Computer Science and Information Technologies
Vol. 6, No. 1, March 2025, pp. 8~19
ISSN: 2722-3221, DOI: 10.11591/csit.v6i1.pp8-19

Power of analytic tools in Oxygen Forensic® Detective based on NIST cybersecurity framework

Tole Sutikno[1], Iqbal Busthomi[2]
[1]Master Program of Electrical Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Institute of Advanced Engineering and Science, Yogyakarta, Indonesia

Article Info

Article history:

Received Jul 30, 2024
Revised Dec 10, 2024
Accepted Feb 20, 2025

Keywords:

Cybersecurity
Digital forensic tool
Digital investigation
NIST cybersecurity framework
Oxygen Forensic® Detective

ABSTRACT

The National Institute of Standards and Technology (NIST) cybersecurity framework is a systematic approach for assessing and improving cybersecurity procedures in digital investigations. Oxygen Forensic® Detective is a digital forensic software that integrates multiple analytic tools to assist investigators in extracting valuable insights from digital evidence. The analytic tools, including timeline, social graph, image categorization, facial categorization, maps, data search, key evidence, optical character recognition, statistics, and translation, assist investigators in thoroughly analyzing digital artifacts, establishing connections, and accurately classifying images with precision and effectiveness. By incorporating these analytical resources into Oxygen Forensic® Detective, a comprehensive strategy is established to effectively combat cyber threats. The NIST cybersecurity framework is incorporated into the tool, offering a methodical approach to identifying and reducing cybersecurity risks. Law enforcement agencies can enhance the productivity and effectiveness of their forensic methodologies by implementing these advanced technologies. This can result in successful prosecutions and improved cybersecurity practices. Overall, the utilization of analytical tools in criminological inquiries has experienced a substantial rise in the contemporary digital era.

Corresponding Author:

Tole Sutikno
Master Program of Electrical Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan
Ahmad Yani Street (South of Ring Road), Tamanan, Yogyakarta 55191, Indonesia
Email: tole@ee.uad.ac.id

1. INTRODUCTION

Within contemporary digital epochs, the utilization of analytic implements has seen a notable augmentation in criminological inquiries. As technological advancements progress, investigators are afforded access to an extensive array of potent devices that facilitate the extraction of significant information from electronic contrivances [1]. Such instruments, inclusive of timeline scrutiny, social graph delineation, image classification, facial recognition, alongside data retrieval functionalities, are integral in the unveiling of evidentiary materials and the resolution of intricate cases [2]. Through the employment of these analytical resources, investigators are capable of tracing the digital imprints left by suspects, scrutinizing affiliations amongst individuals, classifying imagery and facial representations, executing searches for pertinent data, as well as extracting pivotal evidence from extensive data sets. These analytic implements not only optimize the procedural dynamics of investigations but also bolster the precision and efficacy of forensic evaluations, which ultimately contributes to more favorable resolutions in criminal prosecutions [2], [3].

The foundational aspect of Oxygen Forensic® Detective is rooted in extensive capabilities regarding mobile forensic examination. Through ongoing advancements and the amalgamation of state-of-the-art

technologies, Oxygen Forensic® Detective has positioned itself prominently as a preeminent instrument within the domain of digital forensics [4]. In terms of features, the product encompasses timeline analysis, social graph mapping, image and facial categorization, as well as data search functionalities, availing investigators of a substantial platform to methodically retrieve, evaluate, and understand digital evidence in an effective manner. Moreover, the tool integrates sophisticated modules, inclusive of maps, key evidence identification, optical character recognition, statistics, and translation functionalities, thereby offering a comprehensive methodology for forensic scrutiny. By conforming to the principles outlined in the National Institute of Standards and Technology (NIST) cybersecurity framework, Oxygen Forensic® Detective guarantees compliance with best practices and standards pertinent to digital forensic inquiries, ultimately rendering it a formidable resource for forensic specialists amidst the continually evolving cyber environment today [5].

In scrutinizing the NIST cybersecurity framework, it becomes imperative to take into account its function in the improvement of the overall cybersecurity posture within entities. The framework, by virtue of presenting a comprehensive outline of optimal practices and guidelines, aids in the identification, safeguarding, detection, response, and recovery in regard to cyber threats. Additionally, it fosters a risk-based methodology which permits organizations to efficaciously prioritize resources contingent upon their distinctive risk profile. The amalgamation of the NIST framework with potent analytical instruments such as timeline, social graph, image categorization, facial categorization, maps, data search, key evidence, optical character recognition, statistics, and translation module can further augment cybersecurity endeavors. These instruments facilitate proficient data analysis, visualization, and the extraction of significant insights, thereby assisting organizations in remaining ahead of the shifting landscape of cyber threats. By harnessing the NIST framework in conjunction with sophisticated analytical tools, organizations can bolster their capacity to avert, detect, and respond to cybersecurity incidents in an effective manner [6].

Within the domain of digital forensics, the implementation of analytic instruments holds a crucial significance in amplifying investigative functionalities and optimizing the examination procedure. Instruments such as timeline, social graph, image categorization, and facial categorization afford investigators streamlined modalities to visualize and scrutinize digital evidence, thereby revealing essential insights that may have been missed [7]. The maps instrument facilitates geospatial analysis, permitting investigators to monitor the movements of individuals and comprehend the situational context of their actions. Moreover, capabilities like data search, key evidence, and optical character recognition support the rapid identification of essential information, while statistics and translation modules provide comprehensive analysis and interpretation of data. Through the integration of these analytic instruments within digital forensics methodologies, practitioners can bolster their proficiency in drawing significant information from digital artifacts and unearthing vital evidence that aids investigations effectively. The diligent application of these instruments is in alignment with the NIST cybersecurity frameworks principles surrounding detection and response, thereby enhancing the overarching cybersecurity stance of organizations [8].

Analytic apparatuses hold a significant position in the augmentation of the effectiveness of digital forensic scrutiny. The Oxygen Forensic® Detective software integrates an extensive variety of instruments including timeline, social graph, image categorization, facial categorization, maps, data search, key evidence, optical character recognition, statistics, and translation module, thus furnishing investigators with a holistic toolkit. This integration facilitates a meticulous examination of digital evidence amassed from manifold sources. By employing these apparatuses, examiners are capable of revealing obscured connections, scrutinizing communication trends, organizing imagery, extracting vital data from documentation, and even rendering translations of foreign languages for enhanced understanding. The adaptability and productivity of these analytic tools considerably streamline the investigative endeavor, allowing examiners to derive actionable intelligence from large data sets in a prompt manner [9]. Consequently, this improves both the overall efficacy and precision of forensic evaluations.

The analytical instruments available within Oxygen Forensic® Detective present a broad spectrum of functionalities that correlate with the principal objectives articulated within the NIST cybersecurity framework. To illustrate, the timeline tool plays a pivotal role for investigators aiming to piece together events and chronological sequences, thus bolstering the detect function by offering insights into possible threats. Similarly, the social graph tool significantly amplifies the awareness of interpersonal relationships and connections, which supports the identify and protect functions through the discernment of weaknesses and possible avenues for attack. Furthermore, the modules for image categorization and facial categorization contribute to the respond function by enabling swift recognition of suspects or individuals of interest. Through a seamless integration of these tools into the investigative workflow, Oxygen Forensic® Detective equips examiners to manage cyber incidents in adherence to the stipulated guidelines of the NIST framework. When utilized appropriately, these analytical instruments markedly improve both the efficacy and precision of digital investigations [10].

2. NIST CYBERSECURITY FRAMEWORK

In the context of examining digital evidence via Oxygen Forensic® Detective, the application of the NIST cybersecurity framework presents a structured methodology for evaluating and enhancing cybersecurity protocols [11]. By coordinating with this framework, analysts can more effectively recognize and prioritize significant assets, spot potential dangers, shield sensitive data, react proficiently to incidents, and recuperate promptly from breaches. The analytical instruments such as timeline, social graph, image categorization, and facial categorization play vital roles in advancing the investigative procedure by organizing the amassed data, discerning connections among entities, and categorizing multimedia content accurately. These instruments contribute to an exhaustive analysis that conforms to the guidelines of NIST, thereby ensuring that every facet of cybersecurity is considered and properly managed. Integrating the principles of the NIST framework with sophisticated analytic tools empowers forensic examiners to perform meticulous and efficient investigations while upholding rigorous security benchmarks. Moreover, additional features—namely maps, data search, key evidence, optical character recognition, statistics, and translation modules available within Oxygen Forensic® Detective—further bolster the implementation of the NIST cybersecurity framework in the realm of digital investigations. The maps tool enables analysts to visualize geographical data and accurately identify locations pertinent to the case, thereby enriching the comprehension of circumstantial evidence. The data search function facilitates the effective retrieval of information from multiple sources, assisting in the identification of crucial data points for further scrutiny. Both key evidence and optical character recognition tools are instrumental in extracting and interpreting key evidence from various forms of media, including images and documents, which aids in unearthing valuable insights. Additionally, the statistical analysis features afford quantitative backing to the findings of investigations, thereby enhancing the reliability and comprehensiveness of the derived conclusions. The translation module also plays an essential role in decoding foreign language materials, thus broadening the investigative scope and ensuring that language obstacles do not impede analytical endeavors. By harnessing these varied analytical tools within Oxygen Forensic® Detective in accordance with the NIST cybersecurity framework, examiners can ensure that their investigations are thorough, precise, and compliant with established cybersecurity best practices [12].

2.1. Core functions of NIST framework

The NIST framework acts as an essential reference for organizations aiming to enhance their cybersecurity stance. It incorporates five principal functions as shown in Figure 1 i.e., identify, protect, detect, respond, and recover [13]. Each function contributes significantly toward the formation of a solid cybersecurity strategy. The identify function concentrates on gaining an understanding of assets, risks, and vulnerabilities within an organization. Conversely, protect stresses the importance of enacting safeguards to secure critical infrastructure. The detect function entails ongoing monitoring for security incidents and threats. The respond component highlights the necessity for a structured methodology to effectively tackle and mitigate cybersecurity incidents. Finally, the recover function is concerned with the reinstatement of operations and services following a cyber incident. By embedding these fundamental functions into their cybersecurity framework, organizations are positioned to proactively confront potential threats while adapting to the continuously shifting cyber terrain. The NIST Framework, when coupled with robust analytic tools such as timeline, social graph, and image categorization, offers a thorough approach to managing cybersecurity risks [10].

Figure 1. NIST five principal functions

2.2. Implementation of NIST framework in digital forensics

Incorporating the NIST cybersecurity framework into practices related to digital forensics could augment the overall efficacy of investigative procedures. Through alignment with the guidance articulated by NIST, forensic examiners might ascertain a standard approach toward the management and examination of digital evidence. This framework provides a structured methodology aimed at the identification, protection, detection, response to, and recovery from cyber occurrences, which is critical in sustaining the integrity and dependability of forensic investigations [14]. Additionally, the employment of analytic tools such as timeline, social graph, image categorization, and facial categorization on platforms like Oxygen Forensic® Detective may further simplify the forensic workflow and aid in the extraction of significant insights from digital evidence. Such tools potentially grant investigators enhanced abilities for data searches, the identification of key evidence, and the conduct of statistical analyses, ultimately improving the overall efficiency and precision of forensic evaluations. Through the integration of advanced analytic tools with the NIST framework, forensic professionals might elevate their investigative capabilities to unprecedented levels while complying with recognized best practices within the cybersecurity domain [8].

2.3. Relationship between NIST framework and Oxygen Forensic® Detective

Additionally, the interplay between the NIST framework and Oxygen Forensic® Detective manifests in several dimensions that serve to bolster endeavors within the realm of digital forensic investigation. As an example, the directives set forth by the NIST framework regarding cybersecurity risk management can find practical application within the analytical resources provided by Oxygen Forensic® Detective, specifically the tools known as timeline, social graph, and image categorization. Such tools are instrumental in delineating the connections among individuals, elucidating communication patterns, and classifying images to facilitate the extraction of evidence. Furthermore, the Translation module incorporated within Oxygen Forensic® Detective resonates with NIST's prioritization of inter-agency and cross-sector communication and information dissemination. By capitalizing on the capabilities of Oxygen Forensic® Detective in aspects such as data exploration, identification of crucial evidence, and statistical scrutiny, investigators are capable of refining their methodologies in accordance with the cybersecurity objectives outlined by the NIST framework [15]. The confluence of these two frameworks culminates in an all-encompassing strategy for digital forensic evaluation, ensuring rigorous adherence to the prevailing industry benchmarks and optimal practices.

2.4. Benefits of aligning analytic tools with NIST framework

By aligning analytic instruments with the NIST cybersecurity framework, entities can obtain various advantages within their digital forensic inquiries. The NIST framework offers a systematic methodology for managing and mitigating cyber threats, supplying a standardized vernacular for interactions and comprehension among different involved parties. When analytic instruments are incorporated into this framework, investigators can ascertain that their methodologies comply with sector benchmarks and superior practices, thereby amplifying the legitimacy and dependability of their outcomes. Moreover, utilizing instruments like timeline analysis, social graph visualization, image and facial categorization, maps, data search functionalities, identification of key evidence, optical character recognition, statistics, and translation modules amid the architecture of the NIST Framework can significantly refine the investigative procedure, facilitating a more efficient and effective extraction of pertinent digital evidence [12]. This concordance not only fortifies the holistic cybersecurity stance of an establishment but also enhances the precision and profundity of forensic examinations.

2.5. Case studies demonstrating NIST framework integration

Within the scope of digital forensic analysis, the integration of the NIST cybersecurity framework into investigative practices is of significant importance as it aids in fostering a thorough and standardized methodology. The amalgamation of this framework with the robust analytical functionalities provided by Oxygen Forensic® Detective has been substantiated through case studies that indicate noteworthy enhancements in both efficiency and precision when addressing intricate cybercrime scenarios. To illustrate, the application of the timeline feature in conjunction with the NIST directives facilitates the establishment of a lucid chronology of incidents, which is instrumental in deciphering the order of occurrences pertaining to a security breach or assault. Additionally, the image categorization tool can be synchronized with the NIST risk management framework to methodically classify and scrutinize visual evidence, thereby ensuring that no aspect is neglected during the investigatory phase. The harmonious fusion of NIST principles with the analytical prowess of Oxygen Forensic® Detective heralds a new paradigm for forensic investigations, extending the horizons of both cybersecurity and digital forensics [10].

3. ANALYTIC TOOLS IN OXYGEN FORENSIC® DETECTIVE

The adoption of analytical instruments within Oxygen Forensic® Detective is shown in Figure 2. The modules serve to augment the operational efficacy of digital inquiries by yielding extensive insights across multiple dimensions of the case [5]. Amidst the continual progression in technology and data analysis apparatuses, Oxygen Forensic® Detective encompasses supplementary analytic modules that assist examiners in deriving significant insights from digital evidence. These modules comprise timeline, social graph, image categorization, facial categorization, maps, data search, key evidence, optical character recognition, statistics, and the translation module [5].

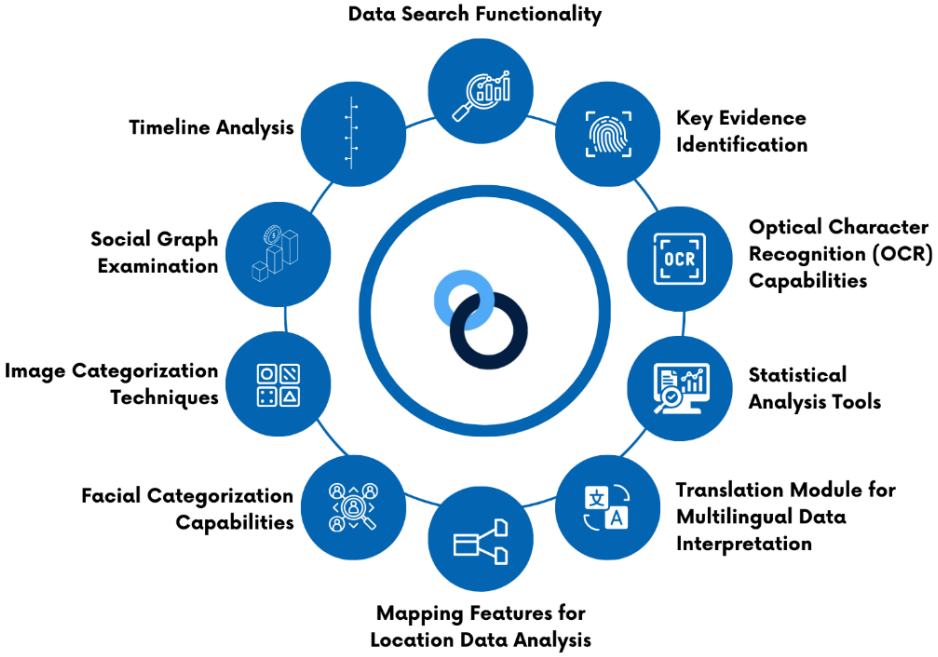

Figure 2. Analytic tools available in Oxygen Forensic® Detective

The timeline functionality permits the reconstruction of events in a chronological framework, thereby facilitating the establishment of timelines and activity sequences. Moreover, the social graph apparatus supports the mapping of affiliations among individuals and their interconnections, which is critical for grasping the case dynamics [8]. In addition, both image categorization and facial categorization contribute to the organization and identification of images, which is vital for the recognition of suspects or victims. The application of maps assists in the geolocation of pertinent data, illuminating the geographic context relevant to the investigation. Additionally, the data search utility grants investigators the ability to navigate through extensive datasets effectively, allowing for the rapid identification of key pieces of evidence. The optical character recognition capability enhances the extraction of textual information from images, thereby facilitating the examination of text-based material. The statistics module aids in quantifying trends and patterns within data, contributing to the development of conclusions grounded in empirical evidence. Ultimately, the translation module enables the comprehension of multilingual data, effectively dismantling linguistic barriers in investigative processes. Collectively, these analytical tools embedded in Oxygen Forensic® Detective furnish a solid framework for executing comprehensive and insightful digital investigations, which meets the rigor and depth demanded within the contemporary cyber forensic sphere.

The deployment of these modules permits investigators to facilitate the examination of digital artifacts, delineate relations among individuals and occurrences, and categorize images with both precision and efficacy. Moreover, the inclusion of optical character recognition along with translation modules allows for the extraction and rendition of text across a spectrum of languages, thereby augmenting the investigative functionalities of Oxygen Forensic® Detective. By utilizing these analytical tools, investigators possess the potential to reveal essential information that might have otherwise remained concealed, ultimately fortifying the investigative procedure.

3.1. Timeline analysis

In addition, the timeline analysis aspect of Oxygen Forensic® Detective serves a vital function within investigations by offering a sequential overview regarding actions occurring on a digital instrument. By systematically arranging data into a timeline structure, those conducting the investigation can more readily follow the order of events, decipher trends, and establish relationships among various evidence components. This apparatus empowers examiners to reconstruct the timeline of user engagements, communications, and alterations of files, assisting in discerning the motivations behind suspects' actions and potential linkages to illicit activities. Furthermore, timeline analysis facilitates the representation of data in a manner that is easier to grasp, which can support the exposition of findings within judicial settings. The capacity to scrutinize data from a temporal perspective bolsters the investigation process and enhances the overall efficacy of digital forensic evaluations [16].

3.2. Social graph examination

Within the domain of digital forensic investigations, a critical analytic instrument offered by Oxygen Forensic® Detective is the social graph examination capability. This particular tool grants examiners the ability to conceptualize and scrutinize relationships among individuals on the basis of communication behaviors, affiliations, and interactions proliferating across a multitude of digital arenas. By delineating these social interconnections, investigators are positioned to disclose significant revelations concerning possible suspects, collaborators, or witnesses pertinent to a case. The social graph examination function substantially boosts the efficacy of investigative undertakings by facilitating the recognition of concealed relationships and networks that might not be readily observable through conventional forensic analytical techniques. Furthermore, this mechanism empowers examiners to probe further into the social intricacies of a case, thereby assisting in the establishment of motives, chronologies, and associations that are vital for the construction of a thorough investigative narrative. The utilization of social graph analysis within Oxygen Forensic® Detective has the potential to notably enhance the overarching effectiveness of digital forensic inquiries and aid in the resolution of intricate cases [10].

3.3. Image categorization techniques

Within the scope of digital forensics, methodologies pertaining to image categorization assume a pivotal function in the extraction of evidence and insights from visual datasets. Such methodologies pertain to the classification and arrangement of images according to predetermined categories or attributes. Leveraging sophisticated algorithms alongside machine learning paradigms, investigators are afforded the capacity to scrutinize substantial quantities of images with both efficiency and precision. Techniques related to image categorization facilitate the ability of forensic analysts to pinpoint pertinent images, recognize patterns, and derive significant information from visual content, thereby contributing to the overall investigative framework. Furthermore, these approaches may prove vital in the identification and correlation of individuals, locations, objects, or activities illustrated in images, thereby amplifying the overall investigative proficiency of forensic instruments such as Oxygen Forensic® Detective. The amalgamation of image categorization instruments permits forensic specialists to optimize their workflows, prioritize analytical efforts, and extricate actionable intelligence from digital visual data sources [17].

3.4. Facial categorization capabilities

Within the realm of forensic examination, the functionalities pertaining to facial categorization that are provided by Oxygen Forensic® Detective assume significant importance in the identification of persons implicated in illicit activities [18]. This particular instrument facilitates the scrutiny and classification of faces discerned in digital artifacts, encompassing images or video recordings, which in turn aids in the formulation of a more holistic investigative timeline. The amalgamation of facial categorization with complementary analytical mechanisms, such as social graph examination and image categorization, permits investigators to delineate connections amongst suspects, victims, and geographical points, thereby enriching the overall structure of the investigatory endeavor. Additionally, the capability to cross-reference facial data with various forms of information, including text communications or call records, can yield insightful revelations regarding the interpersonal dynamics and behaviors of the individuals being examined. In summation, the facial categorization proficiencies afforded by Oxygen Forensic® Detective constitute a formidable resource within the repertoire of forensic analysts who are endeavoring to unearth pivotal evidence in the sphere of digital investigations.

3.5. Mapping features for location data analysis

A fundamental aspect of Oxygen Forensic® Detective that contributes to the analysis of location data is the mapping tool. The incorporation of mapping functionalities into the forensic toolkit enables investigators to visualize and analyze geospatial data sourced from mobile devices. By charting location

information such as GPS coordinates, Wi-Fi connections, and cell tower data onto a map, analysts are able to discern patterns, monitor movements, and establish connections among individuals and locations. Such spatial visualization not only enhances the comprehension of the data but also facilitates the reconstruction of timelines and the identification of notable places frequented by the device user. Additionally, the mapping tool is applicable in conjunction with other analytical features like the timeline and social graph in order to offer a holistic representation of the findings from the investigation. The synthesis of mapping capabilities with other functionalities within Oxygen Forensic® Detective notably amplifies the analysis of location data and bolsters the overall investigative endeavor [10].

3.6. Data search functionality

Moreover, the data search function found in Oxygen Forensic® Detective serves an essential purpose in facilitating digital investigations. By taking advantage of this tool, investigators can adeptly navigate through extensive amounts of data to reveal pivotal evidence that could be significant for a particular case. The capability to query across diverse sources, including social media, messaging platforms, and device memory, broadens the investigative scope and guarantees that no pertinent information is missed. This instrument is especially beneficial when confronted with substantial datasets, as it provides sophisticated search functionalities that conserve time and resources throughout the examination process. With the incorporation of the principles set forth by the NIST cybersecurity framework, the data search feature in Oxygen Forensic® Detective offers a uniform approach to data management, ensuring that investigations comply with optimal methodologies and align with industry norms. This effective tool enhances the productivity and precision of digital forensic inquiries, ultimately resulting in more reliable and timely outcomes [10].

3.7. Key evidence identification

In the domain of digital forensic examinations, the recognition of significant evidence is of utmost importance for revealing relevant details and arranging the chronological series of occurrences. Oxygen Forensic® Detective, which comprises a collection of analytic instruments based on the NIST cybersecurity framework, presents a substantial platform for the detection and recovery of vital evidence from diverse digital origins. By employing tools such as timeline, social graph, image categorization, and facial categorization, investigators are able to create links among individuals, events, and digital artifacts. Furthermore, the integration of maps, data search, and optical character recognition tools permits a proficient harvesting of geolocation information, text-related data, and contextual understanding from digital proof [8]. This all-encompassing strategy concerning the identification of evidence does not only amplify the investigative procedure but also guarantees the precision and credibility of the outcomes in digital forensic assessments.

3.8. Optical character recognition capabilities

Within the domain of digital forensic analysis, the functionalities associated with optical character recognition hold significant importance for the purpose of text extraction from visual artifacts such as images or documents, thereby facilitating investigatory processes [19]. The capability of optical character recognition to transform scanned documents or pictorial representations containing textual information into formats that are amenable to machine processing serves to augment both the efficacy and precision of data evaluations within forensic analytical tools. The implementation of optical character recognition within Oxygen Forensic® Detective is done in a manner that is both harmonious and integrated into its suite of analytic tools, which bestows upon investigators the ability to retrieve pertinent information from an array of sources, including but not limited to scanned materials, imagery, or screen captures. By way of engaging optical character recognition technology, investigators are presented with the opportunity to reveal obscured clues, interpret pivotal evidence, and ultimately fortify their results in various investigative scenarios. This sophisticated feature facilitates a more profound level of text extraction and analytical assessment, thereby empowering forensic professionals to conduct efficient text retrieval and utilize optical character recognition methodologies for extensive investigative revelations.

3.9. Statistical analysis tools

Furthermore, the utilization of statistical analysis tools holds significant importance in the extraction of valuable insights amid the extensive datasets gathered during the course of digital forensics inquiries. Through the application of various statistical methodologies, investigators are enabled to discern patterns, trends, and anomalies that exist within the data, which, in turn, fosters a more profound comprehension of the particular case being examined. Such tools facilitate analysts in quantifying the relevance of evidence, thus assisting in the prioritization of leads and the effective distribution of resources. To illustrate, through the use

of statistical analysis, it becomes feasible for investigators to ascertain the likelihood concerning a suspect's presence at a designated location as inferred from geolocation data. Furthermore, these statistical mechanisms can be instrumental in recognizing potential correlations that manifest between disparate pieces of evidence, thereby bolstering the overarching case hypothesis [10]. In summation, the integration of statistical analysis tools within Oxygen Forensic® Detective significantly augments the investigative procedure by rendering objective and quantifiable insights that support the process of decision-making.

3.10. Translation module for multilingual data interpretation

The establishment of a translation module in the Oxygen Forensic® Detective software presents novel opportunities for analysts engaged in the deciphering of multilingual data. This module ostensibly augments the efficacy and precision of investigations by facilitating the translation of text from diverse languages into a vernacular that is recognizable to the user. By the integration of this apparatus, investigators can surmount language obstacles that may have previously obstructed their analytical endeavors. The translation module is in accordance with NIST cybersecurity framework principles, as it fosters effective communication and the sharing of information. Moreover, this capability permits a more all-encompassing comprehension of digital evidence, thereby ensuring that no vital information is neglected due to linguistic impediments. Additionally, the translation module ostensibly enhances the general usability of the software, rendering it a notable asset for professionals in the forensic field [20].

4. APPLICATION OF ANALYTIC TOOLS IN DIGITAL FORENSICS

Within the domain of digital forensics, the utilization of analytic instruments assumes a significant role within the investigative framework. The employment of tools such as Timeline analysis permits investigators to chronologically reconstruct occurrences, thereby yielding a detailed perspective on the available digital evidence. This particular approach assists in assembling the series of actions, consequently enhancing the identification of potential patterns or irregularities that could be crucial to the investigation. Moreover, the application of tools such as image categorization, facial categorization, and optical character recognition bolsters the capability to extract pertinent data from multimedia assets, including images and documents, thus facilitating a more profound understanding of the evidence at hand. The amalgamation of statistics and data search tools further sharpens the analytical process, allowing investigators to reveal concealed correlations or patterns within extensive datasets. When these analytic instruments are adeptly employed, they not only optimize the investigative workflow but also augment the precision and thoroughness of the outcomes, ultimately aiding in the efficacious resolution of digital forensic inquiries [8].

4.1. Case study 1: Solving cybercrime using Oxygen Forensic® Detective

Within the domain of investigations regarding cybercrime, the Oxygen Forensic® Detective manifests as an influential apparatus that exploits a range of analytic functionalities to assist in unraveling multifaceted cases. The application of features such as timeline, social graph, image categorization, and facial categorization enables investigators to construct a holistic perspective of digital evidence, thereby facilitating the assembly of intricate aspects surrounding a cybercrime episode. Furthermore, the maps function empowers investigators to monitor the geographical locations linked to suspect activities, thus augmenting the investigative procedure. The data search and key evidence components additionally optimize the examination process by rendering swift access to vital information, while optical character recognition, statistics, and the translation module contribute to the extraction, systematization, and comprehension of data across varied formats sourced from multiple origins. Through the methodical amalgamation of these analytic instruments, Oxygen Forensic® Detective furnishes investigators with the necessary skills to proficiently confront cybercrime and ensure that offenders are held accountable [21].

4.2. Case study 2: Analyzing digital evidence in legal investigations

The application of digital evidence within the scope of legal investigations has become progressively significant in the contemporary age. Within the framework of case study 2, the examination of digital evidence holds a central importance in revealing essential information pertinent to legal matters. Utilizing analytic instruments such as timeline, social graph, image categorization, and facial categorization allows investigators to construct a detailed picture of the occurrences and individuals connected to the case. The incorporation of maps, data search, and key evidence modules further amplifies the thoroughness and precision of the investigation, offering important insights into both the context and significance of the evidence collected. In addition, tools including optical character recognition, statistics, and translation modules assist in the deciphering and interpretation of the digital evidence, aiding in a more comprehensive grasp of the information available. These sophisticated analytic tools not only optimize the investigation procedure but also safeguard the integrity and legitimacy of the evidence put forth in legal contexts [8].

4.3. Case study 3: Enhancing law enforcement operations with analytic tools

Within the framework of operations associated with law enforcement, the amalgamation of analytic instruments such as timeline, social graph, and image categorization possesses the potential to markedly improve investigative methodologies. The employment of these instruments in conjunction with Oxygen Forensic® Detective enables law enforcement entities to optimize their operational routines, unveil significant insights, and competently scrutinize digital evidence. The incorporation of facial categorization alongside data search capabilities further facilitates the recognition of individuals and pertinent information that is vital for the resolution of criminal cases. Additionally, the integration of mapping features and critical evidence modules delivers a thorough overview of case particulars, which assists investigators in formulating an integrated narrative. When these tools are combined with optical character recognition, along with statistical analysis and translation components, they furnish a comprehensive strategy for gathering and scrutinizing information in law enforcement domains. The application of such sophisticated technologies is consistent with the suggestions articulated in the NIST cybersecurity framework, which underscores the necessity of utilizing advanced solutions to bolster law enforcement operations [10].

4.4. Ethical considerations in utilizing analytic tools

In discussions regarding the ethical aspects pertinent to the use of analytic instruments, it emerges that such considerations are crucial for preserving the integrity associated with digital forensic inquiries. When deploying instruments such as timeline, social graph, image categorization, and facial categorization within the Oxygen Forensic® Detective suite, it becomes imperative for investigators to adhere to data privacy norms as well as legal constraints. Furthermore, engaging with maps, data search, key evidence, optical character recognition, statistics, and translation divisions mandates a nuanced approach in order to mitigate risks pertaining to any potential exploitation or illicit access to sensitive data. Compliance with the protocols set forth in the NIST cybersecurity framework can prove beneficial in fostering principles of ethical conduct throughout the investigative procedures [22]. In addition, maintaining transparency and accountability while utilizing these analytic resources stands as a fundamental aspect of sustaining professional standards and credibility within the digital forensics' domain [23]. By integrating ethical considerations into the operationalization of analytic tools, investigators have the capacity to preserve the trust conferred by stakeholders and ascertain that the results derived are both ethically obtained and legally defensible.

4.5. Future trends and innovations in analytic tools for digital forensics

With the swift progressions seen in technology, one can assert that the impending landscape of digital forensics analytic instruments stands on the brink of noteworthy expansion and inventive developments. A notable trend that is emerging pertains to the assimilation of artificial intelligence along with machine learning algorithms within forensic software, which allows for a more proficient and precise examination of digital evidence. Such advanced analytic instruments hold the promise to automate monotonous activities, ranging from data searching to the categorization of images, thereby conserving precious time for forensic analysts [24]. Furthermore, the integration of avant-garde technologies, including but not limited to facial categorization and optical character recognition, is capable of enhancing investigative depth and unveiling novel pathways for the discovery of pivotal evidence within digital devices. As the arsenal of digital forensic tools advances, efforts to integrate functionalities like timeline analysis, social graph mapping, and statistical data inquiries will indubitably play an essential role in fortifying investigative prowess and safeguarding the integrity of digital evidence throughout legal processes. Additionally, the addition of translation modules may streamline the analysis of multilingual materials, thus broadening the horizon of digital forensic examinations [25]. Ultimately, the prospective trends and innovations surrounding analytic instruments in the realm of digital forensics hold significant potential to transform the discipline and substantially influence the methodologies by which cybercrimes are scrutinized and prosecuted.

5. RESULTS AND DISCUSSION

Oxygen Forensic® Detective presents a diverse range of analytical instruments that augment the investigatory process. The timeline feature permits investigators to visually delineate events, thereby constructing a coherent chronological order of activities and communications. The social graph offers a visual depiction of interrelations and connections amongst individuals, which assists in comprehending networks and affiliations. The image categorization and facial categorization utilities employ sophisticated algorithms for the categorization and scrutiny of images, thereby aiding investigators in pinpointing pertinent visual evidence. Furthermore, the integration of maps facilitates the visualization of geographical data, underscoring locales pertinent to the case at hand. The data search, key evidence, optical character recognition, statistics, and translation modules additionally furnish users with extensive capabilities to

extract, analyze, and interpret digital evidence in an efficient manner. Collectively, these tools empower investigators to unearth critical insights and construct robust cases in alignment with the guidelines established by the NIST cybersecurity framework [8].

Through the incorporation of the NIST cybersecurity framework within the Oxygen Forensic® Detective platform, it acquires an augmented capacity for confronting cyber threats and addressing vulnerabilities. This framework delivers a systematic methodology aimed at enhancing cybersecurity efficiency by means of its fundamental functions which include identify, protect, detect, respond, and recover. In this regard, Oxygen Forensic® Detective exploits these functionalities to optimize and fortify its analytical instruments, such as timeline assessment, social graph representation, image and facial classification, maps amalgamation, data search functionalities, key evidence detection, optical character recognition, statistically derived outputs, and translation components. Such integration conforms Oxygen Forensic® Detective to prevailing industry best practices and benchmarks, thereby guaranteeing that users are equipped with a holistic array of resources requisite for effectively probing and alleviating cybersecurity events. The congruity between the NIST framework and Oxygen Forensic® Detective amplifies the analytical capabilities of the platform as well as its comprehensive efficacy in the struggle against cyber threats.

Through the utilization of analytic instruments for digital inquiries, law enforcement bodies can markedly improve the productivity and efficacy of their forensic methodologies. The employment of instruments like timeline examination, social graph depiction, image and facial categorization, maps integration, data searching functionalities, key evidence determination, optical character recognition, statistical analysis, and translation modules can facilitate the investigative workflow and bring to light crucial insights. These instruments not only hasten the extraction and evaluation of digital proof but also permit investigators to produce thorough reports that conform to the specifications set forth in the NIST cybersecurity framework [8]. By adopting these sophisticated technologies, investigators are positioned to outpace cybercriminals and adjust to the shifting milieu of digital offenses, resulting in a greater likelihood of prosecutions that are successful and enhanced practices in cybersecurity.

In order to optimize the efficacy of analytic instruments like timeline, social graph, image categorization, facial categorization, maps, data search, key evidence, optical character recognition, statistics, and translation functionalities found within Oxygen Forensic® Detective, various suggestions can be enacted. Primarily, it is of utmost importance to perpetually update the software for the purpose of obtaining the most recent capabilities and enhancements. Following that, conducting frequent instructional sessions targeting investigators regarding the adept utilization of these tools may significantly bolster their competencies and output [10]. Furthermore, the establishment of a delineated protocol pertaining to data interpretation and examination could facilitate a more efficient investigative procedure and ensure uniformity in outcomes. Additionally, collaboration with specialists in specific fields, including but not restricted to linguistics or the visual representation of data, could yield invaluable perspectives and improve the precision of discoveries. Through the integration of these suggestions, law enforcement agencies alongside digital forensic teams can effectively tap into the comprehensive potential of analytic tools to reveal crucial evidence and resolve cases in a timely manner.

6. CONCLUSION

The incorporation of the NIST cybersecurity framework into Oxygen Forensic® Detective serves to bolster the functionalities of the software, thus providing a more extensive and uniform method for conducting digital forensic inquiries. By conforming to the NIST directives, Oxygen Forensic® Detective presents a systematic procedure that aids investigators in discerning and alleviating cybersecurity threats with heightened efficacy. The efficacy of analytical instruments such as timeline, social graph, image categorization, facial categorization, maps, data search, key evidence, optical character recognition, statistics, and translation modules further enhances the software's proficiency in the examination and elucidation of digital artifacts. These utilities not only optimize the investigative workflow but also empower investigators to reveal critical insights and trends, which ultimately contribute to the precision and dependability of the outcome. Given the ongoing progression of technology and the nature of cyber threats, the integration of analytical resources within Oxygen Forensic® Detective remains vital for maintaining a competitive edge in the continuously shifting domain of digital forensics. To conclude, it has become evident that the analytic tools within Oxygen Forensic® Detective, framed by the NIST cybersecurity framework, play a critical role in the augmentation of digital investigations. The amalgamation of various tools, which include but are not limited to timeline, social graph, image categorization, facial categorization, maps, data search, key evidence, optical character recognition, statistics, and the translation module, has notably contributed to the enhancement of both efficiency and efficacy in the realm of forensic analysis. As we look ahead, it is imperative that forthcoming research concentrates on the progression of these analytic instruments in order to adequately address the dynamically changing landscape of cyber threats and technological innovations.

Moreover, examining the prospective incorporation of artificial intelligence and machine learning algorithms, aimed at amplifying the functionalities of Oxygen Forensic® Detective, may potentially unlock novel pathways within the sphere of digital forensic studies. By persistently honing and broadening the functionalities of these analytic tools, forensic investigators may effectively outpace cybercriminals, thereby bolstering the protection of digital assets.

FUNDING INFORMATION

This research used the author's personal funds.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Tole Sutikno	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓
Iqbal Busthomi				✓		✓	✓		✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] B. K. Jaisawal, Y. Perwej, S. K. Singh, S. Kumar, J. P. Dixit, and N. K. Singh, "An empirical investigation of human identity verification methods," *International Journal of Scientific Research in Science, Engineering and Technology*, pp. 16–38, Jan. 2023, doi: 10.32628/IJSRSET2310012.

[2] G. Sarkar and S. K. Shukla, "Behavioral analysis of cybercrime: paving the way for effective policing strategies," *Journal of Economic Criminology*, vol. 2, 2023, doi: 10.1016/j.jeconc.2023.100034.

[3] H. Swofford and C. Champod, "Probabilistic reporting and algorithms in forensic science: stakeholder perspectives within the american criminal justice system," *Forensic Science International: Synergy*, vol. 4, 2022, doi: 10.1016/j.fsisyn.2022.100220.

[4] "Oxygen forensic detective," *Oxygen Forensics*. Accessed: Oct. 12, 2024. [Online]. Available: https://www.oxygenforensics.com/en/products/oxygen-forensic-detective/

[5] "Top 10 analytic features available in oxygen forensic® detective," *Oxygen Forensics*, 2024. Accessed: Oct. 12, 2024. [Online]. Available: https://www.oxygenforensics.com/en/resources/10-analytical-features-available-in-oxygen-forensic-detective/

[6] NIST, *The NIST cybersecurity framework (CSF) 2.0*. United States: National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.CSWP.29

[7] S. Sachdeva, B. L. Raina, and A. Sharma, "Analysis of digital forensic tools," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 6, pp. 2459–2467, 2020, doi: 10.1166/jctn.2020.8916.

[8] S. Satpathy and S. Mohanty, *Big data analytics and computing for digital forensic investigations*, 1st ed. Boca Raton, Florida: CRC Press, 2020.

[9] C. Pollard and R. Anzaldua, *Computer forensics for dummies*, 1st ed. Hoboken, United States: John Wiley & Sons, 2008.

[10] A. Zannin and L. Huber, "Crime scene investigation," in *Manual of Forensic Science: an International Survey*, 1st ed., Boca Raton, Florida: CRC Press, 2017.

[11] F. R. Moreira, D. A. D. S. Filho, G. D. A. Nze, R. T. D. S. Junior, and R. R. Nunes, "Evaluating the performance of nist's framework cybersecurity controls through a constructivist multicriteria methodology," *IEEE Access*, vol. 9, pp. 129605–129618, 2021, doi: 10.1109/ACCESS.2021.3113178.

[12] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response: recommendations of the National Institute of Standards and Technology," in *Computer Security*, vol. 10, 2006, pp. 800–886.

[13] NIST, "Cybersecurity framework," *National Institute of Standards and Technology*. [Online]. Available: https://www.nist.gov/cyberframework

[14] NIST, "The CSF 1.1 five functions," *Cybersecurity Framework*. [Online]. Available: https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

[15] W. Akpose, "NIST cybersecurity framework: a practitioner's perspective," 6igma Associates, 2016.
[16] Y. Chabot, "Construction, enrichment and semantic analysis of timelines - application to digital forensics," *Ph.D Thesis*, Department Computer Science, University College Dublin, Belfield, Ireland, 2015.
[17] R. Ayers, S. Brothers, and W. Jansen, *Guidelines on mobile device forensics*, National Institute of Standards and Technology, US Department of Commerce, 2014, doi: 10.6028/NIST.SP.800-101r1.
[18] "Advanced analytics: facial categorization," *Oxygen Forensic*. Accessed: Oct. 12, 2024. [Online]. Available: https://www.oxygenforensics.com/en/resources/advanced-facial-categorization/
[19] D. Wolf, T. Göbel, and H. Baier, "Hypervisor-based data synthesis: on its potential to tackle the curse of client-side agent remnants in forensic image generation," *Forensic Science International: Digital Investigation*, vol. 48, Mar. 2024, doi: 10.1016/j.fsidi.2023.301690.
[20] S. Latifi, *Information technology-new generations*. Switzerland: Springer Cham, 2018, doi: 10.1007/978-3-319-32467-8.
[21] K. Ruan, *Cybercrime and cloud forensics: applications for investigation processes*. IGI Global, 2013, doi: 10.4018/978-1-4666-2662-1.
[22] A. W. Malik, D. S. Bhatti, T. J. Park, H. U. Ishtiaq, J. C. Ryou, and K. Il Kim, "Cloud digital forensics: beyond tools, techniques, and challenges," *Sensors*, vol. 24, no. 2, 2024, doi: 10.3390/s24020433.
[23] C. M. Miller, "A survey of prosecutors and investigators using digital evidence: a starting point," *Forensic Science International: Synergy*, vol. 6, 2023, doi: 10.1016/j.fsisyn.2022.100296.
[24] T. Göbel, H. Baier, and F. Breitinger, "Data for digital forensics: why a discussion on 'how realistic is synthetic data' is dispensable," *Digital Threats: Research and Practice*, vol. 4, no. 3, 2023, doi: 10.1145/3609863.
[25] S. Majumdar, P. Shirani, and L. Wang, *Innovations in digital forensics*. World Scientific Publishing, 2023, doi: 10.1142/13330.

BIOGRAPHIES OF AUTHORS

Tole Sutikno is a lecturer and the head of the Master Program of Electrical Engineering at the Faculty of Industrial Technology at Universitas Ahmad Dahlan (UAD) in Yogyakarta, Indonesia. He received his Bachelor of Engineering from Universitas Diponegoro in 1999, Master of Engineering from Universitas Gadjah Mada in 2004, and Doctor of Philosophy in Electrical Engineering from Universiti Teknologi Malaysia in 2016. All three degrees are in electrical engineering. He has been a Professor at UAD in Yogyakarta, Indonesia, since July 2023, following his tenure as an Associate Professor in June 2008. He is the Editor-in-Chief of TELKOMNIKA and Head of the Embedded Systems and Power Electronics Research Group (ESPERG). He is one of the top 2% of researchers worldwide, according to Stanford University and Elsevier BV's list of the most influential scientists from 2021 to the present. His research interests cover digital design, industrial applications, industrial electronics, industrial informatics, power electronics, motor drives, renewable energy, FPGA applications, embedded systems, artificial intelligence, intelligent control, digital libraries, and information technology. He can be contacted at email: tole@te.uad.ac.id.

Iqbal Busthomi received his Master of Computing in Informatics Engineering from Universitas Ahmad Dahlan, Yogyakarta, Indonesia in 2021. After receiving his degree, he became a member of the Institute of Advanced Engineering and Science (IAES) as Information and Communication Technology Team. His research interests include cyber security, web application, and digital forensics. He can be contacted at email: iq.iaes@gmail.com.