forensic sciences

Article

A Conceptual Framework to Improve Cyber Forensic Administration in Industry 5.0: Qualitative Study Approach

Amr Adel

Auckland University of Technology, Auckland 1010, New Zealand; amr.adel@aut.ac.nz

Abstract: As organizations strive to be compliant in a digitally evolving world, they need to ensure that they are forensically ready. Digital forensic readiness ensures compliance in legal, regulatory, functional, and operational structures. A literature review revealed a gap in detailed and comprehensive guidance on how such readiness ought to be accomplished. This is as a result of unfamiliar concepts and terms that revolve around digital forensic readiness. This research paper highlights and elaborates on a framework that can be achieved from research within focus groups. The insights drawn from the focus groups are used to critically assess the issues affecting practitioners in achieving complete digital forensic readiness.

Keywords: digital forensic; expert evaluation; forensic readiness; Industry 5.0; forensic culture; digital evidence; human-centric; forensic policy; qualitative research; resilient

Citation: Adel, A. A Conceptual Framework to Improve Cyber Forensic Administration in Industry 5.0: Qualitative Study Approach. *Forensic Sci.* **2022**, *2*, 111–129. https://doi.org/10.3390/forensicsci2010009

Academic Editor: Ricardo Jorge Dinis-Oliveira

Received: 5 January 2022
Accepted: 28 January 2022
Published: 3 February 2022

1. Introduction

Industry 5.0 was formally established in 2021 by the European Commission [1]. This establishment was made after conducting critical analysis among scientists and industry experts in different branches of research, academia, and technology [2]. Therefore, digital transformation is slowly taking shape in the Industry 5.0 revolution. The concept of Industry 5.0 is driving research and innovation into human-centric, sustainable, and European industry. The core values of Industry 5.0, as shown in Figure 1, can be summarized into three main elements: human-centric, sustainable, and resilience. These three core values have been established to promote the diversity and talents of people, to consider the planet boundaries and environmental space, and to adapt new technologies with flexibilities.

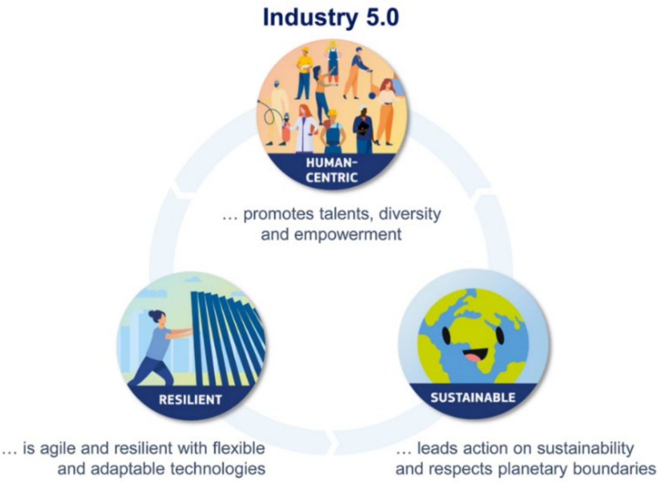

Industry 5.0
HUMAN-CENTRIC
… promotes talents, diversity and empowerment
RESILIENT
… is agile and resilient with flexible and adaptable technologies
SUSTAINABLE
… leads action on sustainability and respects planetary boundaries

Figure 1. Industry 5.0 core values [2].

It is clear that Industry 5.0 is value-driven not a technology-driven, which leads to a number of changes and responses that could affect digital forensic readiness in organizations in the future. As one of the main focuses of Industry 5.0 is human-centric, this means that digital forensic investigations have to be adjusted to comply with the new changes to create effective and inclusive forensic policies, considering this dimension in a way that allows for digital forensic investigators conducting comprehensive analysis and acquiring credible evidence, when needed.

There is an excessive need for organizations to digitize their operations in a bid to become viable in the long run [3]. To help curb the issues emerging from the legal and regulatory compliance of digitization, there is a need to conduct investigations using digital forensics [4]. The diversity in computing platforms and the organizational rate of digitization have been proven to be challenging for collection and investigation using digital forensics [5]. Overcoming the challenges in forensic investigations is required so that organizations can be "digitally forensic ready". This involves the collective capability to process, review, and store digital information [6]. Although organizations are undergoing digital transformations worldwide, studies indicate that close to 98% of Australian-based companies lag in the adoption of digital forensics [7].

Organizations still struggle to become forensically ready because of the inefficiencies in how this can be mutually achieved [8]. A literature review that was conducted indicates that academic and professional forensic readiness is not coherent and does not reflect the existing knowledge on the subject [9]. Informal methods are also used to define and establish existing forensic readiness capabilities. These informal methods have been conducted in several ways, such as trial runs, evidence gathering anecdotally, and sometimes based on investigator's curiosity. This, therefore, has demotivated organizations into planning to build a capacity for forensic readiness [10].

This research project is based on the following question of analysis: How can individual organizations achieve forensic readiness? The reason this question has been formulated, is that within the organizations in Industry 5.0 with its core values, there will be a wide range of cybercrimes, such as theft and fraud, that require specific forensic guidelines to be in place along with digital evidence, not just information security defenses. One of main process that will be followed is data collection/information gathering, requiring admissible evidence [11]. This would require organizations to review the legality of their monitoring procedures. Answering this question will help in many ways in understanding the different aspects that need to be considered, such as humans who will be involved in forensic investigations and their roles.

This research is based on previous research documented in [4], who elaborate on a digital forensic readiness (DFR) framework encompassing the factors inhibiting organizations from achieving the desired forensic objectives. [4] advanced on the term "digital forensic readiness" and had then been used in the literature analysis for advanced frameworks.

A set of three focus groups are used in this paper to elaborate and test the DFR framework in order to discuss three given case studies in the same field. Expert opinions based on the agreement and disagreement points of the framework are extensively reported. A comprehensive list of the factors affecting the preparation of an organization for digital forensics is the overall objective of this report. This framework can also be used by organizations in the evaluation and advancement of measures to become digitally forensically ready.

This research paper follows the following content structure. The background segment highlights the literature reviews on digital forensics and organizational readiness. It also critically reviews the DFR framework presented by [4]. The next segment describes the research method utilized in this research. Research findings from the various focus groups are also indicated in the next segment. The discussion segment extensively provides an elaborate explanation of each of the focus group findings. It also explains how each insight contributes to the discussion in this research report. Finally, a discussion of the findings concerning the validated model is carried out.

2. Background: Digital Forensic Readiness

Barske, Stander, and Jordaan (2010) advanced on the idea of digital forensic readiness (DFR) with an emphasis on organizations. To optimize the organization's ability to gather reliable digital evidence while minimizing costs, organizations should set up digital forensic frameworks. A further literature review defines forensic readiness as the present conditions an organization has in place to aid in digital forensic processes [12]. In that regard, forensic readiness encompasses all of the processes in the forensics collection chain, instead of focusing only on the collected digital evidence [13].

Previous research on forensic readiness focuses on resources used [14], technology selected and used [15], training [16], legal investigations [17], incident response [18], and policy [19]. However, this research does not extensively discuss digital forensic readiness. They aligned it to their specific field of study. The increased need for regulatory compliance for organizations has forced organizations to become forensic ready. This, therefore, facilitates the need for an all-inclusive forensic readiness perspective [20]. Organizations thus need to produce forensic material in real-time in order for them to be effective enough [21].

For organizations to be completely forensic ready, they must ensure readiness in operational and infrastructural aspects [22,23]. Operational readiness focuses on the individuals involved in forensics, while infrastructural readiness entails the processes of ensuring that organizational data are properly stored [24,25]. The same analogies are also highlighted by Ariffin and Ahmad (2021), who mention that elements of planning, policing, preparation, and control are necessary for the improvement of organizational forensic readiness in the era of Industry 4.0. Therefore, it should be remembered that DFR is a holistic practice and therefore other organizational dimensions should be integrated into every organization's forensic preparation [26].

All of these studies enable organizations to be forensically set. However, their focus on specific study aspects within forensic readiness limits their applicability. Their implementation is thus conflicting and not streamlined.

An initial framework to be used for digital forensic readiness was established in the previous research carried out [4]. Figure 2 shows the framework, which entails the following: (1) a set of forensic considerations that deal with the various fields of forensic preparation, and (2) a set of organizations' forensic readiness capabilities to be achieved. The details in the initial framework are defined from the literature.

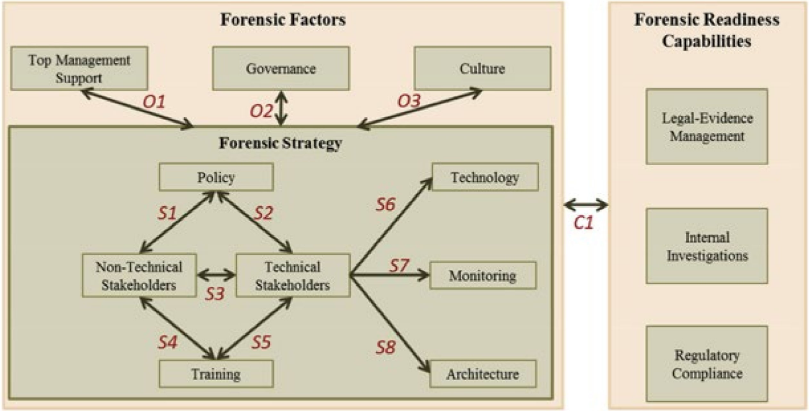


Figure 2. DFR framework [9].

Figure 1 shows the process of the DFR framework designed by Elyas et al. Different factors have been identified to be the key factors. They are top management support, governance, and culture. The forensic strategy was fundamentally defined with different elements and components to be integrated with forensic readiness capabilities. Technical and non-technical stakeholders are an essential part for understanding and analyzing digital evidence.

3. Research Method

The data collection technique used in this research was a focus group. In this data collection technique, a group of people ascertained their perceptions on a topic presented by the researcher for general reactions that could be expected from a larger population [27,28]. Focus groups took advantage of the interactions between the small groups of people to generate ideas [8]. Leonardi et al. (2014) details how researchers have used focus groups in the evaluation of information systems. An advantage of focus groups is the capability to gather additional feedback from respondents from interactions within themselves [29], which results in better quality data being collected. Focus groups provide a hidden perspective as they encourage participants to explore the research topic in their understanding [8]. Kamberelis and Dimitriadis (2014) suggest that holding three or four focus groups ensures complete saturation of points. Moser and Korstjens (2018) also advises that a particular focus group should consist of four to eight participants.

Here, researchers conducted focus groups on three different groups with participants from diverse expertise in digital forensics. These experts have backgrounds either in business, consulting, law, or military professions. A total of 11 experts were selected, with each focus group consisting of about four participants (see selection criteria of experts in Table 1).

Table 1. Selection criteria of experts.

Inclusion Criteria	Exclusion Criteria
Holds a Master's degree or PhD in a forensic field	Holds a bachelor's degree or below
Minimum of 5 years of experience in forensics in complex systems, such as Industry 4.0 and/or Industry 5.0	Experience less than 5 years
Proven track record of research	New to research
Technical evidence of digital forensics tools	At a junior level
Actively engaged in research or industry	Not actively engaged with research or industry
Experience in critical infrastructures (Industry 4.0 and/or Industry 5.0	No experience in critical infrastructures

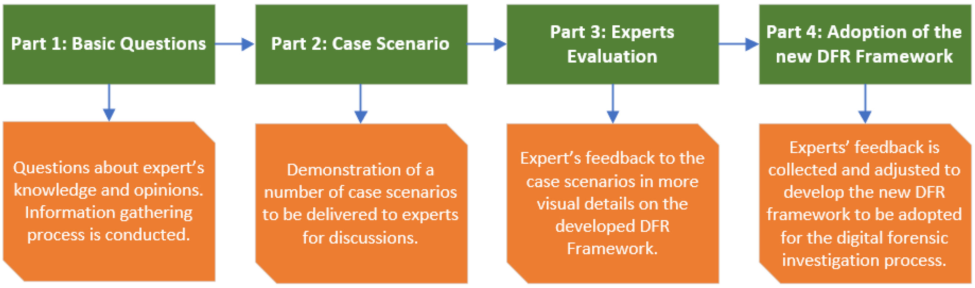
Based on the selection criteria of the experts, the 11 experts were selected based on their experience, and academic and/or industry profiles. Table 2 clearly demonstrates a brief profile of each expert.

To elaborate on the digital forensic preparation process, focus groups were carried out. Participants in the focus groups drove the questions adopted in the study. Appendix A lists different sets of questions that were used. The senior researchers moderated each of the two-hour-long focus group sessions. The phases in each session included identifying the participants' knowledge on forensic readiness, discussing the framework aspects seamlessly based on the case study provided to each group (see Appendix B), and collecting feedback on the framework adopted for forensic readiness (as shown in Figure 3).

According to Leonardi et al. (2014), there are four categories in the analysis of focus groups. This research focused on one of the four: a complete transcript of the recordings from the focus group discussions. Additional ideas were also gathered by observant researchers in each of the other focus groups. The outcomes from each focus group were then discussed and documented. The analysis of the collected data focused on the insights drawn from the focus group participants.

Table 2. Participants Background.

Code	Focus Group	Industry	Staff Size	Role	Forensic Experience
Expert 1	1	Law Enforcement (Army)	39,000+	Digital Forensic Consultant	6+ Years
Expert 2	1	IT Consultancy	3000+	Cyber Forensic Examiner	10+ Years
Expert 3	1	FinTech Industry	300+	Blockchain Legal Consultant	5+ Years
Expert 4	2	Law Enforcement (Police)	16,000+	Digital Forensic Investigator	15+ Years
Expert 5	2	Business	2600+	Digital Forensic Analyst	8+ Year
Expert 6	2	Business	800+	Team Lead	6+ Years
Expert 7	2	Auditing	5000+	Auditing Senior Advisor	6+ Years
Expert 8	2	Agriculture Technology	500+	Senior Consultant	8+ Years
Expert 9	3	IT Consultancy	1000+	Regional Manager	15+ Years
Expert 10	3	Education	4000+	Professor	20+ Years
Expert 11	3	Research	150+	Senior Researcher	9+ Year


Part 1: Basic Questions
Part 2: Case Scenario
Part 3: Experts Evaluation
Part 4: Adoption of the new DFR Framework

Questions about expert's knowledge and opinions. Information gathering process is conducted.

Demonstration of a number of case scenarios to be delivered to experts for discussions.

Expert's feedback to the case scenarios in more visual details on the developed DFR Framework.

Experts' feedback is collected and adjusted to develop the new DFR framework to be adopted for the digital forensic investigation process.

Figure 3. Research Methodology Phases.

Using what Pandey (2019) called content analysis, the collected data were then analyzed. Objectives and factors derived from the focus groups were used to create a categorization matrix. Reviewing the transcripts ensured that all important aspects were recorded. Comments from each stakeholder were reviewed regarding the categorization matrix to determine what each participant thought, as demonstrated in Figure 4. Those free categories that did not align with either of the categorization matrices were examined regarding their contribution to the research questions.

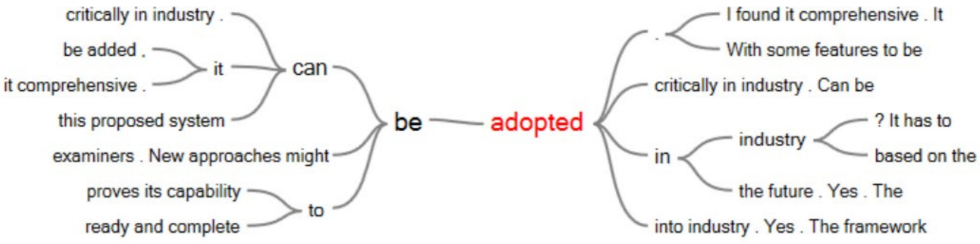


Figure 4. Stemmed word query for the word "adopted".

Based on the analysis of the comprehensive matrix, NVivo software was implemented to evaluate the experts' feedback in order to find the useful relationships and identify the areas of improvements.

A mixture of generalizability, reliability, and significance would guarantee the validity of the focus group [30]. If participants in the focus groups were well selected, their views would serve as a representation of peer opinions in the same field; thus, selecting experts in digital forensics ensured that the research achieved generalizability [31]. Reliability, on the other hand, ensured that the study could be replicated to other focus groups, from design to analysis. The experts in this study had diverse experience in digital forensics and worked across different industries, thus ensuring that the study remained relevant, and the participants could provide realistic points of view [32].

4. Findings

To determine whether the perspectives of the focus group participants aligned with the study area, they were asked to share their views on organizational forensic readiness. The views ranged from concrete evidence selection, storage, planning, and presentation. Other views ranged from the need for organizations to have adequate resources and support from senior management to ensure the effectiveness of a program for forensic preparation.

Expert 1 based their argument on how organizations ought to prepare their systems to ensure the preservation and timely retrieval of relevant information for forensic investigations. Expert 2 claimed that digital forensic information should not be tampered with, and thus maintain the confidentiality rule. Expert 6 suggested that digital forensic readiness revolves around making sure that all tools, processes, and people are aligned to the ultimate goal, regardless of their role in the organization. They further stated that identifying the data points of the information collected, where it is preserved, and who has access control ensures that the organization is forensically ready. Expert 9 mentioned that organization management must identify the need to be forensic ready and support the implementation process.

4.1. Forensic Readiness Process

The experts expressed their views on what being forensic ready means to an organization and its probable use. These views were aligned with the beliefs on how organizations use their forensic ready capabilities. Forensic readiness capabilities are better termed as objectives, as organizations have better and more capabilities that can be achieved, besides what Elyas et al. (2014) stated on legal evidence management, regulatory compliance, and internal investigation capabilities. Expert 5 mentioned that these diverse objectives help the organization to assess and react adequately to the underlying cause of an incident. It also guarantees that organizations act on whoever is accountable and responsible for the incident. Impact on the DFR Framework: objectives in forensic readiness will include the capabilities of forensic readiness.

4.1.1. Legal Evidence Administration

In the focus groups, a common theme is that forensic evidence needs to be documented with detailed evidence. This will ensure that the evidence can, later on, be used for a variety of investigations. However, some participants claimed that the non-essential evidence did not need to be backed by proof, as it may not even be viable in a court of law. Expert 1 said that an organization's objective is crucial for determining the level of evidence to be collected, whereas Expert 10 claimed that in a court of law, all evidence should be relevant to the case.

Forensic readiness can also be used in the case of automatic detection. Automatic detection involves the use of electronic data as proof in a law court. Expert 4 claimed that being forensically ready is ensuring that all paperwork is electronic and can be produced upon request. Impact on DFR Framework: the management of legal evidence should incorporate e-discovery to ensure that the organization is forensically ready, even in legal aspects.

4.1.2. Supervisory Control

A forensic preparation capability needs to be developed if companies aim to achieve enforcement in the industry. Expert 6 stated that to escape the financial consequences of non-compliance, this needs to be done. Expert 9 gave several examples of how compliance regulations in the US and UK cost organizations millions of dollars if not adhered to. According to Expert 4, some organization reports eliminate the word "investigations" to avoid the wrath of non-compliance. Impact on DFR Framework: regulatory compliance is perceived as an important goal in the DFR model. The DFR model is designed to support different compliance regulations, for instance, General Data Protection Regulation (GDPR), as the model processes the personal information of individuals in the EU zone.

4.1.3. Internal Audit

Internal audits, especially those related to security, should be done to ensure that the organization is forensically ready. Expert 5 suggested that this can range from hiring people to hack into the organization's system, to determining when a hack is happening and taking preventive measures in advance. Expert 3 stated that these internal audits and forensic investigations can be used to determine where errors in a system occurred, and have nothing to do with crime or fraudulent activities. Impact on DFR Framework: forensic response covers investigations that aim to determine what happened and to complete internal audits.

4.1.4. Business Goals

Some supplementary business goals include support for information management strategies, personnel accountability, credibility, and recovery of missing resources. Expert 5 noted that forensic readiness helps the organization to maintain its reputation in the event of an incident occurrence. However, Expert 9 claimed that organizations can adopt the forensic capabilities for retribution reasons, aside from those from the initially intended capability. Expert 6 highlighted that these can be inclusive of accessing systems to mine customer data. Overall, the participants agreed that being forensic ready ensures that an organization can recover lost assets and avoid financial losses. Impact on DFR Framework: business objectives are an important aspect of being forensically ready and are thus included in the DFR framework.

4.2. Organizational Dynamics

Good remarks were made by the focus group participants on the forensic preparation of the DFR framework. However, criticism was focused on training, policy, and stakeholders. The participants agreed that the items on the left side of the framework are the capabilities of the forensic system and should not be confused with forensic factors. This is because forensic readiness capability describes the components in the DFR model. Impact on DFR Framework: the forensic readiness capability segment encompasses all forensic factors.

4.2.1. Forensic Top Management Level

The participants accepted that support from top management is crucial for ensuring the success of any forensic readiness initiative. Expert 1 stated that any initiative backed by top management has a higher likelihood of success. Expert 4 added that continuous funding and staff allocation would prove to be a difficult task without initial management support. Expert 2 suggested that the plan can only be accepted by management if there is a risk of being held accountable if an event happens and the company does not act accordingly. Expert 7 and Expert 8 stated that if management does not set the tone, then resources will be redirected elsewhere. According to Expert 9, these organizational factors are intertwined. Generally, top management supports forensic readiness success. Impact on DFR Framework: as a result, senior management support is also part of the organizational factors.

4.2.2. Forensic Control

Good forensic governance is characterized by the capacity of an organization to be forensically ready and the forensic program's effectiveness. Expert 3 stated that efficiency is measured from the technology, system, and architecture implemented. As per Expert 9, accountability in the compliance regulations determines good governance and therefore penalties should exist in the non-compliant forensic readiness model. This ensures the right governance within the organizational processes. Impact on DFR Framework: inside situational members, governance is encompassed.

4.2.3. Forensic Culture

There is a need to instill a forensic culture into any organization. This culture should be driven by top management. Expert 9 stated that this culture is defined by top management. Expert 7 added that they inspire the changes to the forensic culture. Expert 2 advised on the need to educate staff about forensics, right from the start. However, it was noted that most forensic readiness culture is instilled when organizations become victims of major incidents. Expert 4 claimed that there is a need for digital forensics to become mature, so that organizations can globally accept and integrate the idea into their organization. Expert 6 noted that being aware of the functional aspects of a system makes employees more aware and can result in behavioral change. Impact on DFR Framework: organizational culture is also embodied in organizational variables.

4.3. Forensic Strategic Plan

Participants in the focus group agreed that a forensics strategy is important for forensic readiness and should therefore be designed as per the organization's objectives. Strategy issues such as risk management, planning, and resourcing are key to a successful forensic readiness as per Expert 6. Expert 9 emphasized that a forensic strategy should be focused on the objectives intended to be achieved. Expert 10 added that this can range from compliance, prosecution, to legal requirement to contract requirements. Impact on DFR Framework: as a forensic readiness factor, a forensic strategy defines the organization's scope and purpose in forensic preparedness.

4.3.1. Experts

The experts consisted of technical and non-technical stakeholders in the forensic preparation system. The focus group participants concluded that stakeholders in the DFR framework have dynamic roles and can therefore change, as per the forensic framework's lifecycle. For instance, law enforcement is a forensic stakeholder during an incident, and they are non-forensic stakeholders afterwards. Therefore, all other stakeholders are considered non-forensic stakeholders until when they are needed for a forensic investigation. Forensic stakeholders are thus not permanent positions. Expert 9 described a forensic stakeholder as a person who is involved in a system's forensic functionality. The participants agreed that stakeholders such as law enforcement, security experts, and forensic experts are thus categorized as forensic stakeholders based on their role in the forensic investigation. Impact on DFR Framework: forensic and non-forensic stakeholders, who can either be internal or external to the organization, encompass technical and non-technical stakeholders.

4.3.2. Forensic Infrastructure

A driving force towards forensic potential is some of the essential forensic infrastructural factors, such as surveillance, design, and technology. Expert 6 noted that without the correct architecture, technology cannot be successful. Expert 7 added that the available technology defines the architecture's functionality. The design of the architecture given the technology revolves around this implied relationship. Impact on DFR Framework: forensics infrastructure houses the architecture and technology that provides a complete relationship between the factors.

4.3.3. Monitoring

System monitoring should be accurately managed to ensure that incidents are detected promptly. In this regard, monitoring was viewed by most participants as a security feature. Expert 8 was reluctant to recognize tracking as a forensic role, but agreed on its significance for forensic readiness. Expert 4 also agreed that monitoring comes with security software, which is essential for identifying anomalies that would result in forensic audits.

As a result, monitoring is not considered a major factor in the forensics framework. Tools for monitoring are part of forensic technology and are intended to detect irregularities and protect the integrity of the system. Therefore, systems that need to be monitored ought to be planned, documented, and adequately prepared for. Forensic stakeholders include system managers and security officers who control the system. Organizational factors also do influence monitoring. Impact on DFR Framework: the DFR framework no longer contains monitoring.

4.3.4. System Architecture

The extent to which the forensic process is complemented by the design and configuration of IT systems was also denoted as a very important factor by most participants. Expert 3 highlighted the need to ensure continuous recording of information using IT systems and using them to ensure data integrity. Expert7 further suggested that forensic systems should be aligned with the existing systems in an organization. Expert 6 added that technology would not be implemented without the right architecture in place and that architectural changes result in technological changes to a forensically designed system—systems that log and capture occurrences at particular events in occurrence. Expert 1 stated that these forensic systems might require additional reconfiguring and adjustments that aim to solve specific user needs. Internet cookies that are created by the browser to speed up access to recently explored websites are an example of this. Such artifacts are a mining ground for forensic investigations. Impact on DFR Framework: system architecture is, therefore, part of the forensic infrastructure.

4.3.5. Technology

The innovations implemented by the organization are represented by this factor. The group participants were not concerned with the functionalities of each technology, aside from the fact that they should have logging features. They should also integrate the features that ensure that the technology architecture should make it easier for forensic activities to be conducted. Various views have been expressed based on ensuring that the presence of forensic technologies streamlines forensic activities. Expert 1 claimed that a forensic toolkit should be utilized by every organization. Expert 2 claimed that the technologies used for forensic investigations should be verified through industry certifications and expert testimony. Expert 5 noted that forensic technologies are sophisticated and require adequate practice and experience. Expert 7 insisted on the need to keep the technology updated with the latest security and software patches. Expert 11 noted that the cost of implementing these technologies is high and thus there is the need to have well-trained personnel and processes set out. Impact on DFR Framework: the forensic infrastructure also includes technology.

4.3.6. Forensic Policy

Rules should exist that govern people, processes, and technology in organizations that intend to become forensic ready. Such policies should be endorsed by top leadership, created by stakeholders, and implemented to fit the structure of the company. A clear forensics policy is essential in forensic readiness capability. Expert 3 indicated that a clear forensic policy helps an organization to achieve a forensic strategy. Expert 8 emphasized that forensic policy includes areas of forensics in the infrastructure and the system. The other respondents agreed with their comments. Expert 5 stated that the policy's function was to assess the regulations on how organizations ought to do things. It provides guidance, preset rules to be followed regarding what is appropriate in terms of the forensic policy.

Expert 9 emphasized that as an independent document, a forensic policy should be recorded or incorporated into other organizational policies. Expert 3 stated that this policy is integral in whatever is intended to be achieved. The participants thus agreed that all employees should be made conversant with the policy compliance requirements and the repercussions of non-compliance. Expert 10 added that this would greatly reduce the "blame game" when an employee was found in violation of the policies in place. Impact on DFR Framework: the policy indicated on the DFR framework is now known as a forensic policy.

4.3.7. Forensic Training

Forensic training is essential and should be done for both forensic and non-forensic stakeholders. Forensic stakeholder training encompasses how to use forensic equipment to perform forensic investigations. This includes providing the appropriate tools and techniques to be utilized in forensic investigations. Educating non-forensic stakeholders covers how to respond professionally to incidents and the elements of forensic policy. This requires knowledge and awareness of the proper application of forensic protocols and procedures.

Additional training can be conducted on a case-by-case basis, as indicated by Expert 2. Expert 4 indicated the need for technical training for the forensic team and data preservation training to the general staff. Each of these training sessions ought to address the specific requirements of each stakeholder. The lack of appropriate training for stakeholders implies that the organization is not forensically ready. Non-forensic stakeholders ought to know the processes involved after an incident has been reported and thus execute them appropriately. Expert 3 added on the value created to these staff when they recognize the need to be forensically ready. They further added that by knowing that the process proves innocence through evidence, there is an increased likelihood to appreciate and support forensic readiness. Impact on DFR Framework: the different types of training conducted are now known as forensic training and are encapsulated in the forensic training factor.

4.4. Relationships between Factors

Participants were instructed to identify and give their views on the interactions between the various forensic preparation factors. The participants drew relationships between the identical lists of DFR factors and added comments. It was identified that the relationships were similar to those initially identified [4] (see Figure 1). A strong relationship involving forensic technology and forensic architecture was established. These two categories were therefore grouped and labeled as "forensic infrastructure". A similar connection was also identified in senior management support, organizational culture, and forensic governance categories. These were therefore grouped, as shown in Figure 5, into "organizational factors". Finally, the participants unanimously recommended the implementation of the proposed relationships—the DFR model from the analysis of the focus group.

4.4.1. R1 (C1)—Digital Forensic Operation—Data Acquisition and Investigation and Forensic Readiness Process

Participants accepted generally that the partnership, R1, exists and is bi-directional between forensic readiness priorities and forensic readiness capability. There was a suggestion by Elyas et al. (2014) that what the initial DFR framework that inquiries would be handled differently because the variables were distinct from legal-evidence management and internal investigations. It was noted that investigations should be done as though the proof will be required in a court of law. A Focus Group 1 participant mentioned that the relationships between the entities need to reflect the objectives of the entity before the strategy to be implemented is identified.

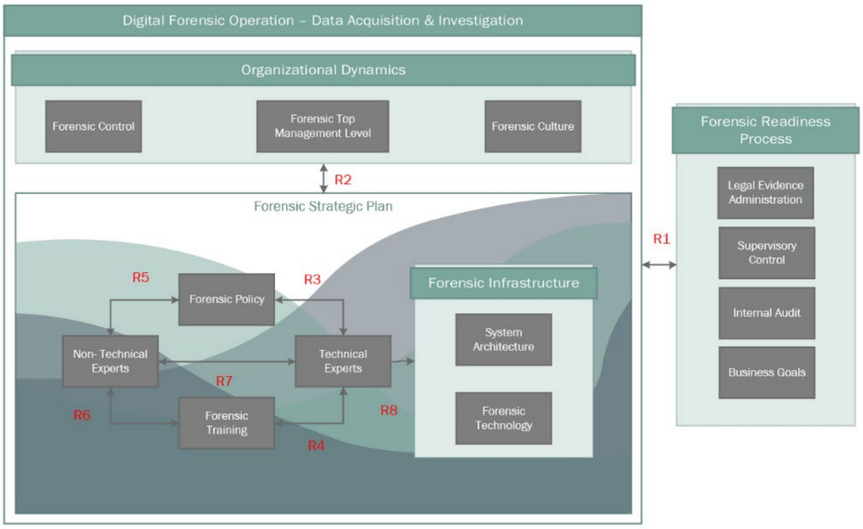


Figure 5. New DFR framework structure.

4.4.2. R2 (O1, O2, and O3)—Organizational Dynamics and Forensic Strategic Plan

The forensic approach and its components are related to all three organizational factors. Top management is a crucial part of fostering policy by providing stakeholders with resources and more support. Expert 4 asserted that the success of a forensic strategy is determined by the level of support from top management. The stakeholders should also have a sense of ownership of forensics. Expert 6 seconded this by stating that management ought to ensure robust energy and allocate the right number of resources. Expert 8 claimed that governance is crucial to ensuring that the strategy is accomplished, whereas Expert 6 suggested that what is more important is the organizational culture.

Organizational factors and forensic strategy components are also intertwined. Expert 7 stated that the success of forensic training is also determined by senior management's buy-in. It is important to identify the right procedures and tools for training, as this helps build a better governance perspective. Governance also directs the implementation of forensic policies. Expert 6 stated that a transparent system has a robust governance system. A philosophical change in the organization's culture must align with what the forensic strategy aims to achieve. The top leadership must support this cultural shift to all stakeholders.

4.4.3. R3 (S2)—Forensic Experts and Forensic Policy

R3 indicates a relationship evident in writing the forensic policy. Expert 6 agreed that the workable policy should be fulfilled by stakeholders. Expert 7 pointed to the value of involving stakeholders as a shared advantage to policymakers in the process of forensic policy development.

4.4.4. R4 (S5)—Forensic Experts and Forensic Training

In the process of training non-forensic stakeholders, forensic stakeholders may become involved. They may also include other members of the forensic team. Expert 7 indicated that preparation should be focused on the organization's role of each stakeholder. Forensic stakeholders need to continuously familiarize themselves with new forensic software tools and techniques in the industry. Expert 4 suggested that this training be conducted by external trainers to the organization. Expert 7 reiterated the need to learn new training techniques and policies, and to obtain feedback on what is being achieved in the industry.

4.4.5. R5 (S1)—Non-Forensic Experts and Forensic Policy

R5 denotes the need for non-forensic stakeholders to be part of the documentation of the forensic policy. The participants in the focus group agreed that the participation of these non-forensic stakeholders in the formulation of a policy is significant. These stakeholders should also define and comply with a workable policy. Participating in this policy creation document ensures that the non-technical people know what to do in case an incident occurs.

4.4.6. R6 (S4)—Non-Forensic Experts and Forensic Training

The relationship, R6, is bidirectional. Non-forensic stakeholders can be educated on forensic matters such as data storage policy and capability, while in return they provide insights on the effectiveness of the training and probable areas of improvement. Forensic training, despite its difference across forensic and non-forensic stakeholders, is important. Expert 4 stated the need for these forensic and non-forensic stakeholders to attend training set aside. The non-forensic stakeholder and forensic training partnership, R6, is bidirectional. On forensic issues such as data storage policy and capabilities, these non-forensic stakeholders should be trained.

4.4.7. R7 (S3)—Non-Forensic Experts and Forensic Experts

There is regular two-way coordination between forensic and non-forensic stakeholders. In the development and implementation of forensic policy and training, and after an incident has occurred, this contact is important. Expert 7 stated that this communication is essential for identifying the root cause of an incident after the occurrence, as well as identifying how to amicably address the issue. Table 3 shows all the changes of the framework updated with the latest modifications.

Table 3. Framework changes.

Initial	Change
Regulatory Compliance	Now a high priority
Forensic Readiness Capabilities	Now Forensic Readiness Process
Organizational Factors	Now includes Forensic Control, Forensic Top Management Level, and Forensic Culture
Internal Investigations	Internal Audit
Forensic Infrastructure	Monitoring is removed.
Technical Stakeholders	Renamed Technical Experts
Legal-Evidence Management	Added Automatic Detection
Non-Technical Stakeholders	Renamed Non-Technical Experts.
Forensic Strategy	Forensic Strategic Plan.
Monitoring	Removed From the Digital Forensic Operation—Data Acquisition & Investigation.
Non-Technical Stakeholders	Renamed Non-Technical Experts.
Technical Stakeholders	Renamed Technical Experts
Forensic Infrastructure	Monitoring is removed.
Training	Forensic Training is the New Name.
Culture	Now Forensic Culture.
Forensic Factors	Now Digital Forensic Operation—Data Acquisition & Investigation
Technology	Included in Forensic Infrastructure.

4.4.8. R8 (S6, S7, and S8)—Forensic Experts and Forensic Infrastructure

A one-way partnership is reflected by the engagement of forensic stakeholders in the creation and use of an organizational forensic framework. The technical stakeholders are responsible for shaping the forensic infrastructure and ought to be aware of what needs to be done to respond to a reported incident. Expert 7 and Expert 10 agreed that the involvement of these stakeholders is important in forensic infrastructure testing and maintenance. Expert 4 believed that forensic stakeholders are the key to ensuring a well-implemented forensic infrastructure and policy. They also believed that these factors are interchangeably influential for well-structured forensic readiness. Expert 5 indicated that forensic policy could influence the impact on a forensic system's infrastructure. Standards should therefore be developed to ensure that privacy is upheld in the technology used in creating the forensic infrastructure.

4.5. Summary

This report utilized a DFR framework illustrated by Elyas et al. (2014). This framework has been modified regarding the insights drawn from the focus group discussions. The framework structure has been refined to reflect the illustration in Figure 5.

The revised structure incorporates governance, support from top management, and culture into the organizational variables into organizational factors. Therefore, the link between these variables is integral for the operation of the entity. Similarly, technology and architecture have been merged into forensic infrastructure, as they are interrelated. The intrinsic nature of the framework inhibits the display of this relationship.

5. Discussion: Expert Perspectives

A forensic strategy is a proposal from the discussions that closely relates to the forensic goals of the organization and incorporates all considerations, except those deemed to be external to the DFR system and internal to the organization. Top management support, governance, and corporate culture are included here.

The discussions also focused on to what extent the organizational culture relates to the DFR framework. A key question was based on the awareness and post-incident experiences, as discussed. Some focus group participants believed that organizational culture would be more prone to improvements in DFR. Forensic readiness could also ensure that an organization uses forensic investigations to conduct internal audits in the organization.

The participants were divided around how the various stakeholders in the DFR should be represented. It was eventually decided that forensic and non-forensic stakeholders, based on their involvement in the investigation, would better represent dynamic positions. These different stakeholders also ought to be trained differently regarding their roles in the organization and forensic investigations. They both participate in the development of the forensic policy and give continual feedback on the improvement of the forensic process. Stakeholders external to the organization are expected to adhere to the set guidelines when they become part of DFR.

Incident detection was viewed as a security feature instead of a forensic one regarding the technology and architecture used in forensic readiness. The systems should be designed and configured to capture evidence of a particular kind, as per the business objectives.

During the discussion of the factors to consider in forensic readiness, participants had diverse views. The development of better information systems to preserve and retrieve evidence with ease was perceived to integrate the cloud computing technologies. The need for forensic readiness is also determined by the organization's size. SMEs require little stakeholders for the implementation of such a system, whereas big organizations require cross-functional involvement of different stakeholders. Forensic readiness has been identified as an important capability for organizations. The focus group participants assumed that only two goals were the most relevant of the four forensic readiness goals: (1) organizations should adhere to set regulations, and (2) there is a dire need to manage evidence in case of legal issues. The role of forensic readiness should shift from being capable of conducting internal investigations to providing a detailed forensic response to incidents.

Organizations become more security-aware if a forensic readiness plan has been implemented [33]. The digital forensic readiness supports the security software for information by strengthening the security posture and deterring possible attackers. The reports generated from an infestation can be utilized for reviewing and assessing the current security loopholes. This can, in turn, be used to modify the security strategy and policy [18]. The focus group participants backed this by stating that some vulnerabilities might only be seen when an investigation has been conducted. Forensic readiness ensures that the organization demonstrates its capability to protect information assets, as well as ensure that security incidents are reported and investigated.

The objectives of a forensic readiness structure are divided among the need to collect evidence and the level of evidence to collect. The cost of conducting forensic investigations is quite high. However, the higher cost of financial implications as a result of non-compliance ensures that organizations take the high-end road and conduct in-depth investigations. Most organizations are not forensic ready and thus only act upon the need to be forensic ready once an incident occurs.

6. Using Focus Groups in This Study

The digital forensics field is broadly practice driven. A review of the different articles published on forensic readiness generally concludes that propositions are based on conceptual development and lack of validation. Some researchers have made pleas on the need to conduct in-depth investigations in digital forensics [34]. These conceptual studies are not backed by any logical data, and thus the experience of the researcher is focused on [35]. Testing guarantees that a model is accurate enough for the intended intent [36]. Our review concludes that the researchers have little or no validation of the best forensic readiness criteria to follow.

Okoli (2015) presented a systematic system literature review, which was adopted in this study. A knowledge synthesis approach of the Grounded Theory described by Corbin and Strauss (2011) was also used for a better forensic readiness holistic understanding [37]. This then accelerated the development of a new framework. The new framework was validated by three different independent focus groups consisting of computer forensic experts. Focus groups ensure that diverse and detailed information is gathered in a short period based on reflections of other participants [38]. The participants' work experience spanned across different industries in several organizations. Adopting these focus groups ensures that researchers get better insights from individuals who are representative of their peers. A larger number of focus groups should be used to acquire better-detailed information from the participants. The idea of digital forensic readiness (DFR) with an emphasis on organizations has been discussed through context [39]. Content analysis, and data gathered for to be analyzed qualitatively [40,41]. Focus groups on studies have been conducted along with systematic literature review have proved its credibility to provide more insights to further research [42,43].

7. Conclusions and Future Research Challenges

This study provides a better new model that can be utilized by organizations to determine and set up their forensic readiness protocols. This includes the need for organizations to determine their forensic strategy and objectives. This forensic readiness can be achieved by identifying the factors and relationships that can be used collectively. For example, the framework suggests the following to be achieved: senior management commitment, training, and staff awareness, organizational commitment towards forensics, a forensically inclined organizational culture, enforcement of appropriate forensic policies, and continuous analysis and improvement of system activities.

Organizations that do not have existing forensic structures can also utilize this framework to set up a forensic readiness capability. DFR factors enable organizations to identify the critical aspects that need to be considered. Finally, the connections in the model explain how the factors found contribute to achieving the forensic preparation desired. This framework can also be transformed and utilized on an industrial massive scale to ensure industrial forensic readiness.

This framework also highlights the benefits that organizations can acquire when they become forensic ready. Organizations can then become compliant with set regulations, appropriately handle collected digital evidence, and forensically respond to incidents that occur. The identification of the intended objectives makes the organization's decision-makers more decisive on the benefits to be reaped from forensic readiness. The implementation of the framework for organizational readiness will ensure that diverse organizational structures can quickly integrate forensic readiness. This flexibility in the framework ensures that forensic readiness can be established even in different organizational sizes.

Discussions from the experts in the focus groups implied that forensic readiness can greatly benefit IT security structures. Organizations can therefore use this framework to improve their overall IT security strategies. This is because the internal investigations can elicit vulnerabilities in the system that would otherwise prove fatal if identified by malicious personnel. The identification of these vulnerabilities enables the organization to strengthen its defenses. Organizations that have a security focus in mind should consider investing in forensic readiness.

The stakeholders in a forensic program each play diverse, but very important roles. Training, legislation, and core facets of forensic implementation are accountable to forensic stakeholders. In comparison, non-forensic stakeholders are essential in creating forensic awareness across the organization so that employees align with the forensic process. These stakeholders also give feedback to improve the forensic processes. All staff in the organization ought to be part of the forensic awareness training and adhere to the set forensic policies.

The experts selected to be part of the focus groups have greatly contributed to the success of the proposed framework. An increased number of participants will be used in the future to critically analyze the findings in this framework. The study will focus on the objectives, the factors, and the relationships in the DFR model. The future study will be a Delphi study and will focus on the framework's components with the definitions and descriptions of each.

Funding: This research received no external funding.

Institutional Review Board Statement: No ethical approval required for this study.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data available within the article.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A. Questions Utilized in Focus Groups

Appendix A.1. Protocol for Focus Group 1

Part 1. Basic Questions:

- Define digital forensic readiness?
- By being forensically prepared, what goals can a company accomplish?
- How to become forensically ready from an organizational perspective?
- Where to start?
- Describe a "good" forensic system?
- Can security be linked with forensic readiness?
- How does learning happen?

Part 2. Case Scenario: A case scenario was presented to participants and discussions were based on:

- What are the considerations in a forensics readiness process?
- Who can participate in the program?
- What technologies to be used?
- Would surveillance help in the program?

- What kind of practices does an organization need to consider maximizing its preparation for forensics? Will the readiness of forensics impact device setups?
- Is there a need for a forensics policy?
- Would training in forensics be required?
- What are the best practices in forensics?
- What is the senior management role?
- What is the relationship between governance and forensic readiness?

Part 3. Visual representation. The participants are presented with the forensic preparation diagram. The following questions were then asked:

- Any additional objectives?
- Any additional factors?
- Comment on the relationships shown between the forensic strategy components
- What is the influence of forensic readiness objectives on strategy?

Appendix A.2. Protocol for Focus Group 2

Part One: Generic Questions. Generic questions regarding priorities and factors of forensic preparation, to capture the participants' impartial opinion. They were asked the following questions:

- What is DFR in an organization?
- What are the advantages of being forensically ready?

Part Two: Participant Opinion. For Sections 2–5 of the focus group, form-based questions were issued to respondents. Participants were presented with the three objectives of forensic preparation and ten variables. Respondents justified their reasons in selecting either true or false:

- Forensic Readiness Objectives.
- It is believed that adopting forensic readiness improves objectives.
- Giving your reasoning, indicate agree or disagree on the objectives.
- Add extra objectives not included in the handout.
- Forensic Readiness Factors.
- These factors contribute to forensic readiness.
- Agree or disagree on the factors with reasons.

Part Three: Factor fill-ins. DFR considerations and goals lists were presented. Participants were asked to integrate the variables/objectives that they think are lacking. These were then debated among all the respondents.

Part Four: Expert views on relationships. The participants were presented with two similar lists of the ten considerations. They were asked to add to the blank spaces of the list any considerations that they suggested in the last section. In the two lists, the participants were then asked to draw the top eight correlations between the variables. The goal was to find out, from the point of view of an expert, the most critical relationships within the model.

Part Five: Proposed model relationships. The suggested forensic readiness model (with relationships) was finally introduced. In the given questionnaire form, the suggested relationships were defined. The participants were asked whether the proposed relationships and their explanations agreed or disagreed with them, and to provide other links.

Appendix A.3. Protocol for Focus Group 3

Part 1: Generic Questions. Generic questions are asked:

- What is organizational DFR?
- What gain is there for the forensically equipped?
- How to become ready forensically?

Part 2: Forensic readiness objectives. Questions based on type were circulated to the participants. The suggested goals for forensic preparation are illustrated in the form.

Respondents were asked to indicate whether they agreed or disagreed, and to provide justifications. If they though some were lacking, the participants were also given room to add more targets. Participants began discussing the goals among each other.

Part 3: Forensic readiness factors. Questions based on type were circulated to the participants. The factors suggested were listed. Justifications for responses should were indicated. Participants were also given room to add more variables if they thought they were missing some. Participants then analyzed the variables among each other.

Part 4: The forensic readiness framework (Relationship). Participants are presented with the proposed framework. In the given form, the suggested relationships are defined. Participants are asked whether the proposed relationships and their explanations support and justify their answers. They then share their responses.

Part 5: Concluding questions. The following questions conclude the session:

- Any relationships that are not indicated?
- Does the framework accurately represent forensic capability?
- How can the framework be utilized?

Appendix B. Case Studies Provided to the Focus Groups Relevant Industry 5.0 Challenges, where Human Is One of Main Focuses in the Study

Appendix B.1. Case Study 1: Focus Group 1

Introduction: Apache Hadoop HDFS is one of highly implemented distributed computer architectures for dealing with big data in terms of storage and management. Hadoop has been implemented in critical structures thanks to its capability of handling large amounts of data in a short period of time. The efficiency of the proposed system has been positively investigated using a customized and complex scenario for the protection of critical infrastructures. Therefore, Hadoop HDFS platform implementation was chosen to propose and test live forensics in order to facilitate the process of data acquisition in the digital investigation. Simulating a data break attack on a Hadoop cluster was the aim of this case study in order to provide a suitable framework for live forensic examination process for protecting critical data against cyber-attack.

Challenge: A full audit was established to maintain and verify the confidentiality and stability of sensitive information in the Big Data room of a critical infrastructure against suspicious activities and cyber-attacks. The testing laboratory at Amazon Web Services showed the sample configurations and specifications. According to the design, three interconnected nodes were installed. These nodes are the primary node, secondary node, and data node. Physical configurations varied from one node to another, based on the work nature of each node. Furthermore, the design showed other devices were connected to the target network. Case 1 involves part of Hadoop HDFS as it is the main server for the Big Data Room.

Appendix B.2. Case Study 2: Focus Group 2

Introduction: The complexity of systems is evolving rapidly. This leads to more vulnerabilities in critical sectors. These vulnerabilities can be exploited by hackers to get unauthorized access. Penetration testing can work effectively in such situations to identify hole-loops in those critical systems to protect critical infrastructures. In some situations, protection of critical systems requires being one step ahead to get all vulnerabilities identified before a hacker does. Penetration testing can be very useful in a post-attack stage, as it can conduct live data acquisision processes to get valuable information about particular systems within the critical infrastructures.

Challenge: A full remote and physical investigation is confirmed to reveal and analyze potential information on the engineering workstations against suspicious activities such as data theft. Sec-1 has detected suspicious activities from an employee who is working in the engineering workstations that host the supervisory control and data acquisition (SCADA) system and control all incoming and outgoing data to the control room. The computer workstation is being suspected of compromise but there is no exact evidence. Digital investigation is required.

Appendix B.3. Case Study 3: Focus Group 3

Introduction: Enhancements in technologies and shifting trends in customer behavior have resulted in an increase in the variety, volume, veracity, and velocity of available data for conducting digital forensic analysis. In order to conduct intelligent forensic investigation, open-source information, and entity identification must be collected. Consistency assists in adding value to data subsets. Testing these types of data will result in locating additional information relevant the existing entities in the data subsets, which will lead to required evidence in the real-world forensic analysis.

Challenge: Organized crimes are now involved in drug trafficking, murder, fraud, human trafficking, and high-tech crimes. Criminal intelligence using Open-Source Intelligence Forensic (OSINT Forensic) is established to perform data mining and link analysis to trace terrorist activities in critical infrastructure by revealing and analyzing the email addresses and IP addresses, which could lead to useful information. FireEye has found some suspicious activities on a device owned by an employee working there, namely, to switch all inbound and outbound information. The device is to be investigated for evidence.

References

1. Xu, X.; Lu, Y.; Vogel-Heuser, B.; Wang, L. Industry 4.0 and Industry 5.0—Inception, conception and perception. *J. Manuf. Syst.* **2021**, *61*, 530–535. [CrossRef]
2. Breque, M.; De Nul, L.; Petridis, A. *Industry 5.0: Towards a Sustainable, Human-Centric and Resilient European Industry*; European Commission, Directorate-General for Research and Innovation: Luxembourg, 2021.
3. Mihardjo, L.; Sasmoko, S.; Alamsjah, F.; Elidjen, E. Digital leadership role in developing business model innovation and customer experience orientation in industry 4.0. *Manag. Sci. Lett.* **2019**, *9*, 1749–1762. [CrossRef]
4. Elyas, M.; Maynard, S.B.; Ahmad, A.; Lonie, A. Towards a systemic framework for digital forensic readiness. *J. Comput. Inform. Syst.* **2014**, *54*, 97–105. [CrossRef]
5. Ruan, K.; Carthy, J.; Kechadi, T.; Crosbie, M. Cloud forensics. In Proceedings of the IFIP International Conference on Digital Forensics, Orlando, FL, USA, 31 January–2 February 2011; pp. 35–46.
6. Pangalos, G.; Ilioudis, C.; Pagkalos, I. The importance of corporate forensic readiness in the information security framework. In Proceedings of the 2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, Larissa, Greece, 28–30 June 2010; pp. 12–16.
7. Richards, K.; Davis, B. Computer security incidents against Australian businesses: Predictors of victimisation. *Trends Issues Crime Crim. Justice* **2010**, *399*, 1.
8. Mouhtaropoulos, A.; Li, C.T.; Grobler, M. Digital forensic readiness: Are we there yet. *J. Int. Commer. Law Technol.* **2014**, *9*, 173.
9. Raghavan, S. Digital forensic research: Current state of the art. *CSI Trans. ICT* **2013**, *1*, 91–114. [CrossRef]
10. Trenwith, P.M.; Venter, H.S. Digital forensic readiness in the cloud. In Proceedings of the 2013 Information Security for South Africa, Johannesburg, South Africa, 14–16 August 2013; pp. 1–5.
11. Chander, B.; Pal, S.; De, D.; Buyya, R. Artificial intelligence-based internet of things for industry 5.0. In *Artificial Intelligence-Based Internet of Things Systems*; Springer: Cham, Switzerland, 2022; pp. 3–45.
12. Valjarevic, A.; Venter, H.S. Towards a digital forensic readiness framework for public key infrastructure systems. In Proceedings of the 2011 Information Security for South Africa, Johannesburg, South Africa, 15–17 August 2011; pp. 1–10.
13. Oh, J.; Lee, S.; Lee, S. Advanced evidence collection and analysis of web browser activity. *Digit. Investig.* **2011**, *8*, S62–S70. [CrossRef]
14. Kristyan, S.A. Forensics Readiness survey in cloud computing with a meta-analysis approach. In Proceedings of the 2018 International Conference on Information Technology Systems and Innovation (ICITSI), Padang, Indonesia, 22–26 October 2018; pp. 574–581.
15. Agarwal, A.; Gupta, M.; Gupta, S.; Gupta, S.C. Systematic digital forensic investigation model. *Int. J. Comput. Sci. Secur.* **2011**, *5*, 118–131.
16. Karie, N.M.; Karume, S.M. Digital Forensic Readiness in Organizations: Issues and Challenges. *J. Digit. Forens. Secur. Law* **2017**, *12*, 5. [CrossRef]
17. Yeboah-Ofori, A.; Brown, A.D. Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *Forens. Legal Investig. Sci.* **2020**, *6*, 045.
18. Ahmad, A.; Hadgkiss, J.; Ruighaver, A.B. Incident response teams—Challenges in supporting the organizational security function. *Comput. Secur.* **2012**, *31*, 643–652. [CrossRef]

19. Reddy, K.; Venter, H.S. The architecture of a digital forensic readiness management system. *Comput. Secur.* **2013**, *32*, 73–89. [CrossRef]
20. Martini, B.; Choo, K.K.R. Cloud storage forensics: Own Cloud as a case study. *Digit. Investig.* **2013**, *10*, 287–299. [CrossRef]
21. Chryssanthou, A.; Katos, V. Assessing forensic readiness. In Proceedings of the WDFIA 2012: Seventh International Workshop on Digital Forensics & Incident Analysis, Crete, Greece, 6–8 June 2012; pp. 107–118.
22. Taylor, M.; Haggerty, J.; Gresty, D.; Hegarty, R. Digital evidence in cloud computing systems. *Comput. Law Secur. Rev.* **2010**, *26*, 304–308. [CrossRef]
23. Akilal, A.; Kechadi, M.T. An improved forensic-by-design framework for cloud computing with systems engineering standard compliance. *Forens. Sci. Int. Digit. Investigat.* **2022**, *40*, 301315. [CrossRef]
24. Alenezi, A.; Hussein, R.K.; Walters, R.J.; Wills, G.B. A framework for cloud forensic readiness in organizations. In Proceedings of the 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), San Francisco, CA, USA, 6–8 April 2017; pp. 199–204.
25. Sol, D.C.; Devidas, A.R.; Anjana, M.S.; Ramesh, M.V. Design and implementation of context aware cyber physical system for sustainable smart building. In Proceedings of the 2018 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), Kajang, Malaysia, 29 May–1 June 2018; pp. 162–167.
26. Pooe, A.; Labuschagne, L. A conceptual model for digital forensic readiness. In Proceedings of the 2012 Information Security for South Africa, Johannesburg, South Africa, 15–17 August 2012; pp. 1–8.
27. Kamberelis, G.; Dimitriadis, G. Focus group research: Retrospect. In *The Oxford Handbook of Qualitative Research*; Oxford University Press: Oxford, UK, 2014; p. 315.
28. Moser, A.; Korstjens, I. Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *Eur. J. Gen. Pract.* **2018**, *24*, 9–18. [CrossRef] [PubMed]
29. Stahl, B.C.; Tremblay, M.C.; LeRouge, C.M. Focus groups and critical social IS research: How the choice of method can promote emancipation of respondents and researchers. *Eur. J. Inform. Syst.* **2011**, *20*, 378–394. [CrossRef]
30. Leonardi, C.; Doppio, N.; Lepri, B.; Zancanaro, M.; Caraviello, M.; Pianesi, F. Exploring long-term participation within a living lab: Satisfaction, motivations and expectations. In Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, Helsinki, Finland, 26–30 October 2014; pp. 927–930.
31. Benjumea, C.D.L.C. The quality of qualitative research: From evaluation to attainment. *Texto Contexto-Enferm.* **2015**, *24*, 883–890. [CrossRef]
32. Wang, G.; Gunasekaran, A.; Ngai, E.W.; Papadopoulos, T. Big data analytics in logistics and supply chain management: Certain investigations for research and applications. *Int. J. Prod. Econ.* **2016**, *176*, 98–110. [CrossRef]
33. Webb, J.; Ahmad, A.; Maynard, S.B.; Shanks, G. A situation awareness model for information security risk management. *Comput. Secur.* **2014**, *44*, 1–15. [CrossRef]
34. Horsman, G. Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics. *Comput. Secur.* **2018**, *73*, 294–306. [CrossRef]
35. Poeppelbuss, J.; Niehaves, B.; Simons, A.; Becker, J. Maturity models in information systems research: Literature search and analysis. *Commun. Assoc. Inform. Syst.* **2011**, *29*, 27. [CrossRef]
36. Lacerda, T.C.; von Wangenheim, C.G. Systematic literature review of usability capability/maturity models. *Comput. Stand. Interfaces* **2018**, *55*, 95–105. [CrossRef]
37. Wolfswinkel, J.F.; Furtmueller, E.; Wilderom, C.P. Using grounded theory as a method for rigorously reviewing literature. *Eur. J. Inform. Syst.* **2013**, *22*, 45–55. [CrossRef]
38. Savin-Baden, M.; Major, C.H. *Qualititaive Research: The Essential Guide to Theory and Practice*; Routledge: Oxford, UK, 2013; pp. 10–11.
39. Barske, D.; Stander, A.; Jordaan, J. A digital forensic readiness framework for South African SME's. In Proceedings of the 2010 Information Security for South Africa, Johannesburg, South Africa, 2–4 August 2010; pp. 1–6.
40. Ariffin, K.A.Z.; Ahmad, F.H. Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. *Comput. Secur.* **2021**, *105*, 102237. [CrossRef]
41. Pandey, J. Deductive approach to content analysis. In *Qualitative Techniques for Workplace Data Analysis*; IGI Global: Hershey, PA, USA, 2019; pp. 145–169.
42. Okoli, C. A guide to conducting a standalone systematic literature review. *Commun. Assoc. Inform. Syst.* **2015**, *37*, 43. [CrossRef]
43. Corbin, J.M.; Strauss, A. Grounded theory methodology. In *Handbook of Qualitative Research*; SAGE: Thousand Oaks, CA, USA, 2011; pp. 273–285.