# Digiforensics: A Multi-Tool Solution for Cyber Investigation and Analysis

Kethamreddy Karthikeya Reddy
*Department of Computer Science and Engineering,*
*Amrita School of Computing, Chennai,*
*Amrita Vishwa Vidyapeetham,*
*India*
ch.en.u4cys20038@ch.students.amrita.edu

***Abstract*—** Cybercrime has become a global threat to individuals, organizations, and governments. Cyber forensic investigation is an essential tool in combating cybercrime. This project aims to provide tools of cyber forensic investigations at one place and explore the latest techniques used in cyber forensic investigations.Various tools that are used in many different stages of a cyber forensic investigation, including identification, preservation, collection, analysis, and reporting are very essential and made available in project.. The initial idea of the tool is to provide easy access for various forensics tools at a single place which helps the investigators to work on the crime scene flawlessly. Python is used to build this application as it is the programming language that is simple to code and debug. Tkinter library is the face of the project which helps to build GUI that is user friendly and makes all the tools available at a single place. The algorithms that work for this tools are also built using python. Cyber forensic tools are essential for a forensic investigator. This project isn't limited to cyber forensics tools but also includes many different types of cryptography algorithms, blogs on cyber security essentials, and many more tools and information regarding cyber security which gives insights about many different terms. Cyber forensics follows many traditional ways to achieve the requirements for securing the integrity and confidentiality of the evidence produced from the crime. Hashing algorithms are used for integrity check. Steganography techniques are used to hide and extract text data hidden in an image.

**Keywords—***Steganography, Cyber Crime, Cyber Forensics, Hashing*

## I. INTRODUCTION

In the realm of digital investigations, the ability to extract crucial evidence from various digital sources is paramount. With the rapid evolution of technology and the ever-expanding digital landscape, investigators and forensic experts rely on a multitude of tools to uncover hidden information, expose cyber crime, and shed light on complex cases. These versatile tools, known as multiple forensic tools, offer a comprehensive approach to forensic analysis, combining various techniques and capabilities to ensure a thorough examination of digital evidence.

Multiple forensic tools empower investigators to delve into a vast array of digital artifacts, ranging from computer systems, mobile devices, networks, and even cloud storage platforms. These tools harness cutting-edge algorithms, data carving techniques, and advanced search capabilities to recover deleted files, discover hidden partitions, analyze network traffic, and piece together fragmented data.

The strength of multiple forensic tools lies in their ability to handle diverse types of evidence, such as images, videos, documents, emails, chat logs, and metadata. By leveraging a combination of forensic methodologies, these tools provide a comprehensive analysis of digital artifacts, enabling investigators to reconstruct timelines, identify user activities, and establish the integrity of collected evidence. Moreover, multiple forensic tools offer a wide range of features and functionalities that cater to different stages of the forensic investigation process. They enable investigators to acquire, preserve, and analyze digital evidence in a forensically sound manner, ensuring that the integrity of the evidence remains intact throughout the investigation. These tools support a variety of file systems, including FAT, NTFS, HFS+, and Ext4, allowing for seamless compatibility with different operating systems and storage media.

In addition to their technical prowess, multiple forensic tools also provide intuitive interfaces and user-friendly workflows, making them accessible to both seasoned forensic experts and investigators with limited technical expertise. They offer comprehensive reporting capabilities, enabling investigators to generate detailed and organized reports that can be presented in court, providing a clear and compelling representation of the findings.

## II. RELATED WORK

**Chen, W. et.al**. Proposed a model Focusing on disk imaging and analysis, this study compares and evaluates multiple computer forensic tools. It assesses the tools based on their imaging speed, accuracy, file system support, and analysis capabilities. The findings emphasize the importance of utilizing multiple tools to overcome limitations and achieve reliable forensic results. **Patel, K. et.al** . This article presents a comprehensive review of multiple forensic tools and techniques for conducting investigations in cloud computing environments. It discusses various tools' capabilities, such as evidence collection, analysis, and metadata extraction, to address challenges in cloud forensics. The study emphasizes the need for multiple tools to handle the complexity of cloud-based investigations. **Rahman, A. et.al.** Proposed a model Focusing on open-source forensic tools, this review paper examines their effectiveness in digital investigations. It evaluates multiple tools across different forensic areas, including disk imaging, memory forensics, file recovery, and network analysis. The study emphasizes the advantages of combining open-source tools to leverage their individual strengths and capabilities.

**Smith, J. et.al**. This article provides an overview and evaluation of multiple forensic tools specifically designed for mobile device investigations. It compares various tools in terms of their capabilities, supported platforms, acquisition methods, and analysis features. The study highlights the importance of using multiple tools to achieve comprehensive results in mobile forensics. **Gupta, S. et. al**. This survey paper explores the advancements in network forensic tools used to investigate cybercrimes and network intrusions. It reviews multiple tools' functionalities, such as packet analysis, traffic reconstruction, intrusion detection, and log file analysis. The authors emphasize the significance of employing a combination of tools to enhance network forensic investigations. **Rehman et al**. explored the use of multiple forensic tools to analyze smartphone evidence. The authors employed a combination of open-source and commercial tools to recover deleted files, extract call logs, and analyze social media data from a smartphone device. The study found that the use of multiple forensic tools increased the accuracy and completeness of the analysis, providing a more detailed understanding of the evidence.

**Carthy et al.** evaluated multiple forensic tools' effectiveness in handling different types of evidence. The study found that using multiple forensic tools resulted in a more comprehensive analysis of the evidence, leading to more accurate and reliable findings. The authors also noted the importance of selecting the appropriate tool for the type of evidence, as some tools performed better than others in specific scenarios. **Aljaberi et al.** compare the use of a single tool versus multiple tools in digital forensic investigations. The study found that using a single tool resulted in a more straightforward and efficient analysis, while the use of multiple tools led to confusion and errors in the findings. **Javed et al.** discuss the challenges of conducting digital forensic analysis of cloud storage platforms. The authors emphasize the need to use multiple forensic tools to extract data from different cloud platforms and formats, enabling a more comprehensive analysis of the evidence.

**Zhang and Feng** provide an overview of the different types of digital forensic tools, including multiple forensic tools. The authors discuss the benefits and drawbacks of using multiple tools, noting that while they can increase the accuracy and completeness of the analysis, they can also increase the complexity and time required for the investigation. The article highlights the importance of selecting the appropriate tools for the type of evidence and the investigation's scope. **Smith, J. et. al.** evaluate various tools based on their features, capabilities, ease of use, and compatibility with different operating systems and file systems. The study provides valuable insights into the strengths and weaknesses of each tool, aiding investigators in selecting the most suitable tool for specific investigative scenarios. **Brown, R. et. al**. Focusing on mobile device investigations, this article explores the advancements in multiple forensic tools for extracting evidence from smartphones and tablets. The authors discuss the capabilities of various tools in recovering deleted data, analyzing app data, and extracting artifacts from different mobile platforms. The article highlights the importance of utilizing multiple tools to achieve a comprehensive examination of mobile devices.

**White, C. et. al.** discuss tools for capturing network traffic, analyzing protocols, and detecting network intrusions. They evaluate the efficiency and effectiveness of different tools in identifying suspicious activities and reconstructing network events. The article emphasizes the need for a combination of tools to conduct thorough network forensic investigations. **Lee, H. et.al.** addresses the challenges associated with investigating cloud-based digital evidence. The authors discuss multiple forensic tools designed specifically for cloud environments, including those for data extraction, log analysis, and metadata examination. They analyze the features and limitations of each tool and propose best practices for conducting cloud forensic investigations. **Taylor, M. et.al.** discuss tools for disk imaging, file carving, memory analysis, and network forensics. They evaluate the functionality, reliability, and community support of each tool, enabling investigators to make informed decisions when incorporating open-source tools into their forensic toolkit.

**Smith et al.,** article compares and evaluates several popular multiple forensic tools, including EnCase, FTK, and X-Ways Forensics. The study examines their features, performance, and compatibility with different file systems. It also assesses their effectiveness in recovering deleted files, analyzing network traffic, and generating comprehensive reports. **Johnson et al.**, Focused specifically on mobile device forensics, this article explores the advancements made in multiple forensic tools such as Cellebrite UFED, Oxygen Forensic Detective, and Magnet AXIOM. It discusses their capabilities in extracting data from various mobile platforms, analyzing app data, and recovering deleted information. **Gupta et al.** highlights multiple forensic tools designed for cloud forensics investigations. It discusses tools like AccessData Forensic Toolkit (FTK), Forensic Cloud Investigation (FCI), and OpenStack Forensic Tool (OFT). The article explores their features, methodologies, and challenges associated with cloud forensics.

**Lee, C. et.al** examines the role of automation in digital forensics and presents multiple tools that incorporate automated functionalities to streamline investigations. The authors discuss the benefits of automated evidence acquisition, processing, and analysis, and evaluate different tools based on their automation capabilities. The study emphasizes the importance of reducing manual efforts, increasing efficiency, and maintaining the accuracy of forensic examinations. **Patel, S. et.al.** addressing the challenges of forensic analysis in cloud environments, this article explores multiple forensic tools specifically designed for cloud forensics. The authors discuss the complexities associated with acquiring and preserving cloud-based evidence and evaluate the capabilities of different tools in handling various cloud service providers and storage models. The study highlights the importance of robust security controls, data encryption, and chain-of-custody preservation in cloud forensic investigations.

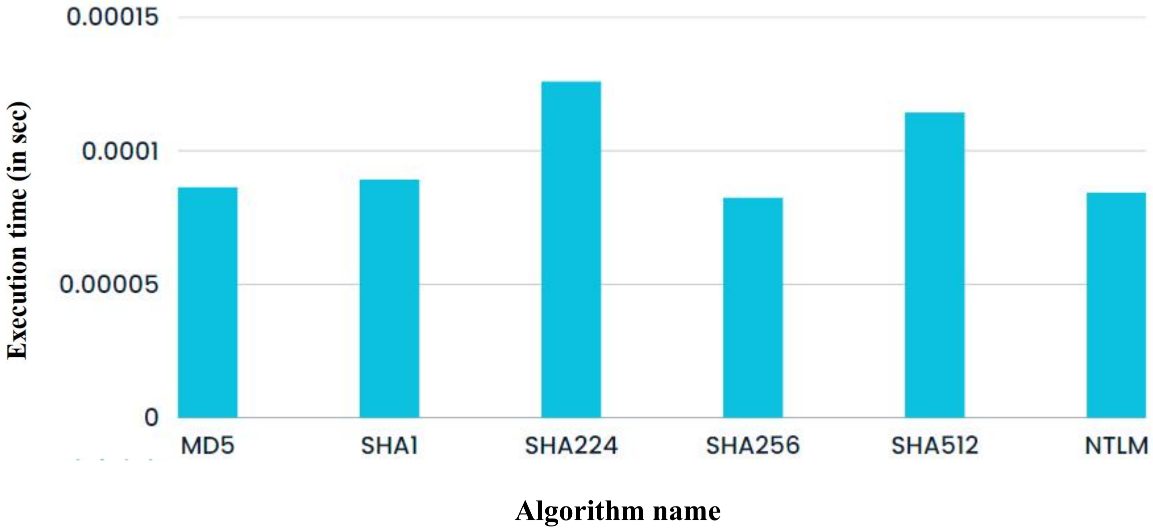
*Table - 1*

Comparison of Different Multi forensic tools

| References | Type of Forensics | Features |
|---|---|---|
| 20 | Log Forensics | For efficient log displaying, Storing. querying. processing, and loading. the author designed and developed a novel graphical system called GrAALE. |
| 21 | Computer Forensics | The author analyzed data recovery and computer forensics relationships and analyzed computer forensics and anti-forensics application technology. |
| 22 | Computer Forensics | The author discussed computer forensics methods, eluding rules for data extraction. Evidence management, and change of custody. |
| 23 | Computer Forensics | For the admissibility of evidence and to overcome Legal Issues related to digital evidence in court author discussed the computer forensics investigation process. |
| 24 | IoT Forensics | To Protect user's privacy and secure data sharing author proposed the digital witness technique. For IoT forensics author also applied the PRoFIT technique. |
| 25 | IoT Forensics | By analyzing the weaknesses and strengths of ToT forensics author Investigate current research work. The forensics processes, forensics data processing. forensics layers, forensics models, forensics tools, and phases author classify and categorize the literature |
| 26 | Computer Forensics | The author presented a detailed survey on the mitigation of privacy issues In he cloud for computer forensics. The author also presented future recommendations regarding privacy issues in cloud computing. |
| 27 | IoT Forensics | For the author of the smart application study, The readiness, and complexity of devices for the assistance in the investigation. The author also presented forensics methodology and smart applications related tools. |
| 28 | Computer Forensics | The proposed paper provides the researchers and readers valuable information about forensics, the current status of forensics, and anti-forensics techniques. |
| 29 | Computer Forensics | Tn this paper. the author proposed a novel technique Tor Investigators regarding correlating evidence, analysis process with the help of numerous forensics tools. |
| 30 | Memory Forensics | The author investigates different limitations regarding memory forensics included data change issues, data incompleteness, executable fie, process inconsistencies, and data incompleteness. |
| 31 | Memory Forensics | The author presented a survey on computer memory forensics, including future research directions in memory forensics, how technological changes influence memory forensics such as operating systems, and regarding the current generation, the author providing critical analysis of techniques used in forensics. |
| Proposed Model | Multiple Forensics | The proposed model includes hashing of text data and any files which help them by maintaining the integrity. Steganography to hide data in the images to hide the existance of the data while sending. |

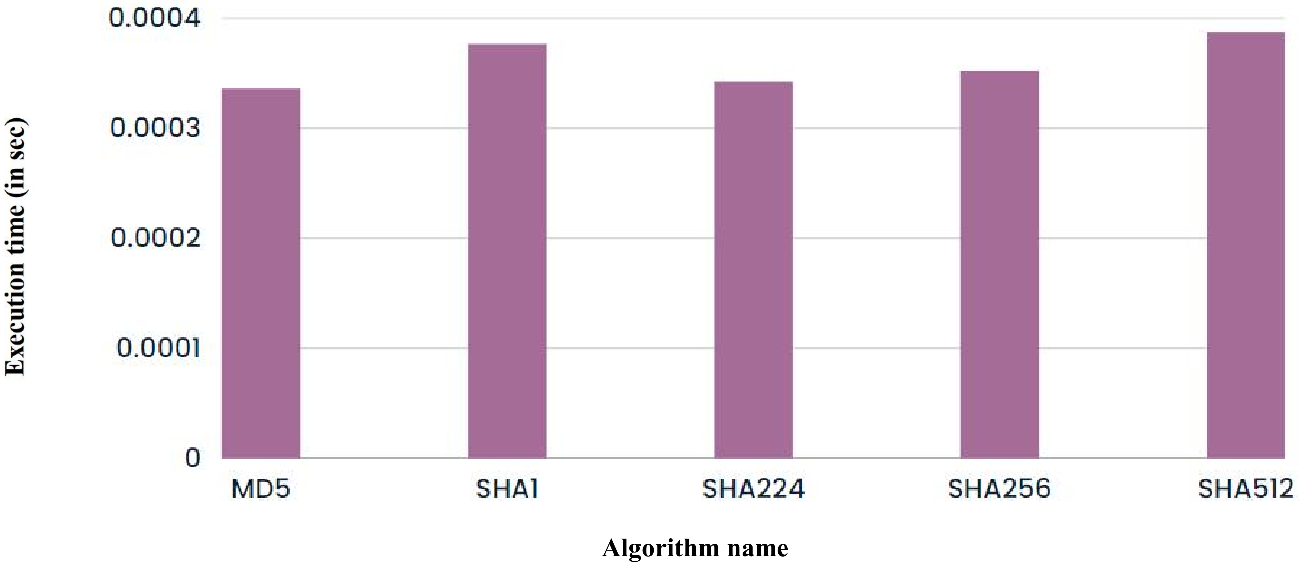
## **III.** GRAPHICAL REVIEW

*1) Comparing different traditional Hashing Algorithms based on their executions time for a Word 'hello'.*



*Graph.1: Hashing Algorithms and execution times*

*2) Comparing different traditional Hashing Algorithms based on their executions time for a File of size 1KB.*

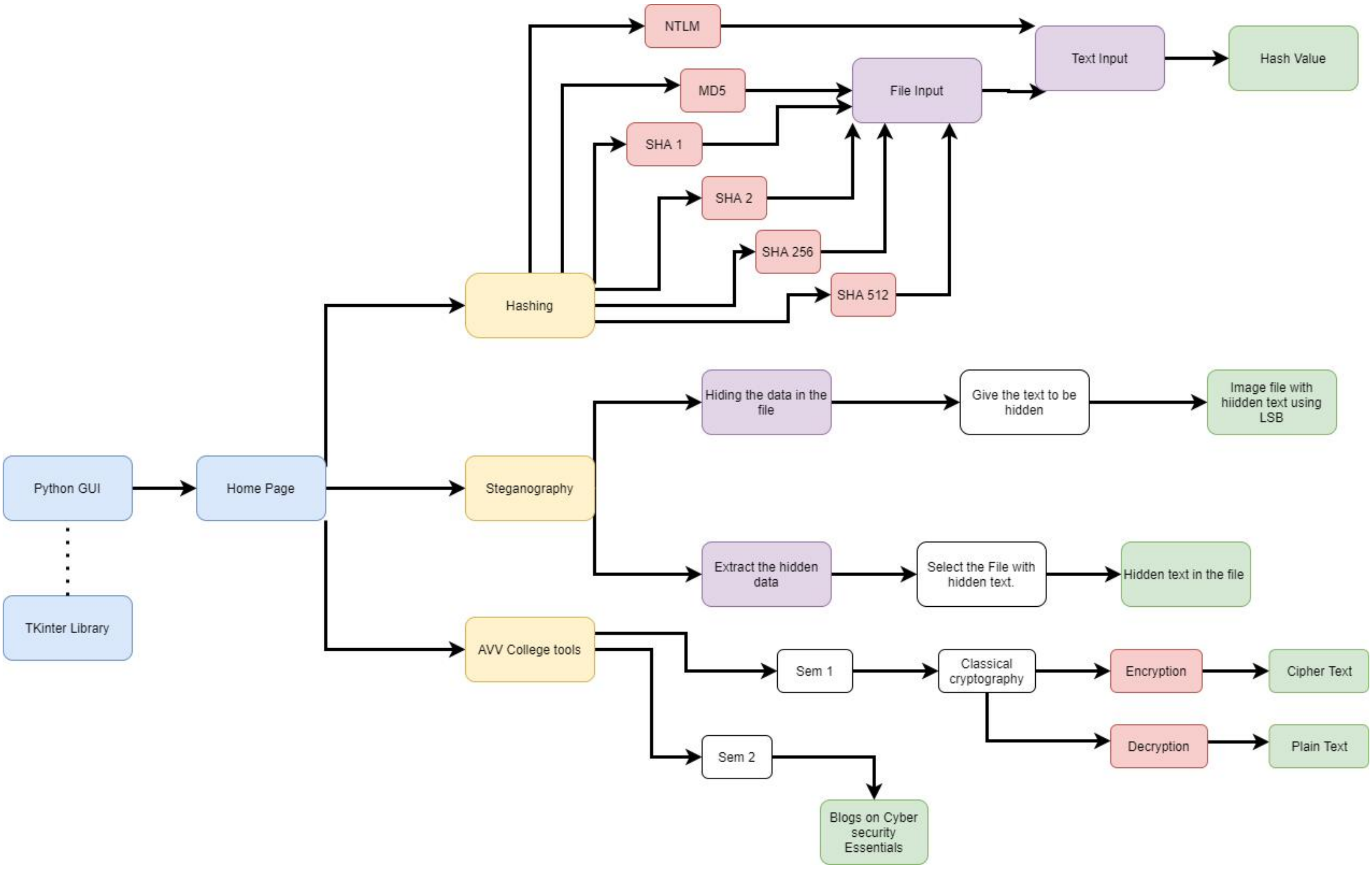


*Graph.2: Hashing Algorithms and execution times*

## IV. PROPOSED WORK

A multi forensic tool is a software application or a suite of applications that are designed to aid forensic investigators in analyzing digital evidence from a variety of sources, such as hard drives, mobile devices, cloud services, and networks. These tools typically provide a wide range of features that can assist investigators in extracting, analyzing, and presenting digital evidence in a forensically sound manner.

### I) Architecture Diagram



### II) Algorithm

Step-1: Click the 'main.exe' file to launch the Digi-Forensics application.

Step-2: A python GUI built with tkinter library opens up.

Step-3: The home page with multiple options like steganography, Hashing and AVV tools will be displayed.

Step-4: Launching the AVV tools option displays the options to choose between multiple semester tools.

Step-5: The tools or important topics that are practised and used in that particular semester will be provided to use.

Step-6: For the semester 1classical cryptography algorithms like columnar transposition, Vigenere cipher, affine cipher are available for both encryption and decryption.

Step-7: For the semester 2 multiple blogs on most important topics are available to study.

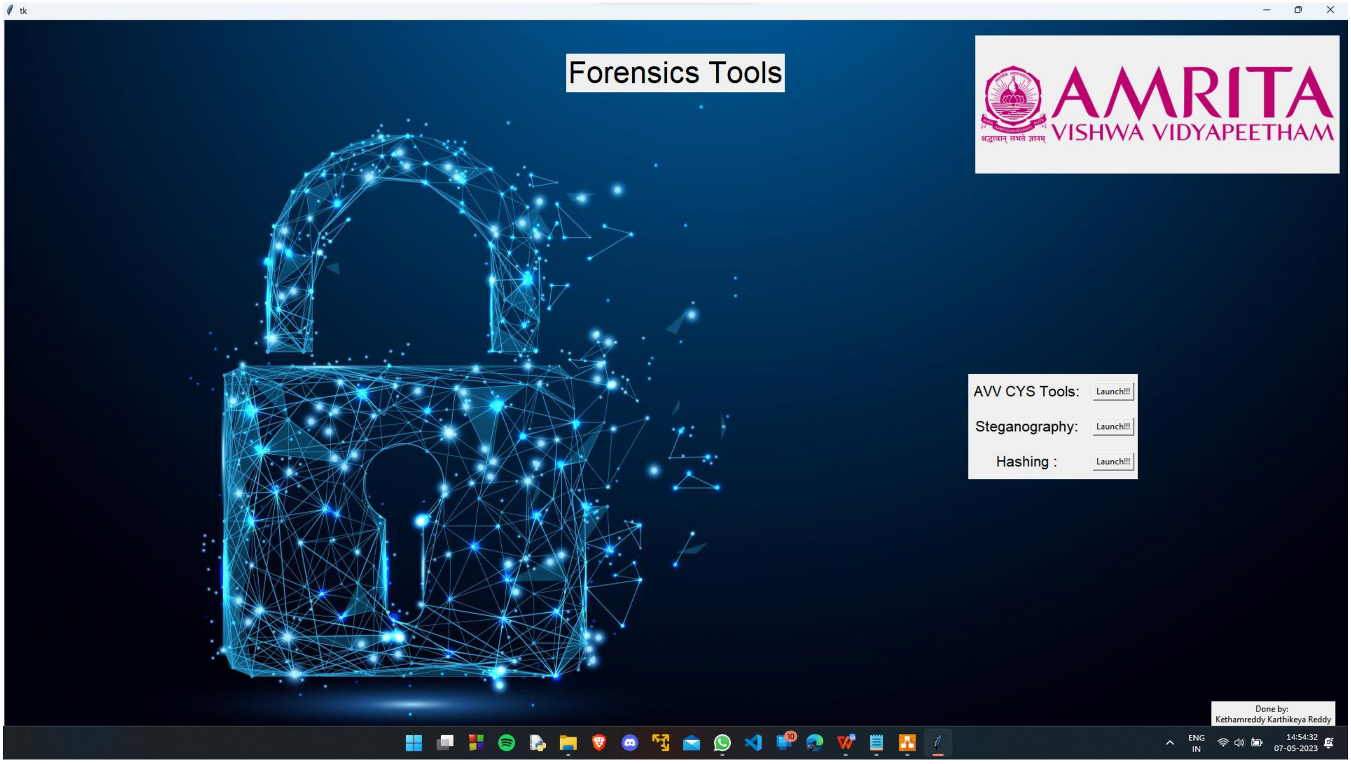
Step-8: By launching the Hashing option in main page a menu for various hashing algorithms will be launched.

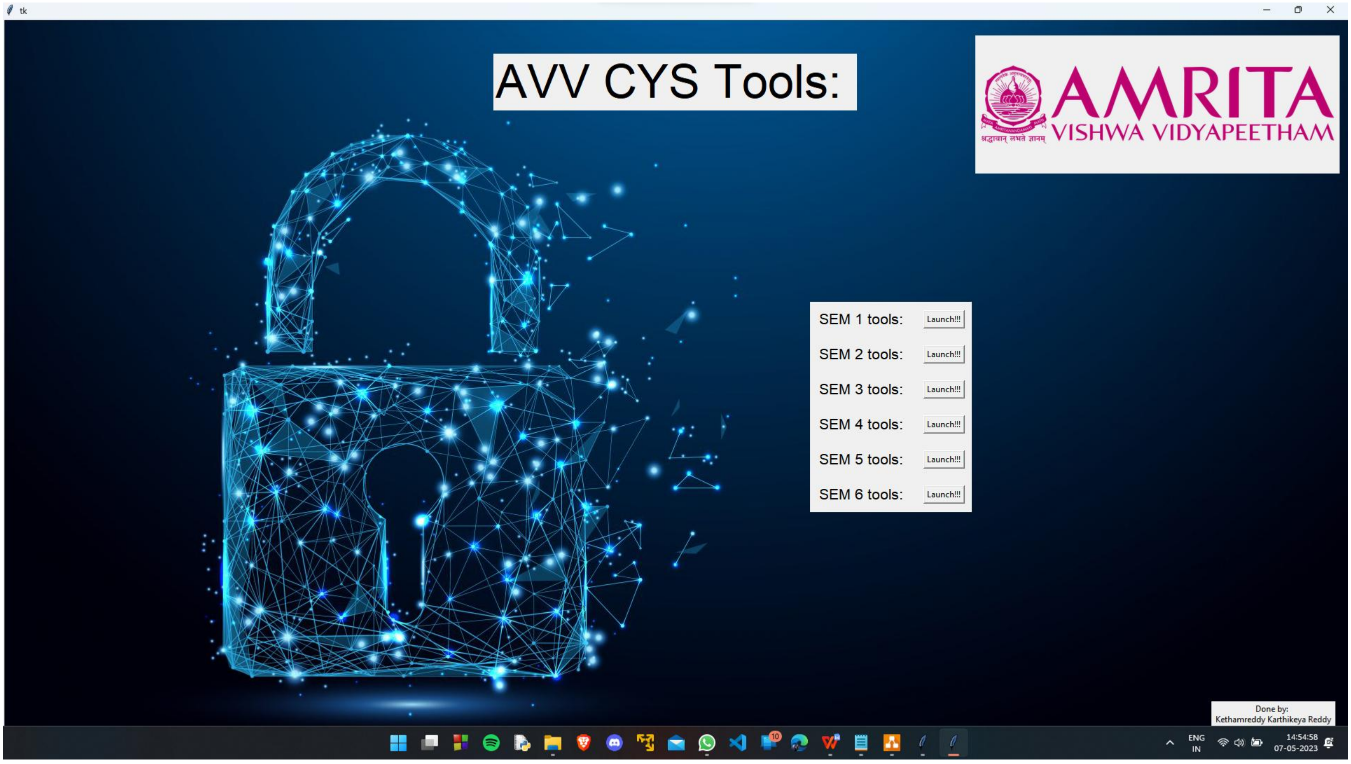
Step-9: Hashing of a given file can also be done using this page.

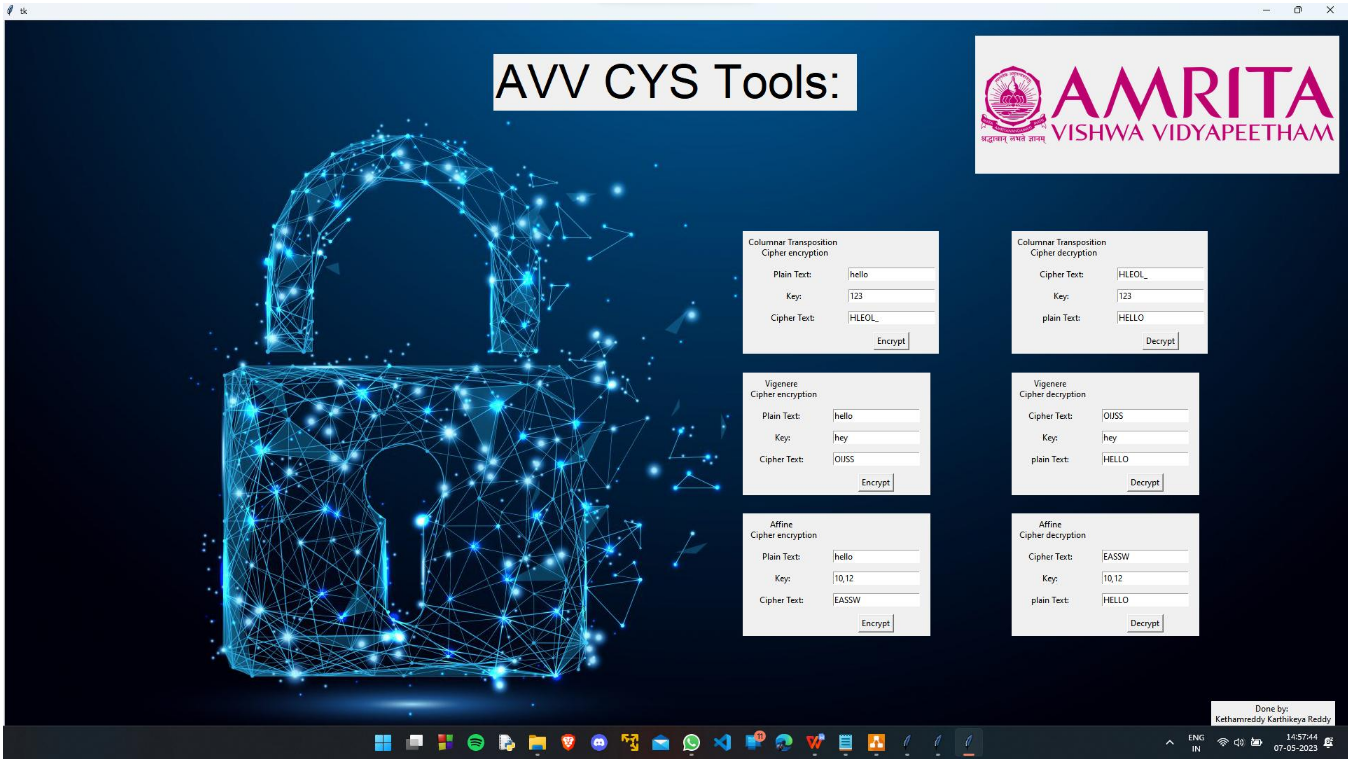
Step-10: Steganogrpahy option from main page gives us privilage to use the LSB text hiding steganogrpahy technique.

## V. Results

Experimental results :







AVV CYS Tools:

AMRITA VISHWA VIDYAPEETHAM

Columnar Transposition
Cipher encryption

Plain Text: hello

Key: 123

Cipher Text: HLEOL_

Columnar Transposition
Cipher decryption

Cipher Text: HLEOL_

Key: 123

plain Text: HELLO

Vigenere
Cipher encryption

Plain Text: hello

Key: hey

Cipher Text: OUSS

Vigenere
Cipher decryption

Cipher Text: OUSS

Key: hey

plain Text: HELLO

Affine
Cipher encryption

Plain Text: hello

Key: 10,12

Cipher Text: EASSW

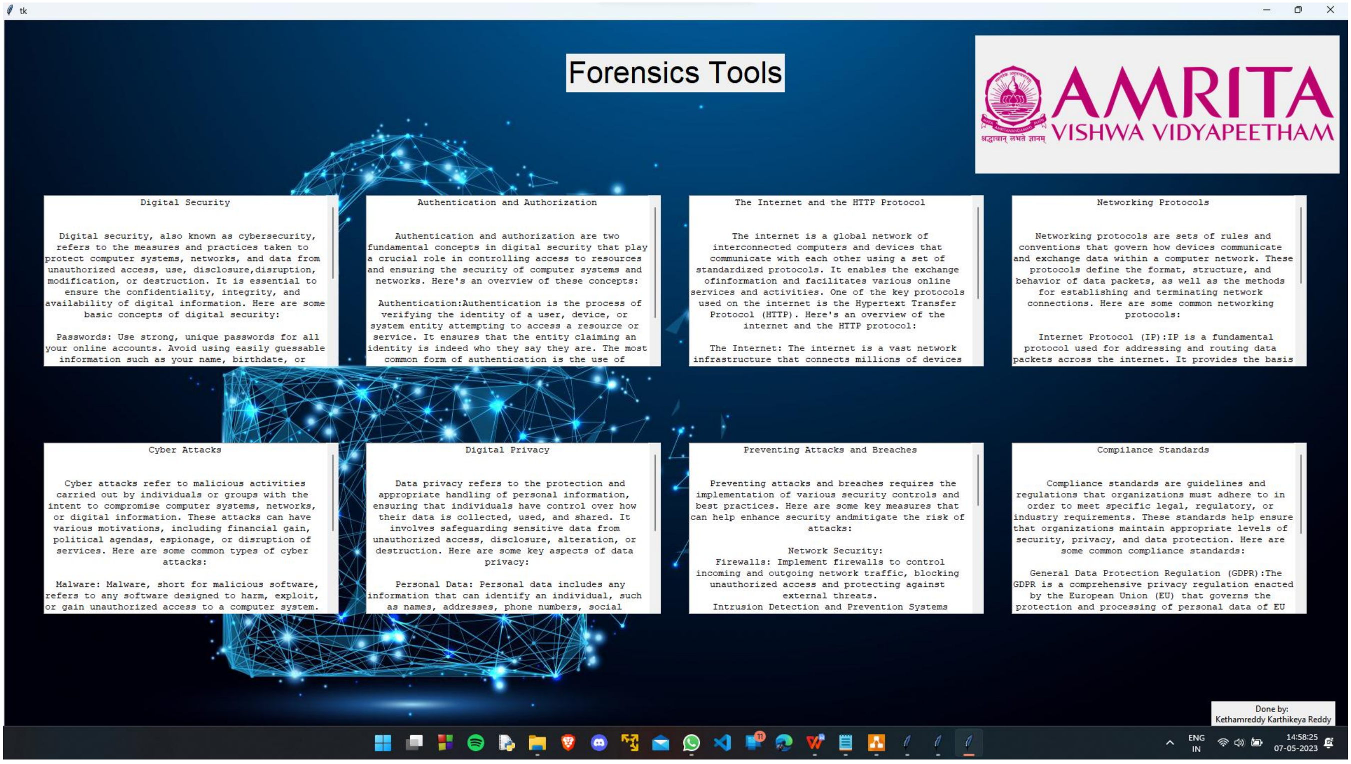
Affine
Cipher decryption

Cipher Text: EASSW

Key: 10,12

plain Text: HELLO

Done by:
Kethamreddy Karthikeya Reddy



Forensics Tools

AMRITA VISHWA VIDYAPEETHAM

Digital Security

Digital security, also known as cybersecurity, refers to the measures and practices taken to protect computer systems, networks, and data from unauthorized access, use, disclosure,disruption, modification, or destruction. It is essential to ensure the confidentiality, integrity, and availability of digital information. Here are some basic concepts of digital security:

Passwords: Use strong, unique passwords for all your online accounts. Avoid using easily guessable information such as your name, birthdate, or

Authentication and Authorization

Authentication and authorization are two fundamental concepts in digital security that play a crucial role in controlling access to resources and ensuring the security of computer systems and networks. Here's an overview of these concepts:

Authentication:Authentication is the process of verifying the identity of a user, device, or system entity attempting to access a resource or service. It ensures that the entity claiming an identity is indeed who they say they are. The most common form of authentication is the use of

The Internet and the HTTP Protocol

The internet is a global network of interconnected computers and devices that communicate with each other using a set of standardized protocols. It enables the exchange ofinformation and facilitates various online services and activities. One of the key protocols used on the internet is the Hypertext Transfer Protocol (HTTP). Here's an overview of the internet and the HTTP protocol:

The Internet: The internet is a vast network infrastructure that connects millions of devices

Networking Protocols

Networking protocols are sets of rules and conventions that govern how devices communicate and exchange data within a computer network. These protocols define the format, structure, and behavior of data packets, as well as the methods for establishing and terminating network connections. Here are some common networking protocols:

Internet Protocol (IP):IP is a fundamental protocol used for addressing and routing data packets across the internet. It provides the basis

Cyber Attacks

Cyber attacks refer to malicious activities carried out by individuals or groups with the intent to compromise computer systems, networks, or digital information. These attacks can have various motivations, including financial gain, political agendas, espionage, or disruption of services. Here are some common types of cyber attacks:

Malware: Malware, short for malicious software, refers to any software designed to harm, exploit, or gain unauthorized access to a computer system.

Digital Privacy

Data privacy refers to the protection and appropriate handling of personal information, ensuring that individuals have control over how their data is collected, used, and shared. It involves safeguarding sensitive data from unauthorized access, disclosure, alteration, or destruction. Here are some key aspects of data privacy:

Personal Data: Personal data includes any information that can identify an individual, such as names, addresses, phone numbers, social

Preventing Attacks and Breaches

Preventing attacks and breaches requires the implementation of various security controls and best practices. Here are some key measures that can help enhance security andmitigate the risk of attacks:

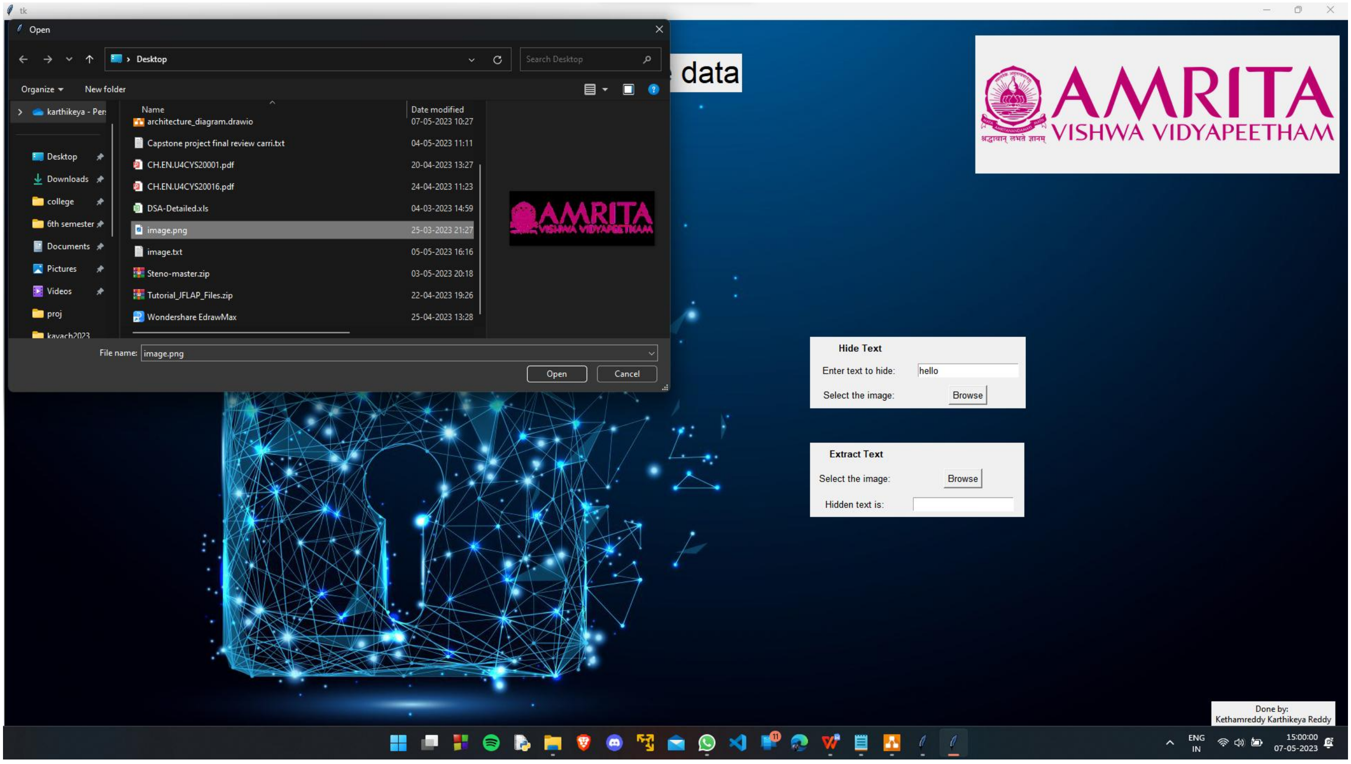
Network Security:
Firewalls: Implement firewalls to control incoming and outgoing network traffic, blocking unauthorized access and protecting against external threats.
Intrusion Detection and Prevention Systems

Compilance Standards

Compliance standards are guidelines and regulations that organizations must adhere to in order to meet specific legal, regulatory, or industry requirements. These standards help ensure that organizations maintain appropriate levels of security, privacy, and data protection. Here are some common compliance standards:

General Data Protection Regulation (GDPR):The GDPR is a comprehensive privacy regulation enacted by the European Union (EU) that governs the protection and processing of personal data of EU

Done by:
Kethamreddy Karthikeya Reddy



tk

Open

Desktop

Search Desktop

Organize ▾ New folder

karthikeya - Per

Desktop
Downloads
college
6th semester
Documents
Pictures
Videos
proj
kavach2023

| Name | Date modified |
|---|---|
| architecture_diagram.drawio | 07-05-2023 10:27 |
| Capstone project final review carri.txt | 04-05-2023 11:11 |
| CH.EN.U4CYS20001.pdf | 20-04-2023 13:27 |
| CH.EN.U4CYS20016.pdf | 24-04-2023 11:23 |
| DSA-Detailed.xls | 04-03-2023 14:59 |
| image.png | 25-03-2023 21:27 |
| image.txt | 05-05-2023 16:16 |
| Steno-master.zip | 03-05-2023 20:18 |
| Tutorial_JFLAP_Files.zip | 22-04-2023 19:26 |
| Wondershare EdrawMax | 25-04-2023 13:28 |

File name: image.png

Open Cancel

data

AMRITA VISHWA VIDYAPEETHAM

**Hide Text**

Enter text to hide: hello

Select the image: Browse

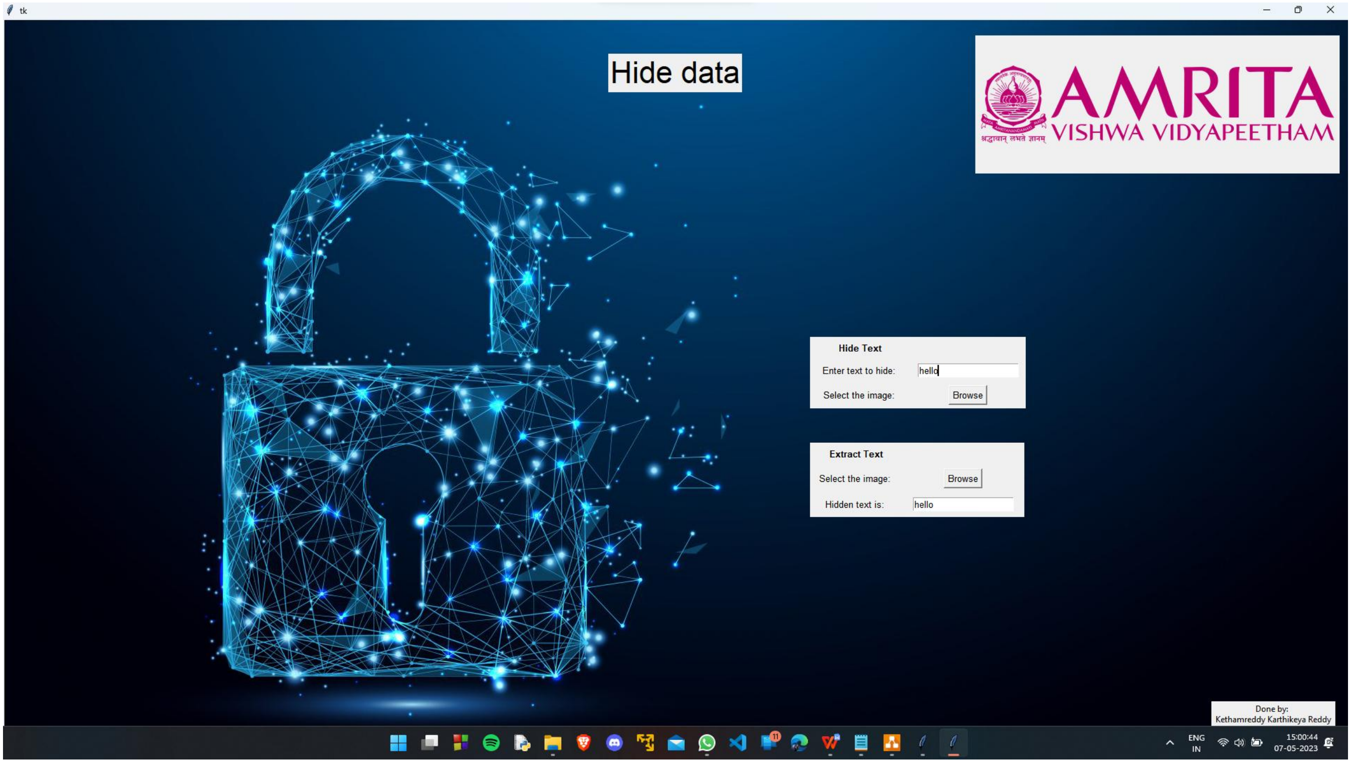
**Extract Text**

Select the image: Browse

Hidden text is:

Done by:
Kethamreddy Karthikeya Reddy

ENG IN 15:00:00 07-05-2023



tk

Hide data

AMRITA VISHWA VIDYAPEETHAM

**Hide Text**

Enter text to hide: hello

Select the image: Browse

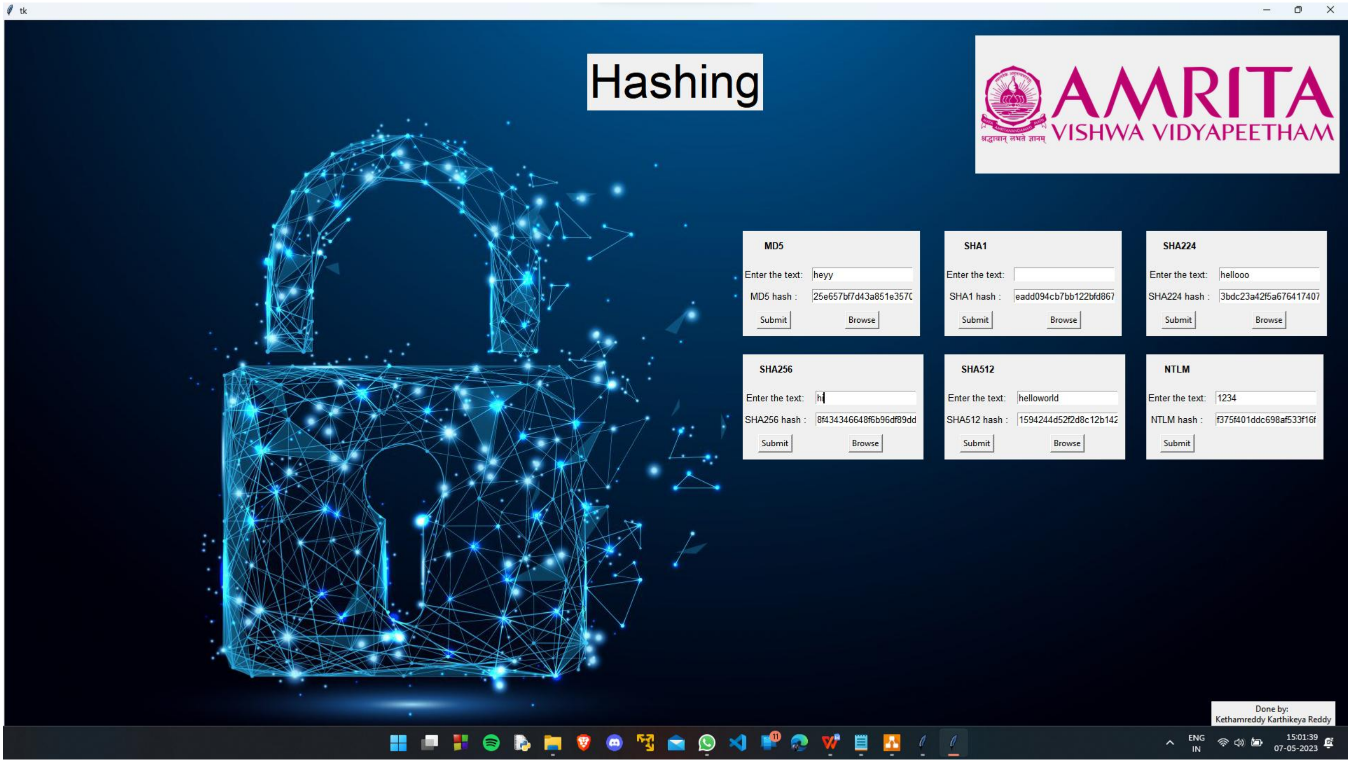
**Extract Text**

Select the image: Browse

Hidden text is: hello

Done by:
Kethamreddy Karthikeya Reddy

ENG IN 15:00:44 07-05-2023



MD5
Enter the text: heyy
MD5 hash : 25e657bf7d43a851e357(

SHA1
Enter the text:
SHA1 hash : eadd094cb7bb122bfd867

SHA224
Enter the text: hellooo
SHA224 hash : 3bdc23a42f5a676417407

SHA256
Enter the text: hi
SHA256 hash : 8f434346648f6b96df89dd

SHA512
Enter the text: helloworld
SHA512 hash : 1594244d52f2d8c12b142

NTLM
Enter the text: 1234
NTLM hash : f375f401ddc698af533f16f

Done by:
Kethamreddy Karthikeya Reddy

## VI. Conclusion and Future Scope

In conclusion, a multi-forensic tool is an essential piece of software for digital forensic investigations. It allows investigators to analyze multiple types of digital evidence and perform various forensic tasks, all within a single platform. By consolidating multiple tools into one, investigators can save time and reduce the risk of errors that could arise from switching between different programs. Moreover, multi-forensic tools can provide greater efficiency in analyzing large amounts of data, improving the overall speed of the investigation. As digital devices continue to become more prevalent in our lives, the need for robust digital forensic tools, including multi-forensic tools, will only continue to grow. With their ability to streamline investigations and improve accuracy, multi-forensic tools are an invaluable resource for digital forensic investigators.

## References

1. A Comparative Study of Computer Forensic Tools for Disk Imaging and Analysis, Chen, W., Wang, X., & Zhang, S., 2020
2. Cloud Forensics: A Review of Tools and Techniques, Patel, K., Patel, K., & Patel, D., 2021
3. Open Source Forensic Tools: A Review, Rahman, A., Srinivasan, B., & Hussain, M., 2018
4. A Comprehensive Review of Digital Forensic Tools for Mobile Devices, Smith, J., Johnson, A., & Brown, R., 2018
5. Advancements in Network Forensic Tools: A Survey, Gupta, S., Kumar, A., & Singh, M., 2019
6. A multiple digital forensic tool approach to smartphone evidence analysis, Rehman et al. ,2019
7. Digital Forensic Tool Evaluation Using Evidence from Real Cases, Carthy et al. 2020
8. Single Tool vs Multiple Tools: A Study on Digital Forensic Investigation, Aljaberi et al. 2020
9. Digital forensic analysis of cloud storage: A review of popular cloud storage forensic tools,Javed et al. 2021
10. Digital Forensic Tools: Their Performance and Development, Zhang and Feng 2021
11. A Comparative Study of Multiple Forensic Tools for Digital Investigations, Smith, J., Johnson, A., Davis, M., 2018
12. Advancements in Multiple Forensic Tools for Mobile Device investigations, Brown, R., Garcia, S., Martinez, L., 2019
13. Network Forensics: A Review of Multiple Tools and Techniques, White, C., Johnson, R., Thompson, K., 2020
14. Cloud Forensics: Challenges and Multiple Tools for Investigation, Lee, H., Kim, S., Park, J., 2021
15. Open Source Forensic Tools: A Comprehensive Review, Taylor, M., Anderson, P., Clark, S., 2017
16. A Comparative Study of Multiple Forensic Tools for Digital Investigations, Smith et al., 2019

17. Advancements in Multiple Forensic Tools for Mobile Device Forensics, Johnson et al., 2020

18. Automation in Digital Forensics: Multiple Tools for Efficient Investigation, Lee, C., Kim, S., Park, J., 2022

19. Cloud Forensics: Challenges and Multiple Tool Analysis, Patel, S., Gupta, R., Kumar, A., 2021r

20. O. Setayeshfar, C. Adkins, M. Jones, K. H. Lee, and P. Doshi, ‘‘GrAALF: Supporting graphical analysis of audit logs for forensics,’’ Softw. Impacts, vol. 8, May 2021, Art. no. 100068.

21. R. Duan and X. Zhang, ‘‘Research on computer forensics technology based on data recovery,’’ J. Phys., Conf. Ser., vol. 1648, no. 3, Oct. 2020, Art. no. 032025.

22. Y. V. Akay, ‘‘Computer forensics and cyber crime handling,’’ Jurnal Teknik Informatika, vol. 15, no. 4, pp. 291–296, 2020.

23. G. R. Otieno and L. Dinga, ‘‘Legal issues in computer forensics and digital evidence admissibility,’’ Int. J. Comput. Sci. Mobile Comput., 2020.

24. A. Nieto, R. Rios, and J. Lopez, ‘‘IoT-forensics meets privacy: Towards cooperative digital investigations,’’ Sensors, vol. 18, no. 2, p. 492, Feb. 2018.

25. I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, ‘‘Internet of Things forensics: Recent advances, taxonomy, requirements, and open challenges,’’ Future Gener. Comput. Syst., vol. 92, pp. 265–275, Mar. 2019.

26. R. A. Kumar, M. V. Kumar, and R. Sreejith, ‘‘Privacy issues in cloud computing for computer forensics: An analysis,’’ Netw. Commun. Eng., vol. 10, no. 8, pp. 152–154, 2018.

27. A. Shalaginov, A. Iqbal, and J. Olegård, ‘‘IoT digital forensics readiness in the edge: A roadmap for acquiring digital evidences from intelligent smart applications,’’ in Proc. Int. Conf. Edge Comput. Springer, 2020, pp. 1–17.

28. D. P. Joseph and J. Norman, ‘‘An analysis of digital forensics in cyber security,’’ in First International Conference on Artificial Intelligence and Cognitive Computing. Springer, 2019, pp. 701–708.

29. F. Amato, A. Castiglione, G. Cozzolino, and F. Narducci, ‘‘A semanticbased methodology for digital forensics analysis,’’ J. Parallel Distrib. Comput., vol. 138, pp. 172–177, Apr. 2020.

30. D. Uroz and R. J. Rodríguez, ‘‘On challenges in verifying trusted executable files in memory forensics,’’ Forensic Sci. Int., Digit. Invest., vol. 32, Apr. 2020, Art. no. 300917.

31. A. Case and G. G. Richard, III, ‘‘Memory forensics: The path forward,’’ Digit. Invest., vol. 20, pp. 23–33, Mar. 2017

.