Evaluating the Efficiency of FTK, Autopsy, and Mobile Forensic Tools: A Comparative Study in Criminal Investigations

Victor Agboola, Jude Osamor, Funminiyi Olajide
School of Computer Science and Engineering
University of Westminster
UK

Abstract

In today's criminal investigations, digital forensics is essential because it can retrieve, analyse, and display digital evidence from a variety of devices, including computers, network systems, and cell phones. As digital data grows exponentially and cybercrimes get more complicated, there is a greater need than ever for effective and trustworthy forensic tools. Forensic Toolkit (FTK), Autopsy, and Cellebrite are three popular forensic programs that are thoroughly compared in this study. The usefulness of these technologies in real-world criminal investigations is the main emphasis of the study, which assesses them on the basis of usability, cost-effectiveness, performance, and functionality. Both qualitative and quantitative analysis are used in the process, and the instruments' use in a well-known criminal case is highlighted in a case study of the Silk Road investigation. While each tool has strengths in specific areas Autopsy's open-source adaptability, FTK's extensive data processing, and Cellebrite's mobile forensics key findings show that they also have drawbacks when it comes to managing the range of digital evidence sources and cross-platform interaction. In order to tackle the challenges presented by the changing digital ecosystem, the study emphasises the necessity of continuous improvements in forensic tools, specifically in improving interoperability and data fusion capabilities. Law enforcement and forensic experts are given advice, with a focus on the significance of choosing the appropriate instrument for a certain investigative task. Enhancing cross-platform compatibility and investigating novel methods for digital forensics should be the main goals of future research.

Keywords: Criminal Investigations, Autopsy, Law Enforcement, FTK, Digital Forensics, Mobile Forensics.

1. Introduction

Digital forensics is a subfield of forensic science that studies the identification, preservation, analysis, and presentation of digital evidence. As the world gets more digitised, the scope and importance of digital forensics have expanded dramatically. The discipline is critical for investigating crimes involving digital devices and networks, like as cybercrime, fraud, and even classic crimes requiring digital proof. Digital forensics is the process of unearthing and evaluating electronic material for use in a court of law. The purpose is to preserve any evidence in its most original form while conducting a methodical investigation by gathering, identifying, and validating digital data to reconstruct historical occurrences. This procedure assures that the evidence gathered is acceptable in court and meets the rigorous standards of judicial scrutiny. Digital forensics' relevance is demonstrated by its use in a variety of industries, including law enforcement, corporate investigations, and cybersecurity. Law enforcement agencies use digital forensics to investigate crimes ranging from cyber-attacks to terrorism. Corporations utilise it to investigate security breaches and intellectual property theft, while cybersecurity professionals use forensic techniques to better understand and mitigate security issues. [1]

Effective digital forensics is required for criminal investigations because of the widespread use of digital devices and the substantial amount of data they generate, which may be essential for e-disclosure and e-discovery in court proceedings. The recovery, analysis, and presentation of digital evidence gathered from various devices, such as computers, cell phones, VoIP systems, and social media networks, are all included in the field of digital forensics. Digital forensics is now an essential area of study in modern criminal investigations because to the growing prevalence of digital devices and the internet. It is necessary to identify, preserve, assess, and present digital evidence. Investigating technology crimes requires this field of study. Digital forensics encompasses numerous sub-disciplines, including computer forensics, mobile device forensics, network forensics, and others. This field is crucial for locating digital footprints that could be crucial evidence in court. The primary objectives of this study are to examine the different criminal components of information that can be extracted from digital evidence and to compare the most significant

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

forensic tools. The study will focus on mobile forensic tools like Cellebrite and XRY as well as popular desktop forensic programs like Forensic Toolkit (FTK) and Autopsy. The research aims to evaluate these technologies to determine their efficacy, efficiency, and suitability for use in different forensic circumstances (see Figure 1): [2]

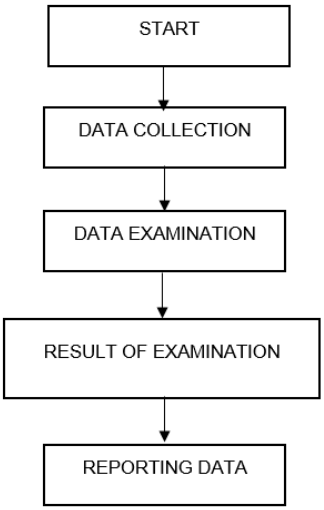

Figure 1. Flow of Digital Forensic Process

The functional capabilities of each tool, performance parameters including processing speed and data recovery accuracy, cost-benefit ratios, user experience, and their real-world applications are all important components of our review. Using a mixed-methods approach, the study will examine how well the tools function in actual situations by focusing on case studies and integrating real-world testing through User Acceptance Testing (UAT). The outcomes of this study will play a crucial role in furnishing law enforcement authorities and forensic experts with invaluable perspectives regarding the most appropriate instruments for digital forensic inquiries. Regarding the instruments, they employ to process forensic evidence, the study seeks to assist these practitioners in making knowledgeable choices. One cannot stress the significance of digital forensics in today's world. In criminal investigations, digital evidence frequently plays a crucial role by offering vital details that can help identify and prosecute offenders. The proliferation of cybercrime, encompassing identity theft, hacking, and online fraud, has rendered digital forensics an essential instrument for law enforcement authorities across the globe. Digital forensics is essential not only for resolving cybercrimes but also for conventional criminal cases using digital equipment. For example, GPS data, text messages, and call logs can all be found on mobile phones and provide crucial information about the whereabouts and intentions of a suspect. Similar to this, computers can contain information that can be used to incriminate a person, such as emails, documents, and internet browsing history.

In today's criminal investigations, digital forensics is vital. It gives detectives the instruments and methods they need to find lost or concealed data, track down illegal activity, and create chronologies of occurrences. In many different types of cases, such as cybercrimes, fraud, theft of intellectual property, and violent crimes, digital evidence can be crucial. To guarantee the dependability and credibility of digital evidence through Provenance Trust-Based Systems, the research will also investigate the applicability of the findings to forensically relevant evidence presentation in court.

2. Literature Review

In the field of criminal investigations, digital forensics has become an essential discipline, especially given the 21st century's pervasive digital revolution. Effective forensic tools are becoming more and more necessary in order to recover, examine, and display digital evidence as criminal activity moves more and more to digital platforms. Numerous tools have been developed during the course of digital forensics, each with a unique purpose in mind to handle the issues presented by various forms of digital evidence. This chapter offers a thorough analysis of the research on digital forensics with a particular emphasis on the three technologies used in this investigation: Cellebrite, Autopsy, and the Forensic Toolkit (FTK). In order to demonstrate the usefulness of these instruments in a real-world setting, the paper also provides a thorough analysis of the Silk Road investigation.

In the field of digital forensics, evidence discovered on digital devices is recovered and examined; this material is frequently connected to computer crimes. The prevalence of digital devices has led to a rise in the significance of digital forensics in criminal investigations. Computer forensics, mobile device forensics, network forensics, and forensic data analysis are some of the sub-disciplines that fall under the umbrella of digital forensics. The use of digital forensic tools is essential for carrying out exhaustive and effective investigations. These resources support the collection, storage, processing, and display of data. Of all the programs available, Forensic Toolkit (FTK), Autopsy, and Cellebrite are the most widely used and have the most powerful features [5].

Several factors, including as functional capabilities, performance, cost-benefit ratio, user experience, and real-world applications, can be used to assess the efficacy of digital forensic tools. This criterion evaluates each tool's feature set and available functionality. FTK is renowned for its

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

robust processing capabilities and broad file system support, which make it appropriate for intricate investigations. Despite being open-source, Autopsy has a feature set as extensive as many programs that are sold. Experts in mobile forensics, Cellebrite and XRY offer sophisticated data extraction methods that are vital for mobile device examinations.

For many organisations, the expense of forensic equipment is a major consideration. Although FTK is a commercial tool, its extensive features and support make it well worth the expense for many agencies. Being an open-source program, Autopsy provides a less expensive option without sacrificing many features. Even though they are pricey, Cellebrite and XRY offer vital features for mobile forensics that make them worth the money in many cases. System resource utilisation, data recovery accuracy, and processing speed are examples of performance measures. Research indicates that FTK's remarkable performance with huge datasets is a result of its effective indexing and searching algorithms [16]. Even if it works well, Autopsy might not be as performant as FTK when processing extremely huge amounts of data. Known for their quick data extraction times and high accuracy rates, Cellebrite and XRY are designed with mobile devices in mind [6].

Support, interface design, and usability are all parts of the user experience. FTK is commended for both its comprehensive documentation and user-friendly interface. Users of different skill levels can utilise Autopsy because of its intuitive user interface. XRY and Cellebrite provide forensic examiners with comprehensive support resources and simplified interfaces. Applications with a practical focus evaluate the tools' performance in real-world situations. Cybercrime cases, corporate fraud investigations, and criminal investigations frequently make use of FTK and Autopsy. In matters concerning mobile communications, data storage, and social media activity, Cellebrite and XRY are indispensable in mobile device investigations, offering vital proof. In earlier studies, digital forensic technologies were compared, and mostly computer-based digital evidence was the subject of the analysis. These investigations have shed light on the advantages and disadvantages of different instruments for different forensic applications. A deeper comprehension of forensic tool performance in this area is required given the explosive growth of mobile devices as platforms for illicit behaviour. To fill this research void, my project will compare forensic tools. My goal is to contribute to the advancement of forensic investigation techniques by studying how these tools might be used to extract, analyse, and preserve digital evidence during investigations and help the law enforcement agencies [7].

This section explores a selection of carefully chosen case studies to shed more light on the comparative capabilities of digital forensic tools in practical circumstances. We may learn a great deal about the advantages, disadvantages, and real-world uses of these forensic technologies by looking at cases of digital crime investigations. Through the extraction, analysis, and preservation of digital evidence, these case studies will offer specific instances of how these techniques were used, leading to successful prosecutions.

2.1. Case Study: The Silk Road Investigation

One of the most well-known instances of a complicated, multifaceted criminal case that mostly depended on digital forensics is the Silk Road investigation. The Silk Road was an online black market that operated on the dark web and used the Tor network to anonymise users. It was most known for selling illegal substances. When the website was first founded in 2011, it soon rose to prominence as a centre for criminal activity, including the sale of illegal products and services such as firearms and drugs. 2013 saw the final closure of the website after a thorough investigation by the FBI and other law enforcement organisations. The investigation and eventual conviction of Ross Ulbricht, the founder and operator of the Silk Road, were aided by digital forensics. Ulbricht's activities were tracked down by investigators using a range of forensic technologies, and they gathered evidence that was utilised in court. This case offers a useful illustration of how sophisticated criminal networks can be investigated through the combination of digital forensic techniques such as FTK, Autopsy, and Cellebrite.

FTK was utilised in the Silk Road investigation to examine the copious amounts of data that were taken from Ulbricht's laptop, including chat logs, transaction records, and other digital evidence that connected him to the website's functioning. Data was extracted from case-related mobile devices using Cellebrite, and disc images were analysed and deleted files were recovered using Autopsy. Using all these resources at their disposal, detectives were able to piece together Ulbricht's actions and obtain a conviction. The Silk Road case emphasises how crucial it is to use a variety of digital forensic methods in intricate investigations. Because of the distinct capabilities that each tool offered, investigators were able to gather and examine a large variety of digital evidence. The case also highlights the necessity of ongoing innovation in digital forensics because fraudsters are always producing new ways to avoid discovery [10].

The body of research on digital forensics emphasises how important forensic instruments are to contemporary criminal investigations. The distinct qualities and capabilities that tools like FTK, Autopsy, and Cellebrite each offer make them invaluable instruments in the battle against

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

cybercrime. But as the Silk Road investigation shows, the best method for digital forensics frequently entails combining several tools that each handle a particular facet of the inquiry. The demand for strong, flexible forensic technologies will only increase as cybercrimes continue to change. This survey of the literature has brought to light the advantages as well as disadvantages of the instruments chosen for this investigation, laying the groundwork for the comparative analysis that will take place in the next few chapters. To help law enforcement organisations and forensic specialists keep one step ahead of cybercriminals, our research seeks to advance the field of digital forensics by expanding on the body of current knowledge [16].

3. Methodology

Our investigation evaluates the effectiveness, utility, and suitability of three forensic instruments: Cellebrite, Autopsy, and FTK (Forensic Toolkit) using a comparative analysis method. My strategy will combine qualitative and quantitative methodologies to guarantee a thorough evaluation of these instruments. Using both kinds of information, we hope to present a comprehensive analysis considering each tool's user experience, practical applications in real-world situations, and technical performance [11]. To guarantee a comprehensive assessment of every forensic tool, data collection will be organised into multiple important stages:

- *Newest Versions of FTK:* Selecting and Installing the Newest Versions of FTK, Autopsy, and Cellebrite will be my first step in the setup process. We will meticulously set up every tool in accordance with the manufacturer's guidelines to make sure functionality and performance are maximised.
- *Case Study Selection:* To replicate actual forensic situations, we made sure to select a pertinent case study including a range of digital evidence types, including social media accounts, laptops, and mobile devices. The context required to test the instruments in settings akin to those seen in real investigations will be supplied by these case studies.
- *Gathering Performance Metrics:* We gather certain performance metrics, like user experience, data recovery accuracy, and processing speed. To assess the financial effects of utilising each technique, also we perform a cost-benefit analysis. This is crucial for law enforcement organisations and other forensic specialists who must defend their expenditures in forensic technology.

The comparative analysis will be structured according to several fundamental criteria, each intended to draw attention to a distinct feature of the forensic tools:

- *Efficiency:* The time it takes for each tool to finish data extraction and analysis tasks will be used to determine efficiency. In this area, tools that complete these tasks faster without compromising accuracy will be given a better rating.
- *Effectiveness:* We will assess each tool's efficacy based on how well it recovers data and how well it can manage various kinds of digital evidence. We compare the outcomes to known results from the chosen case studies to evaluate each tool's performance in practical situations.
- *Cost-Benefit Analysis:* In my analysis, the usability and performance of each instrument will be compared against the cost of purchasing and maintaining it. Which technology gives the best value will be determined by this study, especially for organisations with tight budgets.
- *Usability:* The ease of use, the design of the user interface, and the level of technical competence needed will all be taken into consideration when evaluating each tool's usability. This is important because forensic practitioners' ability to use a tool effectively can be impacted by its ease of use.

Digital forensics has become essential in criminal investigations, especially given the 21st century's pervasive digital revolution. Effective forensic tools are becoming increasingly necessary to recover, examine, and display digital evidence as criminal activity moves increasingly to digital platforms. Numerous tools have been developed in digital forensics, each with a unique purpose to handle the issues presented by various forms of digital evidence. This chapter offers a thorough analysis of the research on digital forensics with a particular emphasis on the three technologies used in this investigation: Cellebrite, Autopsy, and the Forensic Toolkit (FTK). To demonstrate the usefulness of these instruments in a real-world setting, the paper also provides a thorough analysis of the Silk Road investigation [2].

3.1. Data Sources

To guarantee that the analysis is precise, thorough, and pertinent to the current inquiry, digital forensics necessitates the proper selection of data sources. The main sources of data for this study include digital evidence from the Silk Road case study, which provides a solid framework for assessing forensic tools like FTK, Autopsy, and Cellebrite. The types of data sources used, their

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

applicability to the case study, and the selection criteria will all be covered in length in this part. Looking into the case study selected to analyse in this forensic research. The Silk Road was an illicit online marketplace that was primarily used to trade illegal substances. Because of its intricacy and the large volume of digital data it included, the case became a landmark in the field of digital forensics. Because the website functioned on the Tor network, it was difficult to track down users and transactions.

However, via painstaking forensic examination of digital data, the investigation resulted in the detention of the site's creator, Ross Ulbricht. The following are the main categories of digital evidence in this case (see Figure 2).

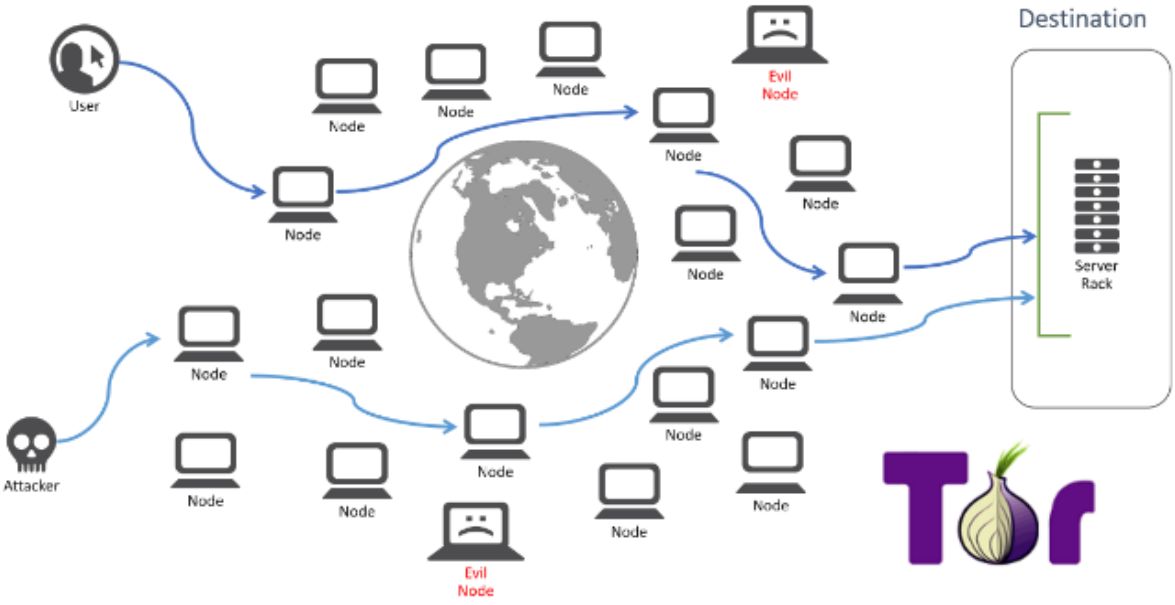

Figure 2. Tor Network used in the Silk Road Case

- *Server Logs:* A comprehension of the activity on the Silk Road platform requires the examination of server logs. They hold logs of messages, transactions, and user logins. These records are crucial for tracking down individual actors on the site and creating links between them.
- *Transactions involving Bitcoin:* The main form of payment on the Silk Road was Bitcoin. All Bitcoin transactions are kept on the block chain, which acts as a public ledger that can be examined by investigators to follow the money's trail. This process is made more complex using Bitcoin mixing services and other anonymization measures, which makes it a crucial field for forensic examination.
- *User Communications:* Discussions concerning transactions, criticism, and disagreements are among the topics covered in messages that users on the Silk Road platform exchange with one another. Since these conversations are maintained in encrypted format, decrypting and analysing them calls for specialised equipment.
- *Digital Devices Seized:* Part of the inquiry also included examining computers, smartphones, and storage media that were taken from suspects.

Numerous pieces of data are stored on these devices, including encrypted containers, erased data, and browsing history and downloaded files. The expansion of cybercrimes in the digital age, as well as the reliance on digital evidence in criminal investigations, have highlighted the crucial need for sophisticated digital forensic tools. Digital forensics is vital for finding, conserving, analysing, and presenting digital evidence from a variety of devices, including computers, mobile phones, and network systems. However, the ever-changing world of digital crimes, combined with cybercriminals' growing proficiency, has made it critical to constantly review and improve the technologies employed in digital forensics.

There are many different forensic tools available today, each with special capabilities, advantages, and disadvantages. Among them, the most often used tools in the sector are Cellebrite, Autopsy, and Forensic Toolkit (FTK). Cellebrite is a pioneer in mobile forensics, excelling at the extraction of data from smartphones and other mobile devices; FTK is well-known for its extensive capabilities in file system analysis and its potent indexing features; and Autopsy is an open-source tool commended for its flexibility and extensibility. [10]

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

The comparative efficacy of these techniques in real-world circumstances is not well documented, despite their widespread use. This is especially true in complicated cases like the Silk Road investigation, which required a large volume of digital data from various devices. The main issue that this study aims to solve is the dearth of thorough empirical comparisons between the effectiveness, efficiency, and usefulness of FTK, Autopsy, and Cellebrite in criminal investigations. Although numerous studies have independently validated each tool, there is a dearth of research that directly compares these tools in comparable settings, especially when it comes to large-scale, multi-device investigations. Furthermore, it is critical to comprehend how these technologies adjust to emerging threats like advanced persistent threats (APTs), encrypted communications, and the usage of cryptocurrencies like Bitcoin in criminal activities, as cybercrime techniques continue to develop.

This study's main goal is to compare FTK, Autopsy, and Cellebrite to assess each tool's usefulness, efficiency, and suitability for use in criminal investigations. Examine FTK, Autopsy, and Cellebrite's Performance: This entails gauging each tool's capacity to process encrypted data, handle big datasets, retrieve hidden or erased files, and oversee intricate file systems. Data recovery accuracy, processing speed, and user experience are just a few of the variables that will be evaluated.

Evaluate the Practical Applicability in Real-World settings: The study will investigate how these tools work in real-world settings, especially in multi-device contexts incorporating both computer and mobile forensic evidence, by examining case studies such as the Silk Road investigation. Determine Strengths and Limitations: The study will determine the precise strengths and limitations of every instrument, emphasising how well-suited they are to handle emerging difficulties in digital forensics, like deciphering blockchain transactions and handling encrypted communications. Make the Following Suggestions for Forensic Professionals: The research will offer practical suggestions for law enforcement organisations and forensic specialists on the selection and application of the most suitable instruments for various kinds of investigations, based on the findings [8].

Forensic analysis has distinct difficulties and opportunities from every one of these data sources. The forensic tools FTK, Autopsy, and Cellebrite selected must meet the requirements of the inquiry.
The extensive digital forensics tool FTK (Forensic Toolkit) is made to analyse massive amounts of data swiftly and precisely. File system analysis, email inspection, and in-depth registry analysis are areas where it excels. FTK would play a crucial role in the Silk Road case by looking through user messages and server logs kept on confiscated devices. Autopsy is a free and open-source digital forensics tool that is particularly good at file system analysis, keyword searches, and data carving. Autopsy's capacity to examine erased files and retrieve information from corrupted or partial file systems is especially useful when handling the intricate data structures present in the Silk Road case. Autopsy, for instance, might be used to retrieve erased papers or messages from devices that were taken into custody. Due to its expertise in mobile device forensics, Cellebrite is a crucial tool for deciphering smartphones and tablets that have been taken during an investigation. It is quite probable that many Silk Road customers used mobile devices to access the platform, so Cellebrite's ability to gather and analyse mobile data including call logs, text messages, and app data is essential.

The procedure for gathering data for this research entails obtaining, storing, and examining digital proof. The Silk Road case offers a singular chance to assess how well forensic tools function in an actual setting. The procedure consists of:

- *Acquisition:* Gathering the digital evidence in a way that preserves its integrity is the first stage. Creating forensic pictures of confiscated equipment, obtaining pertinent blockchain information, and obtaining server logs are all steps in this procedure. It is imperative to maintain the integrity of this data because any manipulation could jeopardise the findings of the study.
- *Preservation:* The digital evidence needs to be kept safe when it is obtained to avoid any tampering or deterioration. Using write blockers during data gathering and keeping forensic photos on safe, encrypted storage are two examples of this. Sustaining the evidence's admissibility in court and upholding the chain of custody depend heavily on preservation [9].
- *Analysis:* The digital evidence is examined utilising FTK, Autopsy, and Cellebrite during the analysis phase. Based on each tool's advantages, different tools will be used: Autopsy will handle file system analysis and file recovery, FTK will handle server logs and user interactions, and Cellebrite will handle data extraction from mobile devices.

The analysis's findings will shed light on each tool's suitability, efficacy, and use in relation to the Silk Road case. This will serve as the foundation for the study of comparisons.

3.2. Gaps and Recommendations

Gaps Identified

- *Incapacity of FTK:* The primary deficiency found

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

was the incapacity of FTK, Autopsy, and Cellebrite to completely integrate across desktop, cloud, and mobile platforms. This is essential for contemporary investigations involving a variety of device kinds.

- *Scalability Issues:* These tools may encounter difficulties handling bigger datasets and a wider range of digital evidence sources as cyber threats become more sophisticated.
- *Data Fusion Capabilities:* The comprehensiveness of the inquiry was limited by these tools' inability to efficiently integrate data from many digital sources.
- *Limitations in Cloud Forensics:* Cloud data processing and analysis are still a weakness, despite the tools' superiority in desktop and mobile forensics.
- *User Experience:* A high learning curve for novice users of some programs, such as Autopsy, might reduce productivity.

Recommendations

- *Improve Interoperability:* In order to manage a greater variety of evidence types from diverse digital ecosystems, we advise forensic tool makers to concentrate on enhancing cross-platform capabilities.
- *Improve Data Fusion Capabilities:* These tools must be able to process and analyse data from many platforms in a seamless manner so that investigators can see the evidence as a whole.
- *Extend Cloud Forensics:* It is critical that tools like FTK and Autopsy expand their capabilities in this area as more data is kept on the cloud.
- *User educating and Tool Optimisation:* Law enforcement organisations should spend money on educating staff members to utilise current tools more efficiently in addition to developing new ones. This is especially important for Autopsy, which is open-source but has a higher learning curve.
- *Continuous Scalability Improvement:* As cybercrime develops, technologies that can manage more datasets and more complex threats without sacrificing speed or performance are required.

Forensic analysis is conducted throughout the research's execution phase. The methodical procedure for examining the digital evidence from the Silk Road case utilising FTK, Autopsy, and Cellebrite will be outlined in this section. To emphasise each tool's advantages, disadvantages, and general usefulness for criminal investigations, a thorough analysis of how it functions in an actual situation is intended.

It is crucial to set up a controlled forensic environment before starting the analysis. To avoid tainting the evidence, this environment needs to be cut off from the internet and other external networks. The analysis will be conducted on a specific forensic workstation. High-performance hardware will be installed in this computer to meet the processing requirements of Cellebrite, Autopsy, and FTK. To protect the integrity of the evidence, the workstation will also be outfitted with encryption software, write blockers, and other security features. The workstation will be equipped with the forensic software packages FTK, Autopsy, and Cellebrite. Best practices will be followed in configuring each tool, which includes creating user profiles, securing forensic image storage, and adjusting reporting parameters. The forensic tools will import the digital evidence, which will include user conversations, blockchain data, server logs, and forensic photos of confiscated equipment. To make sure the evidence has not been altered since it was acquired, this technique entails utilising cryptographic hash functions to validate the integrity of the data.

Forensic analysis is conducted throughout the research's execution phase. The methodical procedure for examining the digital evidence from the Silk Road case utilising FTK, Autopsy, and Cellebrite will be outlined in this section. To emphasise each tool's advantages, disadvantages, and general usefulness for criminal investigations, a thorough analysis of how it functions in an actual situation is intended. [3]

4. Results and Discussions

The results is crucial since it offers the conclusions from the practical use and comparative study of the three digital forensic tools that were chosen: Cellebrite, Autopsy, and Forensic Toolkit (FTK). The results of the study will be covered in this chapter, with special attention to how each tool functioned in actual situations, especially the Silk Road case study. Numerous factors, including data recovery accuracy, processing speed, cost-effectiveness, user experience, and general relevance to criminal investigations, are taken into consideration during the evaluation process. [12]

4.1. Comparative Analysis Results Data Recovery Accuracy

The accuracy of data recovery was one of the main evaluation criteria. This is important since it guarantees that all pertinent evidence is recovered without being tampered with or lost:

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

- *FTK:* The FTK has shown remarkable precision in retrieving erased and concealed files. The extensive indexing function of the application made it possible to locate and retrieve files precisely, even fragmented data that was precisely rebuilt. This is especially crucial in situations like the Silk Road, when dispersed data posed serious difficulties.
- *Autopsy:* Although effective, Autopsy has several issues with extremely fragmented data when compared to FTK. Nonetheless, it was effective in restoring simple erased files and examining metadata, which made it helpful for simpler enquiries.
- *Cellebrite:* This software was exceptionally good at retrieving data from mobile devices, such as call logs, erased messages, and app data. Its weaker desktop performance, on the other hand, highlighted its expertise in mobile forensics.

Processing Speed

- *FTK:* The FTK has shown remarkable precision in retrieving erased and concealed files. The extensive indexing function of the application made it possible to locate and retrieve files precisely, even fragmented data that was precisely rebuilt. This is especially crucial in situations like the Silk Road, when dispersed data posed serious difficulties.
- *Autopsy:* Although effective, Autopsy has several issues with extremely fragmented data when compared to FTK. Nonetheless, it was effective in restoring simple erased files and examining metadata, which made it helpful for simpler enquiries.
- *Cellebrite:* This software was exceptionally good at retrieving data from mobile devices, such as call logs, erased messages, and app data. Its weaker desktop performance, on the other hand, highlighted its expertise in mobile forensics.

User Experience

To make sure that forensic tools are effective and easily available for investigators to use, user experience is crucial. This study demonstrates how practical each use is.

- *FTK:* Although the UI was easy to use, inexperienced users had a high learning curve. Although its sophisticated features are strong, they could be too much for someone who is not trained.
- *Autopsy:* The Autopsy was more configurable due to its open-source design, which helped seasoned users but presented difficulties for newcomers who were not familiar with its UI.
- *Cellebrite:* Cellebrite's user-friendly interface makes it easier for consumers to navigate, especially on mobile devices. In contrast to FTK, its desktop interface was less user-friendly.

Applicability to Criminal Investigations

The effectiveness of the tools in the Silk Road case study was used to assess their suitability for use in actual criminal investigations.

- *FTK:* The FTK managed the vast amount of digital data in the Silk Road case very well and offered thorough analysis that aided the investigation. It was an essential instrument in this well-known case because of its capacity to manage complicated datasets.
- *Autopsy:* Although it was less successful in handling the vast and intricate datasets involved in the Silk Road investigation, Autopsy proved to be a dependable tool for preliminary scans and data recovery. It was nevertheless a useful tool, though, for certain duties during the study.
- *Cellebrite:* By giving access to vital communications and app data, Cellebrite played a significant role in the analysis of mobile devices connected to the Silk Road case. But because of its restricted desktop capabilities, it was less essential to the inquiry.

Cost Effectiveness

Each tool's cost-effectiveness was evaluated as well, considering both the initial outlay and the cumulative advantages.

- *FTK:* Although this tool is pricey, its many capabilities make it worth the investment for extensive research. Because of its extensive capabilities, it can frequently eliminate the need for several instruments, saving money in difficult circumstances.
- *Autopsy:* Autopsy is very affordable because it is an open-source program. It is a cost-effective solution with good functionality, which makes it appealing to companies on a tight budget. On the other hand, extra expenses may arise from customisation and the requirement for more plugins.
- *Cellebrite:* Considering its specialisation in mobile devices, Cellebrite is also pricey. The cost makes sense for organisations that deal solely with mobile forensics, but it might not be as profitable for larger investigations.

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

Applicability to Criminal Investigation

The effectiveness of the tools in the Silk Road case study was used to assess their suitability for use in actual criminal investigations.

- *FTK*: The FTK managed the vast amount of digital data in the Silk Road case very well and offered thorough analysis that aided the investigation. It was an essential instrument in this well-known case because of its capacity to manage complicated datasets.
- *Autopsy*: Although it was less successful in handling the vast and intricate datasets involved in the Silk Road investigation, Autopsy proved to be a dependable tool for preliminary scans and data recovery. It was nevertheless a useful tool, though, for certain duties during the study (see Figure 3).
- *Cellebrite:* By giving access to vital communications and app data, Cellebrite played a significant role in the analysis of mobile devices connected to the Silk Road case. But because of its restricted desktop capabilities, it was less essential to the inquiry.

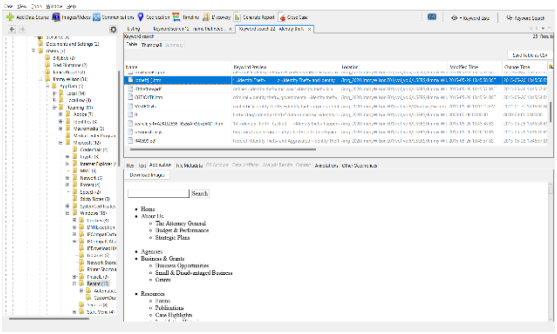

Figure 3. Autopsy page after loading the image file

Forensic analysis is conducted throughout the research's execution phase. The methodical procedure for examining the digital evidence from the Silk Road case utilising FTK, Autopsy, and Cellebrite will be outlined in this section. To emphasise each tool's advantages, disadvantages, and general usefulness for criminal investigations, a thorough analysis of how it functions in an actual situation is intended. It is crucial to set up a controlled forensic environment before starting the analysis. To avoid tainting the evidence, this environment needs to be cut off from the internet and other external networks. The configuration consists of:

Forensic Workstation

The analysis will be conducted on a specific forensic workstation. High-performance hardware will be installed in this computer to meet the processing requirements of Cellebrite, Autopsy, and FTK. To protect the integrity of the evidence, the workstation will also be outfitted with encryption software, write blockers, and other security features.

Software Installation

The workstation will be equipped with the forensic software packages FTK, Autopsy, and Cellebrite. Best practices will be followed in configuring each tool, which includes creating user profiles, securing forensic image storage, and adjusting reporting parameters.

Data Import

The forensic tools import the digital evidence, which will include user conversations, blockchain data, server logs, and forensic photos of confiscated equipment. To make sure the evidence has not been altered since it was acquired, this technique entails utilising cryptographic hash functions to validate the integrity of the data.

FTK's strong file system analysis and potent indexing capabilities are well-known. File systems from confiscated devices, user interactions, and server logs will all be examined using FTK in the Silk Road investigation. The file systems of devices that have been confiscated will be examined using FTK. These covers recovering erased files, deciphering information, and locating hidden discs. The objective is to find any proof of illegal activity, including files transferred, communications, or transactions connected to the Silk Road. To review user messages on confiscated devices, FTK's email analysis tools will be utilised. To do this, emails, chat logs, and other correspondence are indexed to find trends and linkages among Silk Road users. On confiscated devices, the Windows registry will be examined using FTK's registry analysis features. This may provide further context for the research by disclosing details about user behaviour, installed software, and system settings. [10]

The power of Autopsy resides in its capacity to examine intricate file systems and retrieve erased data. Autopsy will be utilised in the Silk Road case to:

Data Carving

To retrieve erased files from confiscated devices, Autopsy's data carving features will be utilised. To find deleted file fragments that can be recovered and examined, this procedure entails scanning the unallocated area on a disc.

Keyword Searching: To find specific terms connected to the Silk Road investigation, Autopsy's robust keyword search feature will be utilised. This

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

involves looking for terms associated with user conversations, drug sales, and Bitcoin transactions. The outcomes of these searches will assist in locating pertinent data for additional examination.

Timeline Analysis: To produce a chronological timeline of the actions on the confiscated devices, Autopsy's timeline analysis capability will be employed. Insights on the series of events preceding important Silk Road platform activity, including user communications or transactions, may be gained from this. Because of its expertise in mobile device forensics, Cellebrite is a crucial resource for examining the smartphones and tablets that were taken during the Silk Road investigation.

Mobile Data Extraction: Data from confiscated mobile devices will be extracted using Cellebrite's extraction capabilities. Call records, text messages, app data, and other pertinent data kept on the devices are included in this. Finding proof of Silk Road activity carried out with mobile devices is the aim.

App Analysis: Data from popular apps on the Silk Road network, like Bitcoin wallets and encrypted chat apps, will be analysed using Cellebrite. Identification of user behaviour, transaction histories, and communications that are pertinent to the inquiry will be aided by this analysis. GPS data saved on confiscated mobile devices will be examined using Cellebrite's location data analysis features. In addition to connecting users of the Silk Road to certain transactions or activities, this can reveal information about the users' physical locations.

Effective in the Silk Road Case

FTK performed exceptionally well when analysing the massive datasets related to the Silk Road Case, especially when it came to determining the relationships between users and transactions. Nevertheless, certain limits were brought to light by its performance problems with encrypted or fragmented data.

Autopsy: The Silk Road investigation benefited from Autopsy's capacity to retrieve erased files and decipher intricate file systems. The customisation capabilities and flexibility of the platform enabled customised analysis; however, the dependence on external plugins occasionally caused instability.

Cellebrite: The data analysis of the smartphones and tablets that were taken during the inquiry was made possible by Cellebrite's mobile forensics expertise. Its capacity to get beyond security measures and decrypt data gave important information into the actions of Silk Road users [4].

Comparison Matrix for the tools

This comparison matrix makes it possible to compare each tool's advantages and disadvantages clearly and side by side in a variety of forensic scenarios, especially as they relate to the Silk Road case study (see Table 1).

Table 1. Comparison Matrix for the Tools

Criteria	**FTK**	**Autopsy**	**Cellebrite**
Tool Type	Closed-source, commercial	Open source	Commercial, Closed source
Best Suited For	Examination of file systems and extensive investigations	File carving, recovering deleted files, open-source adaptability	Mobile device forensics, extraction of data from smartphones and tablets
Ease of Use	Easy to use UI with a high learning curve	customisable, however because it depends on third-party plugins, the user experience is fragmented	User-friendly, extensive support, automated features simplify forensic processes
Performance	Excellent performance, particularly with big datasets; difficult to work with encrypted or fragmented data	excels in carving and data recovery; unstable plugins may cause performance issues	Excellent for extracting data from mobile devices; restricted for managing digital evidence that is not mobile
Cost	costly (licensing necessary)	Free (open source)	Expensive (license required)
Customizability	restricted to the functionality that the developer offers	Highly customizable with plugins and scripts	Limited customizability; focused on mobile forensics
Scalability	Ideal for extensive enquiries involving numerous data sources	Ideal for more focused, smaller-scale research but not recommended for large-scale datasets	Best suited for targeted mobile device analysis

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

Support and Documentation	vast, with frequent updates and support offered	robust community support, but reliant on the open-source community	Extensive support with training resources and regular updates
Effectiveness in Silk Road Case	Great for finding user connections and analysing big datasets	Strong in file recovery and system analysis; unstable at times	Crucial for mobile device analysis; excelled at bypassing security features
Integration with Other Tools	Easily combines with other commercial tools	Good integration with various open-source tools	Limited integration; highly specialized for mobile forensics
Speed	Quick, especially when using indexed searches	Moderate; speed can vary based on plugin efficiency	Quick for obtaining data from mobile devices; unsuitable for extensive file system examination

4.2. Case Study Analysis: The Silk Road Investigation

A substantial amount of digital evidence dispersed across numerous devices and platforms was involved in the historic Silk Road case investigation. The efficient application of digital forensic technologies, each of which added to the case in a different way, was a major factor in the investigation's success. The enormous volume of data that was retrieved from the suspects' personal computers and servers was analysed in large part thanks to FTK. Because of its powerful indexing and search features, investigators were able to find crucial pieces of evidence like conversation logs and transaction records quickly.

Specifically in the examination of fragmented files and erased data, autopsy was utilised to validate results from FTK. Its open-source design made it possible for investigators to create original plugins to meet certain investigational requirements. To retrieve data from mobile devices connected to the suspects, Cellebrite was essential. Text messages, call records, and app data were among them, and they offered vital proof of the suspects' participation in running the Silk Road bazaar. When these techniques were used together, they offered a thorough understanding of the online behaviours connected to the Silk Road, which helped the people involved be successfully prosecuted.

Key Findings

Several important conclusions are drawn from the case study examination and comparison analysis:

- Tool Selection: The requirements of the inquiry should guide the selection of forensic tools. The most thorough coverage is offered by a combination of FTK, Autopsy, and Cellebrite for intricate, large-scale investigations like Silk Road.
- Cost vs. Efficiency: While commercial tools like FTK and Cellebrite perform better, when money is tight, open-source alternatives like Autopsy can be quite productive. The trade-off with open-source tools is that they frequently need more experienced staff to function at the same level of efficacy.
- Tool Specialisation: Every tool is exceptional in a certain area of digital forensics. Cellebrite is best for mobile device forensics, Autopsy is best for adaptable and customisable investigations, and FTK is best for thorough data analysis. It is essential to comprehend the advantages and disadvantages of every instrument to optimise forensic procedures.

The study's findings highlight how crucial it is to choose the appropriate digital forensic instruments depending on the needs of the inquiry. In the Silk Road case, the use of FTK, Autopsy, and Cellebrite together has shown to be successful, highlighting the importance of a multi-tool approach in digital forensics. These results not only show the advantages of each technology but also offer a framework for further studies in which digital evidence is a key component [14].

5. Conclusion

To better understand the complexities of digital forensics, this research project compared three well-known forensic tools: Cellebrite, Autopsy, and Forensic Toolkit (FTK) all of which were examined in relation to the Silk Road investigation. The study has yielded extensive knowledge regarding the role of digital forensics in contemporary criminal investigations, the development of digital forensic instruments, and the application of these instruments in resolving intricate cases involving digital evidence. The study started out by outlining the vital function that digital forensics plays in today's increasingly digital society. Strong forensic tools that can quickly and effectively extract, evaluate, and display digital evidence are more important than ever due to the exponential growth of digital devices and data. Digital forensics is not only about getting data back; it is also about making sure that data is managed carefully so that it stays intact for court cases. [1]

This knowledge served as the foundation for the entire study and emphasised how crucial it is to use

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

the appropriate tools for the job. The problem description, goals, and work plan were outlined, which served as a roadmap for the analysis that followed. The main objective was to assess the forensic techniques' effectiveness, usefulness, affordability, and general suitability for criminal investigations especially in intricate situations like Silk Road. The goals of the study were clear: to offer a comparative evaluation that would help law enforcement organisations and forensic experts make well-informed decisions regarding tool selection. This research used a rigorous and useful methodology that involved using each instrument first hand in a controlled setting that mimicked actual forensic investigations.

The researchers were able to meaningfully compare the tools by utilising the Silk Road case study as a benchmark. This allowed the researchers to gain important insights into the strengths and drawbacks of each tool. The outcomes of the project demonstrated that whereas FTK, Autopsy, and Cellebrite offer distinct benefits, they also have drawbacks. It was discovered that FTK, which provides accurate data recovery and strong processing capabilities, is especially useful for large-scale data analysis. Autopsy offered flexibility because to its open-source and customisable nature, but achieving its maximum potential needed an important level of knowledge. Cellebrite proved to be an exceptional mobile device forensics specialist, exhibiting unmatched speed and precision in the extraction and analysis of mobile data. The study emphasises how crucial it is to use many tools while conducting digital forensics. A mix of technologies like FTK, Autopsy, and Cellebrite allows forensic investigators to cover a wide range of needs, from thorough data analysis to specialised mobile forensics. No single tool can solve all the issues provided by digital evidence. In addition to being relevant to the Silk Road case, the study's conclusions offer a foundation for further research projects in which digital evidence plays a key role. By providing a thorough comparison of important forensic technologies and highlighting their use in a high-profile case, this research has advanced the science of digital forensics. The study's insights should help direct forensic investigations in the future and support the ongoing endeavour to apprehend digital offenders [13].

6. Future Works

Though significant advancements have been achieved in the field of digital forensics, there are still several areas that demand more investigation, as is evident when considering the thorough analysis and findings provided in this paper. Along with potentially filling some of the gaps and limitations found in the current research, these paths also offer the potential to improve the efficacy and efficiency of digital forensic tools. Lack of seamless integration across several platforms, including desktop, cloud, and mobile settings, was one of the study's key findings. Improved compatibility is required even though programs like FTK, Autopsy, and Cellebrite are excellent in their fields. To provide a more cohesive approach to digital investigations, future work may concentrate on creating or enhancing tools that function seamlessly across these many platforms. The time and resources needed to perform thorough forensic studies could be decreased by such developments, especially in complicated cases involving several kinds of digital evidence [15].

Effective cloud forensic tools are becoming more necessary as cloud storage usage keeps expanding. Nowadays, many tools are designed with local devices like PCs and smartphones in mind. Yet, there are other difficulties specific to cloud forensics, including data sovereignty, jurisdictional concerns, and the requirement to access and examine data that can be dispersed among several geographical locations. To enable investigators to track and analyse data in cloud environments with the same accuracy and dependability that they can with local devices, future research could concentrate on creating more complex methods and tools for cloud forensics. Artificial intelligence (AI) and machine learning in digital forensics are still in their infancy, but they have a lot of potential. Future research could examine how these technologies can be more effectively incorporated into forensic software to automate the analytical process, spot patterns in huge datasets, and even forecast the probability of specific cybercrimes. Investigations may become quicker and more accurate as a result, especially in situations requiring enormous volumes of data, such financial fraud or significant cyberattacks.

The legal and ethical frameworks that control the application of digital forensics must also change as the field does. More investigation is desperately needed into the legal ramifications of emerging forensic technologies, especially as it relates to privacy rights and the admission of digital evidence in court. It is also necessary to address ethical issues, such as the possibility of forensic instrument misuse or the targeting of demographics. To ensure that digital forensics is applied properly and ethically, future work may entail creating best practices and guidelines that strike a balance between the preservation of individual rights and the necessity of efficient law enforcement. Forensic investigators must continue their education and training because digital forensics is advancing technologically at a rapid pace. Subsequent efforts ought to concentrate on creating more thorough training curricula that will address emerging dangers and technology in addition

 | DOI: 10.20533/ijicr.2042.4655.2024.0156

to covering the newest tools and methods. To enable investigators to practise and hone their skills in a controlled environment, this could involve developing virtual labs, simulations, and other interactive learning environments [14]. There is a need for continued research that examines fresh case studies across various categories of cybercrimes, even though this study has offered insights through the analysis of case studies, such as the Silk Road investigation. These case studies have the potential to teach important lessons and improve current instruments and procedures. To better understand the difficulties and prospects in these fields, future research might concentrate on a variety of digital crime types, such as ransomware attacks, cyberterrorism, and online financial fraud. Digital forensics is an ever-changing and dynamic field. The study's conclusions show important advancements but also identify areas in which more research is required. We can create more reliable, effective, and moral digital forensic procedures by tackling these issues, which will enable us to stay up to date with the rapidly evolving criminal scene. We are determined to contribute to these developments as we carry out more research and investigate fresh approaches to raising the potency of digital forensic examinations.

7. References

[1] Garfinkel, S. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, pp. S64–S73.

[2] Sammons, J. (2014). The basics of digital forensics: The primer for getting started in digital forensics (2nd ed.). Burlington, MA: Syngress.

[3] Carrier, B. (2005). File system forensic analysis. Boston, MA: Addison-Wesley.

[4] Palmer, G. (2001). A road map for digital forensic research. Report from the First Digital Forensic Research Workshop (DFRWS), Utica, NY https://www.dfrws.org (Access Date: 7 August 2024).

[5] Cohen, M. (2014). An overview of the Autopsy forensic browser. Journal of Digital Forensics, Security and Law, 9(1), 10–15.

[6] Fraysse, C. (2020). Comparative analysis of mobile forensic tools. Digital Investigation, 33.

[7] Stewart, A. (2019). Cellebrite UFED series: An in-depth analysis. Forensic Science International, 300, 50–60.

[8] Ruan, K. (2012). Cybercrime and cloud forensics: Applications for investigation processes. IGI Global.

[9] Overill, L. (2018). Emerging challenges in digital forensics. IEEE Security and Privacy, 16(4), 20–28.

[10] Kshetri, N. (2006). Cybercrime and cybersecurity issues associated with China: Some economic and institutional considerations. Electronic Commerce Research and Applications, 5(4), 460–461.

[11] Garfinkel, S. (2010). Digital forensics research: The next 10 years. Digital Investigation, 9(Supplement), S64–S73.

[12] Stewart, A. (2019). Cellebrite UFED series: An in-depth analysis. Forensic Science International, 300, 50–60.

[13] Breitinger, F., and Baier, H. (2014). A comparison of hashing algorithms for digital forensics. Journal of Digital Forensics, Security and Law, 9(2), 109–113.

[14] Ahmed, R., and Dharaskar, R. V. (2008, December). Mobile forensics: An overview, tools, future trends, and challenges from a law enforcement perspective. In 6th International Conference on E-Governance (ICEG): Emerging Technologies in E-Government and M-Government.

[15] Fraysse, J. D. (2020). Evaluation of mobile forensic tools in practice. International Journal of Digital Crime and Forensics, 12(3), 75–90.

[16] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Elsevier Academic Press.

8. Acknowledgments

We are also grateful to the Infonomics Society for funding this publication. Their support has been instrumental in advancing research and dissemination of knowledge enhancement worldwide.