**Digital Forensics Analysis**

**Team Members:**

1. Pravali Rao(Y00860615),
2. Manoj Kumar Kaleru(Y00860656),
3. Shwetha Makineni(Y00866944)**.**

# Abstract

Digital forensics serves as essential for detecting, reacting to, and documenting security breaches. It is vital for revealing evidence of criminality by collecting, examining, and disclosing digital evidence. The need for digital forensics knowledge remains strong due to ongoing concerns of hacking and information intrusions. This field is crucial for examining and settling conflicts involving evidence kept in digital environments, utilizing specific methods for data recovery, verification, and examination. Computer forensics involves several tasks such as identifying, preserving, analyzing, documenting, and presenting digital evidence. The study examines contemporary developments in digital forensics, including IoT, cloud, network, and social media forensics, emphasizing the changing landscape of cyber threats and assaults. Forensic investigators and scientists are responsible for deciphering the complexity of the digital realm. The study highlights the significance of maintaining digital evidence to guarantee its authenticity and validity in court processes. The article intends to better forensic investigation processes by highlighting the importance and techniques of protecting digital evidence, eventually assisting in presenting unmodified data in court.

**Keywords:** Network forensics, Cyber Crime, Digital Evidence, Investigation, IoT forensics, social media forensics, Cloud forensics, Digital forensics.

Table of Contents

[Abstract i](#_Toc160617363)

[List of Figures iii](#_Toc160617364)

[1. Introduction 1](#_Toc160617365)

[2. Background 2](#_Toc160617366)

[3. Problem Statement 3](#_Toc160617367)

[4. Case Study Methodology 4](#_Toc160617368)

[4.1. New Developments in Digital Forensics 4](#_Toc160617369)

[5. Proposed Solution and Its Implementation 9](#_Toc160617370)

[6. Experiment 11](#_Toc160617371)

[6.1. Python Implementation 11](#_Toc160617372)

[7. Discussion 12](#_Toc160617373)

[8. Conclusion 13](#_Toc160617374)

[9. Contribution of Team Members 14](#_Toc160617375)

[References 14](#_Toc160617376)

[Appendix 15](#_Toc160617377)

# List of Figures

[Figure 1: Types of Digital Forensic 1](#_Toc160616903)

[Figure 2: Social media evidence in traditional and Cyber Crimes. 8](#_Toc160616904)

[Figure 3: Differences between cloud storage and regular storage. 10](#_Toc160616905)

[Figure 4: Flow chart showing advantages of cloud storage 11](#_Toc160616906)

# 1. **Introduction**

The huge expansion of computer networks over the past few years, to small regional systems the web, has made the area of digital forensics more well known. This field includes more than just network forensics. It also looks into security holes in systems, breaches of privacy, and data theft. To make sure that digital evidence can be used in court to prove crimes, digital forensics is the careful process of gathering, analyzing, recording, and putting digital evidence onto a timeline. The tools, techniques, and software used to break into private as well as public networks and steal information are getting smarter as the digital world changes. With the rise of social media networks, technology has advanced even faster, and hacking has also gone up. As things change, new threats, attack routes, tools, and tactics appear. These allow criminals to take advantage of weak spots in systems that are getting more complicated or secure, which can cause a lot of harm and is hard to predict. Hackers use anti-forensic means to stop investigations or get rid of all digital evidence. As digital forensic methods improve, correspondingly improve hackers' strategies. The goal of the research is to look at how digital forensics is changing in the field of cybersecurity, focusing on the dangers, possibilities, challenges, and new trends.

A diagram of a network of forensics

Description automatically generated

Figure 1: Types of Digital Forensic

# 2. Background

Digital forensics, which is also called computer forensics, has become an important field for looking into cybercrimes, data leaks, and other types of bad behavior online. It includes finding digital proof on gadgets and digital storage broadcasting, keeping it safe, analyzing it, and showing it to the court. Criminal behavior has changed a lot because of changes in technology, which has made digital proof more important in court cases.

Digital forensics has its roots in the latter part of the twentieth century, around the same time that home computers as well as the internet were first used. At first, forensic analysis was mostly about getting data back from actual storage devices. Yet, as technology has improved, digital forensics has grown to include a lot more digital items, such as messages, Tweets, data stored in the cloud, as well as IoT machines.

In the context of digital forensic analysis, the selection of appropriate tools is crucial for effective and efficient investigation. PyCharm, an Integrated Development Environment (IDE) for the Python programming language, has emerged as a valuable custom toolkit for digital forensic analysts. PyCharm provides a comprehensive set of features and tools that facilitate the development, testing, and debugging of Python scripts and applications, making it well-suited for forensic analysis tasks.

The use of PyCharm in digital forensic analysis offers several advantages. Firstly, PyCharm's intuitive user interface and powerful code editor streamline the development process, enabling forensic analysts to write, execute, and modify Python scripts with ease. Additionally, PyCharm's built-in version control system and project management capabilities enhance collaboration and organization, allowing forensic teams to work efficiently on complex investigations.

Moreover, PyCharm's extensive library of plugins and extensions extends its functionality, enabling forensic analysts to integrate additional tools and libraries for specialized forensic tasks. From data extraction and parsing to pattern matching and data visualization, PyCharm's versatility empowers forensic analysts to perform a wide range of forensic analysis tasks within a single environment.

As digital environments continue to evolve and cyber threats become increasingly sophisticated, the development and utilization of custom toolkits like PyCharm play a crucial role in enhancing the capabilities of digital forensic investigations. This dissertation aims to explore the potential of PyCharm as a custom toolkit in digital forensic analysis, examining its effectiveness, usability, and applicability in real-world forensic scenarios. Through empirical research and case studies, this study seeks to provide insights into the role of PyCharm in advancing the field of digital forensics and addressing the challenges posed by modern cyber threats.

# 3. Problem Statement

Despite advancements in digital forensics tools and techniques, forensic analysts still face challenges in effectively and efficiently conducting investigations in rapidly evolving digital environments. The dynamic nature of digital data, coupled with the increasing sophistication of cyber threats, presents obstacles that traditional forensic tools may struggle to overcome. Additionally, the diversity of digital devices and platforms further complicates the forensic analysis process, requiring forensic analysts to adapt their methodologies and tools to accommodate various data sources and formats.

One of the key challenges in digital forensic analysis is the lack of specialized tools tailored to the unique requirements of modern forensic investigations. While existing forensic tools provide valuable functionality for data acquisition, analysis, and reporting, they may not always address the specific needs of forensic analysts or the intricacies of certain forensic scenarios. Furthermore, the rapid emergence of new technologies and data storage mechanisms necessitates the development of flexible and customizable forensic toolkits capable of handling diverse datasets and forensic tasks.

In this context, the problem addressed by this dissertation is the need for a custom toolkit that can enhance the efficiency, accuracy, and reliability of digital forensic analysis in the face of evolving technological landscapes and emerging cyber threats. Specifically, the research aims to investigate the feasibility and effectiveness of utilizing PyCharm, an Integrated Development Environment (IDE) for the Python programming language, as a custom toolkit for digital forensic analysis. By leveraging PyCharm's powerful features and extensibility, the research seeks to develop a comprehensive toolkit that addresses the challenges inherent in modern forensic investigations and empowers forensic analysts to perform a wide range of forensic tasks within a unified environment.

The primary objective of this research is to evaluate the capabilities of PyCharm as a custom toolkit for digital forensic analysis, assess its usability and applicability in real-world forensic scenarios, and identify opportunities for further enhancement and optimization. Through empirical research, including experimental evaluations and case studies, the dissertation aims to contribute to the advancement of digital forensics by providing insights into the potential of PyCharm as a valuable tool for forensic analysts and forensic investigations. Ultimately, the research seeks to address the existing gaps in digital forensic tooling and support the development of more effective and efficient forensic analysis methodologies in response to evolving cyber threats and technological advancement.

# 4. Case Study Methodology

For this project, the case study methodology will serve as the primary approach for evaluating PyCharm as a custom toolkit in digital forensic analysis. A selection of diverse real-world forensic cases will be carefully chosen to represent various types of digital investigations, ensuring a comprehensive examination of PyCharm's effectiveness across different scenarios. Each case will be meticulously prepared, with relevant digital evidence collected and contextual information documented to provide a thorough understanding of the forensic context.

PyCharm will be customized to meet the specific requirements of each forensic case, with plugins, tools, and scripts integrated to enhance its functionality for forensic analysis.

## 4.1. New Developments in Digital Forensics

In this segment we have provided a short analysis of the types and trends of digital forensics.   
 **A. Network Forensics**

The important job of Network Forensics is to store, retrieve, and analyze network data. This area of digital forensics is very important for keeping an eye while studying network activity in order to find strange data, legal proof, or signs of cyberattacks. In this area, preventative steps are often stressed because network data is temporary and disappears after it is sent. Network forensic experts are in charge of coming up with standard protocols for getting data back after a security breach or hack. They have to make sure that these protocols work with the needs of the company and the network infrastructure. They use full network investigation tools to keep an eye on network activity, record it in an easy-to-find database, and give IT staff the tools they need to find and understand system problems. Network forensics helps IT teams figure out what kind of breach happened and how it affected IT assets as well as services, like computers and databases. They can then add additional safeguards to protect sensitive information in the network's deeper layers.   
  
**Challenges**  
This is because networks create so much data every day—gigabytes of it—that it's hard to figure out what happened. Due to the large amount of data, looking into cases after a long time has passed can be hard and boring. Also, the research process is made harder by the fact that Internet standards aren't always the same. Different networking levels make it harder to find out where data comes from and where it's going because real (MAC), IP, and email addresses can be changed or hidden. But the field has come a long way thanks to the creation of special forensic programs and instruments that make it easier to solve cases by dealing and processing large amounts of data quickly.   
  
Using these tools doesn't make it any easier to gather enough proof to name a suspect. Network forensics is very important for fighting many types of cybercrime, like hacking, deception, data theft, software copying, and more, because it gives real proof for court cases. The field always has to deal with the task of responding to the constantly changing world of cyber dangers. To stay ahead of bad players, new methods and technologies are always being created.

**B. IoT Forensics:**

The Internet of Things (IoT) is an area of technology that is changing quickly. It includes a lot of different products, from desktops and laptops to smart gadgets and digital helpers. IoT forensics is a specific area of digital forensics that looks into cybercrimes featuring these connected devices by looking at the data that is sent and kept on their networks. Smart systems make operations more efficient and everyday life easier, which is why this field is especially useful in both business and home life. These benefits aren't as great as they could be because IoT networks are open to hacking, spying, malware, and denial-of-service attacks that can damage them.

There are more and more smart devices in private places, like homes, that could be used as digital proof in criminal investigations. This makes investigations into the IoT world more important. To get digital proof, this means looking closely at video and sound data from things like CCTV cams and smart speakers. IoT gadgets frequently offer more immediate and reliable proof than standard computers. These speeds up the investigation process without needing the user to connect directly with the device.

**Challenges:**

The ecosystems of IoT devices are very different from normal forensic tools made for traditional computer settings. This makes IoT forensics difficult. Access to evidence is limited, service agreements put limits on what can be done, device designs change, and software as well as hardware are not standardized, all of these things make the forensic process more difficult. Even with these problems, IoT forensics is very important because it provides accurate and useful digital proof, making it an important part of contemporary investigations involving digital forensics.  **C. Cloud Forensics:**

Investigations in the cloud uses strict scientific methods to plan and analyze events by finding, collecting, examining, and submitting digital evidence in electronic settings. Forensic experts are very interested in this area because cloud computing has so many resources, is cheap, flexible, and can store a lot of data. This makes it an important part of digital investigations that take place in the cloud. Cloud computing has greatly lowered the cost of IT, which has made it more popular in many areas, such as among private businesses as well as the government. However, the qualities of cloud computing that make it hard to do forensic investigations easier, like the ability to do many things at once and extensive data sharing, make they more difficult. Concerns about security holes have made people see the cloud as a possible place for bad things to happen, even though it is growing quickly and has many benefits.

Some of the problems that make cloud forensics so hard are getting back data that has been erased or changed, figuring out who made changes, and the fact that cloud data is spread out across many devices and places. Forensic truth depends on making sure the purity and dependability of data that is spread out in such a way.

**Challenges:**

* One problem with cloud forensics is that it's hard to keep track of and confirm when data is changed or deleted, which is needed to build a believable investigation story.
* The scattering of data across many different cloud services and real devices makes it harder to collect and analyze proof.
* Making sure that the proof shown is a true and unmodified copy of the original data by maintaining data integrity.

Even with these problems, cloud forensics is still a big trend in the field. It uses the benefits of cloud computing, like spread processing and flexibility, to make investigations better and lead to better results.

**D. Social Media Forensics**:

A big part of network forensics is social media forensics, which uses advanced cyber research and digital analytics to get data from sites like Facebook, Instagram, Twitter, and LinkedIn and look at it. This field is all about finding, collecting, and closely looking at digital traces people leave on social networks to find proof of crimes or other bad behavior. Cyberattacks on social media can happen both online and offline, stopping apps and services from working normally. DoS (Denial of Service) attacks, which are meant to briefly stop the normal operation of social media services, are one type of interruption. Social media forensic experts are very important to crime cases because they can sort through the huge amount of different types of social media data. By giving these investigators cutting-edge tools, they can better handle the complexity and sheer size of social media material, which lets them gather strong legal proof for the prosecution.

A diagram of social media crime

Description automatically generated

Figure 2: Social media evidence in traditional and Cyber Crimes.

**Challenges:**

Social media forensics faces several challenges, including:

* Volume and Variety: The huge amount of data that users create across multiple platforms makes it hard to collect, analyze, and store.
* Concerns about privacy and ethics: It's always hard to walk the fine line between getting important evidence and protecting user privacy, which is made harder by the fact that different countries have different laws and platform policies.
* Changing Technology: Because social media sites and their features change so quickly, investigative tools and methods need to be updated all the time.
* Data accuracy: Because it is so easy to change or fake content on social media, checking the accuracy of data is very hard.
* Encryption and Anonymity: Bad people using encrypted messages and private accounts makes it harder to find them and get the right information.

Because of these problems, investigative methods and tools need to keep getting better, and social media sites and law enforcement need to work together to make sure that investigations are legal and successful.

# 5. Proposed Solution and Its Implementation

In this digital age, making sure that data is safe and easy to access is a top concern for everyone, and this is especially true when it comes to forensic proof. Keeping digital proof safe after it has been captured is very hard, especially when it comes to keeping it safe and making sure it can be used in court without being changed. Using cloud storage to back up digital proof, which adds an extra layer of security, looks like a good way to deal with this problem.

**Using cloud storage to store digital evidence**

A graph on a gray background

Description automatically generated

*Figure 3: Differences between cloud storage and regular storage*

It is much better to store digital evidence in the cloud because it protects its privacy, accuracy, and access. When compared to standard portable drives, cloud storage is cheaper, which means that you can store more data for less money. It adds strong security features, like strong encryption and advanced firewall defenses, to keep proof safe from being changed. Access control systems make sure that only authorized staff can get to proof, which lowers the risk of someone else getting to it without permission. By using two-factor authentication, you can add an extra layer of protection, even if your login details are stolen.

When you switch from standard storage methods to cloud storage, you get better protection, speed, and the ability to grow. Cloud services are flexible and easy to use because they can be accessed from almost anywhere and on any device. They also allow multiple users, which makes them even more appealing. But with this plan, you usually have to pay a monthly fee based on how much space you need..

**Putting in place effective security measures for the cloud**

1. **Data Privacy:** Cloud services make it possible to implement access control, so only authorized users can get to private files. By putting private data into groups and controlling who can see them, along with securing important files, data privacy is greatly improved. If data is intercepted, attackers can't use the information because it is encrypted.
2. **Data Availability:** It is very important that proof is available at the time of showing. Physical storage devices that are easy to break or mishandle can make data less accessible. Cloud storage, on the other hand, makes sure that only approved users can always access data, so you don't have to worry about physical damage or loss.
3. **Cost-effectiveness:** As the amount of data stored grows, the ability of cloud storage to be expanded becomes more useful. It might be cheaper to store small amounts of data on physical devices, but the cloud is a more practical and cost-effective way to store big amounts of data, making physical storage choices less useful and more expensive.

A diagram of a cloud computing system

Description automatically generated

Figure 4: Flow chart showing advantages of cloud storage

# 6. Experiment

## 6.1. Python Implementation

A screenshot of a computer program

Description automatically generated

A graph with a blue line and orange line

Description automatically generated

# 7. Discussion

The case study methodology employed in this research provided valuable insights into the effectiveness of utilizing PyCharm as a custom toolkit in digital forensic analysis. By analyzing real-world forensic cases and customizing PyCharm to meet the specific requirements of each case, this study aimed to evaluate PyCharm's performance, efficiency, and applicability in addressing the forensic challenges posed by diverse digital investigations.

The customization process involved integrating plugins, tools, and scripts into PyCharm to enhance its functionality for forensic analysis. As demonstrated in the provided code snippet, PyCharm's flexibility and extensibility allowed for seamless integration with the Pandas library for data manipulation and analysis. The use of Pandas facilitated the exploration of the overall distribution of event types across different event logs, providing forensic analysts with valuable insights into the nature and frequency of digital events.

Through the forensic analysis conducted using PyCharm, several key findings emerged. Firstly, PyCharm's user-friendly interface and powerful features enabled forensic analysts to conduct complex data analysis tasks with ease. The ability to write, execute, and debug Python scripts within PyCharm streamlined the forensic analysis process, allowing analysts to uncover important evidence and patterns within the digital data.

Furthermore, PyCharm's integration with external libraries and tools, such as Pandas, expanded its capabilities for forensic analysis. By leveraging the functionality of Pandas, forensic analysts were able to perform advanced data manipulation and visualization, facilitating deeper insights into the digital evidence. This highlights the importance of custom toolkit development in digital forensics, as it allows forensic analysts to tailor their tools to meet the specific needs of each investigation.

However, despite its strengths, PyCharm may also present certain limitations and challenges in the context of digital forensic analysis. For example, while PyCharm offers extensive support for Python development, it may lack specialized features and tools specifically designed for forensic analysis tasks. Additionally, the learning curve associated with PyCharm and Python programming may pose challenges for forensic analysts with limited programming experience.

Therefore, the case study methodology employed in this research provided valuable empirical evidence of PyCharm's effectiveness as a custom toolkit in digital forensic analysis. By customizing PyCharm to meet the specific requirements of real-world forensic cases and conducting rigorous forensic analysis, this study demonstrated the potential of PyCharm to enhance the efficiency, accuracy, and reliability of digital forensic investigations. Moving forward, further research and development efforts are warranted to explore additional customization options and address any limitations to maximize the utility of PyCharm in digital forensic practice.

# 8. Conclusion

Digital forensics has gained prominence in response to the rapid escalation of cyber-crimes. This paper provides an overview of digital forensics and explores the current trends identified by experts in the field. It argues the benefits of utilizing cloud storage over traditional methods for storing digital forensic data, highlighting improvements in cost efficiency, data protection, integrity, and ease of access. The implementation of these solutions is also explored. Furthermore, the paper emphasizes the need for digital forensic research to adapt and develop in response to specific challenges. It outlines the major obstacles faced by forensic professionals, including security threats and breaches, which underscore the importance of ongoing research in digital forensics. This research is crucial for refining methods of recovering digital evidence from forensic devices, ensuring its admissibility in criminal and civil legal proceedings. The paper calls for investigators to refine their strategies to align with evolving legal standards, focusing on techniques that guarantee the secure and unaltered transfer of digital evidence to the courtroom.

# 9. Contribution of Team Members

1. Introduction, Background – Pravali Rao
2. Problem Statement, Methodology - Manoj Kumar Kaleru
3. Experiment, Discussion and Conclusion - Shwetha Makineni

# References

1. Biggs, Stephen, and Stilianos Vidalis. "Cloud computing: The impact on digital forensic investigations." 2009 International Conference for Internet Technology and Secured Transactions,(ICITST). IEEE, 2009.
2. Koroniotis, Nickolaos, Nour Moustafa, and Elena Sitnikova. "Forensics and deep learning mechanisms for botnets in internet of things: A survey of challenges and solutions." IEEE Access 7 (2019): 61764-61785.
3. Khan, Suleman, et al. "A comprehensive review on adaptability of network forensics frameworks for mobile cloud computing." The Scientific World Journal 2014 (2014).
4. Baig, Zubair A., et al. "Future challenges for smart cities: Cybersecurity and digital forensics." Digital Investigation 22 (2017): 3-13.
5. Yaqoob, Ibrar, et al. "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges." Future Generation Computer Systems 92 (2019): 265-275
6. Sharma, Bhoopesh Kumar, et al. "Emerging trends in digital forensic and cyber security-an overview." 2019 Sixth HCT Information Technology Trends (ITT). IEEE, 2019.
7. Marcus, Aaron, ed. Design, User Experience, and Usability: Design Philosophy, Methods, and Tools: Second International Conference, DUXU 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013, Proceedings, Part I. Vol. 8012. Springer, 2013.
8. Rajput, Mohit, Rohit Agrawal, and Dilip Kumar Sharma. "A study and comparative analysis of web personalization techniques." 2013 IEEE Conference on Information & Communication Technologies. IEEE, 2013.
9. Arshad, Humaira, Aman Jantan, and Esther Omolara. "Evidence collection and forensics on social networks: Research challenges and directions." Digital Investigation 28 (2019): 126-138.
10. Masdari, Mohammad, and Marzie Jalali. "A survey and taxonomy of DoS attacks in cloud computing." Security and Communication Networks 9.16 (2016): 3724-3751.
11. Al-Khateeb, Haider, Gregory Epiphaniou, and Herbert Daly. "Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger." Blockchain and Clinical Trial. Springer, Cham, 2019. 149-168.
12. Kebande, Victor R., and Hein S. Venter. "On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges." Australian Journal of Forensic Sciences 50.2 (2018): 209-238.
13. Nikkel, Bruce. Practical Forensic Imaging: Securing Digital Evidence with Linux Tools. No Starch Press, 2016.
14. Roussev, Vassil, et al. "Cloud forensics–Tool development studies & future outlook." Digital investigation 18 (2016): 79-95

# Appendix

1. Github Link: <https://github.com/pravalirao/Digital-Forensics-Analysis>

2. Example test data and queries if small

A computer screen shot of a computer code

Description automatically generated