Browser Forensics: Extracting Evidence from Browser Using Kali Linux and Parrot OS Forensics Tools

Sirajuddin Qureshi[1], Jingsha He[1], Saima Tunio[1], Nafei Zhu[1], Faheem Akhtar[2], Faheem Ullah[1], Ahsan Nazir[1], and Ahsan Wajahat[1]

(Corresponding author: Nafei Zhu)

Faculty of Information Technology, Beijing University of Technology[1]
Beijing 100124, China
Email: znf@bjut.edu.cn
Department of Computer Science, Sukkur IBA University, Sukkur 65200, Pakistan[2]

(Received May 4, 2021; Revised and Accepted Apr. 3, 2022; First Online Apr. 30, 2022)

Abstract

In today's digitalized world, a lot of information is getting online, and the size of online data is getting huge day by day; thus, the field of data science emerged. Questions arise when there is so much massive size of data. It also makes it vulnerable to people who have malicious intentions. The gateway for surfing the internet is the web browser. Whether people use that for fair means or foul, some data is precious and sensitive. In this research, a related study about web browser forensics specifies its importance in digital forensics. These studies mention the techniques and tools for web browser forensics, investigating the Android platform as different web browsers provide their web applications. Considering all these studies, the authors go in various directions to extract evidence from the browser. This research will utilize tools like dumpzilla (based on python script), Bulk extractor, and SQLite to extract the details of evidence like history URLs, Cookies, Add-ons, and web Sessions and saved passwords in the cloud storage of the browser. For this, A scenario in the virtual environment is created that the victim browser could be exploited. Forensics tools run on two different platforms, Kali Linux and Parrot Security OS. Two other platforms are used to authenticate and verify shreds of evidence collected. There are limitations of tools. While running on different platforms, they missed capturing some shreds of evidence. After gathering the data from the victim machine, the web browser activities were predicted. There are limitations, and research offers future scope by improving the tools' performance—this requires sound knowledge of python, access control, and system architecture.

Keywords: Browser Forensics; Extracting Evidence; Forensics Tools; Kali Linux; Parrot OS

1 Introduction

Digital forensics is used in auditing and investigating whenever criminal activities were reported. DF is the preservation of the artifacts collected. In this process, there are four steps. The first step is the identification of cybercrime activity what happened. Next is the extraction and preservation of pieces of evidence collected from the crime scene. Then there is the thorough analysis of all the facts and shreds of evidence contained. The last step is the documentation of the whole case and forwards it to further proceedings. In Digital Forensics, BF is the central part as any activity starts through the browser. Many obstacles come in this research as there is volatile data, and challenging to recover the browsing history. In background study, the work of previous authors mainly consists of focusing on the artifacts that are emails, browser history, and images. In this research, cookies are focused and are to be extracted using the forensics tools of Kali Linux. Cookies can save plenty of information like the web page's language, websites we visit online shopping, details, passwords, and most importantly it maps would be very helpful in predicting the real cyber culprit who exploited the browser. Man in the Browser (MITB) is the type of cyber threat in which the hacker uses the browser by identifying and hitting on its vulnerabilities. The primary victim of MITB is online banking transactions. The hacker can alter the transactions and launch a DoS on the bank server, making it unavailable to its legitimate users. With such types of threats, it becomes necessary to secure web browsing. Still, when it was exploited, digital forensics investigators must find out the cause of the cyber-attack and make room for the future and overcome the vulnerability that the attacker exploits.

Private browsing is one of the major issues highlighted by [5]. Many browsers nowadays provide privacy modes

like google incognito, where browsing history was not mapped. That's one of the significant issues. Suppose forensics cannot find out what is surfed on the browser. It will create problems in leading the investigation—their research identifies the possible hidden privacy modes in a web browser. Phishing attacks are common these days. Most of the people receive emails scams like a Nigerian widow is offering her seven hundred thousand dollars with the link provided or youngsters mainly targeted by the emails in which some company (which does not exist in reality) offering them a job with a handsome amount of salary and many more like this. So [6] elaborated on these email scams and studied how to avoid malware/spyware phished into your system.

In this discipline of web browsers, forensics legal and technical aspects must be considered while conducting a forensics investigation. A digital forensics investigator must know about these legal aspects to filing a solid case [24] contributed to digital forensics technical development by answering can browser forensics detect a criminal tendency?, What are the legal aspects of conducting web browser forensics? Software tools make our lives easy, but there is still a need for expertise to utilize these tools efficiently for this hands-on tool BrowStExplus studied by [16] for web browser forensics. This tool is used to map the storage of web browser details and helps in extracting the pieces of evidence. WBF is one of the major domains in digital forensics as dependency on the internet increases, thus increasing its vulnerability. Deleted web data, private browsing modes, denial of service DoS attackman in the browser all exploit the web browser and become catastrophic for the online business and e-commerce industry. One of the main obstacles that refrain digital forensics investigators from leading the investigation is the deleted history and using private browsing modes. In this research, the main focus would be on internet cookies that save many things, including online shopping details, saved passwords, and one of the most important things they mapped the browsing activity, which is the key in web browser forensics investigation. For example, an internal malicious user exploited the web browser in an organization and leaked the company's private information on the internet. The problem arises when the investigators reach the IP address from where the information is leaked, but after reaching that device, all the data is vanished and is wiped out from the browser.

This addresses the main problem statement of this project: **"In an organization, an internal malicious user leaked the confidential information on the web by exploiting the browser and deleted all their footprints. For that purpose, a forensics investigation needs to extract all the pieces of evidence like history, cookies, and saved passwords from the cloud space provided by the browser."**
This research follows by utilizing digital forensics tools on the victim's device. The main tools that were used in this project are "Dumpzilla" and "SQLite".

1.1 Research Questions

As mentioned about the browser forensics earlier, the main criminal activity starts from here and it may lead to botnets and denial of service attacks. The main question of this research arises as follow: **Is it possible to run a successful digital forensic investigation in the circumstances when all the browsing data is vanished after being exploited?** Following this question and to barrier the research gaps, this research raises some questions that would lead to the solution of the problem statement to solve the issue of browser cloud forensics investigation.

- **What would be the suitable technique to conduct browser forensic investigation and avoid the chance of losing important shreds of evidence?** Browser data is sensitive and volatile. It is difficult to prevent the data loss that would help lead the investigation. It is also essential for the organization to be equipped with evidence collection methods and techniques.
- **How to extract and predict the culprit?** Here comes the difficult part of the investigation. First, in this research, the shreds of evidence are preserved following the procedures of digital forensics investigation and compiling the report. Finally, the prediction of browser activity to find the real culprit.

The sub-questions help the investigators in leading the research. First of all, the researcher will extract the shreds of evidence from the browser cloud by utilizing the tools of Kali Linux. Some problem arises in experimental analysis while conducting the research this would be later discussed in this paper.

1.2 Paper Structure

Start with part one. The introduction briefly explained the overall concept of research to be conducted and the main hindrances that arise in investigation. It provides the background about how other authors work on this investigation and how it will overcome the gaps. In the next part, the literature would explain the researches of previous authors in this regard, then the thesis would come towards the research methodology, which would elaborate the research scenario of how the research is being conducted in the environment when all the browsing data has vanished. Then the experimental analysis gives the simulations of the tools conducting the investigation. After that comes towards the findings the problem arises in the research then comes towards the conclusion and future aspects of this research.

2 Literature Review

In the cyber world every day there are countless numbers of crimes reported each day which breached many

gigabytes of online data. As the world is digitalizing, the demand of securing the IT industry is a demanding topic these days. Here comes the need for digital forensics and investigation all the criminal activity. There are tools available that need the expertise to capture the malicious activity. Earlier this research, many authors work on this problem as today's world information is digitalized. All your banking and financial details, health reports, and personal credentials are online, making them vulnerable. The beauty of the internet facilitates the users by coping with any type of device connected to it. But in making the architecture of the internet, the layers of TCP, the main focus was on functionality. As time passed, security becomes a loophole for the attacker and cyber criminals to exploit the information.

The work of previous authors mainly centred on the analysis of artifacts related to browser history, emails, and images or videos are discovered or not. This research is a step forward to find the cookies based on that the behaviour of the malicious user on the browser can be determined, and this can be compared with the history and cookies of employees of the organization to find out the real culprit.

In this project, we assume a case study in which a malicious internal user of an organization exploits sensitive information by leaking it on the internet. Someone from the organization found the information randomly on the internet and report it to the IT department. They immediately call the digital forensics investigator. With some initial investigation, the investigators found the PC's IP address from where the information leaked. Now they find out that all the browsing history is deleted, and there is no trace of malicious activity. First, they have to do some research for such type of investigation problem, and with the help of a digital forensics tool, the required shreds of evidence will be extracted.

2.1 Related Study

Heading towards the research, we have to study the brief idea of digital forensics, its significance in cyber security, and the necessary investigation processes. What are the main obstacles that arises and how to overcome these issues smartly and bypass the obstacles that come in the investigation? In understanding the main process, firstly, let's discuss the work of authors in this field.

The field of cyber security moves in both ways defense and attack one can be on the defensive and attacking side. The combination of both is efficiently elaborated by [17]. They combine steganography and forensics with running a security check and overcoming a vulnerability in transferring information between users. In reviewing and leading the digital forensics investigation as studied by [3]. Their framework consists of two steps or phases. The first phase maps all are artifacts and shreds of evidence collected from the crime scene during the investigation. The next phase is the step-by-step and semi-automatic way of investigating a cyber threat despite its intensity. In this phase, first of all, there is the selection of CKC. Then comes the identification by comparing the found CKCs with the organization of the proposed artifacts. Then find the correlation between the CKCs and the artifacts presented. Then there is the construction of the chain of artifacts CoA. After there is analysis of CoA.

Ensuring the quality of investigation and avoiding the flaws and false shreds of evidence [4] gives the QA for the DF investigation. Many practitioners or investigators face challenges while investigating when they came across mismanaged shreds of evidence. Like without proper preservations and proper documentation of the artifacts that can be utilized to solve the case. In this regard, the authors proposed the mechanism of "Verification of Digital Evidences" which helps practitioners keeping track of all the artifacts and proper documentation of sensitive evidences; without proper records, it would be troublesome to lead the investigation. This research is also getting motivation concerning the work of [25]. They set up a virtual environment, exploited IoT devices with Kali Linux Tools, and conducted digital forensics experiments. This research following the same footsteps in experimental learning.

Same in a virtual environment, a web browser is exploited. A web browser forensic investigation is run to extract the shreds of evidence from the browser in a virtual setup and about the forensics tools, FTK imager is also very beneficial in getting all the desired evidence from the web browser studied and implemented [22]. The author gives a detailed study about capturing the user activity on a web browser by utilizing the FTK imager. Also [15] provides the detailed research, tools, and techniques for forensics analysis of shreds of evidence collected from the web browser. The work of previous authors mainly centred on the analysis of artifacts related to browser history, emails, and images or videos are discovered or not. This research is a step forward to find the cookies because the behavior of the malicious user on the browser can be determined. This can be compared with the history and cookies of employees of the organization to find out the real culprit. There is also a study [12] in which the authors discussed the compatibility and efficiency of tools utilized for the Firefox browser.

Internet starts with the search engine, the web browser, and the first thing that comes in search is URLs (uniform resource locator). Data about data or Metadata need to be grabbed when locating or mapping extensive search activities. This research provides the framework for grasping the malicious browser activity like hate content or leaking of sensitive information on social sites by examining and mapping URLs activities to guess the browsing activity. It may help in guessing the browsing activity of the particular user in case of an internal threat or case when an internal malicious user exploits the system. This approach is utilized in this search, but the target will be to extract the cookies. Logging is one of the best ways to keep the record or directory as in [7] authors discussed logging with the help of it a user activity on the browser

can be mapped. A log file helps to collect information about the malicious internal user. All windows systems have log files that keep the arbitrary data. It is called index.dat, which keeps all the data of websites visited from the computer. Also, trace the log file [1], which gives the techniques to identify and locate the log files of the browser. Also contributed to analyzing the gathered information to find out the malicious activity.

Phishing is one of the major attacks that exploit computers and mobile devices. Phishing emails are mostly used in which a user receives an email of a job offering or any marketing scam to overcome such spam. In phishing, there is mostly the negligence of employees who do not timely report any such incident. In a study by [11] they discussed social cognitive theory (SCT) and cyber risk beliefs in SCT. Their major contribution is to give detailed study about the careless attitude from the employees and give awareness for cybersecurity. To secure the browser from such intriguing mails a study by [9] conducted an activity in which 985 participants take place. Their data collected and analyzed have proposed a model for predicting spam and phishing emails. Also, there is a need for user awareness for securing their web browser from phishing because you have applied the most advanced system for security in an enterprise.

Still, there is the negligence of unaware employees that puts the whole enterprise at risk. So [21] studied the behaviour of users and reactions when they received warnings from the browser. Their results would help in improving the browser's security features. Authors (Peter Snyder, 2018) give a cost-benefit approach to secure the browser. They have made a simple extension to avoid the CVE exploits that are available open-source. Another study by [23] in which the proposed system is doing deep scanning of emails and sorting them out in different categories like spam, important, etc. For securing the web browser, one should be aware of the security configuration features of the web browser. A study by [18] studied more than a thousand configuration options for three major web browsers. Out of that, they have found 13 useful features for secure web browsing. A private web browser that was continuously relocating the IP also makes it difficult in a forensics investigation, like Tor Browser. These browsers camouflage the IPs and make it difficult to detect and map the exact location of criminal/malicious activity. Regarding this issue [8] discussed about the forensic of a tor browser. While discussing their design considerations, the project is focused on expanding the previous research to find out that there is an existence of the Tor browser in windows 10. They're also a case study on "Epic" which is a private browser [14]. There is a study about the harsh impact of usage of epic browsers for illegal activities like drug dealing and human trafficking. They run live forensics on an epic browser to capture the exact location of the desired shreds of evidence. Secondly, by capturing the RAM they find out the digital artifacts provided by the Tor browser. The malicious activity can also be done through the android device as the browsers provide the full compatibility in smartphones as well. To run the forensics on the browser in a smartphone [20]. In their framework, they extract the information from the device like serial no, root access, or any sort of encrypted files in the device. Then moved towards checking the root access in the device.

They found the device is rooted, and then it will further process for web browser forensics. Then another module checks and calculates the artefacts and shreds of evidence collected; then there is a thorough analysis of artefacts and shreds of evidence collected.

There is also an issue of resource abuse studies by [2] that there is a covert use of resources of machines for crypto mining or crypto-jacking. Hackers made their transactions in cryptocurrency for that they need the heavily resource-rich device for this purpose. They use botnets to exploit the machines and abuse their resources. Authors have designed an algorithm to guard and protect the browser if botnets exploit resources for crypto mining. To secure the web browser, a fingerprinting method was proposed by [10, 11] in which there is a transaction on identity method imposed. Users with high likely hood and based on their extracted features, they have generated an identity. Every time they browse on the internet, they have to provide that ID for searching. Also, the US patent [19] recommends the authentication factors for secure web browsing. This related study is summarized in Table 1.

2.2 Summarized Literature Review

In summarizing all the related studies mentioned above, it gives the significance of browser forensics in DF as the browser is just like the motherboard of connecting devices to the internet world. Any activity on the internet starts with surfing on the browser. It may be good and maybe sometimes exploited by any malicious user from inside the organization. Sometimes, it becomes cumbersome for the DF investigators when all the browsing history were deleted and someone is using a private browser like Tors. Many browsers offer the private browsing mode or camouflage the IPs of the devices, which makes it challenging to map the browsing activity, leading to the malicious user that exploits the browser.

Prior authors have discussed web browser forensics in this arena. The main focus was on extracting the artifacts and collecting the shreds of evidence. They are going with extracting log files in the windows, utilizing a tool like BrowStExplus. They were also utilizing android toolkits for forensics and running algorithms for identifying phishing attacks via email forensics. While conducting the digital forensics investigation, it is compulsory to consider the legal and technical aspects mentioned in the related study. This research will extract cookies from the browser and save passwords by utilizing the forensics tool dumpzilla and SQLite in the OS Kali Linux.

An experimental learning environment is set up to run a digital forensics investigation on the exploited browser

in the research scenario. By extracting the artifacts like cookies, save passwords in the cloud environment provided by the browser.

The abbrevations used in Table 1 will be discussed in appendix section at the end of this paper. The main research objectives are as follow:

- Conduct a forensic investigation on browser cloud;
- Utilize tool to collect the artifacts and evidences;
- Bypass the hindrance of deleted browsing activities;
- Focused on extracting the cookies of the browser which contains many information related to browsing activity;
- Analyzing all the evidences to capture the malicious internal user.

In concluding all the related studies, it's elaborated the importance of browser forensics in the world of digital forensics. Many authors researched it by utilizing different tools and techniques for the investigations. Also, the legal and technical aspects are mentioned as a digital forensics investigator must be aware of these aspects. Comparison to all the research mentioned in the related study, and after studying their approaches, this research will extract cookies from the browser. These cookies contain many sensitive and volatile data that are very precious for investigators. Most of the investigations got stuck without proper handling of the artifacts and after losing the volatile data. This research utilizes the tool dumpzilla. Dumpzilla is the digital forensics tool developed in python that provides many utilities in conducting the digital forensics investigation on the browser. It helps extract the volatile data and sensitive shreds of evidence that would be a gem for investigators. Getting required traces of evidence in the vital step investigations and after that, there is also need to preserve these documents.

Table 1: Summarized related study

Reference Work	Basics in DF	VoE	DF Tools	HE and SB	Phishing, UB	PB	RA	Remarks
[3, 4, 25]	Discussed	Discussed						CKC, Mechanism for VoDE
[7, 12, 15]		Discussed	Discussed					FTK imager, Firefox forensic tool
[1, 11, 13]	Discussed		Discussed	Discussed				A proposed method to penetrate log files
[9, 21]					Discussed		Discussed	Methodology to mitigate a phishing attack
[8, 18]					Discussed			cybersecurity awarenes
[2, 14, 20]		Discussed		Discussed		Discussed		Methods to extract pieces of evidence in PB
[10]				Discussed				Live Forensics of RAM capturing
[19]						Discussed	Discussed	Resource abuse mitigation algorithm

3 Research Methodology

Describing the qualitative investigation goals is understanding, explaining, discovering, and making theoretical approaches and hypothetical information. Qualitative is flexible structured it can be modified according to the facts collected and gathered. Data collection in qualitative the researcher is the main instrument for gathering and processing the data. This qualitative data can be obtained from various sources like conducting interviews of relevant people of the field, focus groups analyzing and studying the research topics on the basis of their findings and observations. After that, the thorough and intensive study of existing documents of the relevant field. Describe here the three chapters from the book qualitative research (Dawn Goodwin, 2019). It's a difficult task to assess and assure the validity and quality of qualitative research because of its diversity. They mentioned six methods: triangulation, respondent validation, clear

exposition of data collection methods, reflexivity, attention to negative cases, and fair dealing. The theory has an essential role in leading qualitative research. Some considerations underpin the research strategy. They also explained ontology in which is concerned with the questions. Also, epistemology is concerned with the theories of knowledge.

The quantitative is mainly concerned with the statistical and numeric data, logic, and an objective stance. It is a systematic and empirical investigation of observable phenomena via statistical and mathematical techniques. It consists of large numerical data. After that, they conduct data analysis that to find correlations. It involves the generation of data in a quantitative form which can be subjected to rigorous quantitative analysis formally and rigidly. While in mixed methods, there is a hybrid of both qualitative and quantitative to research three different ways. In the first type, the quantitative data are collected first and then the qualitative data. In this process, the qualitative data were served to explain processed quantitative data in contributing to the research. The next type of research is in which first there is qualitative then comes the quantitative for justification of qualitative data collected earlier. The last type is the combined effect of both qualitative and quantitative.

3.1 Research Design

It is moving towards the research design to identify the purpose of this research and its outcomes. About the book chapter (Woodrow, 2014), the first part of the research design is to identify the research purpose. Following this regard, the focus of this research is on web browser forensics. Any activity on the internet starts with surfing on web browse, whether for the searching purpose or exploiting the legitimate resources of any enterprise. It becomes challenging for the investigators to capture the volatile data and manage sensitive shreds of evidence in the environment of the exploited web browser. In this regard, the purpose of this research would become:

"Extracting evidences with the approach of capturing the cookies in the browser which contains plenty of precious data that would lead the digital forensics investigation in right direction"

The next step is identifying the variables, whether it is an independent variable (IV) that impacts the outcome of the dependent variable (DV), that is, the outcome itself. In this research, the impact of extracting the cookies, passwords, add-ons, sessions, etc. (independent variable) with the help of forensics tools (independent variable) to run the browser forensics. From that, the variables are measured. Then decide how these variables will be measured, it is by extracting cookies with the help of dumpzilla and checking the browser details with the help of SQLite. After that analyze all the variables, our main target is to find the internal malicious user. This can be done by setting up a virtual environment in which a digital forensic investigation is run to collect all the cookies and then it's analyzed. As mentioned in the proposal, we are assuming that we have found out the machine that is exploited to leak the data on the internet. Now data from all the devices in that department is analyzed. After that, the data collected from the exploited machine was compared with the collected data of all other department's machines. After that, the report was compiled, and the process is as Figure 1.

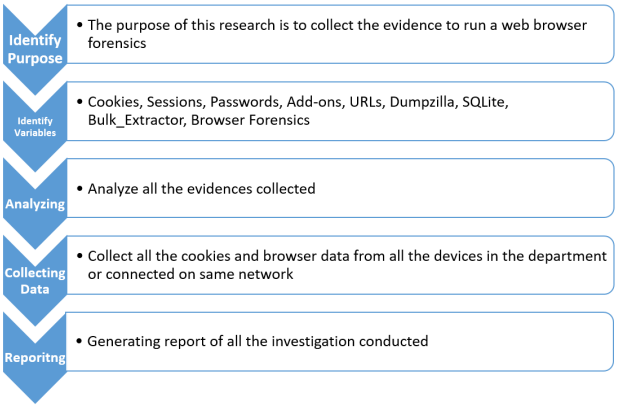

Figure 1: Research design

3.2 Choosing Research Method

They discuss all the related studies work in digital forensics, specifically in web browser forensics. Most of the authors use logging like keeping the record files of all the browsing activity. Some are capturing the RAM file using disk image forensics to get all the activity during web surfing. There is also the discussion of legal and technical aspects of digital forensics research. A DF investigator must be aware of all the legal and technical aspects of the investigation.

In this research, following the research design, the approach collects the shreds of evidence from the web cookies. These cookies are basically the messages that a web server sends to your web browser when you visit internet sites. It's a term of a UNIX program that is Fortune Cookie which contains all the browsing activity information. This research aims to get these cookies pulled out from the browser and start the investigation. The method chosen in this search is the hybrid of qualitative and quantitative analysis. The mixed methodology is in which first the related researches are thoroughly studied and run an experiment of extracting artifacts from the victim machine and concluding the results.

After cookies, we must move towards other data and the saved passwords of different sites that an internal malicious user used for various sites, which could be a gem in extracting more details and making the investigation more concise. Sessions are also important evidence in guessing and predicting the malicious activity along with the Add-ons and all the important URLs we can extract by utilizing our tools in the environment or lab we set up for the investigation.

4 Investigation and Analysis

Getting started with the investigation, we have to set up an environment to conduct the investigation, set up all the necessary tools, and fulfill all the dependencies. Move with the assumption that the investigation has traced the IP addresses of the machines that are being exploited. As they reached that machine, investigators found out that all the browsing activity had vanished, creating a big hurdle in their investigation. They need to extract out all the sensitive shreds of evidence, including sessions, cookies, add-ons, passwords, etc. First, we have set up a forensics environment. We have setup Kali Linux, an operating system providing a platform for penetration testing and digital forensics.

Similarly, another competitor operating system for penetration testing and forensics is used which "Parrot". Using two operating systems makes the investigation more precise and authentic as there is cross-check of results from two different platforms. Experimental analyses are the most critical part of any research, which decides the contributions of the author. Here either you have reached the desired results and contribute by suggesting the gateway toward the solution of the identified problem. On the other way around, after so much intensive work, the desired outcomes are not achieved and, in the end, the research is not going the way you anticipated. In such a case, the author's contribution is that he/she has done so much study to identify the problem and formulate a hypothesis to get the solution. After conducting the intensive series of experiments and calculations when the anticipated method did not lead to the desired solution, the author saved the time of many researchers. The contribution is his or her wide range of study to save the time for literature review and guide the researchers that the anticipated method does not lead towards solution it is either stuck at the end.

4.1 Project Implementation

Following the methodology of the project. The implemented technique or method here is the mixed methodology the combination of qualitative and quantitative research. First, a detailed study has been conducted for the problem identification in which the researches of various authors are mentioned in the detailed study section. This study includes digital forensics' legal and technical aspects to extracting artifacts, sensitive shreds of evidence, and volatile data. These authors work on separate identities like email forensics to detect and prevent phishing attacks. Then some are using log-based analysis to get the log files of saved browsing activities. Some are using image extracting tools to recover the browser's log files in the hard disk image. Also the method of capturing RAM to access the volatile data of the browser.

All these researches and experimental analyses are leading towards extracting as much data as it makes the investigation more authentic and more precise. But there

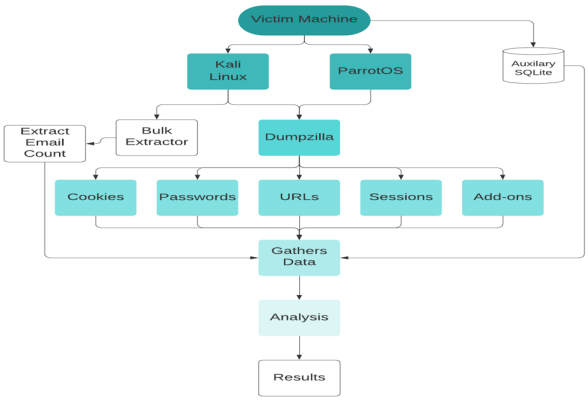

Figure 2: Project implementation

are a lot of methods to pull the same shreds of evidence. This research shows all the shreds of evidence, including the most critical cookies, sessions, passwords, Add-ons, etc. by utilizing "Dumpzilla" and "Bulk Extractor". There is the setup of the virtual environment in which as per assumption the victim machine is found out which is used in the exploitation of the browser. On this machine, investigators installed two operating systems "Kali Linux" and "ParrotOS" which extract the necessary data nd shreds of evidence. The project implementation is illustrated in Figure 2.

4.2 Experimental Enviornment

Coming towards our digital forensics lab where the investigation will capture the cyber culprit/internal malicious user who has exploited the browser and tries to hack into XYZ organization's database to get the sensitive information. Moving with the assumption that forensics experts have traced the IP address of the victim machine, but on reaching that machine, they have found out that all the data has vanished, here comes the hurdle and basis of this research.

There is a need to extract all the data from the browser, including sessions, Add-ons, cookies, and saved passwords. In our lab, we have setup KL and POS in which we are utilizing forensics tools like dumpzilla and bulk extractor, and auxiliary SQLite information of history. The same experimental analysis on two OS makes the research more precise and authentic when verification from more than one source. So moving towards the investigation.

4.3 Investigation in Kali Linux

First, we are extracting the shreds of evidence in the kali Linux lab the required shreds evidence. Let's start with extracting the history of the browser by running the dumpzilla. Starting with dumpzilla

From Figure 3, we can see the interface of dumpzilla and how it makes our work easy. To get the best use of these tools in investigation, an investigator must acquire

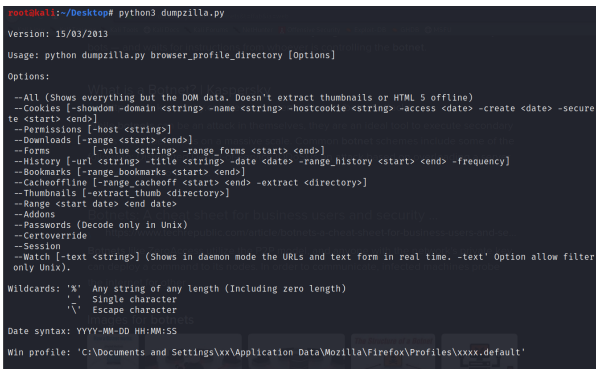

Figure 3: CLI view of Dumpzilla

Figure 4: Mozilla profile

the sound knowledge and hands-on command on Linux usage. Linux gives many utilities over windows, but this is not the discussion of this research. In the interface, it has been seen that the tools instruct extracting the data. Starting with history extraction, we have to locate the browser default file hidden in the system then run that file on forensics investigation. In Figure 4, we get into the directory to locate the default file of the browser.

By running some simple commands on Linux, the investigator's life becomes more accessible and he gets into the default file of the browser from the victim machine. Now, this critical file is to be used in leading the investigation towards predicting the browsing activity of the malicious user.

By getting the comprehensive data, we run the command –All to get complete information about the browser then get step by step into it. The process is shown in Figure 5.

Summarizing the above-collected data information we have got the overall scenario of how much the browser is exploited. So, in Table 2 have a summary of gathered

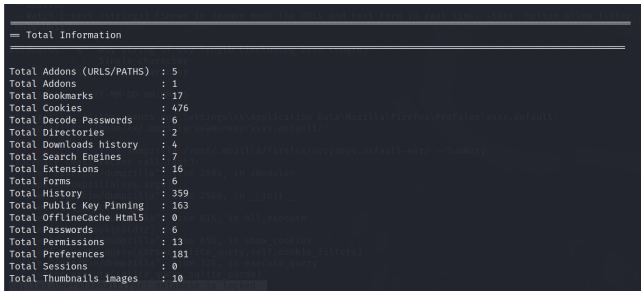

Figure 5: Summary of fetched data

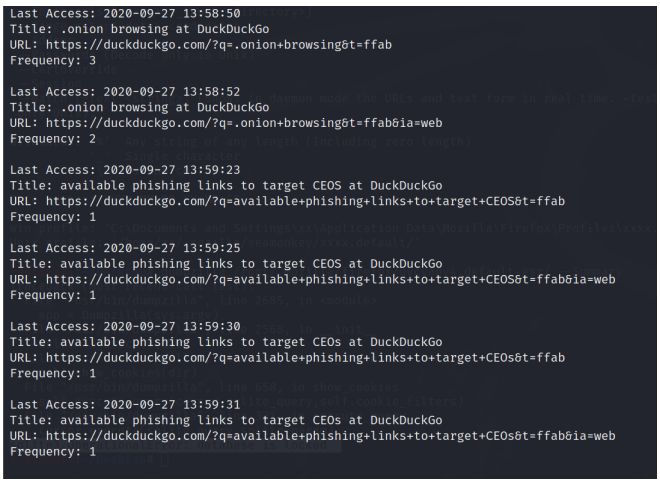

Figure 6: Extracted history

information.

Table 2: Summarized extracted data

Evidence	Frequency of Data
Cookies	290
Passwords Decode	0 (no Saved Passwords)
URLs	116 saved URLs
Sessions	0
Add-ons	0
Bookmarks	10

Now we have moved towards the step-by-step extraction of all the shreds of evidence collected. From above, the frequency of traces of evidence collected now by looking deep into that, the required piece of data is sorted out in coming steps. Moving towards history first. An extracted record is shown in Figure 6.

The figures mentioned above contain all the details about browser history, after deeply analyzing the history details gathered from previous suspicious activities, it has been found that the malicious internal user has tried to make identity anonymous by using Tor browsing and tries to learn about the phishing attacks to trap the company's CEO (mostly they are non-technical people and seldom care about such things). Also, he is continuously surfing to find out ways of accessing the dark web that might exploit the department's PCs for unfair means and activities. Summarizing the history details in Table 3.

From the above tabular data of historical details, the internal malicious user continuously searches the malicious things dark web, phishing, and techniques to install malware and Trojans. On the basis of these searches found from the victim machine, the same data was extracted from the other PCs of the department, and after that, we will compare and analyze to find out who is the real culprit who used someone else computer to exploit the data and for malicious and illegal activities. From cap-

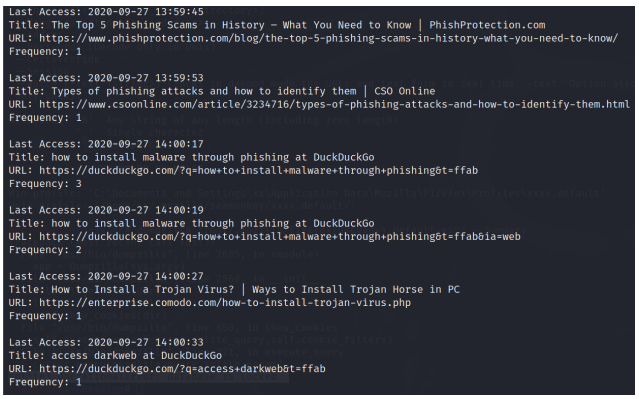

Figure 7: Extracted cookies

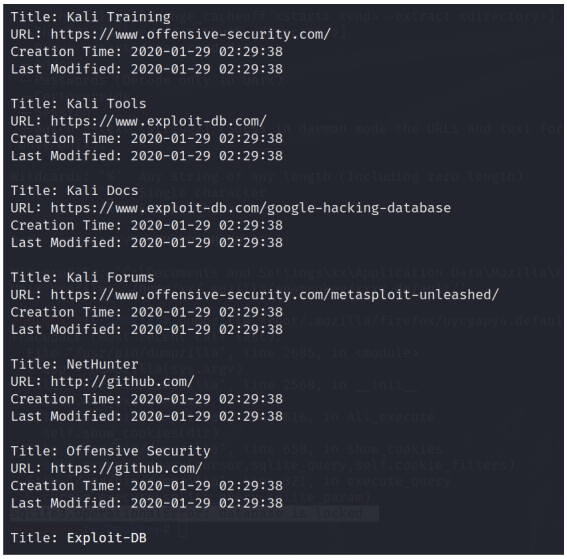

Figure 8: Extracted bookmarks

turing the Tor browser access from the history, it's been confirmed that the malicious user has actions on "Dark Web"; otherwise, nobody needs a Tor browser for any fair method. It has been concluded that he might be selling enterprise's sensitive data to some black hat hackers on the Dark Web. But this can be done when the culprit is being caught then police and investigation agencies will take care of it. Now let's move towards the cookies extraction in Figure 7.

From cookies extraction, it gives us the complete details about the browser activity. It provides the details about the sessions created, domain name, hostname, expiry whether it HTTP or HTTPS its value and all this information from the vanished computer helps a lot in leading the research and closing the case for final analysis now moving towards the bookmarks saved. Extracting and summarizing bookmarks in Figure 8.

It can see the bookmark's details that the malicious user has activities on the tor browser. Now it's sure that he has some linkages on the dark web and might be selling companies sensitive on illegal websites. To further verify shreds of evidence collected and count the emails present

Figure 9: Extracted add-ons

Figure 10: Extracted sessions

in the browser, another tool, "Bulk Extractor" is used for further investigation.

Now moving towards the Addons, Passwords, Thumbnails and further data extraction is shown in Figures 9, 10, & 11.

Now for the Bulk extractor, it can use in terminal mode, and it also provides GUI for the extraction of data. First, let's launch the Bulk extractor, which is shown in Figure 12.

Here adopting the methods of experts, the tool is utilized in the terminal and command line to run the investigation. In this tool, there are utilities in which it creates a whole folder for the directories and all the shreds of evidence it has collected from the victim machine. Starting with Bulk extractor shown in Figure 13.

Here the data extracted from the browser is saved in the folder created by the Bulk extractor (see Figure 14). This tool provides the extracted data from the file directory and keeps it in a folder created. It can also scan the image files, but here in this research, the approach is to get the file directory for investigation. The above also concluded that it has been found from vanished data that 491 Email features were present there. Here the folder created "Case-1-internal_threat", which contains all the data collected from the file directory, and it also has SQLite auxiliary file for further verification of shreds of evidence. The given snapshot gives details about the files created

Table 3: History details

Title	URL	Date and Time	Frequency
.onion browsing at DuckDuckGo	https://duckduckgo.com/?q=.onion+browsingt=ffab	2020-09-27 13:58:50	3
phishing links to target CEOs	https://duckduckgo.com/?q=available+phishing+links+to+target+CEOSt=ffab	2020-09-27 13:59:23	1
Top 5 Phishing Scams in History	https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/	2020-09-27 13:59:45	1
how to install malware	https://duckduckgo.com/?q=how+to+install+malware+through+phishingt=ffab	2020-09-27 14:00:17	3
How to Install a Trojan Virus?	https://enterprise.comodo.com/how-to-install-trojan-virus.php	2020-09-27 14:00:27	1
access darkweb	https://duckduckgo.com/?q=access+darkwebt=ffab	2020-09-27 14:00:33	1

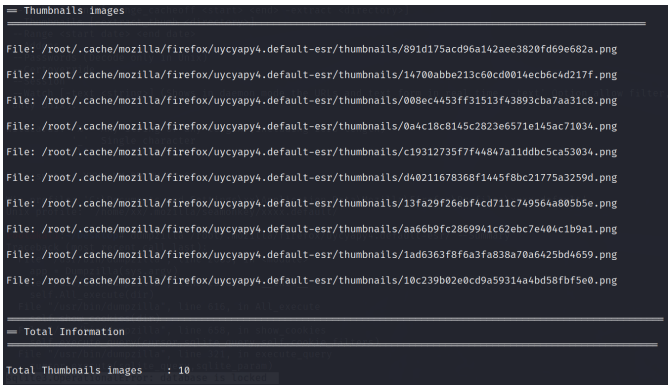

Figure 11: Extracted bookmarks

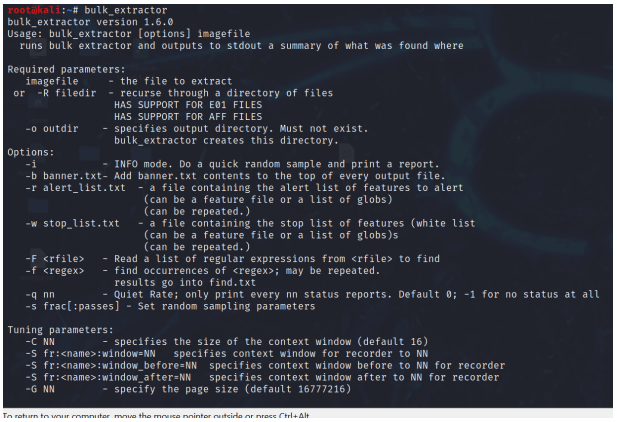

Figure 12: Bulk extractor CLI view

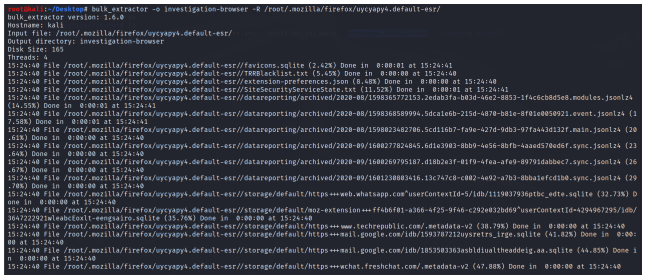

Figure 13: Bulk extractor performing data extraction

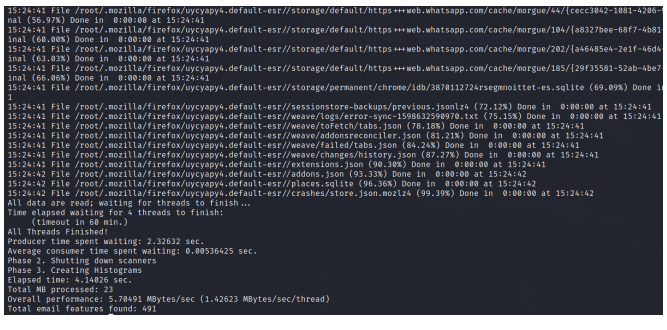

Figure 14: Bulk extractor data

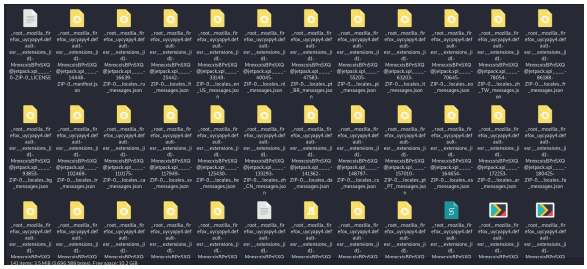

Figure 15: Folder created by bulk extractor

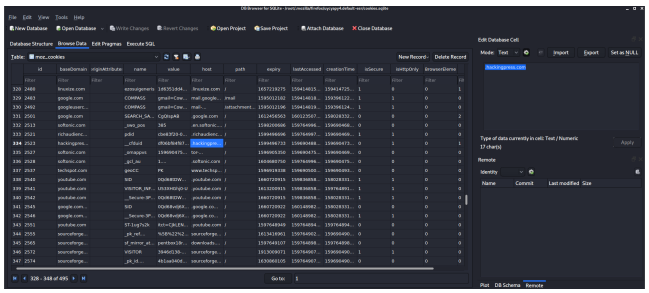

Figure 16: Data of SQLite DB

in folders shown in Figure 15.

Here from the above screenshot, it can be seen that there is the extension (add-ons) of the privacy modes of web browser that is been missed by the dumpzilla. Also with this tool, the shreds of evidence are authenticated and provide us all the details, and helps in compiling all the data. Now with auxiliary SQLite DB browser, we get some information as Bulk extractor also saves data in the files of SQLite database, shown in Figure 16.

By seeing the details on the database created by the SQLite, it gives all the necessary information which was created by the Bulk extractor. Here as focusing on the cookies in Figure 17, many of them are captured for leading the investigation.

The dumpzilla missed this extension information, but the auxiliary database of SQLite is recovered. Ending this discussion here that in the forensic lab setup different tools are utilized to get the data identified from the related study. First dumpzilla is utilized to collect the important evidences and mentioned above. Then Bulk extractor is used to get the information that the dumpzilla

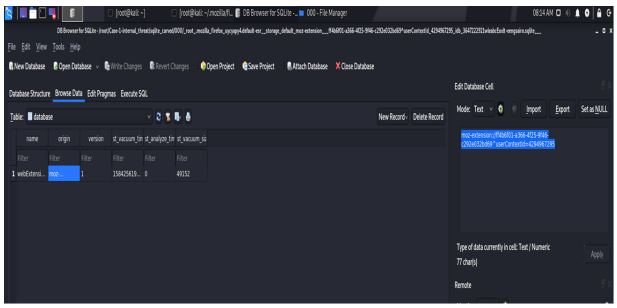

Figure 17: Data analytics from SQLite DB

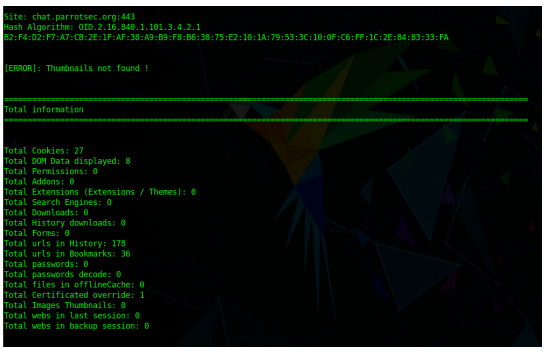

Figure 18: Total information gathered in Parrot OS

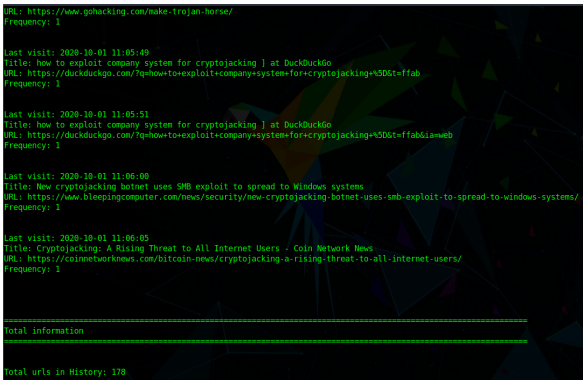

Figure 19: History extraction in Parrot

cannot trace. It not only extract the evidence but also gives the log data in the folder. Then SQLite data base is utilized to get the details about the cookies and the extension that missed by dumpzilla.

As far as the precious information is gathered from utilizing the tools of digital forensics in the previous section. Now comes the part of analysis and authentication of these factors and evidence. For making the investigation precise, the same tools and techniques are run on another operating system, the "Parrot". Parrot Security OS is also a compatible system for penetration testing and digital forensics research. It's the competitor of Kali Linux here in this research it is utilized to get authentication of all the gathered data and evidences. The same investigation is run on parrot OS.

4.4 Investigation in Parrot OS

Starting with the Parrot OS, it's also linux system that has debian system. Provides many tools for ethical hacking as well as digital forensics. The same dumpzilla is run on Parrot to get the results and compare with the results of Kali to verify the evidence collected. Staring with the extraction of history and then compare the results for authentication. Attaching the history snapshot from parrot OS in Figure 18.

As mentioned above in Figure 19, Parrot extracts the same results from the Kali Linux by the dumpzilla. Now summarize the results from both Kali Linux and Parrot

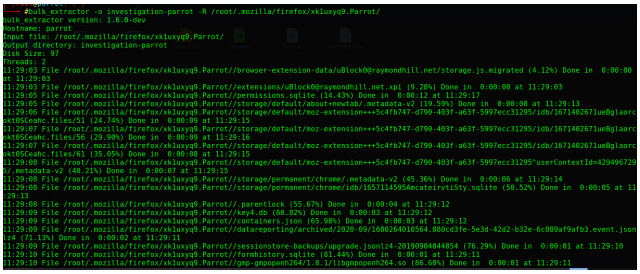

Figure 20: Bulk extractor CLI view in Parrot

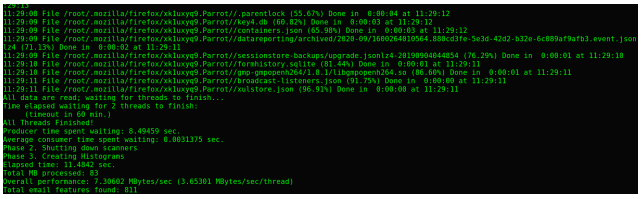

Figure 21: Bulk extractor data extraction

is as in Table 4.

Table 4: Analysis of evidence extraction from both OS

Kali Linux	Parrot Security OS
.onion routing	Trojan Horse Installation
tor browser	Exploiting enterprise Database
Phishing attacks to target company CEOs	Access Dark web with tor browser
Malware installation	Phishing attacks to target company CEOs
Exploit company machine	Cryptojacking
Darkweb	Tor browser

From the above comparative analysis, it shows that the results are almost the same. Duplicate history titles have been extracted from both Kali Linux and Parrot Security OS. After getting the same effect of accessing Tor browser and exploiting enterprise databases and botnets. It has been confirmed that the internal malicious user has some connections with dark web users and tries to sell the company's sensitive data on the dark web. Now dumpzilla comparison is verified, moving towards the comparison of bulk extractor results. The same Bulk extractor tool is run on Parrot to find out the email features that were missed from the dumpzilla. In Figures 20 and 21 shows the result of Bulk extractor.

Analyzing the above, it's found out that there might be some glitch in dumpzilla running on Kali Linux because it has missed the count of verified emails from here. Now check the folder that is the key feature of Bulk extractor that it creates a folder and log all the files of the directory. The attached snip of Figure 22, the folder created by the Bulk extractor in Parrot:

Here it can be seen that the Bulk extractor in Parrot might have missed the extensions that it has captured

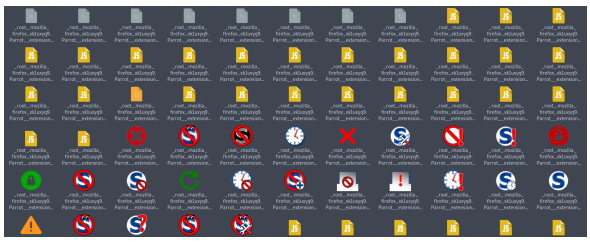

Figure 22: Folder created by Bulk extractor

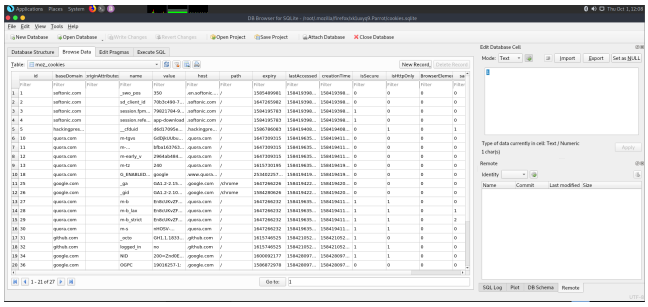

Figure 23: SQLite DB browser data

in Kali Linux. Comparing both and getting verified step by step, some glitches in running tools on the different operating systems are missing evidence. But running the same tool on different platforms gives us the advantage of covering each other's drawbacks. Like if dumpzilla missed any evidence Bulk extractor captured it, and so on. Now the last step is to get the auxiliary information of the SQLite database browser, which keeps the log of all files of the browser is shown in Figure 23.

It can be seen that SQLite Db in Parrot did not capture all the cookies as it logs the details of cookies so here, Kali Linux overcomes the Parrot gives verified details of the Cookies, which helps in leading the investigation.

In concluding the experimental analysis chapter, there is a need to mention the importance of web browser forensics in digital forensics again. Every cyber-criminal activity starts with the web browser because it is the gateway to get anywhere on the internet, especially in the dark web. From the related study, the authors are going in various directions. In contrast, after a thorough study, it is found that these different skills might be a problem for investigators as most of them are not experienced in programming. So, this research adopts the approach of utilizing digital forensics tools to get the identified outcome or variables. Then comes the problem of authentication and verification of tools results. For this purpose, the same tools run on two different platforms in Kali Linux and in Parrot OS. In analyzing and comparing the results, some things are missed by tools in Kali that are overcome by the same tool when it runs on Parrot and vice versa. In the end the experiment becomes successful in extracting data Cookies, URLs, history details, etc. The same information is gathered from the other computers of the department is extracted, and results are compared if the browsing activity of computer slangs been matched, then

the culprit is caught in the virtual scenario who have exploited the browser.

5 Observations and Key Findings

In light of all the results from the experimental analysis, it's been observed that malicious users exploited the browser. By following the history extracted from the victim machine, it's been observed that the user continuously tried to access the dark web from inside the department. Based on these browsing activities it can easily be observed the malicious intentions of the user. The script of dumpzilla written on python is designed on the basis of access control. There is different access of different features and directories of machine. If there are rights from admin, only superuser or admin can add or delete if there is user login on the machine than user cannot install or delete program inside the machine. A US patent (United States Patent No. US10579995B2, 2020) Elaborated about the access control in which the device's utility is extended by allowing the user to get full access of the device. This can become the reason of exploitation because the system administrator allows the maximum access to increase the utilities and boost up the performance of work from the employee. But this also questions the security of the system. If the administrator allows some of its access rights to the users or employees, it jeopardizes the security. No mechanism can find the malicious intentions of the user. In this case, this maximum access control becomes the vulnerability of the system's security, and the user exploited the browser exploiting his full access to the sites. The SA should harden the system according to the standard operation of procedures (SOPs) by the vendor whose devices are being used by the enterprise. If the department is using windows server 2016 than the system administrator should follow all the SoPs for hardening of server as provided by Microsoft (Microsoft, 2017). In most digital forensics cases, it's been coming out in the investigation that there is no following of the SoPs for hardening the system administrator system. Thus, this carelessness most of the time from IT department becomes a vulnerability. This, when being exploited by someone inside becomes the risk and ends up in losing a lot of sensitive data and private information. As discussed by the (Zang, 2019), machine learning-based systems detect suspicious behaviour from internal users based on denoising autoencoders. As this is not the domain of this research but giving this suggestion based on related study and from the experimental analysis, the main reason that leads towards the exploitation of web browser is not following the SoPs for the hardening of the system.

Digital forensics comes at the part of auditing and investigating of the systems and databases. As this research is conducted on the virtual environment in which browser is being exploited and investigation is conducted to find out the evidence which is being analyzed to predict the linkages of malicious user in the dark web, this finding leads to further investigation to the malicious user. In light of related study and results from the experimental analysis, the key findings are being summarized as follow:

- The major finding is the weakness in the systems. In many enterprises most of the systems are not properly hardened which leads vulnerability and after that it is exploited by the internal malicious user.
- The script of Dumpzilla is written in python, which focused on the access control techniques. Although there is logging of all the browsing activity data in the system hard drive which can be extracted by utilizing disk image extractor method or by getting files through directories.
- Disk image method may fails when the disk is damaged. But here in this research directory of file gives the advantage as it locates the exact position of data stored in the hard drive to extract the evidences like history URLs, cookies, extensions, add-ons despite the fact that the web browser data is being vanished.
- There might be some data that is being missed by the Dumpzilla so another tool bulk extractor is used in assistance of main tool.
- Bulk extractor tool not only provides the utility of extracting evidences but also it makes the case folder in which it saves all the evidences.
- Than SQLite browser that saves all the browsing gives some auxiliary information about the evidences.
- For checking the authenticity and verification of the evidences collected, the same tools are run on two different platforms Kali Linux and Parrot Security OS.

It's been found out that both platforms provide different utilities, while comparing the data gathered it almost the same but there are some limitations that Bulk extractor missed some files in running on Parrot as compare to Kali.

6 Conclusion and Discussion

In the process of this research, first, we did the theoretical implementation. Relevant papers, articles, book sections that are readily available on the internet is studied to identify the research problem. In this qualitative part of the research, previous studies' findings include email forensics that gives information about phishing attacks. This phishing was exploiting the user machine by using it resources. There is a discussion on web browser forensics that most authors extract artefacts and evidence with different techniques, as mentioned in the related study portion. These studies provide the various ways of extracting the same data, collecting data from previous research, and analyzing the details; this research goes with finding the

simple method for extracting the evidence. Also, there is a discussion of legal and technical aspects of digital forensics that an investigator must be aware off.

After identifying the research problem in an organization, an internal malicious user leaked the confidential information on the web by exploiting the browser and deleted all his/her footprints. For that purpose, a forensics investigation needs to extract all the evidence like history, cookies and saved passwords from the cloud space provided by the browser. So, an experimental setup is being arranged in a virtual environment. The lab is set up in two different Kali Linux and Parrot Security OS platforms for the quantitative part. The forensics tools like dumpzilla and bulk extractors are used. SQLite database is used in auxiliary with these tools to get the required information. The target data to capture is History, URLs, Cookies, Sessions, Add-ons, Extensions, etc. Two different platforms were used to verify the authenticity of the evidence collected. The dumpzilla is missing some data and bulk extractor in Kali, and some is missed when the same tools run on Parrot OS. So in this way both platforms fills each other's gaps that arise in research. After that the mixed method research is completely conducted when the data from the victim machine is being matched with another machine and the user of that machine is being captured for further investigation

6.1 Contributions of Research

As discussed earlier in chapter three that research can go in both ways. Either it leads to the solution of identified problem via procedural steps (may be qualitative or quantitative or both). In this type the solution acquired from the study or experimental results is the contribution of the research. In other words, after identifying the problem when the procedural steps, tools and suggested techniques do not lead towards the required solution. It still considers contribution because the authors saved the time of other researchers by giving a vast literature review and guide about the path to save the time of other researchers.

This research is being adopted and going with the mixed method. The main contribution is providing the path for leading the digital forensics investigation with the help of tools including dumpzilla, Bulk extractor, and SQLite database browser. After identifying the problem with the related study, it's been said that the browser is the gateway for the whole internet. Where you want to go on the internet, the gate is from the web browser. So browser is the most vulnerable part it needs to be secured. A virtual environment is set up in which a scenario is created where a machine's browser exploits malicious activity. To verify results were generated from the experimental analysis, the same tools are running on two different platforms, and the results are analyzed. The major contribution is finding out the carelessness of enterprises that they do not follow the standard operational procedures for hardening systems. Summarizing the contributions as in Table 5.

Table 5: Contributions of research

Contributions	Type of Study
Enterprise not following the SoPs for system hardening	Qualitative and Quantitative
Dumpzilla script focused to get the root access in the system	Quantitative
Providing solution with utilizing tools of digital forensics	Qualitative
Authenticating evidences by running tools on different platforms	Quantitative

6.2 Conclusion

In concluding all the research discussed in the research, it is supposed that web browser forensics has sound importance in digital forensics research. As mentioned in a related study, discussing work on authors is from using browser forensic tool, running browser forensics on the android toolkit, and suggesting techniques on avoiding phishing attacks via emails to the legal and technical aspects of digital forensics research. All this done in the qualitative part of the research identifies the importance of browser forensics and identifies the problems in running an investigation. After a thorough study of the related articles, this research approach utilizing digital forensics tools dumpzilla, Bulk extractor and SQLite were selected for analysis. In the quantitative part, a virtual environment was set up, moving with the assumption that the investigators traced the victim machine's IP while reaching that machine. The web-browser data is vanished by the malicious user. Then investigation runs on two different platforms including Kali Linux and Parrot Security OS to authenticate the evidence collected from the experimental analyses. The data collected from all the devices in the department then it's compared. The culprit is caught when the victim machine's data was matched with the PC in the department, and the user is caught for further investigation. It has also been found out that the main vulnerability is the enterprise not following the standard operating procedures for system hardening.

6.3 Limitations of Study

Every research has limitations, in this research so far it has achieved the targets of extraction of data from the web browser. But the tools has its limitations like in conducting the investigation dumpzilla has missed the extensions saved in the browsers. Although these extensions get extracted by the Bulk extractor, it still did not extract all the saved extensions. Also, the SQLite has missed some

URLs that being visited by the malicious user. Also, there are still many ways to get this research conducted as it can be more study of related articles.

6.4 Scope of Future Work

In the future study of this research, there is scope for good python programmers and computer experts who are aware of the software architecture and the architecture of operating systems. Also, research in access control is required as this research focuses on getting deep into the system to extract the evidence. A good python programmer makes the script of an existing tool more improved, plus the sound knowledge of operating systems and access control can penetrate deep into the systems. With the combination of all these, research can be conducted on the weaknesses of dumpzilla, and bulk extractors and new tools can be developed that can do similar tasks better.

References

[1] E. Akbal, F. Günes, A. Akbal, " Digital forensic analyses of web browser records," *Journal of Software*, vol. 11, no. 7, pp. 631—637, 2016.

[2] M. Asim, M. F. Amjad, W. Iqbal, H. Afzal, H. Abbas, Y. Zhang, "AndroKit: A toolkit for forensics analysis of web browsers on android platform," *Future Generation Computer Systems*, vol. 94, pp. 781-794, 2018.

[3] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, I. Mavridis, "D41 - Digital forensics framework for reviewing and investigating cyber attacks," *Array*, vol. 5, pp. 22-31, 2020.

[4] H. Graeme, " Part 1: Quality assurance mechanisms for digital forensic investigations: Introducing the Verification of Digital Evidence (VODE) framework," *Forensics Science International: Reports*, vol. 2, pp. 123-133, 2020.

[5] G. Horsman, B. Findlay, J. Edwick, A. Asquith, K. Swannell, D. Fisher, P. McKain, " A forensic examination of web browser privacy-modes," *Forensic Science International: Reports* , vol. 1, pp. 22-29, 2019.

[6] N. A. Hassan, "Web browser and e-mail forensics," in *Digital Forensics Basics*, pp. 247–289, 2019.

[7] M. R. Jadhav, B. B. Meshram, "Web browser forensics for detecting user activities," *International Research Journal of Engineering and Technology*, vol. 5, no. 7, pp. 273—279, 2018.

[8] A. A. Jillepalli, de Leon, D. Conte, S. Steiner, J. Alves-Foss, "Analysis of Web Browsing Security Configuration Options," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 12, pp. 6139—6160, 2018.

[9] K. Parsons, M. Butavicius, P. Delfabbro, M. Lillie, " Predicting susceptibility to social influence in phishing emails," *International Journal of Human-Computer Studies*, vol. 128, pp. 17—26, 2019.

[10] A. Kharraz, Z. Ma, P. Murley, C. Lever, J. Mason, A. Miller, M. Bailey, "Outguard: Detecting in-browser covert cryptocurrency mining in the wild," in *The World Wide Web Conference*, pp. 840—852, 2019.

[11] Y. Kwak, S. Lee, A. Damiano, A. Vishwanath, "Why do users not report spear phishing emails?," *Telematics and Informatics*, vol, 48, 2020.

[12] S. Mahaju, T. Atkison, " Evaluation of firefox browser forensics tools," in *Proceedings of the South-East Conference* , pp. 5—12, 2017.

[13] N. Mays, C. Pope, "Quality in qualitative research," *Qualitative Research in Health Care*, Chap. 15. pp. 211-233, 2019. (`https://doi.org/10.1002/9781119410867.ch15`)

[14] M. Munir, P. Leimich, W. J. Buchanan, "A forensic audit of the tor browser bundle," *Digital Investigation*, vol. 29, pp. 118-128, 2019.

[15] A. Nalawade, S. Bharne, V. Mane, " Forensic analysis and evidence collection for web browser activity," in *International Conference on Automatic Control and Dynamic Optimization Techniques*, pp. 518—522, 2016.

[16] F. Paligu, A. Kumar, H. Cho, C. Varol, "BrowSt-Explus: A tool to aggregate IndexedDB artifacts for forensic analysis." *Journal of Forensics Science*, vol. 64, no. 5, pp. 1370—1378, 2019.

[17] R. Parkavi, S. Anitha, R. Gayathri, *Digital Steganography Security*, Critical Concepts, Standards, and Techniques in Cyber Forensics, *IGI Global*, pp. 33-41, 2020.

[18] C. Parulekar, " Minimize phishing attacks: Securing spear attacks," *International Research Journal of Engineering and Technology*, vol. 6, no. 6, pp. 3054-3058, 2019.

[19] J. S. Queiroz, E. L. Feitosa, "A web browser fingerprinting method based on web audio API," *The Computer Journal*, vol. 62, no. 8, pp. 1106—1120, 2019.

[20] A. Reed, M. Scanlon, N. An Le-Khac, " Private Web Browser Forensics: A Case Study of the Epic Privacy Browser," *arXiv preprint arXiv:1708.01732*, 2017.

[21] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, S. Egelman, "An experience sampling study of user reactions to browser warnings in the field," in *Proceedings of the 2018 CHI conference on human factors in computing systems*, pp. 1—13, 2018.

[22] N. Shafqat, "Forensic investigation of user's web activity on google chrome," *International Journal of Computer Science and Network Security*, vol. 1, pp. 67-75, 2016.

[23] P. Snyder, C. Taylor, C. Kanich, "Most websites don't need to vibrate: A cost-benefit approach to improving browser security," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 179-194, 2018.

[24] Y. U. Sonmez, A. Varol, "Legal and technical aspects of web forensics," in *7th International Symposium on*

Digital Forensics and Security (ISDFS'19), pp. 1—7, 2019.

[25] X. Zhang, T. T. Yuen, K. K. R. Choo, "Experiential learning in digital forensics," in *Digital Forensic Education*, Springer, pp. 1–9, 2020.

Biography

Sirajuddin Qureshi received his bachelor's degree in Computer Sciences from Quaid-e-Awam University of Engineering, Science & Technology, Pakistan. Afterwards, he pursued his Master's in Information Technology from Sindh Agricultural University Tandojam, Pakistan. Currently he is pursuing PhD in Information Technology at Beijing University of Technology, China. He has nine research publications to his credit as main author and co-author, which featured national and international journals and conferences. Sirajuddin's research areas includes but not limited to Network Forensics Analysis, Digital Forensics, Cyber security, Computer Networks and Network Security.

Jingsha He received the bachelor's degree in computer science from Xi'an Jiaotong University, China, and the master's and Ph.D. degrees in computer engineering from the University of Maryland, College Park, MD, USA. He worked for several multinational companies in USA, including IBM Corp., MCI Communications Corp., and Fujitsu Laboratories. He is currently a Professor with the Faculty of Information Technology, Beijing University of Technology (BJUT), Beijing. He has published more than ten articles. He holds 12 U.S. patents. Since August 2003, he has been published over 300 papers in scholarly journals and international conferences. He also holds over 84 patents and 57 software copyrights in China and authored nine books. He was a principal investigator of more than 40 research and development projects. His research interests include information security, wireless networks, and digital forensics.

Saima Tunio received the BSIT (Hons) with gold medal from Sindh Agricture University Tandojam, Pakistan. Afterwards, she pursued her MSIT from Isra University Hyderabad, Pakistan. Currently she is pursuing PhD in Information Technology at Beijing University of Technology, China.She has more than five research publications to her credit as main author and co-author, which featured national and international journals and conferences. Saima's research areas includes but not limited to Information security.IoT security, Digital Forensics, Cyber security, Computer Networks.

Nafei Zhe received the B.S. and M.S. degrees from Central South University, China, in 2003 and 2006, respectively, and the Ph.D. degree in com- puter science and technology from the Beijing University of Technology, Beijing, China, in 2012. She was a Postdoctoral Research Fellow with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, from 2015 to 2017. She is currently an Associate Professor with the Faculty of Information Technology, Beijing University of Technology. She has published over 20 research papers in scholarly journals and international conferences. Her research interests include information security and privacy, wireless communications, and network measurement.

Faheem Akhtar received his Ph.D.degree from the Beijing University of Technology, China,in 2020.He is currently working as an Assistant Professor with the Department of Computer Science, Sukkur IBA University, Pakistan.He is the author of various SCI, EI, and Scopus indexed journals and international conferences.He is part of various indexed international conference at different positions and a Reviewer of various SCI, EI, and Scopus indexed journal. His research interests include data mining, machine learning, deep learning, information retrieval, privacy protection, Internet security, the Internet of Things, and big data.

Faheem Ullah received the M.S degrees from the Xian Jiaotong University, China,in 2017. He is currently pursuing the Ph.D. degree with the Beijing University of Technology, Beijing, China. His research interests include information security, Blockchain and data mining. He has received awards and honors from the China Scholarship Council (CSC), China.

Ahsan Nazir has received his M.Sc degree from University of Engineering and Technology Lahore in 2016. From September 2015 to August 2018 he worked as software Engineer at Dunya Media group Lahore since September 2018 he is doing PhD in Software Engineering from Beijing University of Technology , Beijing China. He has published more than 10 journals and conference papers.His area of research include eGovernment,IoT,Software Engineering and Machine learning applications.

Ahsan Wajahat received the B.S. and M.S degrees in information technology from the Sindh agriculture University, Pakistan, in 2012 and 2016, respectively. He is currently pursuing the Ph.D. degree with the Beijing University of Technology, Beijing, China. His research interests include machine learning, information security, forensic network and data mining. He has received awards and honors from the China Scholarship Council (CSC), China.