Check for updates

Received: 1 September 2020 | Revised: 18 February 2021 | Accepted: 10 March 2021

DOI: 10.1002/wfs2.1418

OVERVIEW

WIREs FORENSIC SCIENCE WILEY

The impact of automation and artificial intelligence on digital forensics

Aaron Jarrett | **Kim-Kwang Raymond Choo**

Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, Texas

Correspondence
Aaron Jarrett, Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, Texas 78249.
Email: aaronckjarrett@gmail.com

Edited by: Sara Belkin, Executive Editor

Abstract

Artificial intelligence (AI; broadly defined to include Machine Learning and Deep Learning) and automation are two current and reciprocal computing disciplines. As such, AI-powered software, programs, operating systems, and devices are developed on a massive scale to automate a wide variety of processes and operations. The principal aims of integrating AI and automation include efficiency, accuracy, and cost-reduction. While there is still an on-going cost associated with automation, the cost is typically many magnitudes smaller than the on-going costs incurred to get the job done manually, which increases the likelihood of generating a high return on investment. One emerging application of AI and automation is digital forensics. For example, US Federal and State Law Enforcement Agencies have started exploring the utility of AI-powered technology to make the job of digital forensics more impactful. This trend can maximize the accuracy of digital forensic investigations, enabling the resolution of more digital investigations.

This article is categorized under:

Digital and Multimedia Science > Cyber Threat Intelligence
Digital and Multimedia Science > Artificial Intelligence
Digital and Multimedia Science > Cybercrime Investigation

KEYWORDS

artificial intelligence, automation, computer forensics, deep learning, digital forensics, forensics, machine learning

1 | INTRODUCTION

Digital forensics applies science to maintain a strict chain of custody during the identification, collection, examination, and analysis of digital data while preserving integrity (Kent, Chevalier, Grance, & Dang, 2006). A key reason behind the use and adoption of digital forensics is the ever-increasing number of malicious cyber activities that involve the use of digital devices or services. Additionally, with the widespread adoption and proliferation of electronic appliances, much of the evidence of non-cyber-related criminal activities is found on cell phones, computers, or other digital devices (Irons & Lallie, 2014).

In recent years, conducting malicious cyber activity is becoming more commonplace as the international corporate sector depends on information and communication technologies (ICTs) and the high tech digital infrastructure. Hacking, information leakage, data breaches, information security breaches, malware injections, ransom ware and malware attacks, botnets, and phishing scams are some examples of malicious cyber activities that have diversified in terms

 © 2021 Wiley Periodicals LLC.

of both number, intensity, scope, and magnitude. For example, the annual cost of cybercrimes in 2019 was well over an estimated $2 trillion (Accenture, 2019). The report also highlighted that the average price of cybercrimes per organization witnessed a tremendous increase, going from $1.4 to $13 million (Accenture, 2019). In response, organizations have increased their spending on cybercrime detection and prevention. The report cites an 11% increase in cybercrime and data breach incidents from 2018 to 2019.

Since 2000 the FBI has run the Internet Crime Complaint Center (IC3). The IC3 provides the general public with a trustworthy agency where they can report suspected internet enabled criminal activity (United States, Federal Bureau of Investigation, Cyber Division, 2001-2019). They have published cybercrime statistics in their yearly Internet Crime Report since 2001. Upon review of each report since 2001, the IC3 has seen an average year-over-year increase of 15.4% in logged complaints as seen in Table 1 and Figure 1. Additionally, they have seen an average of 44.4% yearly increase in total losses seen in Table 1 and Figure 2. The report published in 2010 and all proceeding reports did not include a total loss estimate for the year 2010, that is why it is omitted in the data.

Digital investigations, whether the crime is a cybercrime or crime that involves digital appliances, require investigators to parse through massive troves of data in a short amount of time. The complexity and amount of data in addition to time constraints reinforces the importance of artificial intelligence (AI; broadly defined to include machine and deep learning in this article) and automation on digital forensics (Battiato, Emmanuel, Ulges, & Worring, 2012; Kebande et al., 2020), particularly in informing the global community about methods, frameworks, and approaches through which AI and automation-based digital forensic systems can be developed on a commercial scale. Unless resilient digital forensic systems are designed, it is evident that the size and number of computer-aided crimes will only grow and reach a point of inflicting lasting collateral damage to the industry. It is time to calibrate the impacts of AI and automation in creating performance-driven digital forensic systems.

Automation is the marriage of modern systems and software to complete a task or process with zero or minimal human intervention. The principal motive behind automation is to complete jobs faster and reduce the associated cost of performing that particular task. Automation has become ubiquitous across all business sectors (Lee & See, 2004). These automated systems are involved in moving people and goods across the globe in the airlines, automotive, and locomotive infrastructures. The world's energy delivery infrastructure depends significantly on automation. These systems not only reduce costs but also improve safety (Lee & See, 2004). Automation allows humans to spend their time doing more meaningful and complex tasks that automation has yet to conquer. When in isolation, one downfall of

TABLE 1 The number of total complaints and total losses tracked by the FBI IC3 from 2001 to 2019 (Jarrett, 2021; United States, Federal Bureau of Investigation, Cyber Division, 2001-2019)

IC3 report year	Total complaints	Total losses
2019	467,361	$ 3,500,000,000
2018	351,937	$ 2,710,000,000
2017	301,580	$ 1,420,000,000
2016	298,728	$ 1,330,000,000
2015	288,012	$ 1,070,711,522
2014	269,422	$ 800,492,073
2013	262,813	$ 781,841,611
2012	289,874	$ 525,441,110
2011	314,246	$ 485,253,871
2010	303,809	
2009	336,655	$ 559,700,000
2008	275,284	$ 264,600,000
2007	206,884	$ 239,100,000
2006	207,492	$ 198,400,000
2005	231,493	$ 183,100,000
2004	207,449	$ 68,100,000
2003	124,515	$ 125,600,000
2002	75,064	$ 54,000,000
2001	50,412	$ 17,800,000

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

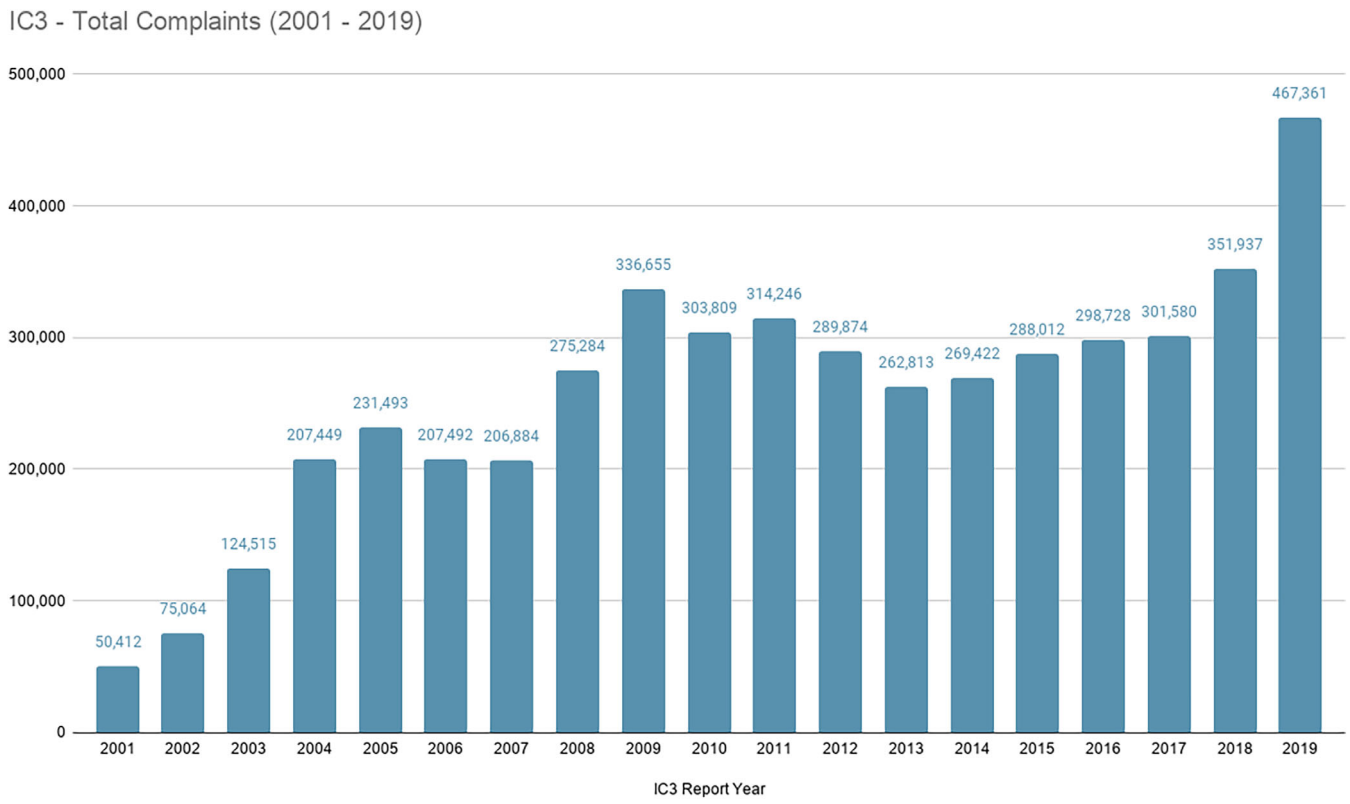

FIGURE 1 Total complaints tracked By IC3 from 2001 to 2019 (Jarrett, 2021)

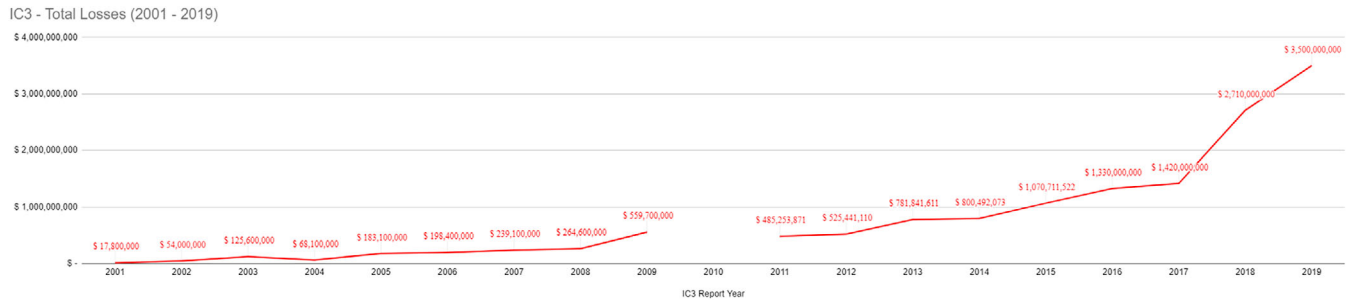

FIGURE 2 Total losses tracked by IC3 from 2001 to 2019 (Jarrett, 2021)

automation occurs when a developer creates an automated process. The developer must code all aspects of the automation, as anything that is not explicitly coded for will not occur, leading to many unintended consequences. To achieve intelligent autonomous automation, one must also look to AI.

The purest definition of AI is the development of computer systems and programs that can act intelligently. In other words, the creation of computer systems or machines that can mimic the behavior and intelligence of human beings (Al Fahdi, Clarke, & Furnell, 2013; Al Fahdi, Clarke, Li, & Furnell, 2016). Others regard AI as demonstrating rational behavior or logical behavior by computer systems, programs, or machines alike (Yeow, Mahmud, & Raj, 2014). Simulated human knowledge enables modern-day systems to automatically and promptly acquire and process large volumes of data and transform them into logical clusters of information. AI-enabled automated processes ultimately allow for autonomous decision making, which results in additional automation when the system takes action on the decisions it has made. When we speak of AI going forward, it is implied that the AI is in combination with Machine Learning (ML) and Deep Learning (DL). Before considering the research, one should understand both ML and DL.

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

ML is the means by which a computer system or algorithm can consume large amounts of data and ultimately make predictions or draw conclusions (Choy et al., 2018). ML uses regression models and classifications to make predictions about the data that the ML is analyzing (Xin et al., 2018). To put it more simply, ML analyzes historical data and forms future predictions. There are two distinct paths an ML algorithm can use to learn, the supervised and an unsupervised route. To fully understand the difference, let us look at popular streaming services that offer content recommendations based on an individual's viewing habits. When the viewer ingests content, an ML algorithm using unsupervised learning can use that data to make recommendations. A disadvantage to this approach is that the algorithm does not know that the viewer wanted to watch the suggested content. However, suppose the user generates inputs by telling the streaming service whether they liked or disliked that content. In that case, the data is now eligible to be used by an ML algorithm that uses supervised learning. In essence, the difference between supervised and unsupervised learning is whether the data is linked to an outcome. Looking back at our streaming example, the more content the viewer consumes with that streaming service, the more the service can accurately predict what the viewer likes and dislikes. At its core, the streaming service utilizes software that uses ML algorithms to learn about the viewer over time. When applying ML to a simple task, it performs very well. However, when adding more data elements for analysis, the learning complexity grows exponentially (Arel, Rose, & Karnowski, 2010). Complex data could also come in the form of images, sounds, and text (Xin et al., 2018). Complex data means traditional ML approaches become too resource-intensive to process data reliably, which is why DL techniques were created.

DL is a specialized subset of ML technology, which solves complex datasets (Arel et al., 2010) using artificial neural networks (ANN). A standard ML algorithm with complex data sometimes needs a developer to correct incorrect learning. DL algorithms do this correction themselves by validating what was learned. Additionally, due to system hardware limitations, a standard ML algorithm may not process complex datasets. To overcome this, DL utilizes ANN to simplify the data in ways that are not possible with standard ML algorithms. Utilizing unsupervised learning networks such as the Restricted Boltzmann Machine and Convolutional Neural Networks (Arnold, Rebecchi, Chevallier, & Paugam-Moisy, 2011 Karie, Kebande, & Venter, 2019), a DL algorithm simplifies the dataset and verifies what it has learned. DL and ML are similar, but DL has automated feature extraction, and model selection is continually being self-evaluated (Xin et al., 2018). Both feature extraction and model selection in traditional ML algorithms are input manually by an expert.

It is essential to understand how these technologies are intertwined. Automation is the overarching technology that holds everything together. ML and DL's primary purpose is to form conclusions or predictions based on large amounts of data. Likewise, AI's primary intent is to determine decisive actions based on the ML/DL output. This relationship is depicted in Figure 3a,b.

Automation and AI appear to have been less utilized in digital forensics in comparison to other application domains. There appears to be a research gap regarding automation and AI's impacts on digital forensics (Hoelz, Ralha, & Geeverghese, 2009). When we take a broader view, some sources classify AI and automation integrated digital forensics as computational forensics. The rationale being that the term "computation" implies an array of disciplines integrated into a single solution to perform a specific task (Franke & Srihari, 2008). For instance, computational vision, linguistics, and optical character recognition functionality combine to formulate advanced software solutions. This software leverages the power of AI to automate processes and mimics human intelligence and decision-making. This article will introduce a new term to refer to technology solutions that utilize AI, Automation, and Machine Learning as Intelligent Automation (IA).

To solidify our understanding of IA, let us look at a financial services example and how these technology solutions have played an integral role in delivering benefits to the companies and the employees and customers. The first example we will review is a high-level example of how IA can impact customer-facing processes to reduce cost, increase time to deliver, and improve experiences. The second example will review how IA has been utilized in securing digital infrastructure utilizing an Intrusion Prevention System (IPS).

As seen in Figure 4, our first example is a customer-facing example where the customer speaks on the phone with an investment representative about reallocating their investment account. Before integrating the IA technologies, the call process flow can be seen in Figure 4a, with Figure 4b being the new process post-implementation of IA technologies.

Figure 4a is the low technology experience that most people are accustomed to. In this situation, the account owner calls in to their financial institution to reallocate their account. A reallocation is when you want to adjust your investments. In this situation the representative, in this case a human, manually performs all actions and adjusts the account investments. In Figure 4b, the intermediate technology solution the account owner calls and speaks with a human to

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

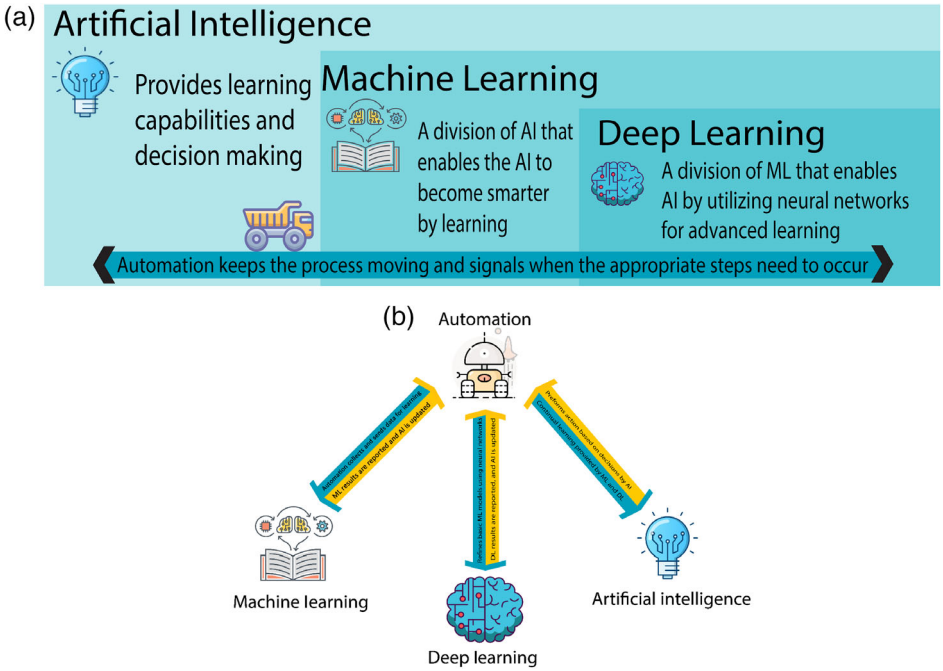

FIGURE 3 (a) The relationship between automation, AI, and ML/DL. (b) A second look at the relationship between automation, AI, and ML/DL

reallocate their account. The representative then initiates a bot, an IA enabled software package, that performs all steps automatically for the representative. This bot will verify the current account investments, and will pull the preferred allocation of the account owner's prior discussion with their financial planner. Then, the bot will calculate the shares to sell and the ones to purchase, then will sell and purchase to complete the transaction. The actions taken by the bot during the call are not anything groundbreaking, rather the innovation here is how the bots learned to perform the tasks. To learn what needed to be done, the learning software monitored what the representatives did over the course of 2 weeks to a month. The software then identified this as a unique process and after the learning period started to perform the task for the representative with minimal human involvement. While the process is IA-enabled as indicated in Figure 4b, to further remove the human aspect of the process, one could use chatbot or speech recognition.

As seen in Figure 5, the second example highlights how the financial services industry would utilize Automation, AI, ML, and DL to secure their networks.

Figure 5 depicts incoming traffic from an unknown source that traffic is then stored in a database so that the IPS system can determine whether or not that traffic is malicious or not. If the traffic is malicious, the requests are blocked via the firewall. The IPS system can determine whether or not traffic is malicious by utilizing IA technologies. Automation enables the process while ML/DL learns from the logged data and teaches the AI what traffic is good or malicious based on traffic patterns or signatures.

The aim of this article is to synthesize secondary research to identify the potential impacts AI and automation have had on digital forensics. The research methodology involved reviewing peer-reviewed research articles published between 2000 and 2020 found via Google Scholar, located using keyword searches relevant to IA. The keywords used to conduct our research were: Automation, Artificial Intelligence, Machine Learning, Deep Learning, Digital Forensics, Computer Forensics, Artificial Neural Networks, Computer Security, Internet-of-things Security, Challenges of Digital Forensics, Network Forensics, and Convolutional Neural Network. We also used organizational websites and credible online (non-peer-reviewed) articles to add weight to the variety of empirical evidence utilized.

The motivation for completing this research is to provide a well-rounded succinct introductory view of how AI and ML have impacted digital forensics. The authors have strived to create an article that is suitable for interdisciplinary consumption. Finally, this study will help identify the gaps underlying digital forensic systems' legacy that may compromise forensic evidence in the near future. Aaron Jarrett was the primary author of the article, Kim-Kwang Raymond Choo's contribution provided editorial support.

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

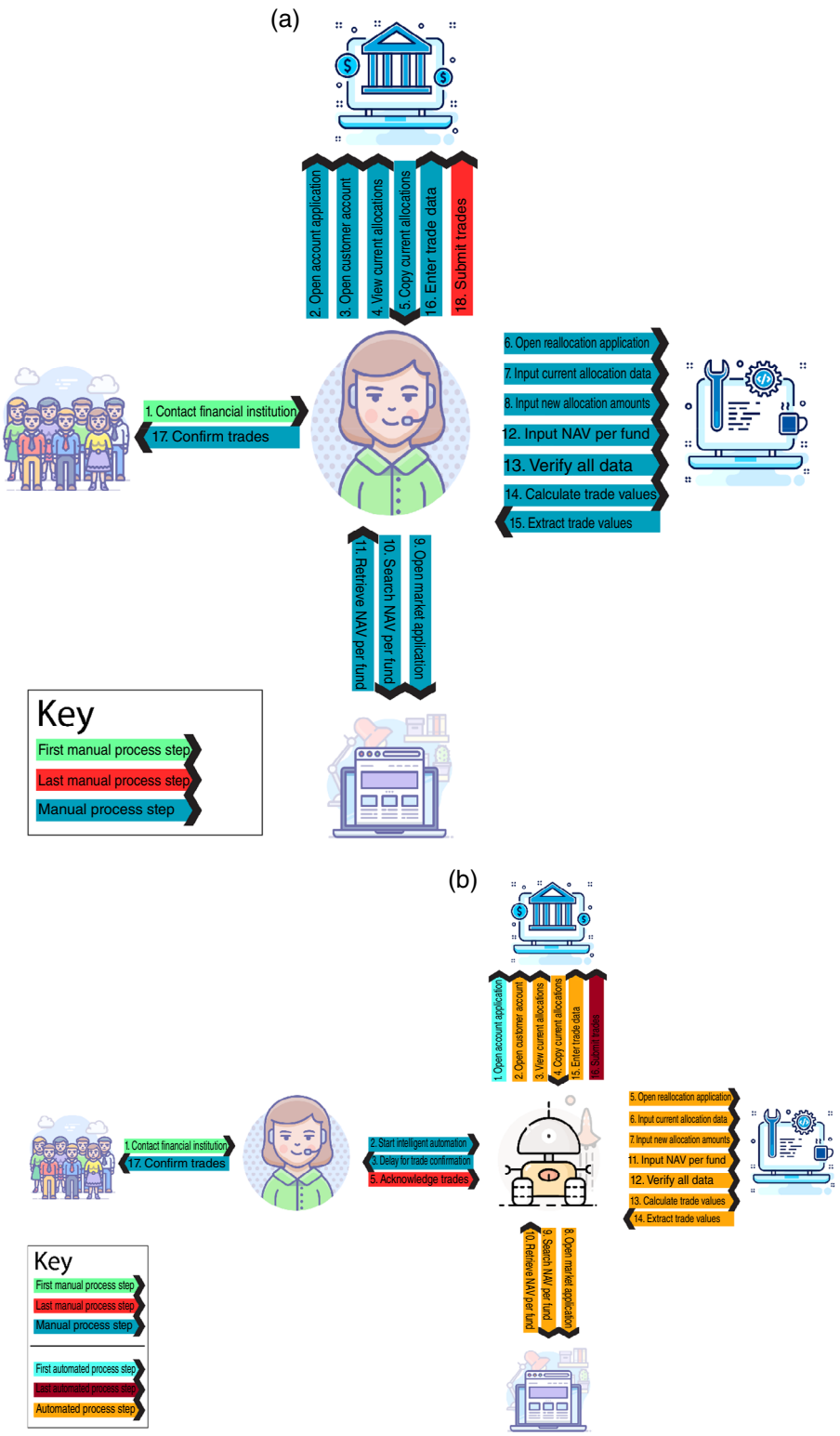

FIGURE 4 (a) Manual process. (b) Automated process

2 | RESEARCH AIM AND OBJECTIVES

The fundamental aim of this research study is to identify and discuss the impacts of IA on digital forensics. Achievement of this central aim is dependent on the completion of the following research objectives:

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

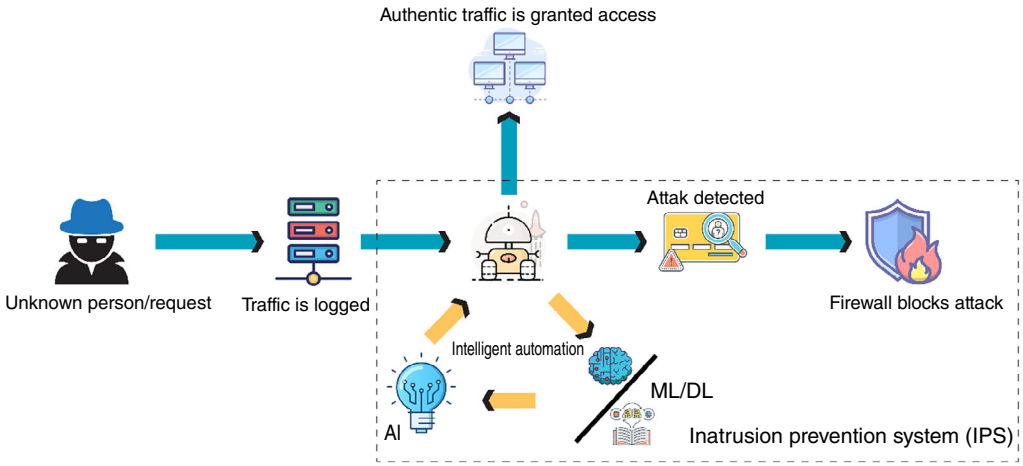

FIGURE 5 Digital infrastructure security utilizing IPS

1. Define automation, AI, machine learning, and deep learning.
2. Identify the major IA tools and technologies that are currently impacting the field of digital forensics.
3. Identify and explain IA-based frameworks for digital forensics.
4. Address the significant impacts of implementing these tools, technologies, and frameworks in digital forensics.
5. Discuss the challenges facing the integration of IA into digital forensics.

The knowledge provided in this article can support the development of more comprehensive courses that educate students on the innovative nature of IA enabled digital forensics techniques—consequently impacting the entire field of digital forensics.

3 | LITERATURE REVIEW

There is much observational evidence that speaks of the application and use of IA in digital forensics. To begin with, the research study by Dilek, Çakır, and Aydın (2015) focuses on the advances made in terms of AI in digital forensics. The study primarily reviews the implementation of AI in defending against cybercrimes (Dilek et al., 2015). Hasan, Raghav, Mahmood, and Hasan (2011) have presented a rigorous AI-based model for an incident response that can be effectively replicated in digital forensics. However, it is appropriate to offer contextual information on artificial intelligence and automation before answering the research question.

3.1 | Artificial intelligence and automation

In a more recent study conducted by Costantini, De Gasperis, and Olivieri (2019), the integration of AI into digital forensics has been explored in adequate detail. The study regards AI as an enabling technology for digital forensics. The researchers identify AI as highly relevant to the "Evidence Analysis" phase of digital forensics. AI-enabled digital forensic tools process objective data, process it and consequently develop valid potential hypotheses that can be presented as evidence to a court of law (Costantini et al., 2019). The study stands out as it considers the applicability of AI coupled with a specific advanced computational, logical tool such as the Answer Set Programming (ASP) software to automatically subject the evidence to analysis (Costantini et al., 2019). One of the critical outcomes was developing a customized Decision Support System (DSS) leveraging the capabilities of AI and ASP to help resolve complex investigations that would be challenging if solved by human intelligence alone. There is an abundance of literature discussing the ability of AI to empower digital forensics. For instance, the research by Xiao, Li, and Xu (2019) proposed an AI-based approach to conduct thorough video-based evidence

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

analysis and data extraction. Masombuka et al. (2018) published an article on the techniques and methodologies for applying AI to digital forensics investigations and purpose an active defense framework.

The research performed by Arsénio et al. (2014) explored the extent to which AI can be embedded to craft an Internet of Things (IoT) network that empowers communication, which was coined IIoT for Intelligent Internet of Things. To help future researchers achieve this goal of AI integration, several research studies have coined an array of algorithms that can ensure the swift functionality of AI in digital forensics.

In another study focusing almost entirely on cybercrimes, Irons and Lallie (2014) regarded the application of AI to digital forensics as a prominent opportunity to overcome the more considerable challenges associated with forensic investigations. The researchers contend that with the increasing complexities of cybercrimes, artificial intelligence holds promise in transforming digital forensics to intelligent forensics, where highly sophisticated technologies can be utilized to identify real cybercrimes and predict the probability of future cybercrimes (Irons & Lallie, 2014). Their research propagates the implementation of artificial intelligence to network forensics, cloud investigations, and big data analytics (Irons & Lallie, 2014). According to this research study, sources of intelligent forensics go beyond the traditional digital forensics to include internet websites, email, social media platforms, organic and paid searches, mobile applications and eCommerce sites, live chat, and other affiliates as sources of data inputs (Irons & Lallie, 2014). Findings from this research study align with more recent research geared toward the development of a suspect-oriented intelligent forensics system that integrates both AI and automation techniques to offer measurable improvements to case proceedings (Al Fahdi et al., 2016).

3.2 | Automation in the context of digital forensics

Automation is the use of computer systems to automate the traditional process of information acquisition, processing, and interpretation. To automate a process, AI is not required, nor is automation required in conjunction with AI systems. Automation and AI are independent concepts that can be utilized together to develop IA systems. The use of Self Organizing Maps (SOMs) and Automated Evidence Profiling (AEP) have been recognized as highly effective by Al Fahdi et al. (2016). The researcher conducted a series of experiments and landed on the conclusion that automation of standard digital forensic procedures is possible through techniques such as SOM and AEP, thereby making the entire process more efficient and less costly (Al Fahdi et al., 2016).

The research by Mohammed, Clarke, and Li (2016) discussed an automation-based approach to process Big Data that was specific to digital forensic investigations. The researchers argued that while processing and analyzing big data is a challenge in itself, the prevalent heterogeneity of the data in criminal cases adds to the difficulty (Mohammed et al., 2016). Complex data systems call for new and improved technologies that can be incorporated into digital forensic settings to help automate the process with high throughput and accuracy. Their proposed metadata-based approach to automate big data as it pertains to digital forensic investigations appears to be effective; however, there are no experimental research studies available that could speak of its actual effectiveness and usability.

In a research study completed by the CARI Institute, the applicability and potential of automation to digital forensics was explored from a multifaceted perspective (Butterfield, Dixon, Miller, & Schreuders, 2018). First, the study provided a comprehensive review of ontological related data (Butterfield et al., 2018). This data was coupled with the collection of primary data directly from the Digital Forensics Units (DFUs). The DFUs were tasked to gather this data and the various trends and interrelationships that were drawn from the data to solve criminal cases (Butterfield et al., 2018). The researchers developed a solution to how automated software can perform the same trend analysis and relationship–identification activities. This software could result in a fraction of the time being spent on drawing the same conclusions as the DFUs obtained (Butterfield et al., 2018).

James and Gladyshev (2013) performed a research investigation to ascertain the prominent challenges facing the merger of automation into contemporary digital forensics. The study begins by highlighting the main motives behind the on-going focus on automating digital forensics. These mainly included the search for financial benefits by the computer forensic investigation agencies to reduce cost. The central focus is to achieve the most accurate digital forensic outcomes in the least amount of time, with the ability to precisely process and analyze large volumes of digital evidence (James & Gladyshev, 2013). The study moves on to identify and elaborate on the significant challenges that can limit the applicability of automated digital forensics. The study identifies inexperienced investigators and practitioners' presence, which can restrict the automation of digital forensic operations due to their limited skillsets (James & Gladyshev, 2013).

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

3.3 | The use of artificial intelligence in digital forensics

AI-enabled digital forensics solutions are continually being enhanced to improve and expedite analysis results. Computer crime profiling is one prominent area where AI is being utilized (Al Fahdi et al., 2016). AI-powered software is being used to facilitate the examination and analysis phases of digital forensics (Al Fahdi et al., 2016). As such, it enables forensic experts to examine and analyze digital evidence across a wide variety of computer crimes, including but not limited to malware, spyware, hacking, data theft, and identity theft (Al Fahdi et al., 2016). The on-going technological advancements have helped computer criminals to plan and implement more sophisticated crimes, which require that AI-powered digital forensics tools be readily accessible (Butterfield et al., 2018).

The constantly diversifying portfolio of IA in digital forensics is evident from the fact that the field has now diverged into specialized sub-categories. Experts have managed to develop AI-based Network Intrusion Detection systems that leverage the power of ANNs to identify intrusive traffic with 99.97% accuracy (Kanimozhi & Jacob, 2019).

A further literature review highlights specific ways in which IA can be used in digital forensics by integrating algorithms with computational methods. These uses include:

- Tracing the evidence in a more enhanced and streamlined fashion to conduct an in-depth investigation (Franke & Srihari, 2008).
- It identifies critical forensic evidence and renders it to further analysis objectively and reproducible (Franke & Srihari, 2008).
- Assessing forensic investigation methods' overall quality and effectiveness and subsequently standardizing these methods (Franke & Srihari, 2008).
- Expediting the search and identification of important trends from large volumes of data followed by visualization of the results (Franke & Srihari, 2008).
- Assisting in the construal of these results reveals trends and patterns that were previously unknown (Franke & Srihari, 2008).

In other words, the use of IA in digital forensics allows human forensic experts to find answers to legal significance questions in less time and cost. To an extent, it is arguable that IA can also be utilized to limit future risks and challenges by thoroughly analyzing current and previous digital evidence. Franke and Srihari suggest that digital forensics is a combination of methodology, application, and technology.

The likelihood of occurrence of future incidents, cybercrimes, and attacks may very well be addressed by intelligently using such technologies and computational methodologies. A more precise explanation of the use of IA in digital forensics can best be explained by first understanding how it has been applied thus far. This includes, but may not be limited to crime-scene investigation or CSI, photographing and documentation of the crime scene, identification, collection, preservation, and analysis of forensic evidence and the subsequent link analysis (Franke & Srihari, 2008). Digital forensics goes beyond computer-related crimes and encompasses computational methodologies to analyze physical evidence retrieved from the crime scene. Such evidence may entail a broad area of substances and objects, such as body fluids, blood, drugs, chemicals, fiber, paint, explosives and toxins, tissue traces, impression evidence such as fingerprints, and electronic data and evidence, among others (Franke & Srihari, 2008). Further review of empirical evidence suggests that digital forensics may also be utilized to determine digital evidence's integrity and credibility while ensuring that it has not been subjected to any tampering or modification (Tanner & Dampier, 2009).

3.4 | Frameworks and tools of intelligent automation in digital forensics

Secondary research yielded two distinct primary research focus areas. The first identified area is digital forensic frameworks, and the second is digital forensic tools. In this section, we will review some of the research in each area.

3.4.1 | Frameworks of intelligent automation in digital forensics

Hasan et al. (2011) have proposed an incident-response model leveraging the capabilities of AI. Here, the researchers focused on the incidents related to computer systems and equipment that consequently damaged the infrastructure in

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

some way (Hasan et al., 2011). The model encompasses clustering, decision support systems, IRSS, and COPLINK altogether (Hasan et al., 2011). This model's critical steps include information gathering, storage, analysis, search, identification, and clustering of data while integrating all the aforementioned technologies (Hasan et al., 2011). Elsaesser and Tanner (2001) proposed an automated system for digital forensics called Automated Diagnosis with the motive of revealing the methods utilized by existing hackers. Their recommended system processes victim configuration and vulnerability related information accompanied by the type of unauthorized access achieved by the attacker (Elsaesser & Tanner, 2001). By doing so, the system automatically processes the specified information to reveal critical insights regarding hackers' attack methods, thereby making it easier to create defensive techniques (Elsaesser & Tanner, 2001).

Similarly, Ribaux and Margot (2003) proposed a model for the forensic investigation of criminal intelligence that considers case-based reasoning as the primary technique. Case-based reasoning is defined by solving new problems based on the solution of past issues of similar nature. A more recent research study that utilized the case-based reasoning approach similar to Ribaux and Margot (2003) involved developing an Intelligent Forensic Autopsy Report System I-AuReSys (Yeow et al., 2014). The methodology considered case-based reasoning as the fundamental principle for formulating this system that performs information extraction, analyzing case similarities by combining the Naïve Bayes learner, thereby creating distinct outcome recommendations (Yeow et al., 2014). The potential application of IA principles to digital forensics has also been reviewed by Irons and Lallie (2014). They propose incorporating cloud investigation techniques, utilization of big data, and the Digital Intelligence Architecture coined by Stanhope (Irons & Lallie, 2014). As such, the researchers argued that intelligent forensics is an approach that combines IA with current digital forensic techniques to adapt according to the complexity of cases (Irons & Lallie, 2014). In another research study, a thorough digital forensics agenda is proposed that incorporates evidence modeling, network forensics, data volume, live acquisition, media types, and control systems (Battiato et al., 2012; Nance, Hay, & Bishop, 2009). This research agenda mainly involves the main constituents of IA to research and develop more effective digital forensic systems.

This literature review has so far illustrated that there is no one-size-fits-all digital forensics model or approach. However, arguably one model known as DFRWS may apply to many cases involving digital forensic investigations (Tanner & Dampier, 2009). The acronym for the Digital Forensics Research Workshop model, DFRWS, contains six phases: identification, preservation, collection, examination, analysis, and presentation (Tanner & Dampier, 2009). Each of the six phases is traditionally involved in a majority of digital forensic investigations. Moreover, the model advocates using concept maps to further simplify the digital forensics investigation process. These concept maps may very well be incorporated into conventional AI technologies to automate concept mapping.

The Digital Forensic Investigation Reduction Model (DIFReM), coined by Shayau (2019), considers the forensic investigation steps proposed by the Digital Forensics Research Workshop to introduce a data reduction model that holds the capability of identifying the modified files, inserted files, and integrity verification through hashing. Several other models and approaches can be of value in crafting a technically well-versed forensic investigation platform (Krivchenkov, Misnevs, & Pavlyuk, 2018).

Digital forensics is a multidisciplinary field of examination and is evident from the model coined by Hasan et al. (2011) as a means of incident response. The researchers initially highlighted the lack of automated and high-performing incident response systems. They proposed incorporating IA technologies to develop a highly effective and efficient incident response system (Hasan et al., 2011). The mode consists of four sequential steps that begin with information gathering, and ends with the presentation of results that can potentially facilitate incident response (Hasan et al., 2011). However, the model suffers from the limitation that the researchers shared no practical or experimental demonstration. Instead, this model's development and testing were included under the “future work” section, indicating its infancy and that it has not been fully realized nor completed. Nevertheless, the authors still propose the collective use of three clustering techniques, including partitioning-based analysis, hierarchy-based analysis, and sequence discovery (Hasan et al., 2011).

The Semantic Web-Based Framework for Metadata Forensic Examination and Analysis has also been posited as an automation framework (Mohammed et al., 2016). The framework leverages metadata's power to identify the digital evidence, subject it to reduction, and subsequently perform metadata extraction to foster digital forensic proceedings (Mohammed et al., 2016). Once the metadata has been extracted, it is populated into XML files and sent to the repository for further evaluation and analysis (Mohammed et al., 2016). This repository can support data gathered from a variety of digital forensics sources that apply to a single criminal case (Mohammed et al., 2016). The Semantic Web technology enables the system to search and locate specific information of heterogeneous nature from the repository (Mohammed et al., 2016).

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

3.4.2 | Tools and methods of intelligent automation in digital forensics

Tian, Jiang, Li, and Dong (2014) have proposed a digital evidence fusion method targeted toward forensic network systems. Their research leverages the provisions of Dempster–Shafer (D–S) theory as a means of proactively identifying and neutralizing network intrusion. Their research involved combining the Transductive Confidence Machines for K-Nearest Neighbors (TCM-KNN) algorithm and the D–S fusion engine theory to achieve artificial intelligence with automation-specific objectives (Tian et al., 2014). They aimed to improve the intrusion detection performance of their network intrusion forensic system to outperform the traditional methods and automate digital evidence fusion from multiple differential sources (Tian et al., 2014). In doing so, the researchers demonstrated their model's efficacy by rendering the KDD Cup 1999 dataset for forensic analysis (Tian et al., 2014). A series of experiments revealed a higher true-positive rate accompanied by a lower false-positive rate, compared with the network forensic methods that were considered standard at the time (Tian et al., 2014).

The software developed by Butterfield et al. (2018) in response to the data extraction and analysis needs of DFUs is also worth discussing. Their research focused on developing the SPARQL analyzer (Butterfield et al., 2018). The SPARQL analyzer comprises four query forms: Select, Construct, Ask, and Describe query forms, each performs their specific functions to help in automated forensic data extraction (Butterfield et al., 2018). The researchers succeeded in making SPARQL extractors for file system information, XRY parsers, UFED XRY parsers, IEF parsers, and CDR records (Butterfield et al., 2018). A key strength of this research study was that it did not stop with SPARQL development, but continued research work to calibrate the most viable options for central data storage (Butterfield et al., 2018).

A more modern digital forensic investigation tool has recently been launched by Magnet Forensics (2019). Magnet Forensics is a large-scale corporation specializing in digital forensics-related research and development and the provision of high-performing technologies. The company recently announced the Magnet AUTOMATE system with the motive of enabling digital forensic experts to investigate and solve cases much faster than before (Magnet Forensics, 2019). The newly launched tool is based on the repeatable forensic workflow mechanism. According to Magnet, AUTOMATE is a flexible platform to quickly build custom automation around a standard workflow. AUTOMATE integrates with a secondary application named Magnet AXIOM that integrates smart parsing and carving techniques to extract data, which furthers Magnet's mission to automate digital forensics (Magnet Forensics, 2019). The tool is worthy of consideration due to its claims to deliver critical evidence on complex criminal cases within 48 hr (Magnet Forensics, 2019). Most of all, Magnet AUTOMATE can be essential in allowing digital forensic agencies to reduce their case backlogs and time to resolution.

A study conducted by Homem (2018) attempts to overcome the challenges of automation and digital forensics. The study formulates a highly resilient program to advance automation in digital forensics (Homem, 2018). The study was a pilot study that initially focused on identifying and acquiring forensic evidence (Homem, 2018). The study proposes a system architecture as a proof of concept to demonstrate how remote evidence acquisition can be carried out via automation (Homem, 2018). The study developed Machine Learning-based Triage methods to test the feasibility of the proposed system architecture in automating the analysis phase of digital forensic investigations (Homem, 2018). The system employs multiple devices over a unified network to engage them during a digital investigation. The designed vital function assists the human analyst in reducing their discovery and analysis burden (Homem, 2018). In this way, analysts gain the ability to resolve critical cases and identify suspects quickly.

4 | POTENTIAL IMPACTS OF INTELLIGENT AUTOMATION ON DIGITAL FORENSICS

The impacts of IA on digital forensics have enabled law enforcement agencies to identify key trends in various crimes (Reiber, 2018). Specifically, incorporating IA into traditional digital forensics can facilitate the spotting of elements in videos, photos, and other forms of digital evidence to make highly accurate decisions regarding where and when a particular crime took place (Reiber, 2018). Similarly, IA helps digital forensic experts to make informed decisions regarding the possible time and location of future crimes based on identified commonalities (Reiber, 2018). Moreover, IA enables digital flag content more quickly and with higher accuracy than traditional, human-intelligence-based, digital forensic procedures (Reiber, 2018).

The use of IA technologies in digital forensic investigations yield three prominent benefits. First, it saves substantial amounts of time for the investigators, consequently enabling them to identify, track, and solve cases more efficiently

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

while minimizing collateral damage. Secondly, it aids digital forensic investigations to track down and curtail any future crimes or incidents that involved similar techniques. Third, a significant factor to consider with regards to digital forensics is the hefty costs involved. According to a scholarly review, the cost of hiring digital forensic experts to solve complex cases is substantial (Vestige Limited, 2018). Research determined that a digital forensic expert's typical image analysis will cost anywhere between $5,000 and $15,000, while analyses and processing of more complex images and videos may exceed $100,000 (Vestige Limited, 2018). Table 2 shows that digital forensics' cost is consolidated into three main classes, where the price ranges are indicated adjacently (Ellis, 2018).

Considering the complex nature of crimes and criminal investigations being managed under law enforcement and government agencies, it is arguable that the costs will be high. In this sense, the implementation of IA-based digital forensics will help to significantly save money. These savings from human resources and a reduction in working hours can resultantly be reinvested to develop improved digital and technology infrastructure that requires minimal human intervention.

Perhaps a more direct view of the impacts of IA on digital forensics comes in the form of enhanced biometric modalities. Present-day digital forensic services (DFS) use biometric modalities to solve critical criminal cases. For instance, through the integration of IA into DFS, key biometric modalities, including feature extraction, feature capturing, feature matching, and feature robustness, have been introduced (Awad & Hassanien, 2014). These biometric modalities have, in turn, been utilized to develop highly accurate and compelling biometric recognition and tracking systems that can be utilized to proactively track and bring down most wanted criminals (Awad & Hassanien, 2014). Critical biometric identification systems include fingerprint identification and matching, facial recognition and profiling, iris recognition, matching, and profiling (Awad & Hassanien, 2014). DNA matching and analysis are also commonly used biometric identification systems utilized by conventional DFS professionals (Awad & Hassanien, 2014).

Soft biometric characteristics can also be tracked and identified, such as hair color or skin color, in order to classify the case suspects for coarse-level investigations (Awad & Hassanien, 2014). On the other hand, efficiency and sustainability are also some substantial impacts of integrating IA into digital forensics (Spencer, 2018). To be specific, IA holds the capability to instill efficiency and efficacy into data acquisition, site analysis, encryption, decryption, and other investigative activities (Spencer, 2018). This efficiency can be achieved by using the IA-based programs to identify and represent trends, patterns, and linkages between forensic evidence more quickly than human analysis (Spencer, 2018). In other words, IA based technology can collectively contribute to expediting the processing and handling of forensic evidence. It can quickly process bulk data utilizing a targeted analysis approach in order to reveal meaningful correlations. Thus, forensic investigations' overall efficiency and accuracy can be further enhanced by coupling digital systems with skilled human investigators.

Another means of looking at the impact of IA-based technology on digital forensics is in terms of the media types involved. There is no denying that modern-day cybercrimes use a wide variety of media types to inflict harm, including pictures, videos, mobile phone applications, and even specific computer programs. Contemporary IA technologies have evolved to the extent that they can readily implement these various media types' forensic analysis. For instance, if a data breach attack involved the use of an Android smartphone, then sophisticated DFS software such as the SPF pro or SmartPhone Forensic System Professional can be utilized to automatically recover, extract, analyze and triage the relevant data (Salvation Data Technology, 2018). Other forensic analysis tools, such as SANS SIFT, CrowdStrike CrowdResponse, and Volatility, are all built with IA based technology that automates the forensic investigation tasks to generate results more quickly and accurately than the traditional systems. Another excellent example of how IA has impacted digital forensics is the innovative Intrusion Detection and Prevention Systems that are purpose-built to perform automated data collection and analysis based on the network traffic (Nance et al., 2009). Intrusion Detection Systems (IDS) are built on top of IA-enabled scripts and tools to automatically detect and alert the network administrators about any anomalous network traffic or suspicious data packets coming from unknown IP addresses or destinations.

TABLE 2 Investigation cost breakdown by complexity (Ellis, 2018)

Investigation complexity	Cost
Level 4	$10,000
Level 2 to 3	$10,000 to $100,000
Level 1	$100,000+

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

5 | CHALLENGES OF INTELLIGENT AUTOMATION ENABLED DIGITAL FORENSICS

There are two challenges faced in particular by IA-based digital forensic systems.

First, IA-based technology can only serve as tools to facilitate investigations, which still requires oversight by expert human investigators. The accuracy of the forensic outcome, to some extent, is dependent on the abilities of the human investigator, since IA enabled tools are still under development and may not always yield accurate, complete, or robust information necessary for forensic cases (James & Gladyshev, 2013). Overcoming this challenge requires that either the investigator be provided with significant training and skills development, or utilize highly skilled investigators. In a possible scenario, inexperienced practitioners act on insufficient information due to their total reliance on the automated systems increasing the probability of failed investigations (James & Gladyshev, 2013). Furthermore, inexperienced investigators' presence is often coupled with a lack of certifications and quality checks of the lab equipment involved in forensic data collection (James & Gladyshev, 2013). Additionally, many digital forensic investigations are awarded to third party contractors, most of whom are self-proclaimed and not certified (James & Gladyshev, 2013). Another issue is the absence of certification institutions and regulatory bodies that ensure only certified digital forensic investigators are operational within the markets.

Another major difficulty facing digital forensics is using multiple and complicated media formats that may prove challenging to acquire or analyze by the current AI systems (Al Fahdi et al., 2013). For instance, steganography, encryption, and anti-forensics media formats may be utilized (Al Fahdi et al., 2013). Researchers further argue that the differential sources of digital evidence may also prove a noteworthy hindrance in the way of digital forensic investigations via IA (Oriwoh, Jazani, Epiphaniou, & Sant, 2013). The widespread adoption and use of Internet of Things (IoT) devices further diversify this specific paradigm's challenges. It widens the spread and flow of data, leading to a less-private and less-secure premise for end-users (Oriwoh et al., 2013). The ever-increasing volume of data and information seized and subjected to digital forensic analysis is a challenge that must be handled by new and improved IA technologies (Quick & Choo, 2014).

Perhaps a rather exciting yet daunting side of IA-based technologies' applicability to digital forensics was explored recently by Spencer (2018). In their study, the complex and unpredictable mindsets of criminals was discussed and consequently formulated the theory that complete automation of digital forensics is potentially impossible (Spencer, 2018). As a result, many criminal cases fail to abide by a standard pattern or historical trends (Spencer, 2018). Furthermore, evolving technologies and techniques pave the way for criminals to adopt new and improved methods of committing crimes (Spencer, 2018).

6 | DISCUSSION

The results of this study reveal that the impacts of IA on digital forensics are significant and have several applications in this field. First, IA can boost digital forensic investigations' overall efficiency by quickly identifying trends and patterns, commonalities, anomalies, and other traits within digital evidence. This speed and efficacy allow forensic experts to generate leads and solve cases with less time and resources. These improvements bring us to the second significant impact, which involves the reduction of costs associated with digital forensic investigation. Research determines that it can take anywhere between $5,000 and $100,000 to hire human resources and fulfill digital forensic analysis manually (Vestige Limited, 2018).

The costs associated with inaccurate forensic investigations and deductions due to human error cannot be overlooked. Thus, IA can help law enforcement and other agencies to automate specific investigative processes that take considerable time and have a high defect rate. Leveraging the systems and frameworks discussed in this article will consequently enable them to save substantial financial resources. These resources can subsequently be rendered to more productive use, such as in the procurement of more improved IA equipment. These findings can further be analyzed to reveal that IA digital forensic systems can increase the probability of solving a higher number of criminal cases in lower amounts of time, which can prevent future attacks from occurring—for instance, a data breach of a large-scale financial institution. The attack can be neutralized through early detection, preventing the loss of millions. Similarly, the occurrence of computer-aided espionage can also be prevented through IA-enabled digital forensics. Advanced criminal profiling can be embedded into the traditional surveillance systems, such as CCTV cameras, to identify and prosecute criminals.

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Several frameworks and models for the incorporation of IA with digital forensics were also identified. The incident-response model proposed by Hasan et al. (2011) encompasses clustering, decision support systems, IRSS, and COPLINK for gathering, storage, analysis, search and identification, and clustering of data. The Automated Diagnosis system proposed by Elsaesser and Tanner (2001) processes victim configuration and vulnerability related information accompanied by the type of unauthorized access that the attacker achieved. The system automatically processed the specified data to reveal critical insights regarding the attack methods utilized by hackers, thereby making it easier to create defensive techniques. Ribaux and Margot (2003) proposed a model centered on case-based reasoning, further explored in a later study where the Intelligent Forensic Autopsy Report System was developed by Yeow et al. (2014). Other frameworks advocated integrating cloud computing, big data analytics, and digital footprints to model forensic evidence and make sense out of the events and happenings involved. A majority of these frameworks utilized Machine Learning, Deep Learning, Big Data analysis, Decision Support Systems, and Incident Response Support Systems. Nonetheless, specific challenges were also identified, such as the presence of forensic evidence in multiple complex media formats and the credibility of sources of data and information. These challenges require discernment on the part of law enforcement organizations and the judiciary.

The study results reveal significant details regarding the current and potential impacts of AI and automation on digital forensics. IA systems enable law enforcement agencies to identify trends in various crimes. It was discovered that the two technologies could readily facilitate the spotting of elements in videos, photos, and other forms of digital evidence to make highly accurate decisions. Automation of specific processes involving digital forensic investigations like flagging content more quickly and with higher accuracy as opposed to traditional digital forensic procedures was identified as a compelling impact. These improvements can enable the investigators to identify, track, monitor, and solve cases more efficiently while minimizing any severe damage to the victim's intellectual property or digital infrastructure. Secondly, the study found that the two technologies streamline digital forensic investigations to predict and prevent future crimes or incidents from innovative tools and techniques. Furthermore, they are highly effective in enabling the traditional investigation systems to identify and neutralize stealthy cybercrimes. Finally, IA-enabled investigations show a remarkable reduction in human-error which decrease investigation time, decrease costs, and decrease the rate of incorrect outcomes.

7 | CONCLUSION AND RECOMMENDATIONS

The purpose of this literature review was to answer the question regarding the impacts of IA on digital forensics. Considering the empirical evidence gathered and analyzed: the main implications of IA included cost-reduction, improved efficiency and speed of forensic investigation, more accurate data and information processing, and increased probability of solving a higher number of cases in limited amounts of time. One reviewer suggested that an additional research area should include the validation of the datasets provided in each of the article's utilized articles. Additionally, it is recommended that future researchers utilize the inputs from this article to design a meta-analysis where statistical analysis and descriptive statistics are used to combine data from multiple research articles summarized here. Another reviewer pointed out that IA also has applications for other forensic science disciplines such as drug testing, as a potential future research.

Based on the overall findings from this literature review, the following recommendations are proposed for the digital forensics industry;

- The policy-makers and government must allocate a budget to empower IA-based digital forensic systems that consider the emerging threat vectors and vulnerabilities, to be directly aligned with the emerging cybersecurity threats on local, national, and international fronts.
- There is a need to encourage global collaboration between IA system developers and digital forensic experts to continually evolve the legacy digital forensic technologies to achieve the maximum degree of responsiveness and protection from future crimes.
- Considering the hefty costs of cyberattacks such as identity theft and data loss, organizations should strongly consider investing in improving the security, privacy, and confidentiality of their cyber infrastructure and information assets. A potential means of enhancing readiness and responsiveness to such crimes is by achieving compliance with the latest privacy regulations, such as CCPA and GDPR.

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

- The results of this study further attest that the cost of identifying and detecting attacks is increasing each day, largely due to the rising complexity, technical nature, and variations in media types used to launch attacks. Therefore, it is advised to embed automation, security intelligence, and advanced analytics to minimize such costs while also gaining the capability to neutralize complicated attacks in the future.

A general recommendation is to raise awareness regarding the use, applicability, and impacts of IA on digital forensics. Specifically, knowledge regarding the positive effects of IA on DFS needs to be communicated to the public, including individuals, organizations, manufacturers, law enforcement, and cybersecurity professionals. This knowledge transfer can best be achieved by publishing similar research studies and conference papers, distributing them across online and offline databases, and holding awareness-raising events with a specific agenda. Encouraging information security experts and programming entrepreneurs to develop high-performing digital forensic tools through crowdfunding can help fulfill the pertinent gaps. Finally, integrating industry best practices regarding digital forensics and forensic investigations across the globe may offer useful information on optimizing the existing DFS services.

Finally, it should be noted that the authors did discover "Digital Forensics: Evidence Analysis via Intelligent Systems and Practices," or DigForAsp. DigForAsp is funded by the European Cooperation in Science and Technology and hosted by the Universidad de Cadiz, a public university in Cádiz, Spain. This network of developers and security professionals explore the application of IA reasoning in the Digital Forensics field ("Digital Forensics: Evidence Analysis via Intelligent Systems and Practices—Sitio web de la Universidad de Cádiz," Digital Fornesics, 2021).

CONFLICT OF INTEREST

Dr. Kim-Kwang Raymond Choo is an Editor of the journal and was excluded from the peer-review process and all editorial decisions related to the publication of this article.

AUTHOR CONTRIBUTIONS

Aaron Jarrett: Conceptualization; data curation; formal analysis; investigation; methodology; writing-original draft; writing-review & editing. **Kim-Kwang Raymond Choo:** Formal analysis; investigation; project administration; writing-review & editing.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are openly available in [OSF.io] at https://doi.org/10.17605/OSF.IO/JHFAW.

FURTHER READING

Dixon, P. D. (2005). An overview of computer forensics. *IEEE Potentials*, *24*(5), 7–10.

Forensic (2020). The Merriam-Webster.com Dictionary. Retrieved from https://www.merriam-webster.com/dictionary/forensic

Kelly, L., Sachan, S., Ni, L., Almaghrabi, F., Allmendinger, R., & Chen, Y. W. (2020). Explainable artificial intelligence for digital forensics: Opportunities, challenges and a drug testing case study. In B. S. Shetty & P. Shetty (eds.), *Digital forensic science*. IntechOpen.

Mehmood, R., Alam, F., Albogami, N. N., Katib, I., Albeshri, A., & Altowaijri, S. M. (2017). UTiLearn: A personalized ubiquitous teaching and learning system for smart societies. *IEEE Access*, *5*, 2615–2635.

ORCID

Aaron Jarrett https://orcid.org/0000-0001-5067-1492
Kim-Kwang Raymond Choo https://orcid.org/0000-0001-9208-5336

REFERENCES

Accenture. (2019). 9th Annual Cost of Cybercrime Study. Accenture.com. Retrieved from https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013). Towards an automated forensic examiner (AFE) based upon criminal profiling and artificial intelligence. 11th Australian Digital Forensics Conference. Held on the 2nd–4th December, 2013 at Edith Cowan University, Perth, Western Australia.

Al Fahdi, M., Clarke, N. L., Li, F., & Furnell, S. M. (2016). A suspect-oriented intelligent and automated computer forensic analysis. *Digital Investigation*, *18*, 65–76.

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Arel, I., Rose, D. C., & Karnowski, T. P. (2010). Deep machine learning: A new frontier in artificial intelligence research. *IEEE Computational Intelligence Magazine*, *5*(4), 13–18.

Arnold, L., Rebecchi, S., Chevallier, S., & Paugam-Moisy, H. An introduction to deep learning. ESANN 2011 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, Bruges, Belgium. (2011).

Arsénio, A., Serra, H., Francisco, R., Nabais, F., Andrade, J., & Serrano, E. (2014). Internet of intelligent things: Bringing artificial intelligence into things and communication networks. In F. Xhafa & N. Bessis (Eds.), *Inter-cooperative collective intelligence: Techniques and applications* (pp. 1–37). Berlin, Heidelberg: Springer.

Awad, A. I., & Hassanien, A. E. (2014). Impact of some biometric modalities on forensic science. In A. K. Muda, Y. Choo, A. Abraham, & S. Srihari (Eds.), *Computational intelligence in digital forensics: Forensic investigation and applications* (pp. 47–62). Cham: Springer.

Battiato, S., Emmanuel, S., Ulges, A., & Worring, M. (2012). Multimedia in forensics, security, and intelligence. *IEEE Multimedia*, *19*(1), 17–19.

Butterfield, E. M., Dixon, M. B., Miller, S., & Schreuders, Z. C. (2018). Automated digital forensics (unpublished).

Choy, G., Khalilzadeh, O., Michalski, M., Do, S., Samir, A. E., Pianykh, O. S., ... Dreyer, K. J. (2018). Current applications and future impact of machine learning in radiology. *Radiology*, *288*(2), 318–328.

Costantini, S., De Gasperis, G., & Olivieri, R. (2019). Digital forensics and investigations meet artificial intelligence. *Annals of Mathematics and Artificial Intelligence*, *86*, 193–229.

Digital Forensics (2021). evidence analysis via intelligent systems and practices – Sitio web de la Universidad de Cádiz. Retrieved from https://digforasp.uca.es/

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *arXiv Preprint*. arXiv:1502.03552.

Ellis, D. (2018). What does a cyber forensic investigation do and how much does it cost? SecurityMetrics. Retrieved from https://www.securitymetrics.com/blog/what-does-cyber-forensic-investigation-do-and-how-much-does-it-cost

Elsaesser, C., & Tanner, M. C. (2001). Automated diagnosis for computer forensics. Technical Report, The Mitre Corporation (1–16).

Franke, K., & Srihari, S. N. (2008). Computational forensics: An overview. International Workshop on Computational Forensics, Springer, Berlin, Heidelberg (pp. 1-10).

Hasan, R., Raghav, A., Mahmood, S., & Hasan, M. A. (2011, November). Artificial intelligence based model for incident response. In 2011 International Conference on Information Management, Innovation Management, and Industrial Engineering (pp. 91-93).

Hoelz, B. W., Ralha, C. G., & Geeverghese, R. (2009). Artificial intelligence applied to computer forensics. In Proceedings of the 2009 ACM Symposium on Applied Computing (pp. 883–888).

Homem, I. (2018). Advancing automation in digital forensic investigations (Doctoral Dissertation). Department of Computer and Systems Sciences, Stockholm University.

Irons, A., & Lallie, H. (2014). Digital forensics to intelligent forensics. *Future Internet*, *6*(3), 584–596.

James, J. I., & Gladyshev, P. (2013). Challenges with automation in digital forensic investigations. *arXiv Preprint*. arXiv:1303.4498.

Jarrett, A. (2021). The Impact of AI & Automation on Digital Forensics IC3 2001–2019. Retrieved from https://doi.org/10.17605/OSF.IO/JHFAW

Kanimozhi, V., & Jacob, T. P. (2019). Artificial intelligence-based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. In 2019 International Conference on Communication and Signal Processing (ICCSP).

Karie, N. M., Kebande, V. R., & Venter, H. S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. *Forensic Science International: Synergy*, *1*, 61–67.

Kebande, V. R., Ikuesan, R. A., Karie, N. M., Alawadi, S., Choo, K. K. R., & Al-Dhaqm, A. (2020). Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments. *Forensic Science International: Reports*, *2*, 100122.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. NIST National Institute of Standards and Technology, Special Publication (pp. 800–86). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Krivchenkov, A., Misnevs, B., & Pavlyuk, D. (2018). Intelligent methods in digital forensics: State of the art. In International Conference on Reliability and Statistics in Transportation and Communication (pp. 274-284).

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, *46*(1), 50–80.

Magnet Forensics. (2019). Magnet AUTOMATE. Retrieved from https://www.magnetforensics.com/products/magnet-automate/

Masombuka, M., Grobler, M., & Watson, B. (2018). *Towards an artificial intelligence framework to actively defend cyberspace*, Reading, England: Academic Conferences International Limited.

Mohammed, H., Clarke, N., & Li, F. (2016). An automated approach for digital forensic analysis of heterogeneous big data. *The Journal of Digital Forensics, Security, and Law*, *11*(2), 137.

Nance, K., Hay, B., & Bishop, M. (2009). Digital forensics: Defining a research agenda. In 2009 42nd Hawaii International Conference on System Sciences (pp. 1-6).

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of things forensics: Challenges and approaches. In The 9th IEEE International Conference on Collaborative Computing: Networking, Applications, and Worksharing (pp. 608-615).

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Quick, D., & Choo, K. K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, *11*(4), 273–294.

Reiber, L. (2018). How does AI contribute to digital forensics?. Forbes.com. Retrieved from https://www.forbes.com/sites/quora/2019/06/05/how-does-ai-contribute-to-digital-forensics/#73e5b212c20a

Ribaux, O., & Margot, P. (2003). Case-based reasoning in criminal intelligence using forensic case data. *Science & Justice*, *43*(3), 135–143.

Salvation Data Technology. (2018). Smartphone forensic system - cell phone forensics tools. Salvationdata.com. Retrieved from http://www.salvationdata.com/spf-smartphone-forensic-system.html

Shayau, Y. H., Asmawi, A., Rum, S. N. M., & Ariffin, N. A. M. (2019). Digital forensic investigation reduction model (Difrem) for windows 10 OS. *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*. (459–464). Shah Alam, Malaysia: IEEE.

Spencer, F.M. (2018). Digital forensics with artificial intelligence internet of things. Retrieved from https://www.researchgate.net/publication/330134282_Digital_Forensics_with_Artificial_Intelligence_Internet_of_Things

Tanner, A., & Dampier, D. (2009). Concept mapping for digital forensic investigations. In IFIP International Conference on Digital Forensics (pp. 291–300).

Tian, Z., Jiang, W., Li, Y., & Dong, L. (2014). A digital evidence fusion method in network forensics systems with Dempster-Shafer theory. *China Communications*, *11*(5), 91–97.

United States, Federal Bureau of Investigation, Cyber Division. (2001-2019). Internet Crime Complaint Center. Retrieved from https://www.ic3.gov/

Vestige Limited. (2018). Considerations for the cost of digital forensic services. Retrieved from https://www.vestigeltd.com/thought-leadership/digital-forensic-services-cost-guide-vestige-digital-investigations/

Xiao, J., Li, S., & Xu, Q. (2019). Video-based evidence analysis and extraction in digital forensic investigation. *IEEE Access*, *7*, 55432–55442.

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365–35381.

Yeow, W. L., Mahmud, R., & Raj, R. G. (2014). An application of case-based reasoning with machine learning for forensic autopsy. *Expert Systems with Applications*, *41*(7), 3497–3505.

How to cite this article: Jarrett A, Choo K-KR. The impact of automation and artificial intelligence on digital forensics. *WIREs Forensic Sci*. 2021;3:e1418. https://doi.org/10.1002/wfs2.1418

25739468, 2021, 6, Downloaded from https://wires.onlinelibrary.wiley.com/doi/10.1002/wfs2.1418 by Iscte, Wiley Online Library on [25/12/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License