1. COMPANY PROFILE

Fig 1: Company Logo

IGeeks Technologies is a multi-disciplinary Information Technology & Services company based in Bangalore, India. It provides a range of technology solutions, academic support services, and internship programs to students and professionals. The company has been operating for over a decade and is recognized for offering practical and industry-oriented training on cutting-edge technologies.

IGeeks Technologies collaborates with universities and institutes, including being a VTU-authorized internship partner, to offer real-time project exposure, certified internship programs, and guidance aligned with academic requirements.

The company focuses on bridging the gap between theoretical education and practical industry skills by providing hands-on training, mentorship, and real project experience across domains such as Cyber Security, Data Science, Machine Learning, Web & Mobile Development, IoT, and Business Analytics.

In addition to internships, IGeeks Technologies offers corporate training, software development services, HR consultancy, project research support, and final-year academic projects to students and corporate clients.

Headquartered in Bangalore, the company operates both online and offline training and internship programs, enabling learners from different regions to gain practical exposure and enhance employability through certified internships and industry mentorship.

2. ABOUT THE COMPANY

IGeeks Technologies is a prominent IT services and training organization headquartered in Bangalore, India. The company was established with the vision of empowering students and professionals by providing industry-oriented skill development programs, internships, and real-time project exposure. Over the years, IGeeks Technologies has earned a reputation as a reliable partner for academic institutions and learners seeking practical experience in cutting-edge technologies.

The core focus of IGeeks Technologies is to bridge the gap between academic learning and industry requirements. It achieves this by offering comprehensive training and internship programs in various domains including Cyber Security, Network Security, Ethical Hacking, Data Science, Artificial Intelligence, Machine Learning, Web & Mobile Development, Internet of Things (IoT), and Software Testing. These programs are designed to enhance hands-on skills and prepare candidates for real-world challenges.

IGeeks Technologies also collaborates with universities and colleges, including being an authorized internship partner of Visvesvaraya Technological University (VTU). Through these collaborations, the company facilitates structured internship programs, project guidance, and certification support tailored to meet academic standards.

In addition to training and internships, IGeeks Technologies provides services such as corporate training, software development support, final year project assistance, and research mentorship. The company combines theoretical knowledge with practical lab sessions, live projects, and expert mentorship to ensure learners acquire job-ready skills.

With a mission to foster innovation and practical learning, IGeeks Technologies continues to contribute significantly to the professional growth of students and professionals, making it a respected name in the field of technology education and training.

3. TASK PERFORMED

During the internship period at **Igeeks Technologies**, the primary focus was on conducting **website forensic analysis** using the FAW (Forensic Acquisition of Website) tool. The work involved studying the process of acquiring and preserving web-based digital evidence in a forensically sound manner. Emphasis was placed on understanding how website content, source files, and metadata can be collected for investigative purposes and how such data can support cybercrime analysis and incident response.

The internship included hands-on training and practical implementation of FAW in a controlled laboratory environment. Various websites were analyzed to capture web artifacts such as HTML pages, scripts, and linked resources. All activities were performed strictly for **educational and ethical cybersecurity learning purposes**, ensuring compliance with legal and professional standards.

3.1 INTRODUCTION

Website forensic analysis is an essential component of modern digital investigations, as a significant amount of information related to cybercrimes, fraud, defamation, data theft, and online attacks is hosted on websites and web applications. Websites often contain valuable digital evidence such as web pages, source code, scripts, multimedia files, server response headers, timestamps, and metadata. Proper forensic analysis of such data enables investigators to reconstruct events, identify malicious activities, and support legal proceedings. Unlike conventional website downloading tools, forensic acquisition tools follow standardized methodologies to ensure the integrity, authenticity, and reliability of collected evidence.

A major challenge in website investigations is preserving the original state of online content, as websites are highly dynamic and can change frequently. Forensic tools address this challenge by capturing web content in a controlled and repeatable manner while documenting the acquisition process. These tools generate cryptographic hash values to verify data integrity, maintain detailed logs, and support chain-of-custody requirements. This ensures that the collected evidence remains unaltered and admissible in courts of law and other investigative forums.

In this project, the **FAW (Forensic Acquisition of Website)** tool was used to perform a structured and systematic forensic acquisition of a selected target website. FAW is specifically designed for website forensics and enables investigators to acquire web pages along with

associated resources such as images, stylesheets, JavaScript files, and linked content. The tool also records important forensic attributes including acquisition time, URLs accessed, server responses, and checksum values, thereby supporting forensic validation.

The project began with the identification and analysis of system requirements required to perform website forensic acquisition effectively. This included defining the necessary hardware configuration, operating system requirements, network connectivity, and supporting software tools. Careful consideration was given to ensuring that the environment was suitable for conducting forensic activities without altering or contaminating the target data.

Following the requirement analysis, a forensic workflow was designed to guide the acquisition and analysis process. The workflow defined the sequence of steps to be followed, starting from target website identification and preparation, to data acquisition, verification, analysis, and report generation. Designing a structured workflow helped ensure consistency, repeatability, and adherence to forensic best practices throughout the project.

The implementation phase involved the practical execution of the forensic acquisition process using the FAW tool. The target website was acquired in a controlled environment, and all actions were carefully documented. The acquired data was verified using hash values to confirm data integrity. Any errors, warnings, or anomalies encountered during the acquisition process were recorded for further analysis.

Finally, the project focused on analyzing the acquired website data and generating detailed forensic reports. These reports included information about the acquisition process, collected artifacts, integrity verification results, and observations made during the investigation. The reports serve as formal documentation that can be used by investigators, cybersecurity professionals, or legal authorities to understand the findings and validate the forensic process followed.

Overall, this project provided valuable hands-on experience in website forensic analysis and demonstrated the importance of using specialized forensic tools for collecting online evidence. It enhanced understanding of digital forensic principles, website investigation techniques, and ethical considerations involved in cybersecurity investigations. The knowledge gained through this project is applicable to real-world cybercrime investigations, incident response, and digital evidence handling scenarios.

3.2 Objective

The primary objectives of this task are to apply digital forensic principles to the acquisition and analysis of web-based evidence using specialized forensic tools. The task aims to provide practical exposure to website forensic investigation while ensuring compliance with legal and ethical standards.

The first objective is to perform a **forensic acquisition of a live website** using the FAW (Forensic Acquisition of Website) tool. This involves systematically collecting website data, including web pages and associated resources, in a controlled environment without disrupting the normal operation of the target website.

Another key objective is to **preserve the website content in its original form without any modification**. Maintaining data integrity during acquisition is essential to ensure that the collected evidence accurately represents the original online content and remains admissible for investigative and legal purposes.

The task also aims to **capture and document relevant metadata, system logs, and cryptographic hash values** generated during the acquisition process. These elements are critical for verifying the authenticity of the collected data, supporting chain-of-custody requirements, and enabling validation of evidence integrity throughout the investigation.

Finally, the objective includes **generating a comprehensive forensic report** that clearly documents the acquisition methodology, tools used, findings, and integrity verification results. The report is structured to meet investigative and legal standards, making it suitable for use in cybersecurity analysis, incident response, and potential legal proceedings.

3.3 System Requirement Specification

The System Requirement Specification (SRS) defines the hardware and software resources required to successfully execute the website forensic acquisition process. It outlines the necessary computing environment, including system performance, storage capacity, operating system, and forensic tools, to ensure accurate and reliable collection of web-based evidence. Proper specification of system requirements helps maintain data integrity, prevent unintended modification of evidence, and support a controlled forensic environment, thereby ensuring that the acquisition process is conducted in a legally acceptable and forensically sound manner.

3.2.1 Requirement Specification

This section outlines the essential hardware and software requirements necessary to run the FAW (Forensic Acquisition of Website) tool effectively. It specifies the system configuration needed to ensure stable performance, accurate data acquisition, and reliable forensic analysis. Defining these requirements helps maintain a controlled environment and supports the integrity and authenticity of the collected website evidence.

3.3.1.1 Hardware Requirement Specification

The hardware requirements for executing the project are as follows:

- Processor: Intel Core i3 or above
- RAM: Minimum 4 GB (8 GB recommended)
- Storage: Minimum 20 GB free disk space
- System Type: 64-bit architecture
- Network: Stable Internet connection

3.3.1.2 Software Requirement Specification

The software requirements for the project include:

- Operating System: Windows 10 / Windows 11 / Linux\
- FAW (Forensic Acquisition of Website) Tool
- Web Browser: Google Chrome / Mozilla Firefox
- Hashing Algorithm Support (SHA-256)
- PDF/HTML Viewer for report analysis

3.3.2 System Requirements

System requirements define how the system should function during the forensic acquisition process.

3.3.2.1 Functional Requirements

- The system shall accept a website URL as input for forensic acquisition.

- The system shall capture complete website content, including web pages and associated resources.
- The system shall record HTTP headers, timestamps, and relevant metadata during acquisition.
- The system shall generate cryptographic hash values to verify data integrity.
- The system shall securely store the acquired data in organized case folders.
- The system shall generate detailed forensic reports for investigation and legal documentation.

3.3.2.2 Non-Functional Requirements

- The system shall ensure high data integrity and accuracy throughout the forensic acquisition process.
- The system shall provide reliable and repeatable website acquisition results under similar conditions.
- The system shall support secure storage of digital evidence to prevent unauthorized access or tampering.
- The system shall offer a user-friendly interface to enable easy operation by investigators and students.
- The system shall comply with standard digital forensic principles and best practices.

3.4 System Design

stem Design describes the overall structure and workflow used for website forensic acquisition. It explains how the input URL is processed, how website data is collected and stored, and how forensic reports are generated. The design focuses on maintaining data integrity, security, and proper documentation throughout the acquisition process.

3.4.1 Design Consideration

The following design considerations were taken into account to ensure a reliable and forensically sound website acquisition process:

- Preservation of the original website data without modification
- Prevention of any unintended data alteration during acquisition
- Accurate recording of timestamps, HTTP headers, and metadata

- Secure storage of acquired evidence to prevent unauthorized access
- Detailed logging of all acquisition activities for traceability and audit purposes

3.4.2 System Architecture

The system architecture is composed of several interrelated components that work together to perform website forensic acquisition in a structured and reliable manner. The architecture includes a User Interface (FAW Tool Interface) that allows the investigator to provide input and control the acquisition process. The Website Acquisition Engine is responsible for retrieving website content from the target URL. The Metadata and Log Collector captures HTTP headers, timestamps, and activity logs during the acquisition process. A Hash Generator Module generates cryptographic hash values to verify data integrity. The Evidence Storage Repository securely stores the acquired website data and associated forensic artifacts. Finally, the Report Generation Module compiles the collected information into a detailed forensic report.

The FAW tool acts as an intermediary between the investigator and the target website, ensuring that all acquisition activities are performed in a forensically sound manner while maintaining data integrity, security, and traceability.

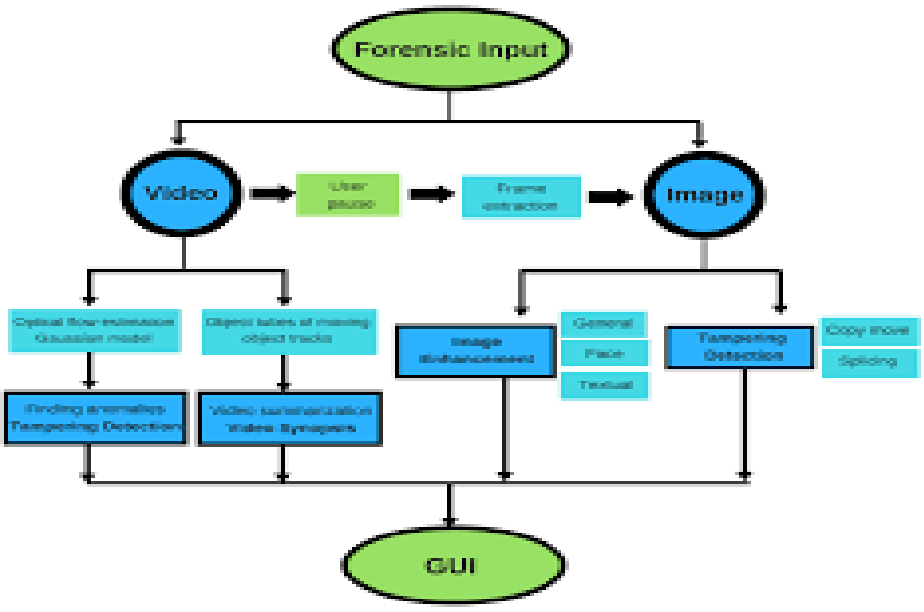

Fig 2 : System Architecture

3.5 IMPLEMENTATION

The practical execution of the website forensic acquisition process was carried out using the FAW tool in a controlled environment. The procedure involved acquiring website data from the target URL, capturing associated metadata and logs, generating cryptographic hash values, and securely storing the collected evidence. All activities were performed in accordance with forensic best practices to ensure data integrity, accuracy, and reliability of the acquired evidence.

3.5.1 Selection of Coding Language

The FAW tool internally utilizes scripting and automation mechanisms to perform website forensic acquisition tasks. As the tool provides a complete graphical and command-driven interface, no custom coding or programming was required from the user side. This approach makes FAW suitable for forensic investigations by enabling investigators to perform website acquisition and analysis efficiently without the need for programming expertise, while still ensuring accuracy and forensic integrity.

3.5.2 Description of Coding Language

- Python-based scripting is used internally to automate website forensic acquisition and data processing.
- Standard web protocols such as HTTP and HTTPS are utilized to retrieve website content from target servers.
- Cryptographic hashing algorithms such as SHA-256 are employed to generate hash values for integrity verification.
- These technologies together ensure accurate data capture, automation, and forensic validation of the acquired evidence.

3.5.3 Input Design

Target Website URL:

The target website URL is the primary input provided to the system, representing the online resource selected for forensic analysis. This URL acts as the entry point for the acquisition process, enabling the FAW tool to connect to the target website and retrieve web pages and

associated content. Accurate entry of the URL is essential to ensure that the correct website is acquired without affecting unrelated online resources.

Acquisition Depth:

Acquisition depth determines the number of levels of linked pages that the system will follow during the forensic acquisition. By specifying the depth, the investigator can control how extensively the website is captured, preventing excessive data collection while ensuring that all relevant linked content is included. This helps balance completeness of evidence with performance and storage considerations.

Capture Options:

Capture options allow the investigator to select specific elements to be included during the acquisition process. These options may include linked resources such as images, scripts, stylesheets, and metadata. Selecting appropriate capture options ensures comprehensive collection of forensic artifacts that may be relevant to the investigation, while also minimizing unnecessary data.

Case and Investigator Details:

Case and investigator details are provided as input to properly document and organize the forensic acquisition. Information such as case identification number, investigator name, date, and description is used to create structured case folders and is included in the forensic report. This input supports traceability, accountability, and chain-of-custody requirements, which are critical in forensic investigations.

3.5.4 Output Design

Captured Website Files:

The system generates a complete set of captured website files, including HTML pages, images, scripts, stylesheets, and other linked resources. These files represent the acquired content of the target website and are stored in their original structure to preserve authenticity and enable detailed forensic analysis.

Metadata Logs:

Metadata logs are generated during the acquisition process to record critical information such as access timestamps, HTTP headers, server responses, and acquisition activities. These logs

provide valuable context for understanding how and when the data was collected and support forensic validation and traceability.

Cryptographic Hash Values:

Cryptographic hash values are generated for the acquired website data using secure hashing algorithms such as SHA-256. These hash values serve as digital fingerprints that verify the integrity of the collected evidence and ensure that the data has not been altered after acquisition.

Forensic Acquisition Report:

The system produces a detailed forensic acquisition report in formats such as HTML or PDF. This report documents the acquisition methodology, tools used, collected artifacts, hash values, and observations, making it suitable for investigative review, documentation, and potential legal proceedings.

3.5.5 Application

The FAW application was utilized to perform the forensic acquisition of the selected target website in a structured and controlled environment. The acquisition process began by providing the target website URL and configuring the necessary capture parameters within the FAW interface. Once initiated, the application systematically accessed the website and collected web pages along with associated resources such as images, scripts, and stylesheets, ensuring that the original content was preserved without modification.

During the acquisition process, the FAW application automatically recorded critical forensic information, including timestamps, HTTP headers, server responses, and detailed activity logs. These records provide valuable context for understanding the acquisition process and support the verification of evidence authenticity. All captured data was securely stored in a dedicated case folder, which was organized using case and investigator details to maintain proper documentation and traceability.

To ensure the integrity of the acquired evidence, cryptographic hash values were generated for the captured website data. These hash values were used to verify that the collected files remained unchanged after acquisition. Any future access or analysis of the data can be validated by comparing hash values, thereby supporting chain-of-custody requirements and forensic reliability.

Following acquisition and verification, the FAW application generated a comprehensive forensic report in a structured format. The report documented the acquisition methodology, system configuration, collected artifacts, hash values, and observations made during the process. This report serves as a formal record of the investigation and can be used for further analysis, cybersecurity assessment, or legal proceedings.

Overall, the application of the FAW tool demonstrated the practical use of website forensic acquisition techniques and highlighted the importance of using specialized forensic tools for collecting and preserving digital evidence. The process ensured that the acquired website data met legal and forensic standards, making it suitable for investigative and evidentiary purposes

3.5.6 List of Figures

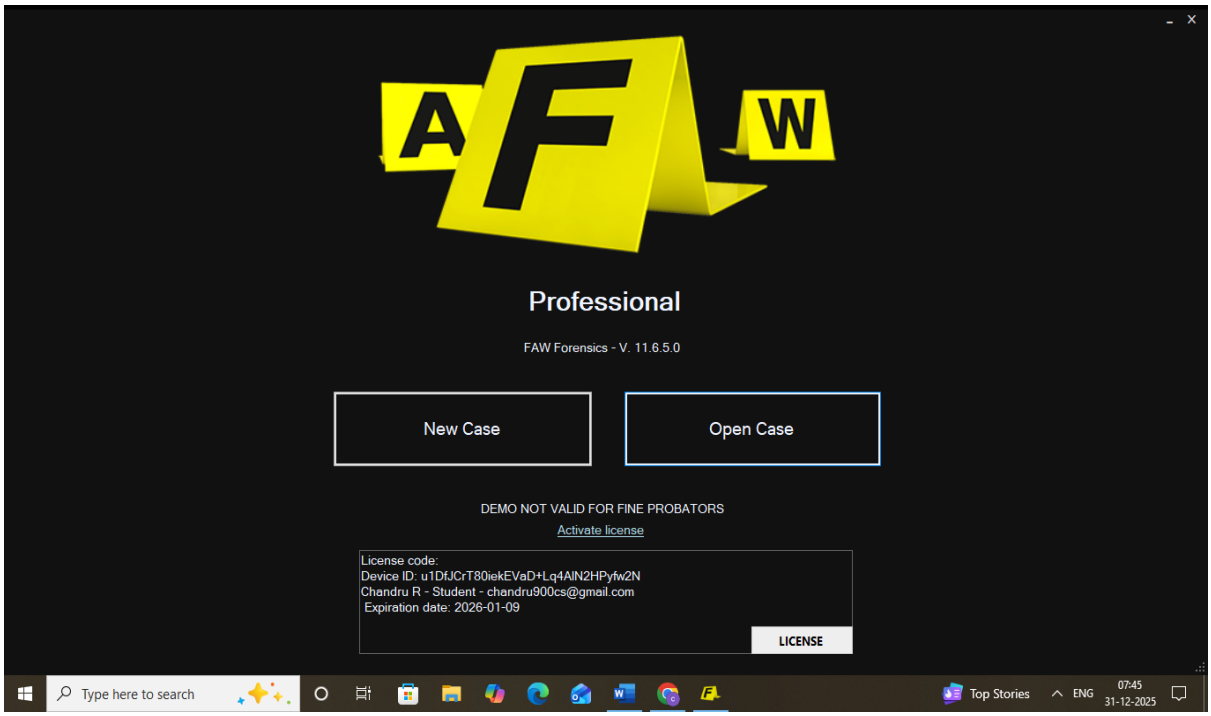

Fig: 3 FAW Tool Initial Dashboard

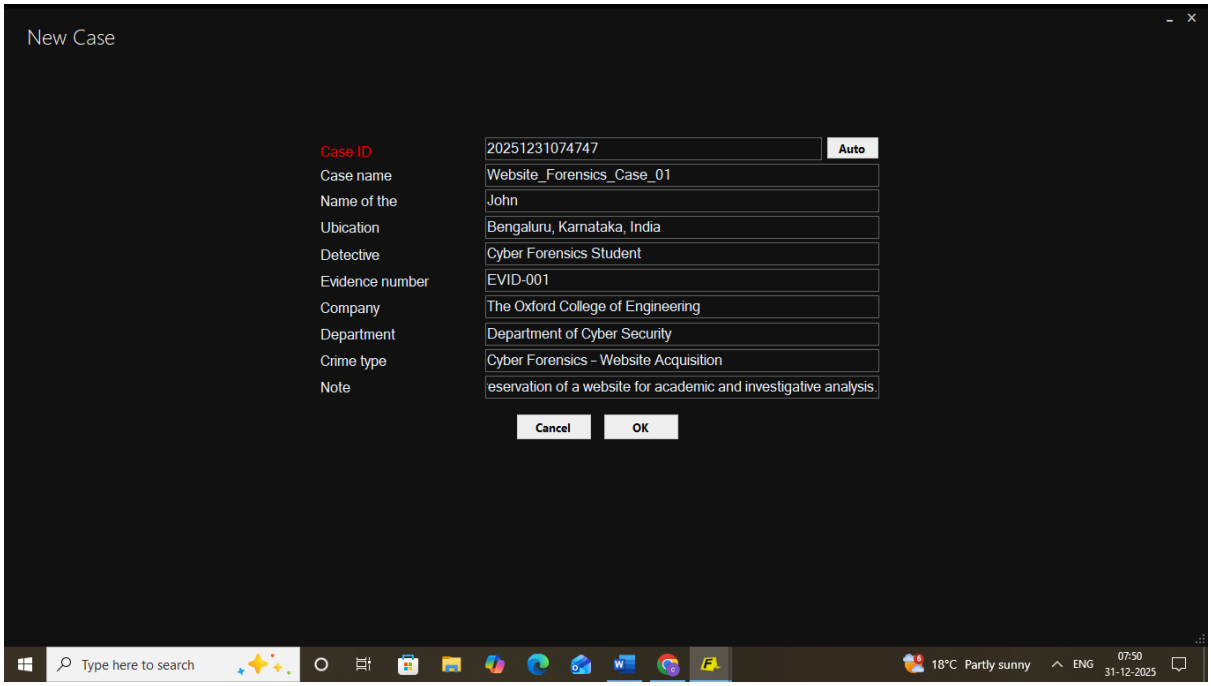

Fig 4: New Case Configuration Interface in FAW

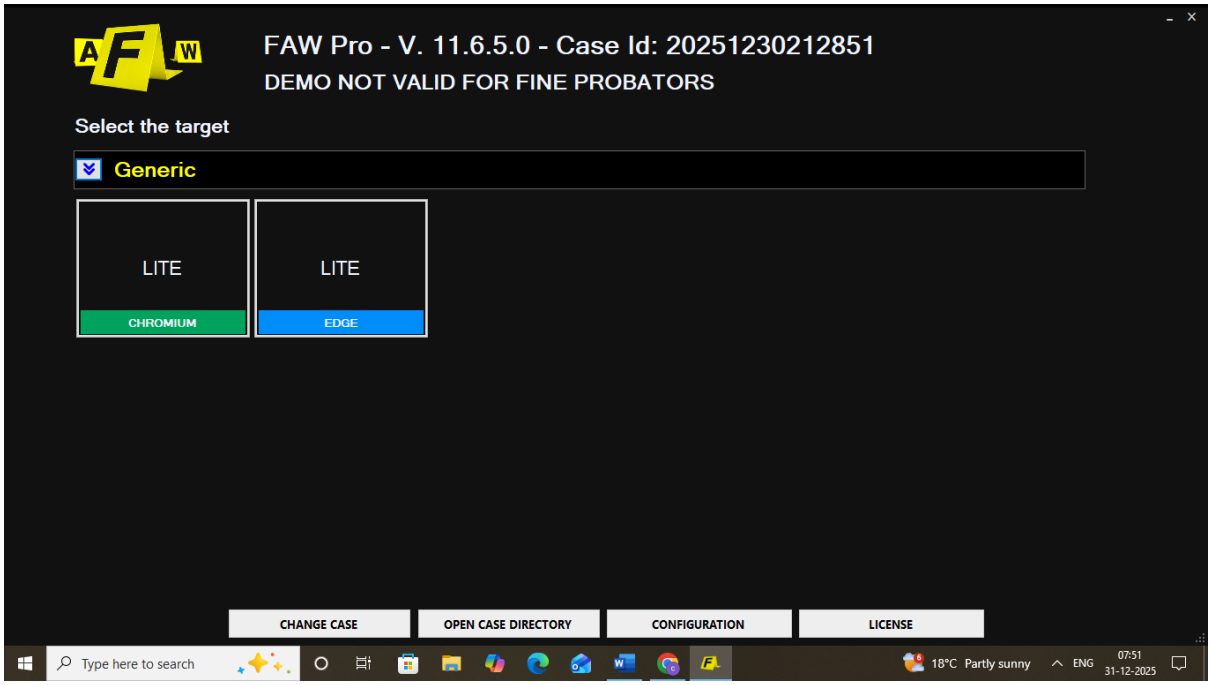

Fig 5: Website Acquisition Target Selection Screen in FAW

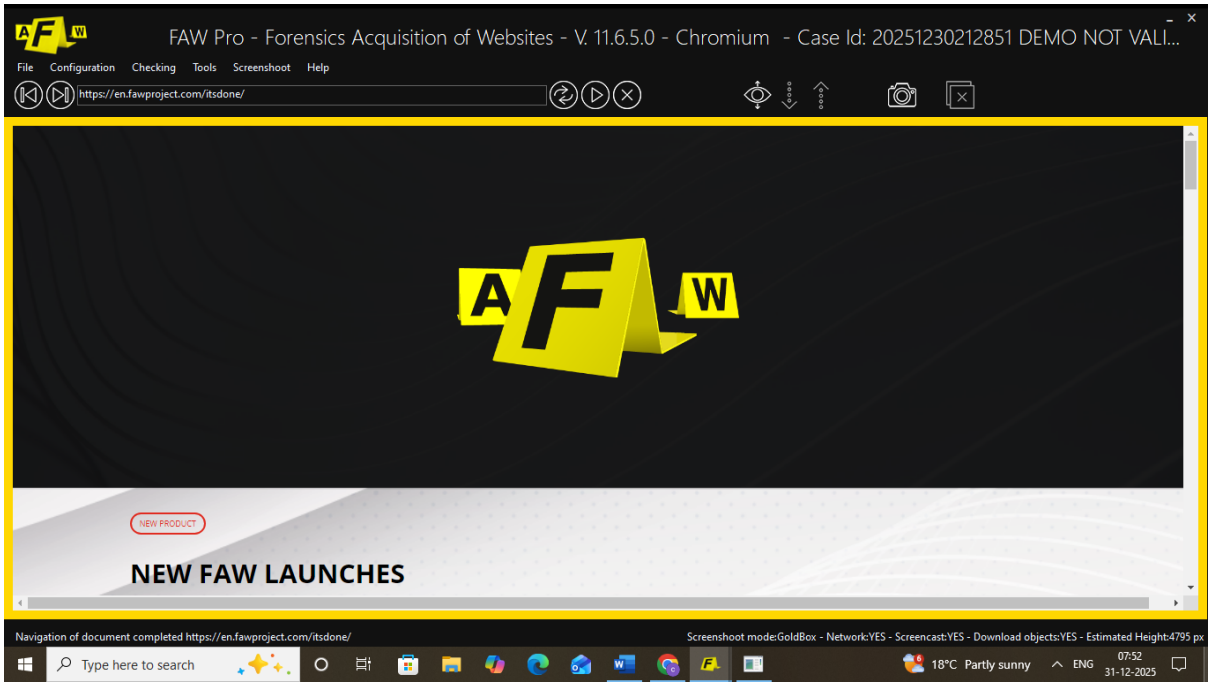

Fig 6: Website Loading and Live Acquisition Interface

Fig 7: Live Acquisition of Target Website

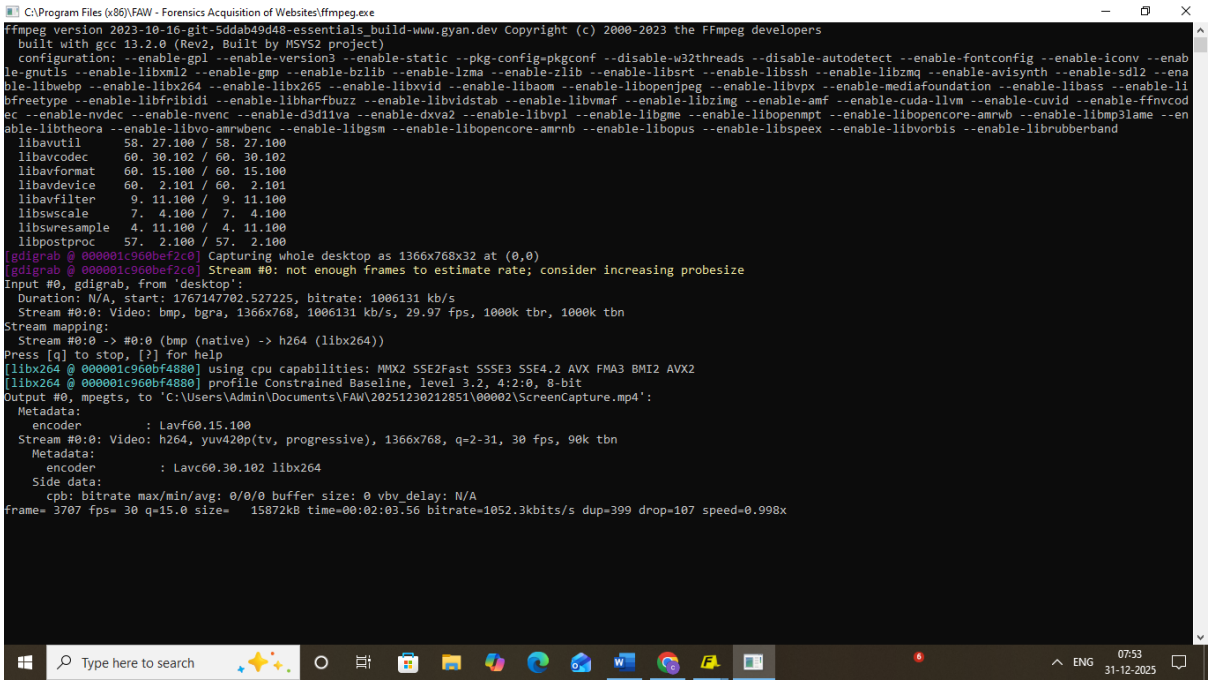

Fig 8: Acquisition Logging and Screen Capture Process

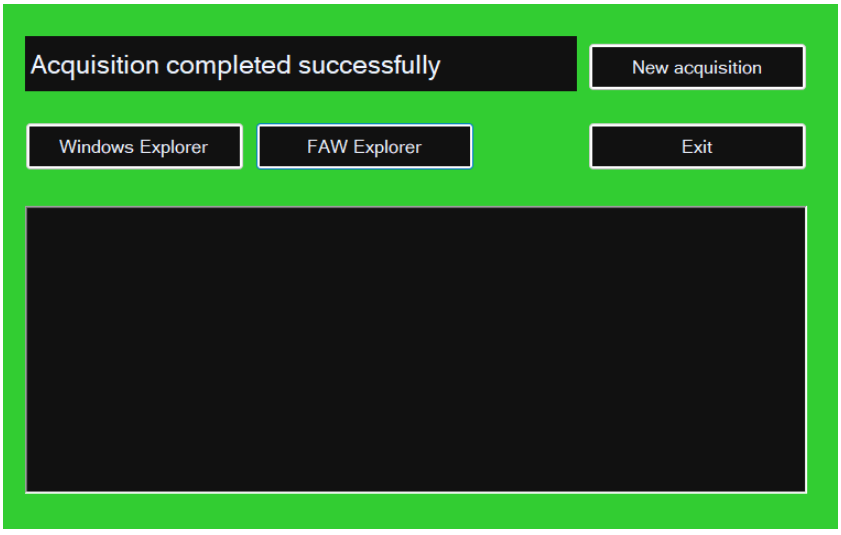

Fig 9: Successful Completion of Website Forensic Acquisition

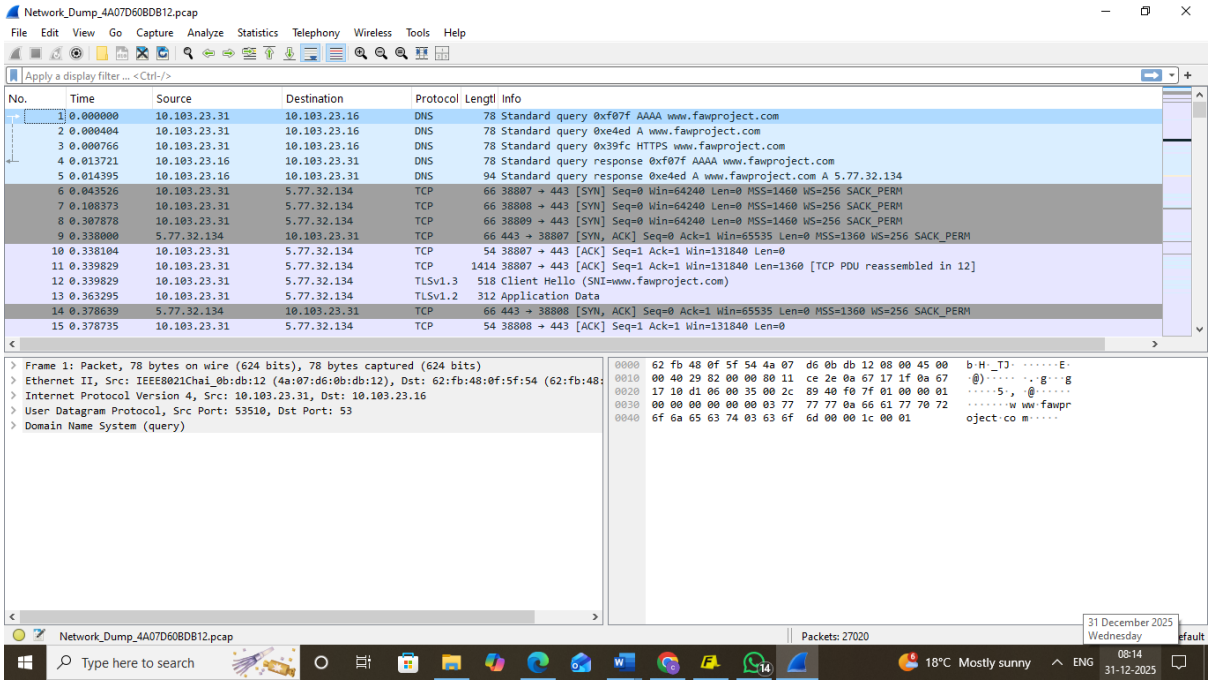

Fig 10: Network Traffic Capture and Analysis of Website Acquisition

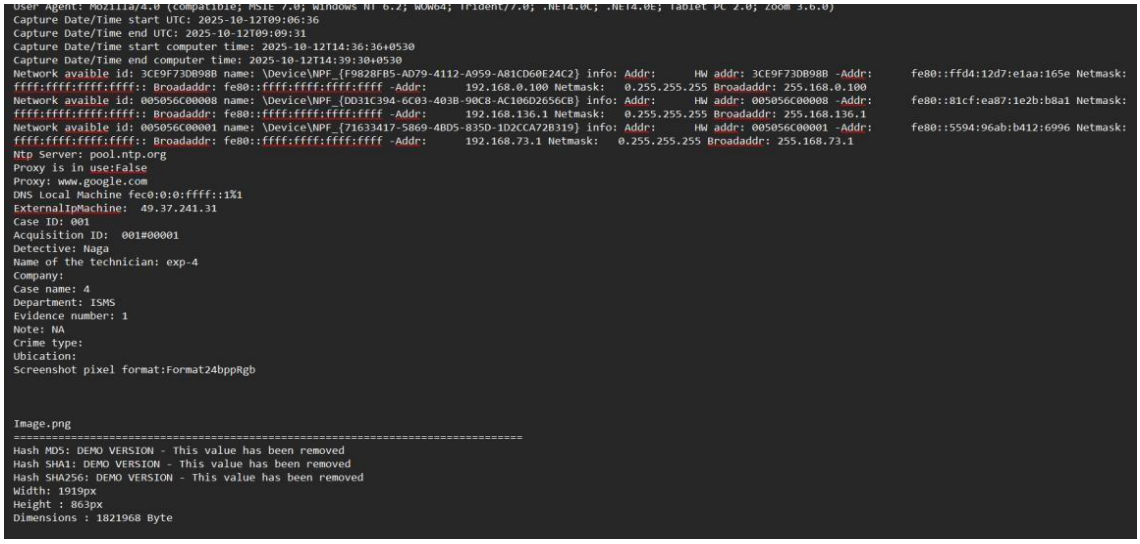

Fig 11: Forensic Metadata, Network Details, and Hash Information Output

4. REFLECTION

This project significantly enhanced the understanding of website forensics and the role it plays in modern digital investigations. Through the practical use of the FAW (Forensic Acquisition of Website) tool, a deeper insight was gained into how online content can be collected, preserved, and analyzed in a forensically sound manner. The project helped bridge the gap between theoretical knowledge of digital forensics and its real-world application in cybercrime investigation scenarios.

Working hands-on with forensic tools provided valuable experience in handling digital evidence responsibly. The process of acquiring website data, capturing metadata, generating cryptographic hash values, and maintaining detailed logs emphasized the importance of accuracy, precision, and consistency in forensic investigations. This practical exposure reinforced the need to follow standardized procedures to ensure the integrity and authenticity of digital evidence.

The project also highlighted the critical role of documentation in digital forensic investigations. Maintaining structured case folders, recording acquisition steps, and generating detailed forensic reports demonstrated how proper documentation supports traceability and chain-of-custody requirements. These practices are essential for ensuring that digital evidence remains legally admissible and credible during investigative and legal proceedings.

Additionally, the project improved problem-solving skills and technical confidence by allowing independent execution of forensic tasks in a controlled environment. It fostered an appreciation for ethical considerations in cybersecurity and digital investigations, reinforcing the importance of conducting forensic activities within legal boundaries. Overall, this project served as a valuable learning experience that strengthened foundational knowledge in website forensics and prepared for future challenges in the field of cybersecurity and digital investigations.

5. CONCLUSION

The *Website Forensic Analysis using FAW* project successfully demonstrated the practical application of digital forensic principles in the acquisition and preservation of web-based evidence. The project highlighted the importance of using specialized forensic tools for investigating online content, as websites often serve as critical sources of digital evidence in cybercrime investigations, incident response, and legal proceedings. Through this project, a systematic approach to website forensic acquisition was implemented, ensuring that all collected data remained accurate, authentic, and legally admissible.

The use of the FAW (Forensic Acquisition of Website) tool played a key role in achieving the project objectives. FAW enabled the structured collection of website content, including web pages and associated resources, while preserving the original state of the data. The generation of cryptographic hash values ensured data integrity, allowing verification that the acquired evidence remained unchanged after collection. Additionally, the automatic recording of metadata, timestamps, and activity logs strengthened the reliability and traceability of the forensic process.

The project also emphasized the significance of proper documentation and reporting in digital investigations. The detailed forensic reports generated by FAW provided a clear record of the acquisition process, tools used, collected artifacts, and integrity verification results. Such documentation is essential for maintaining chain-of-custody and for presenting digital evidence in investigative and legal contexts.

Overall, this project provided valuable hands-on experience in website forensic analysis and reinforced the importance of ethical and legally compliant forensic practices. The knowledge and skills gained through this project are directly applicable to real-world cybersecurity investigations and contribute to a strong foundation in digital forensics. The project successfully met its objectives and demonstrated the effectiveness of FAW as a reliable tool for website forensic acquisition and analysis.

6. REFERENCES

1 **Digital Forensics Concepts and Practices** – Reference materials and textbooks covering fundamental principles of digital forensics, evidence acquisition, preservation, chain-of-custody, and legal considerations involved in cybercrime investigations.

2 **FAW – Forensic Acquisition of Website Tool Documentation** – Official documentation and technical resources related to the FAW tool, including installation guidelines, usage procedures, acquisition methods, and forensic reporting features.

3 **Cybercrime Investigation and Website Forensics Resources** – Online articles, research papers, and learning materials focused on cybercrime investigation techniques, website forensic analysis, and web-based evidence handling methodologies.

4 **Network and Web Security Fundamentals** – Reference books and educational resources covering networking concepts, HTTP/HTTPS protocols, web application architecture, and security principles relevant to understanding website behavior and forensic acquisition.

7. CERTIFICATES

iGeeks
Bridging Technology

30/12/2025
Bangalore

Successful Internship Completion of Ms. Kavya Krishna Chinchankar (USN: 1OX24SCR07)

TO WHOMSOEVER IT MAY CONCERN

This is to certify that **Ms. Kavya Krishna Chinchankar** of **The Oxford College of Engineering** successfully completed her internship with us from **17/11/2025 to 30/12/2025.** She has shown a consistent progress and has been successful in working with our R&D Team in areas like **"CYBER SECURITY"** internship. She has been quite regular in attendance. We found her Knowledgeable in programming with great interpersonal skills during her interactions with the project team as well as the HR team. She was duty-bound, punctual and hard working.

We also found her quite inquisitive on what she had to work and has performed well.

Her associations with us were fruitful and wish her Good Luck in all her future endeavors.

For IGEEKS TECHNOLOGIES

Best Regards

Mr. RAHMATHULLA KHAN

Director – HR

+91-7019-28-0372
info@igeekstechnologies.com
No: 19, MN Complex, 2nd Cross,
Sampige Main Road, Malleswaram
Bangalore- 560003
www.igeekstechnologies.com