International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | March – 2026 DOI:10.55041/ISJEM05835
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

An Examination of Legal Guidelines and Procedures in Digital Forensics for Cybercrime Investigation Based on Data

Dr. K. Satyam[1], Sirimavilla Parameswara[2]

[1]Associate Professor, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India.

[2] Post Graduate, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India.

ABSTRACT

Because it makes it possible to systematically gather, examine, and present digital evidence, digital forensics is essential to criminal investigations. However, the validity and legal admissibility of such evidence are frequently impacted by inconsistent forensic reporting, unclear methodology, and differences in reasoning. In order to improve investigative insights, this article provides a web-based decision support system for digital forensic inquiry that was created using the Django framework and incorporates data analysis and visualisation techniques.

Structured forensic data with characteristics like opinion type, source level, activity level, offence level, and categorical judgements are processed by the suggested system. The system finds patterns and inconsistencies in forensic reports through preprocessing and analytical assessment.

Key findings including opinion distribution, risk levels, and methodological variances are shown using a variety of visualisation approaches, such as pie charts, bar graphs, and comparative charts. The experimental findings show that the approach successfully draws attention to methodological ambiguity and inconsistent reasoning in forensic reports, which may have an effect on judicial decision-making. The suggested approach enhances transparency, facilitates better interpretation of forensic data, and helps investigators make well-informed conclusions by offering an interactive and user-friendly interface. The goal of future research is to use machine learning models for automated forensic evaluation and predictive analysis.

Keywords

Digital Forensics, Cybercrime Investigation, Django Framework, Data Analysis, Data Visualization, Forensic Reporting, Decision Support System, Legal Evidence Analysis

I. INTRODUCTION

Data breaches, fraud, identity theft, and network intrusions are just a few of the cybercrime activities that have significantly increased due to the quick development of digital technologies. Because of this, digital forensics has emerged as a crucial field for locating, storing, evaluating, and presenting digital evidence in a way that is compliant with the law. It is essential for helping law enforcement and cybersecurity experts look into cyber events.

Even with the availability of sophisticated forensic techniques, there are still issues with guaranteeing the precision, coherence, and clarity of forensic reports. Forensic results frequently have problems like imprecise methodology, contradictory reasoning, and inadequate validation.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 03 | March – 2026 DOI:10.55041/ISJEM05835
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

These restrictions may make digital evidence less credible and have an impact on its admissibility in court. Systems that can methodically examine forensic data and offer lucid insights for decision-making are therefore becoming more and more necessary.

This study suggests a web-based decision support system for digital forensic inquiry in order to overcome these difficulties. The Django framework was used in the development of the system, which uses data analysis and visualisation methods to assess forensic reports. The technology assists in identifying patterns, discrepancies, and trends in forensic investigations by analysing structured records and producing graphical representations like pie charts and bar graphs. This method facilitates better informed and trustworthy decision-making in cybercrime instances and improves the interpretability of forensic data.

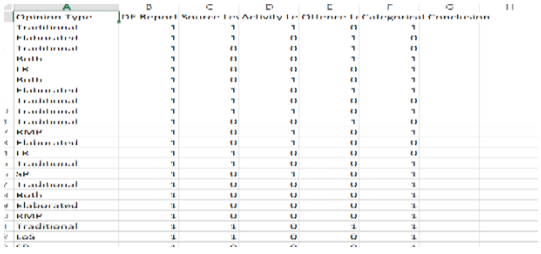
II. PROBLEM STATEMENT

In digital forensic investigations, the accuracy and reliability of forensic reports are critical for ensuring valid legal outcomes. However, many existing forensic reports suffer from issues such as inconsistent reasoning, lack of methodological clarity, and insufficient explanation of key findings. These limitations reduce the effectiveness of digital evidence and may lead to challenges in legal admissibility. Additionally, the absence of structured analytical tools makes it difficult to interpret large volumes of forensic data efficiently. Therefore, there is a need for a systematic, data-driven solution that can analyze forensic reports, identify inconsistencies, and present insights in a clear and interpretable manner to support cybercrime investigations.

III. DATASET DESCRIPTION

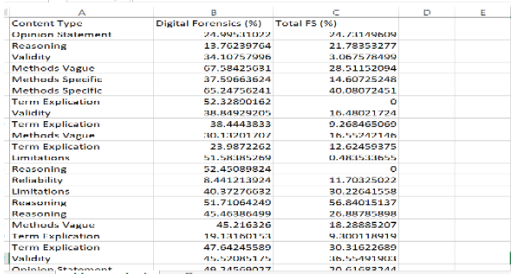
Structured records pertaining to digital forensic investigations make up the dataset employed in this work, which captures both qualitative and quantitative aspects of forensic analysis. Opinion type, the existence of digital forensic reports, source level, activity level, offence level, and categorical judgements are some of its characteristics. Traditional, elaborated, and combined opinions are among the various types of forensic interpretations represented by the opinion type variable. While the severity of the cybercrime is indicated by the offence level, other features like source level and activity level offer contextual information about the origin and nature of the evidence. The investigation's ultimate result is represented by the categorical conclusion.

A comparison between Total Forensic Science (FS) and Digital Forensics (DF) is conducted using a secondary dataset in addition to the core dataset. Opinion statements, rationale, validity, methodologies (both vague and detailed), term explanations, limitations, and reliability are just a few of the content kinds for which this dataset includes percentage-based values. These characteristics are used to assess the efficacy and calibre of forensic reports. Combining these datasets allows for a thorough examination of forensic procedures and reveals distinctions between more general forensic science standards and digital forensic reporting.



Opinion Type	DF Report	Source Lv	Activity Lv	Offence Lv	Categorical Conclusion
Traditional	1	1	1	0	1
Elaborated	1	1	0	1	0
Traditional	1	0	0	1	0
Both	1	0	0	1	1
DE	1	0	0	0	1
Both	1	0	1	0	1
Elaborated	1	1	0	1	1
Traditional	1	1	1	0	0
Traditional	1	1	1	0	1
Traditional	1	0	0	1	0
KMP	1	0	1	0	1
Elaborated	1	0	1	0	0
DE	1	1	0	0	0
Traditional	1	1	0	0	1
SP	1	0	1	0	1
Traditional	1	0	0	0	1
Both	1	0	0	0	1
Elaborated	1	0	0	0	1
KMP	1	0	0	0	1
Traditional	1	1	0	1	1
LCS	1	1	0	0	1

Fig: Dataset-1



Content Type	Digital Forensics (%)	Total FS (%)
Opinion Statement	24.99521022	24.71149809
Reasoning	18.70239704	21.78353277
Validity	34.10757996	3.067578499
Methods Vague	07.58425031	28.51152094
Methods Specific	37.50663624	14.60725248
Methods Specific	05.24750241	40.08072451
Term Explication	52.32890162	0
Validity	38.84929205	16.48021724
Term Explication	38.4443833	9.268465069
Methods Vague	30.13201707	16.50242148
Term Explication	23.9872262	12.62459375
Limitations	51.58385269	0.485513855
Reasoning	52.45089824	0
Reliability	8.441213924	11.70325022
Limitations	40.37276032	30.22641558
Reasoning	51.71064249	56.84015137
Reasoning	45.46386499	26.88785898
Methods Vague	45.216326	18.28885207
Term Explication	19.13160153	9.300118919
Term Explication	47.64245589	30.31622689
Validity	45.52086175	16.56491901
Opinion Statement	49.24569077	20.61683344

Fig: Dataset-2

IV. METHODOLOGY

To enable digital forensic inquiry, the suggested system employs an organised methodology that incorporates data pretreatment, analytical assessment, and visualisation tools. The dataset is first gathered and arranged into a structured manner with a variety of forensic analysis-related characteristics. In order to handle missing values, encode categorical variables like opinion types, and guarantee consistency across all records, data preprocessing is then carried out.

After preprocessing, feature analysis is carried out to assess important elements of forensic reporting, such as methodological clarity, validity, and rationale. To find differences and inconsistencies, a comparison between Digital Forensics (DF) and Total Forensic Science (FS) is conducted using percentage-based criteria. In order to identify trends in forensic reports, such as the frequency of ambiguous techniques or the absence of term explanations, the data are further examined.

The system uses a variety of data visualisation approaches, such as pie charts, bar graphs, and comparative charts, to improve interpretability. These techniques offer a clear depiction of forensic trends and correlations among elements. The Django framework is used to build the complete system as a web-based application. The frontend displays the findings via an interactive dashboard, while the backend analyses the data and produces analytical outputs. This method facilitates effective forensic data exploration and aids in making well-informed decisions during cybercrime investigations.

V. SYSTEM ARCHITECTURE

In order to enable digital forensic investigations, the suggested system is built as a web-based architecture that incorporates data processing, analysis, and visualisation components. Structured forensic datasets are gathered and saved in the data input module, which is where the system starts. After that, this data is sent to the preparation module, which carries out operations such data cleaning, categorical variable encoding, and normalisation to guarantee consistency.

After processing, the data is sent to the analysis module for feature evaluation and a comparison of Total Forensic Science (FS) and Digital Forensics (DF). This module finds trends, discrepancies, and important forensic reporting insights. For simpler comprehension, the visualisation module subsequently converts the analytical results into graphical representations like pie charts, bar graphs, and comparative charts.

Lastly, a web-based user interface created with the Django framework displays the results. Users may engage with the data, get insights, and successfully comprehend forensic trends thanks to the technology. The total effectiveness of cybercrime investigation is increased by this design, which guarantees a smooth transition from data collection to decision support.

VI. CONCLUSION

In order to improve the interpretation of forensic reports, this study offers a web-based decision support system for digital forensic inquiry that incorporates data analysis and visualisation approaches. Significant discrepancies in logic, methodological clarity, and validation among digital forensic procedures are revealed by the dataset analysis. The comparison of Total Forensic Science with Digital Forensics reveals shortcomings such the use of ambiguous techniques and, in some situations, the lack of appropriate term explanations.By offering an organised and interactive platform for evaluating forensic data and displaying important insights, the suggested system successfully tackles these issues. The technology enhances the dependability of digital

evidence in court settings and facilitates improved decision-making by making forensic data more accessible, consistent, and clear. To further improve the system's capabilities, future work can concentrate on implementing machine learning approaches for automated evaluation of forensic reports and predictive analysis.

References

[1] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. Amsterdam, Netherlands: Academic Press, 2011.

[2] National Institute of Standards and Technology (NIST), "Guide to Integrating Forensic Techniques into Incident Response," NIST Special Publication 800-86, 2006.

[3] B. Carrier, File System Forensic Analysis. Boston, MA, USA: Addison-Wesley, 2005.

[4] M. Pollitt, "A history of digital forensics," Digital Investigation, vol. 7, pp. S3–S7, Aug. 2010.

[5] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST, Gaithersburg, MD, USA, Tech. Rep. 800-86, 2006.

[6] A. P. Moore, R. J. Ellison, and R. C. Linger, "Attack modeling for information security and survivability," Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep., 2001.