsoft Edge**

Step 1)Open Microsoft Edge. This app is dark-blue with a white "e" on it. Navigate to a site whose cookies you wish to view. Since Edge doesn't store your cookies in a specific Settings folder, you'll need to visit the site to which the cookies relate.



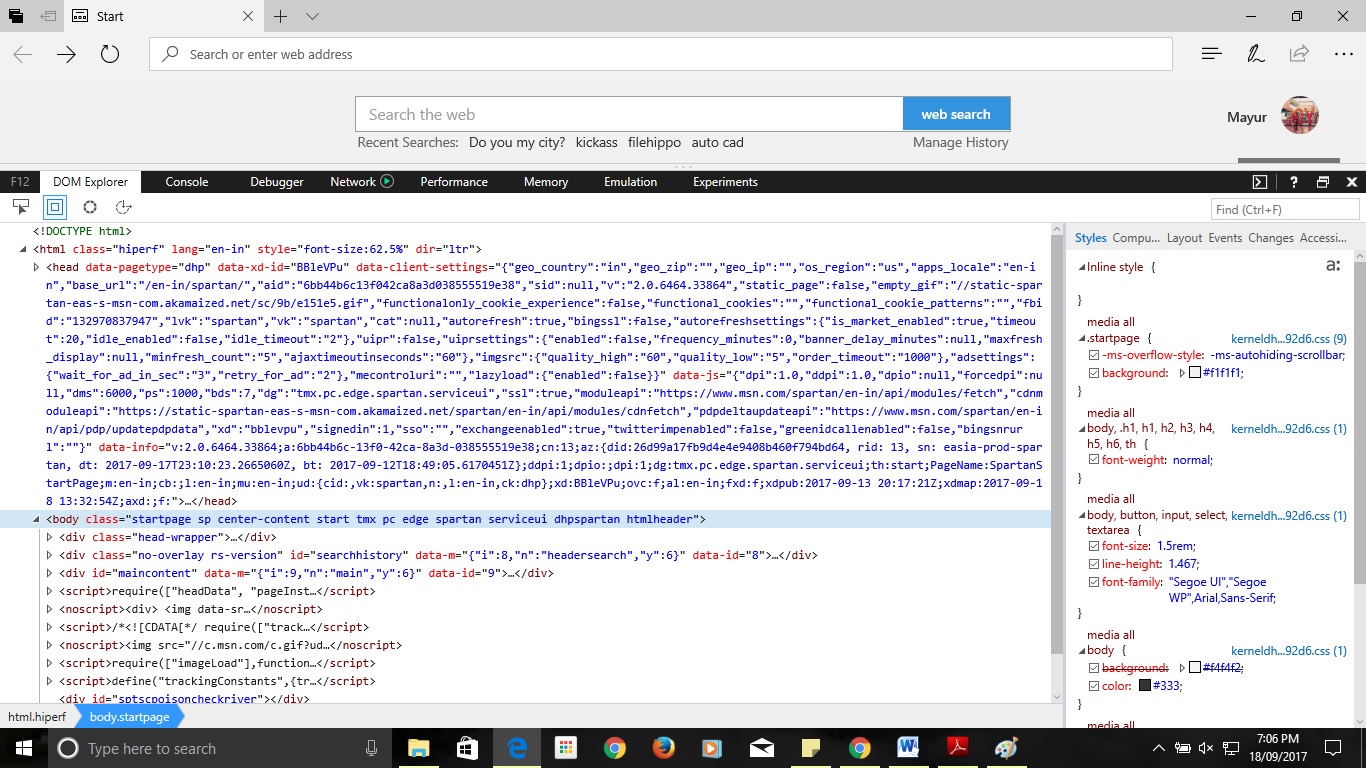
Screenshot 2.11.1 MS Edge History using Cookies Step 1

Step 2) Click Open Menu. It's in the upper-right side of the Edge window. This option is near the middle of the drop-down menu. Clicking this option prompts a pop-up window to appear at the bottom of the Microsoft Edge window. You can also press the F12 key to open this window.

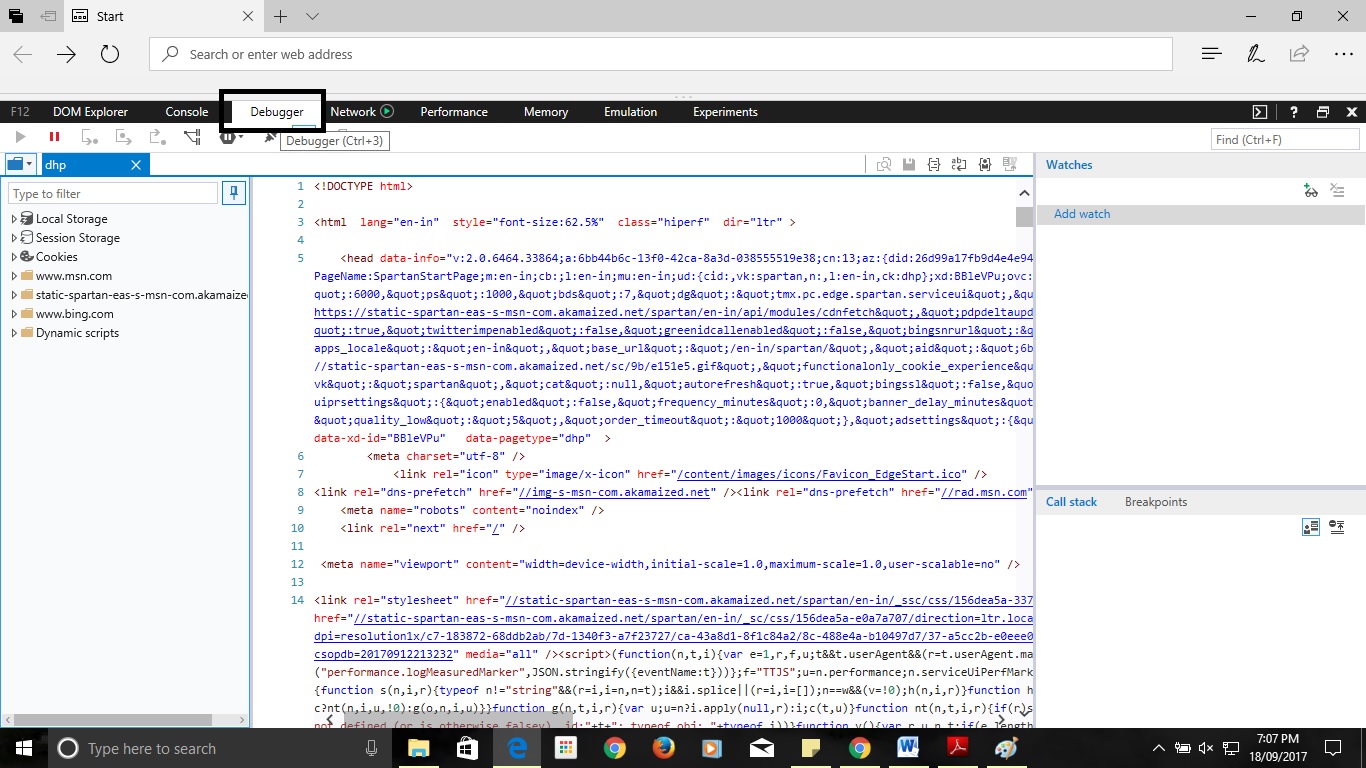


Screenshot 2.11.2 MS Edge History using Cookies Step 2

Step 3) Click the Debugger tab. It's at the top of the pop-up window that's at the bottom of the Edge window.

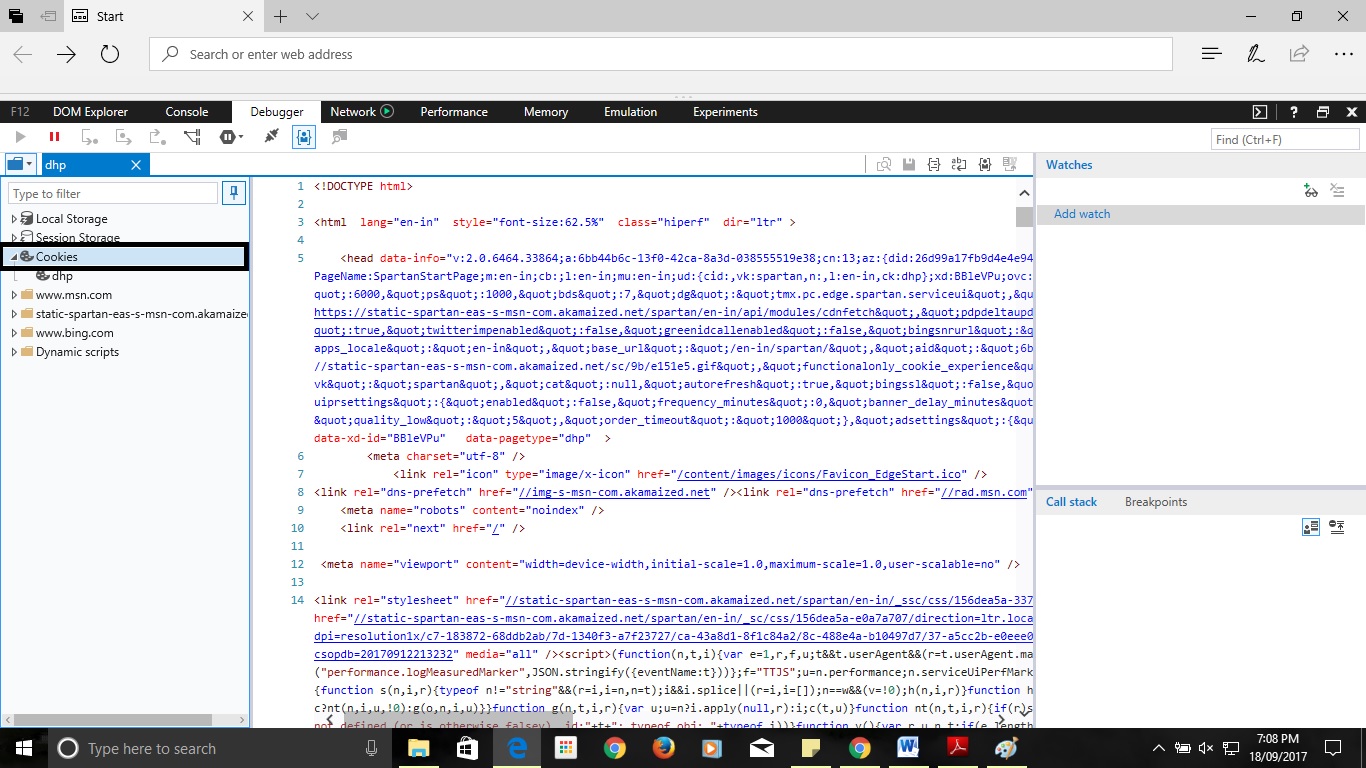


Screenshot 2.11.3 MS Edge History using Cookies Step 3



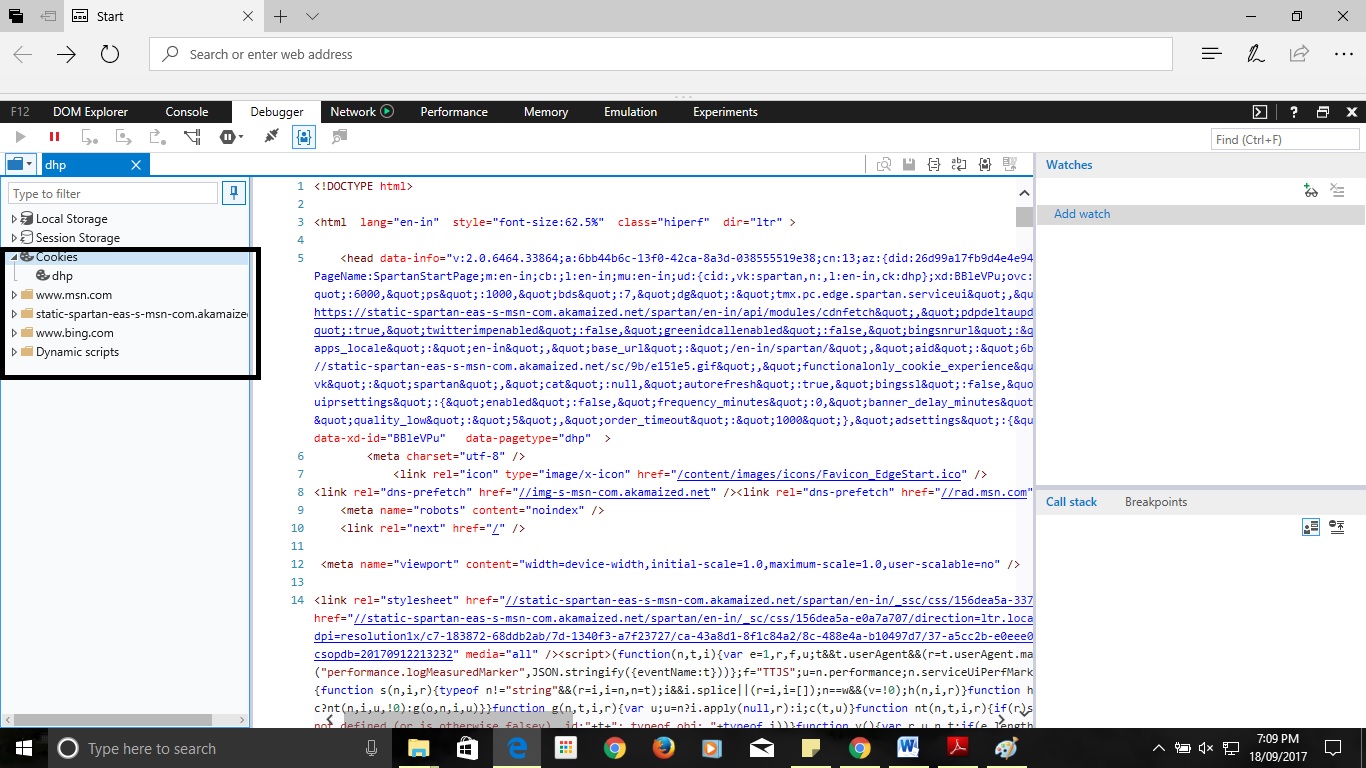
Screenshot 2.11.4 MS Edge History using Cookies Step 4.1

Step 4) Double-click Cookies. It's on the far-left side of the pop-up window.

****

Screenshot 2.11.5 MS Edge History using Cookies Step 4.2

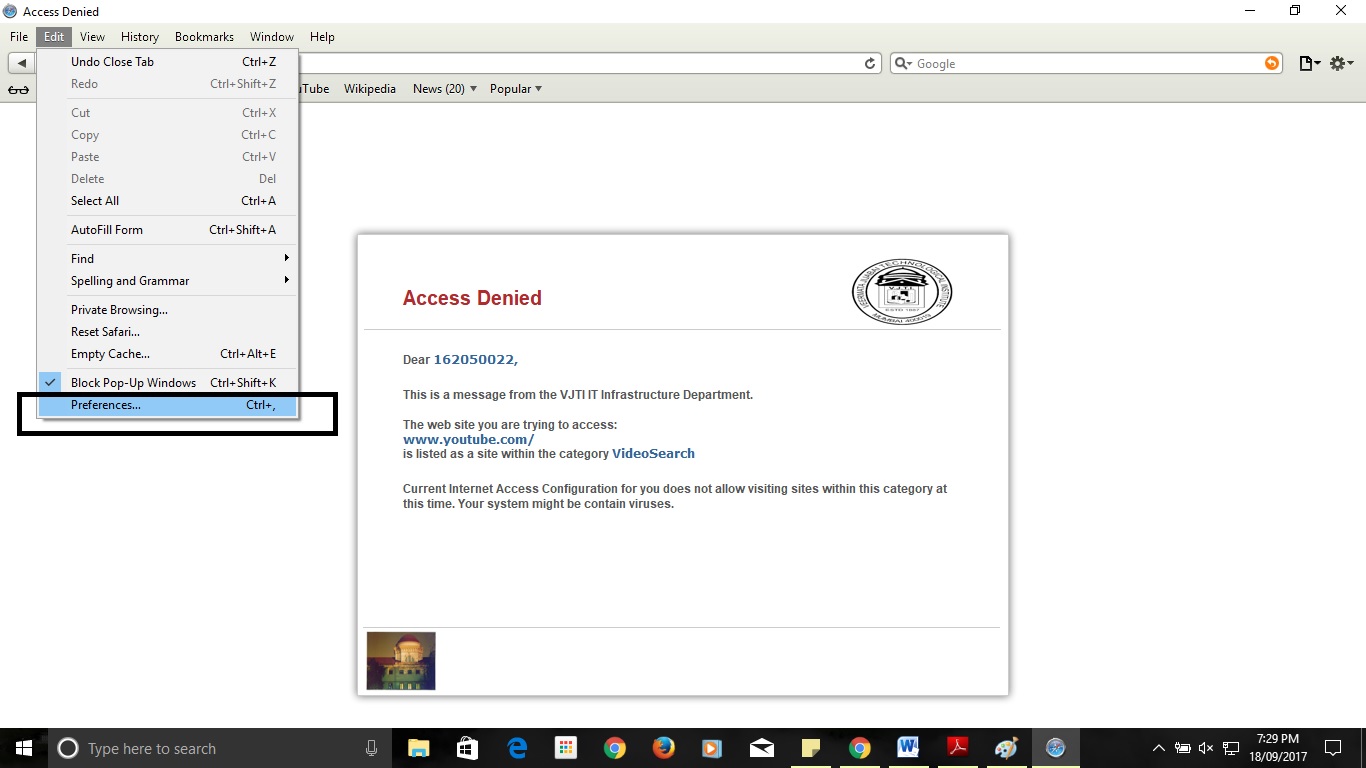
Step 5) Review the site's cookies. You'll see a list of cookies below the Cookies option. Clicking one will display the cookie's attributes.



Screenshot 2.11.6 MS Edge History using Cookies Step 5

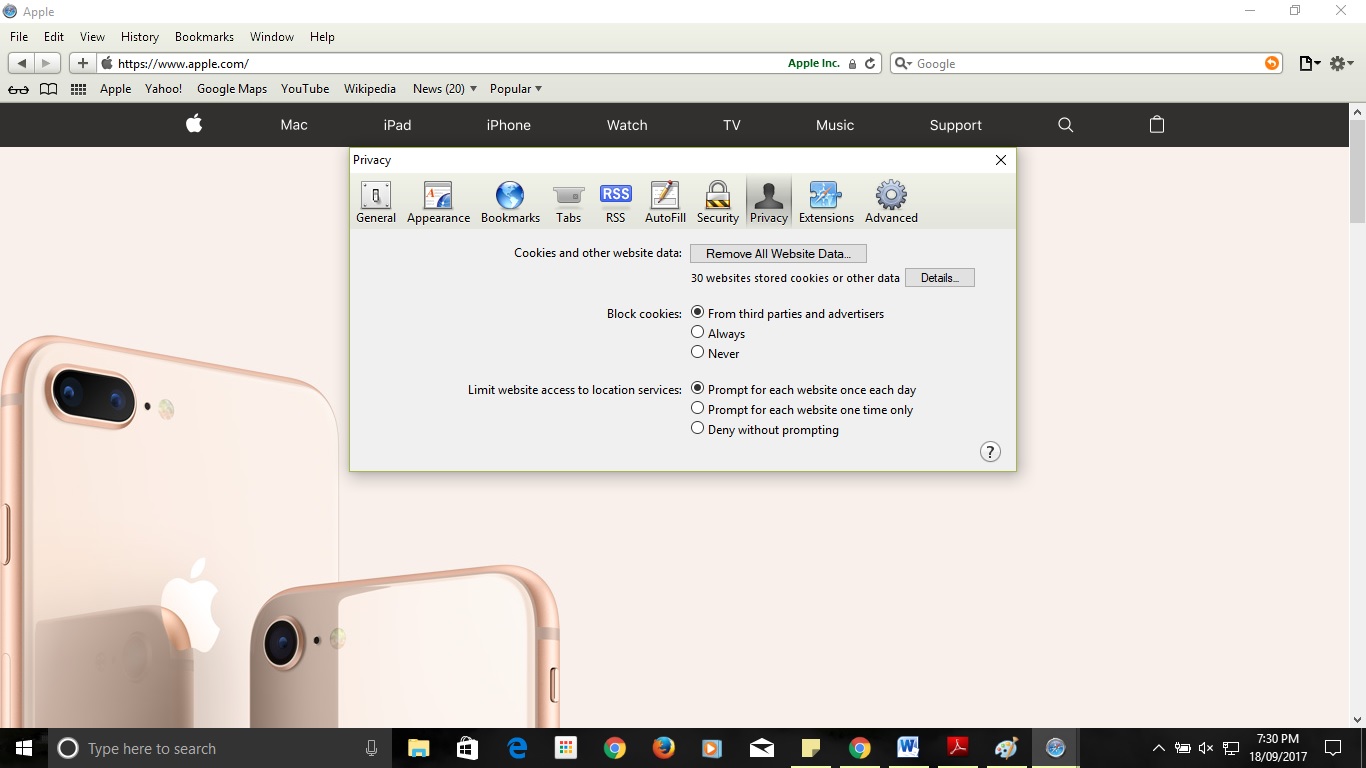
**Safari:**

Step 1) Open Safari. It resembles a blue compass. Click Edit. It's a menu item in the top-left side of the screen. Click Preferences. This option is near the top of the drop-down menu.



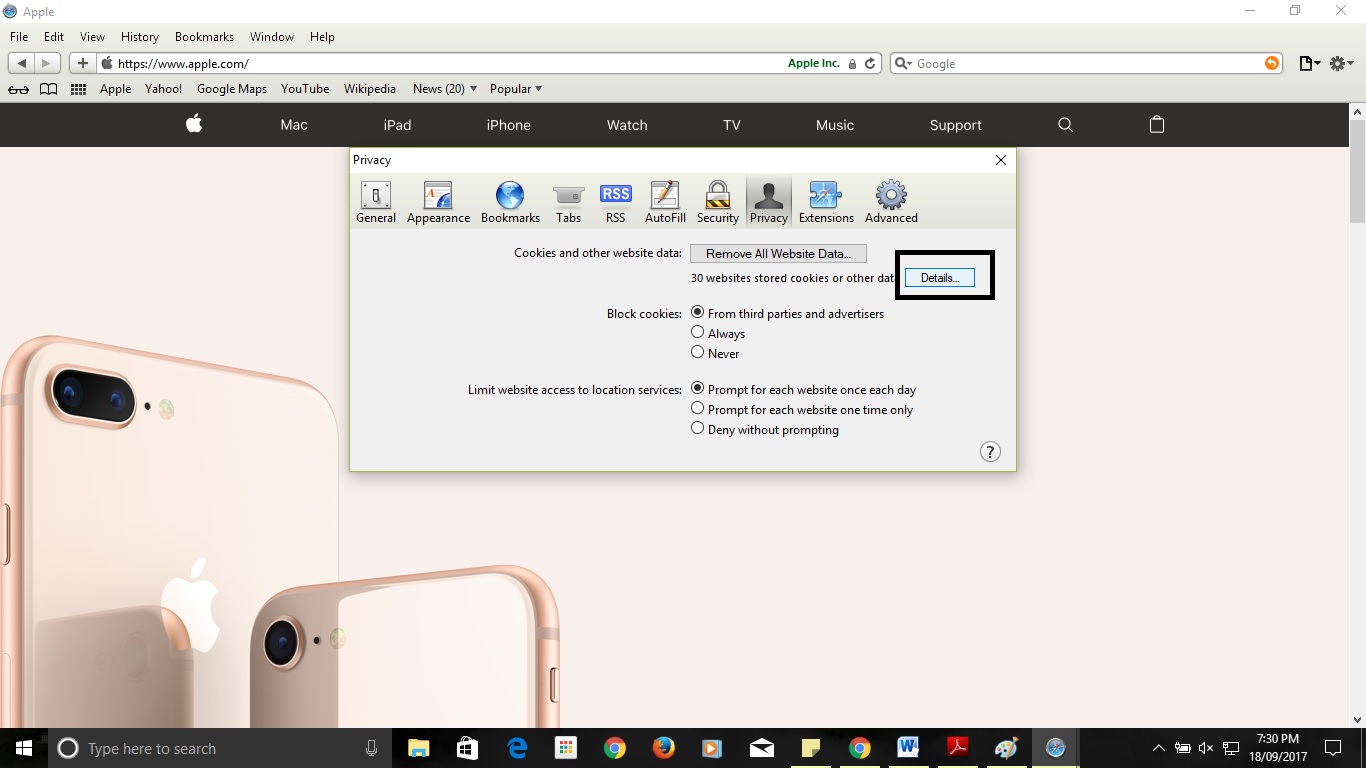
Screenshot 2.12.1 Safari History using Cookies Step 1

Step 2)Click the Privacy tab. It's in the middle of the top row of options on the Preferences window.



Screenshot 2.12.2 Safari History using Cookies Step 2

Step 3) Click Manage Website Data. This option is near the middle of the window. Click Details.



Screenshot 2.12.3 Safari History using Cookies Step 3

Step 4) Review your browser's cookies. All files listed here are temporary website files, though any file with the word "Cookies" below its name is a cookie.



Screenshot 2.12.4 Safari History using Cookies Step 4

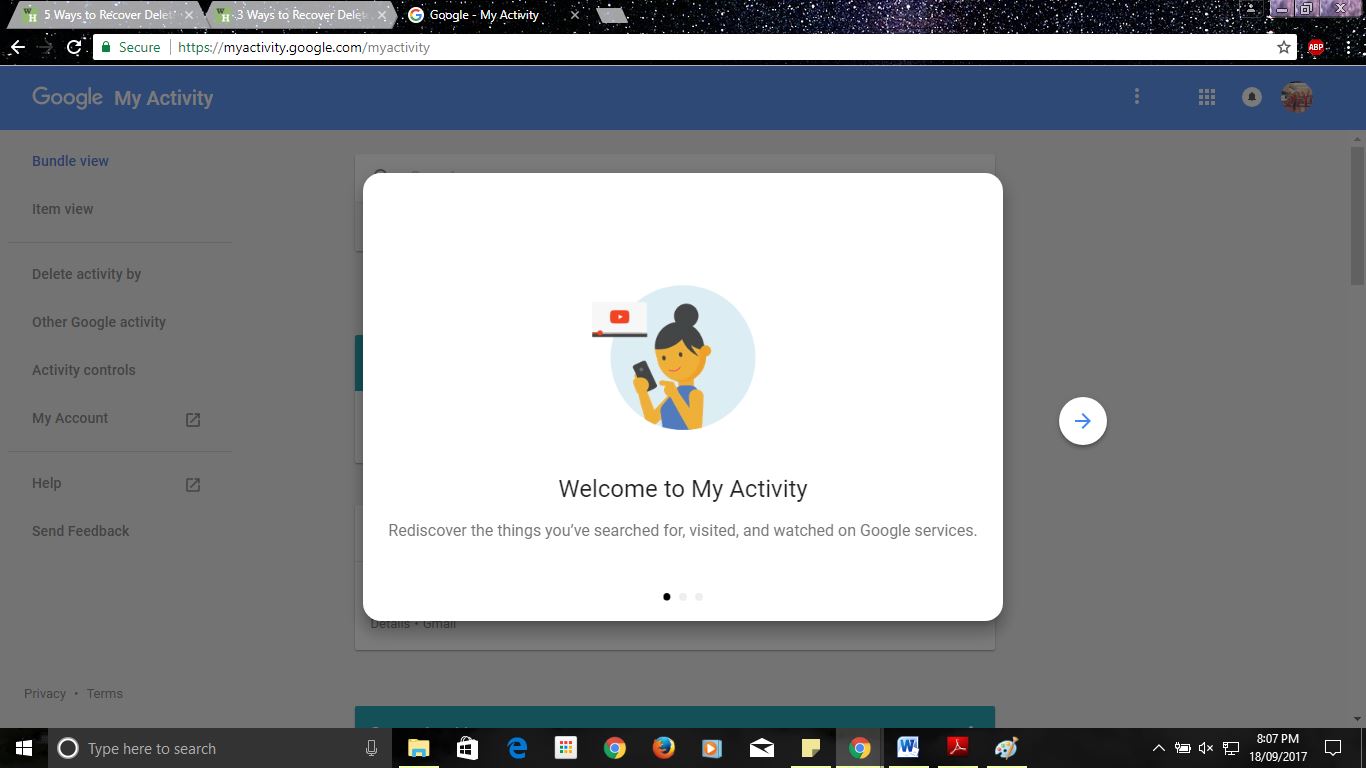
**3) Method 3. Recover deleted browsing history from Google History**

If you have Google Account and logged in everything when you browse websites, you will have a great chance to find and recover browser/internet history. When deleted history from browsers, the Google History is not deleted. It will store all browsing history including all pages that you’ve ever visited and even devices attached to your Google Account.

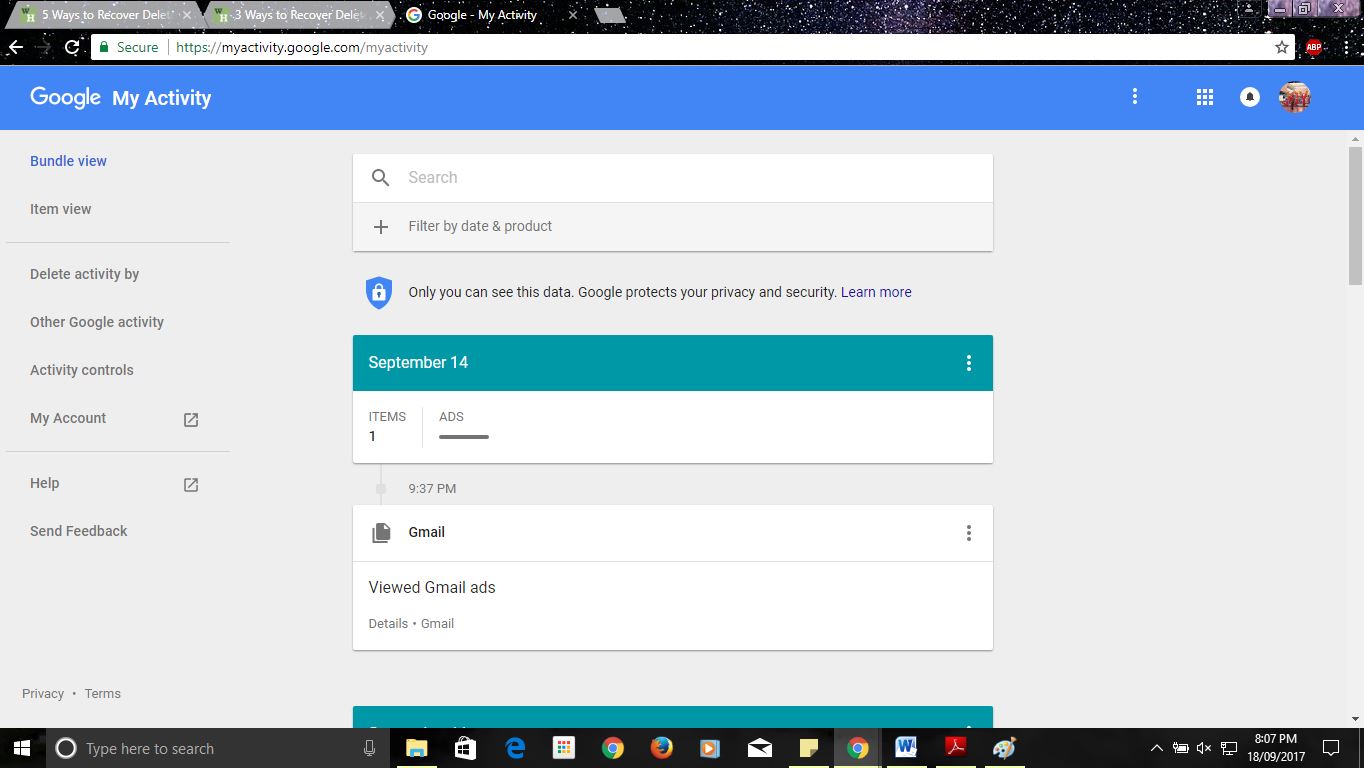
Go to Google History, sign in with Google account.

Then all of your browser/internet history will be displayed along with date/time.

When you carelessly deleted important history bookmarks or lost important websites, don’t worry. Follow this article, EaseUS software will tell you how to recover browser/internet history files and data without any obstacles.



Screenshot 2.13.1 Recover deleted browsing history from Google History Step 1



Screenshot 2.13.2 Recover deleted browsing history from Google History Step 2

This is by far the easiest method but it will only work if you were signed in to your account during the browsing session you wish to access. Sign into your Google Account. Go to www.google.com/history and enter the information for the account that you were browsing with. Review your browsing history. From this page you will be able to see your browsing history according to time and date. If you wish to delete your history, simply click on the cog icon in the upper-right hand corner of the screen and select “Remove Items.”

**2.5 Existing Tools**

**2.5.1 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.

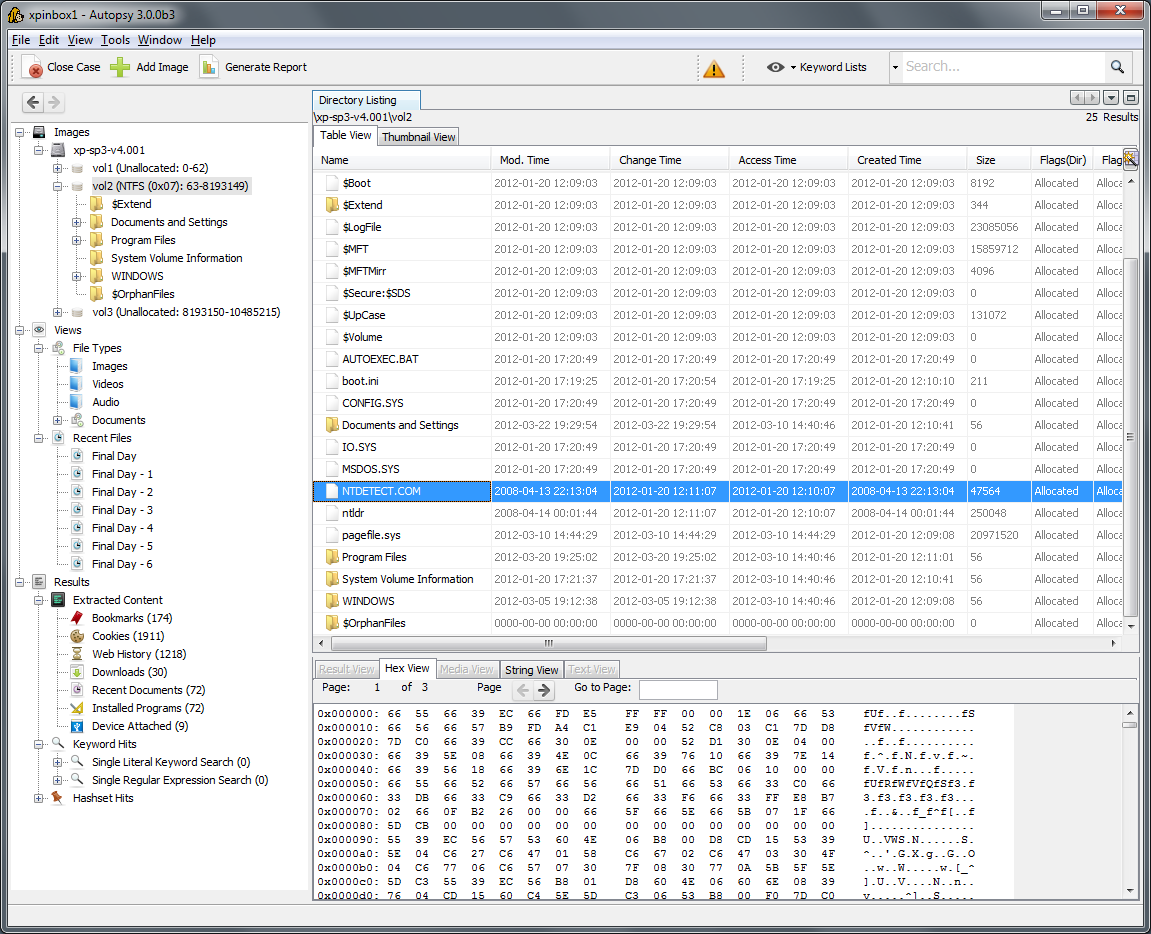
[Keyword Search](https://www.sleuthkit.org/autopsy/keyword.php) - Indexed keyword search to find files that mention relevant terms.

[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)

**2.5.2 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**

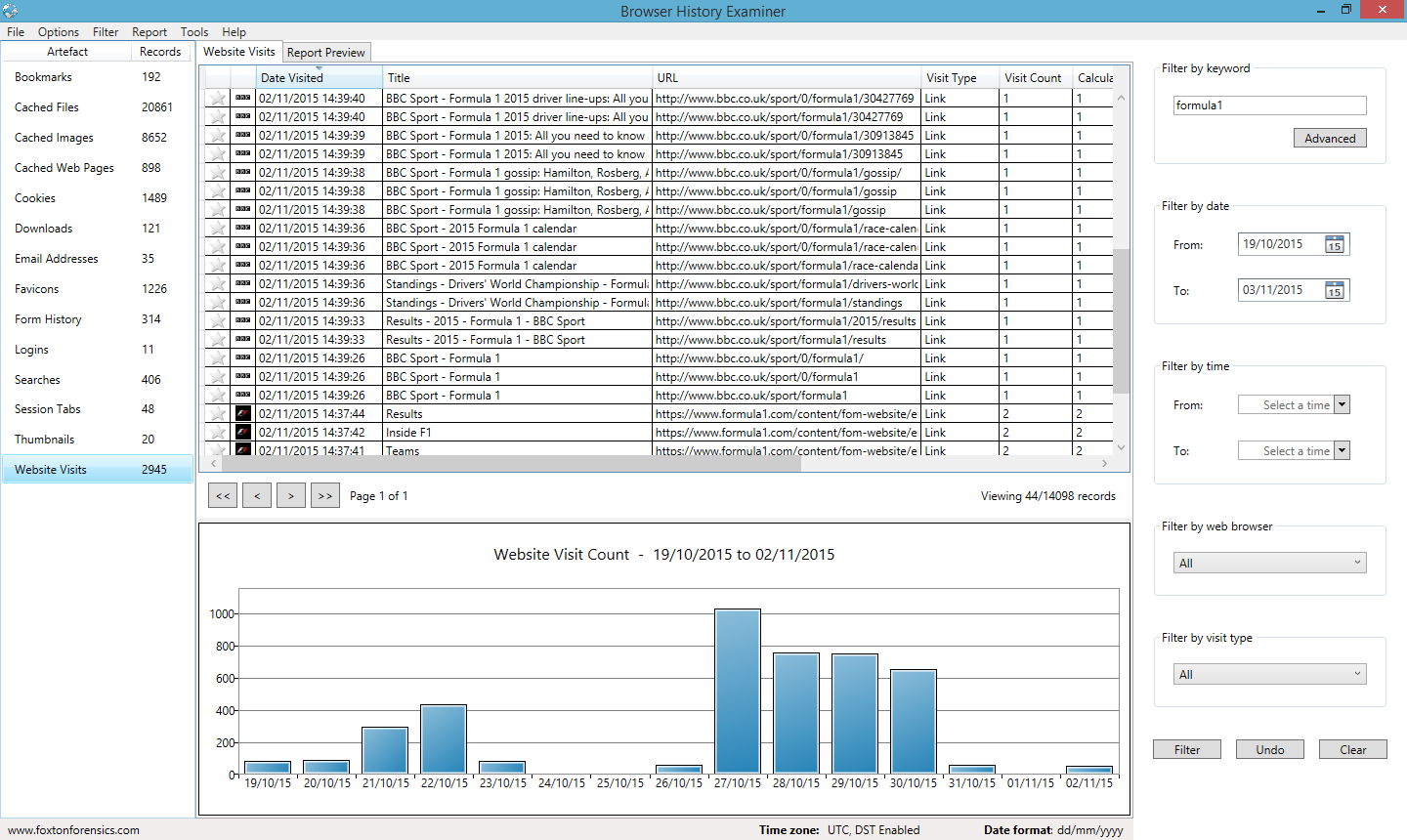
Search history is automatically extracted from multiple sources for popular sites such as Google, Bing, Yahoo, Google Maps, YouTube, Facebook, Twitter and eBay.

**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.



**2.5.3 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.

**2.5.4 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 3: Implementation Details**

**3.1 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.

**3.2 Environment Setup**

**3.2.1 Hardware Requirement**

System: Pentium IV 2.4 GHz or more.

Processor: 2 Physical CPU Cores

Ram: 512 Mb.(Min)

Hard Disk: 20 GB (Min.)

USB Port: 2.0

Monitor: 15 VGA Colour.

1 Mouse

**3.2.2 Software Requirement**

Operating system: - Windows 7 or More

Coding Language: JAVA, SQLite

Tool Used: - Netbean 8.2

**3.3 Tool information for development**

**Netbean 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!

**3.4 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 provide 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.

**3.5 Implementation**

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.

**Screenshots**

1. **Login Page**

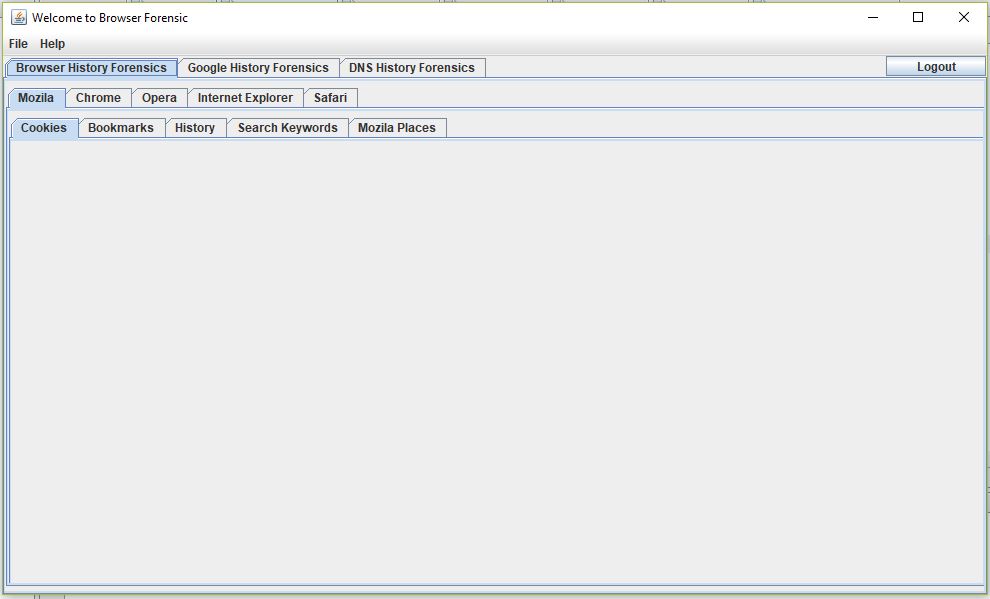
This is Login Page for the system that will use for intering into system. If you have correct credentials then and then only we can login to the system.

****

Screenshot 3.5.1 Login Page

1. **Home Page**

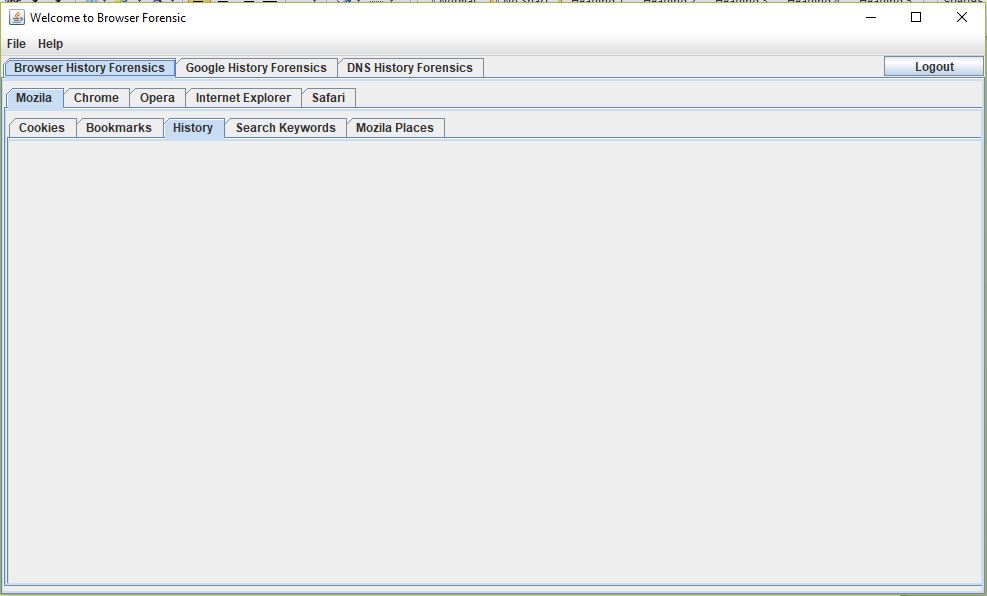
This is the main menu page or Homepage of our system. After login to the system this page is open.

****

Screenshot 3.5.2 Home Page

1. **Forensic of Mozilla Browser**

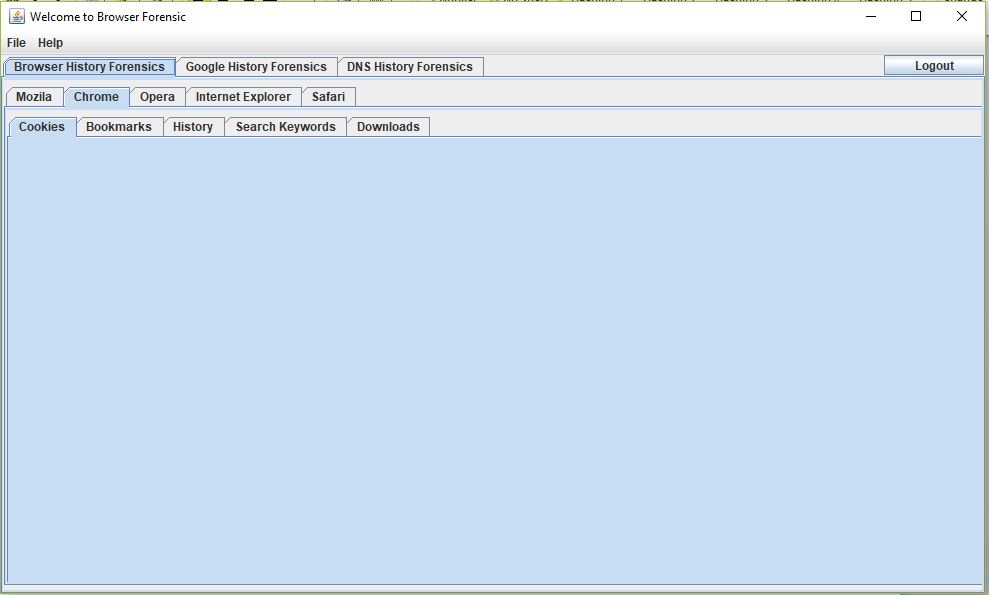
This is the for Mozilla Firefox browser forensic. This contains some more functionality tabs Cookies, Bookmarks, History, Search Keywords and Mozilla Places tab.

****

Screenshot 3.5.1 Forensic of Mozilla Firefox

1. **Forensic of Google Chrome**

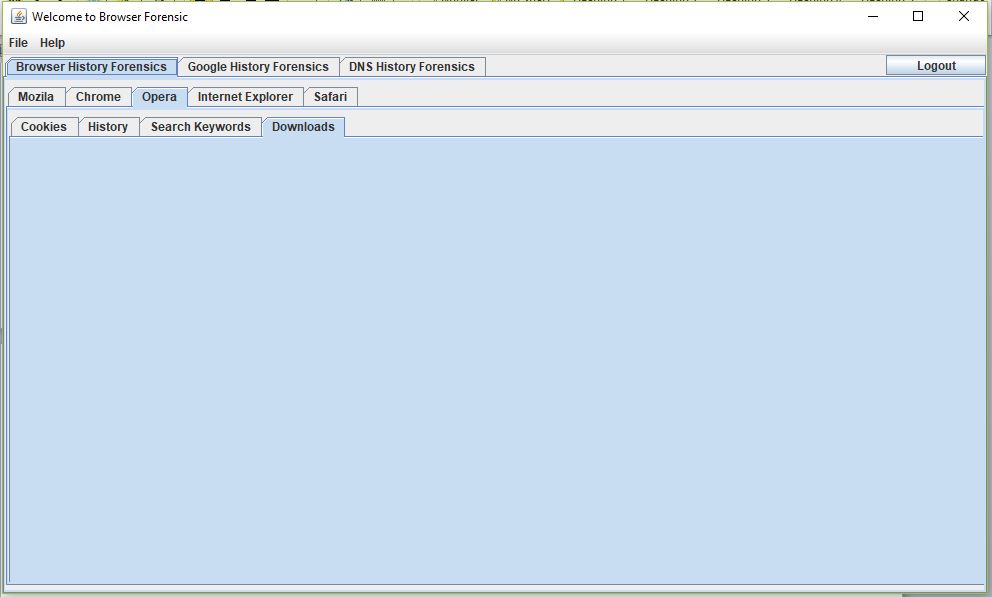
This is the for Google Chrome browser forensic. This contains some more functionality tabs Cookies, Bookmarks, History, Search Keywords and Downloads tab.

****

Screenshot 3.5.1 Forensic of Google Chrome

1. **Forensic of Opera**

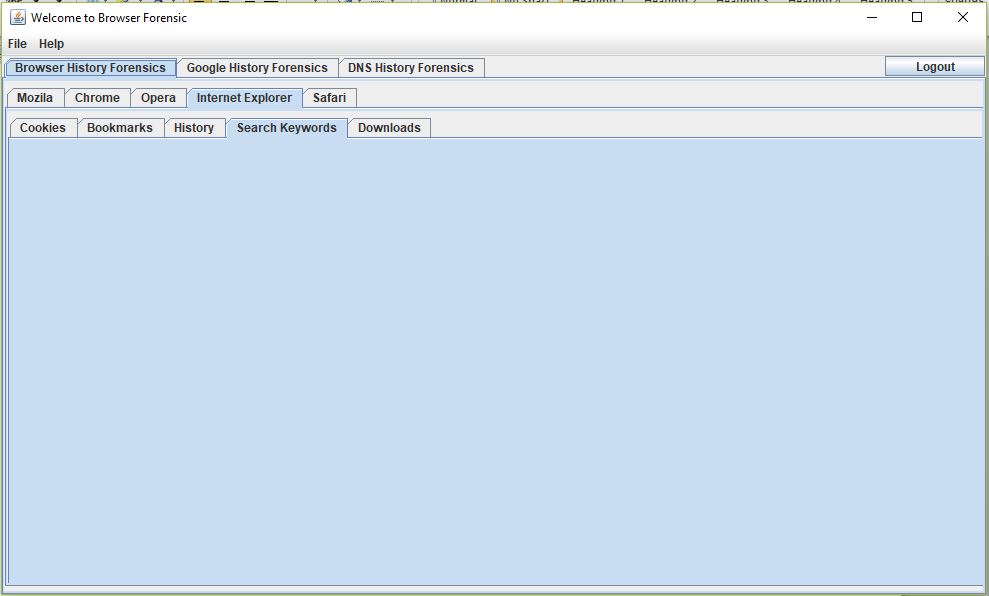
This is the for Opera browser forensic. This contains some more functionality tabs Cookies, History, Search Keywords and Downloads tab.

****

Screenshot 3.5.1 Forensic of Opera

1. **Forensic of Internet Explorer**

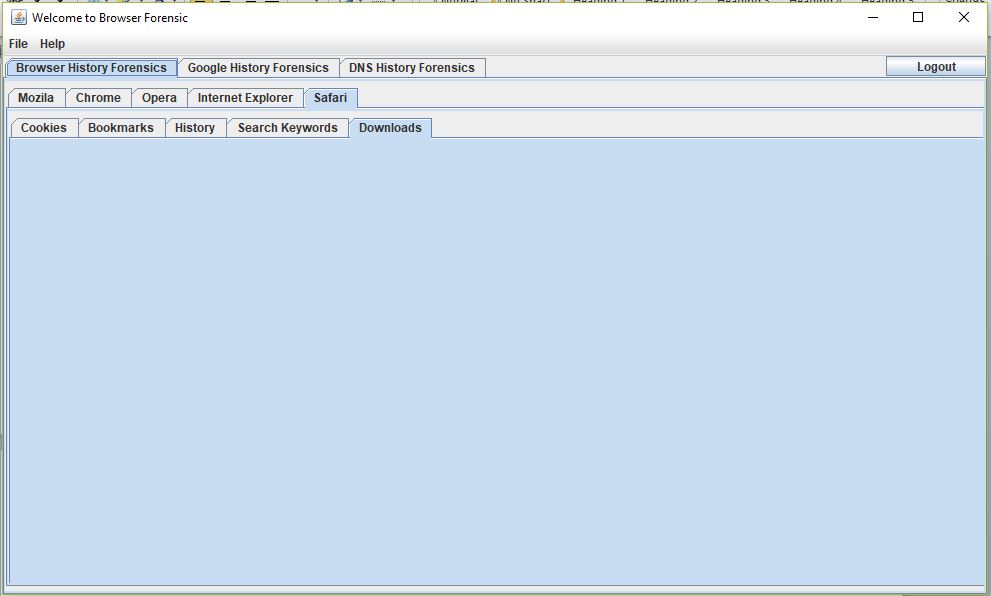
This is the for Internet Explorer browser forensic. This contains some more functionality tabs Cookies, Bookmarks, History, Search Keywords and Downloads tab.

****

Screenshot 3.5.1 Forensic of Internet Explorer

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 3.5.1 Forensic of Safari Browser

**Chapter 4: 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 Güneş, 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