Received: 14 December 2020 | Revised: 11 January 2021 | Accepted: 20 January 2021 | Published on: 16 February 2021

DOI: 10.1002/spy2.151

OPINION PAPER

WILEY

Digital forensic readiness intelligence crime repository

Victor R. Kebande[1] | **Nickson M. Karie**[2] | **Kim-Kwang Raymond Choo**[3] | **Sadi Alawadi**[4]

[1]Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden

[2]Security Research Institute, Edith Cowan University, Joondalup, Western Australia, Australia

[3]Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, Texas, USA

[4]Department of Information Technology, Uppsala University, Uppsala, Sweden

Correspondence
Victor R. Kebande, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden.
Email: victor.kebande@ltu.se

Abstract

It may not always be possible to conduct a digital (forensic) investigation post-event if there is no process in place to preserve potential digital evidence. This study posits the importance of digital forensic readiness, or forensic-by-design, and presents an approach that can be used to construct a Digital Forensic Readiness Intelligence Repository (DFRIR). Based on the concept of knowledge sharing, the authors leverage this premise to suggest an intelligence repository. Such a repository can be used to cross-reference potential digital evidence (PDE) sources that may help digital investigators during the process. This approach employs a technique of capturing PDE from different sources and creating a DFR repository that can be able to be shared across diverse jurisdictions among digital forensic experts and law enforcement agencies (LEAs), in the form of intelligence. To validate the approach, the study has employed a qualitative approach based on a number of metrics and an analysis of experts' opinion has been incorporated. The DFRIR seeks to maximize the collection of PDE, and reducing the time needed to conduct forensic investigation (e.g., by reducing the time for learning). This study then explains how such an approach can be employed in conjunction with ISO/IEC 27043: 2015.

KEYWORDS

digital, forensic, investigations, jurisdiction, readiness intelligence, repository

1 | INTRODUCTION

In recent years, the need for digital forensics and digital investigations have increased significantly,[1] partly due to the interconnectivity in our society and the exponential growth in the number of digital devices (e.g., Internet of Things (IoT) and related devices).[2] Digital forensics is generally defined to be an interdisciplinary area, which combines elements of legal, computer science, computer engineering, and so on, to facilitate the identification, collection, analysis, and reporting of data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.[3-6] Given the constant advances in consumer technologies and the evolving threat landscape, there is a need to be more proactive in digital forensics and digital investigations. For example, researchers have posited the importance of forensic readiness and forensic-by-design to be considered in system design.[7] Having in-place such practices will facilitate faster response time and the availability of digital evidence. Thus, in this paper, this study presents

an approach that can be used to construct a Digital Forensic Readiness Intelligence Repository (DFRIR). DFRIR can be used to cross-reference potential digital evidence (PDE),[8] for example, by employing techniques to capture PDE from different sources (e.g., user's consumer devices such as mobile devices, wearable devices such as smartwatches, and other Internet of Things (IoT) devices), and create a repository that can be able to be shared among digital forensic experts and law enforcement agencies (LEAs). Such an approach complements existing approaches such as those proposed by Zhang, Choo and Beebe.[9] Specifically in the latter, they proposed an IoT forensic knowledge sharing platform, where the forensic community can learn from the prior experience of their peers in the form of a shared digital forensic artifact schema. DFRIR is designed to be technology-neutral, in order to cater for the fast advances in consumer technologies and threat landscape (e.g., adversarial techniques), without affecting the capability to support attack attribution, etc. Specifically, DFRIR is designed to facilitate the investigators to identify and collect as much digital evidence from the broad range of devices. The remainder of this report is structured as follows: Section 2 covers relevant background materials and related literature. In Sections 3 and 4, the authors present the proposed DFRIR and how it can be used in practice. Finally, the paper concludes in Section 5.

2 | BACKGROUND AND RELATED LITERATURE

This section gives a discussion on literature that has been explored in this paper. The focus has mainly been on Digital Forensic Readiness, forensic Intelligence Repositories and Knowledge sharing, and other relevant related work.

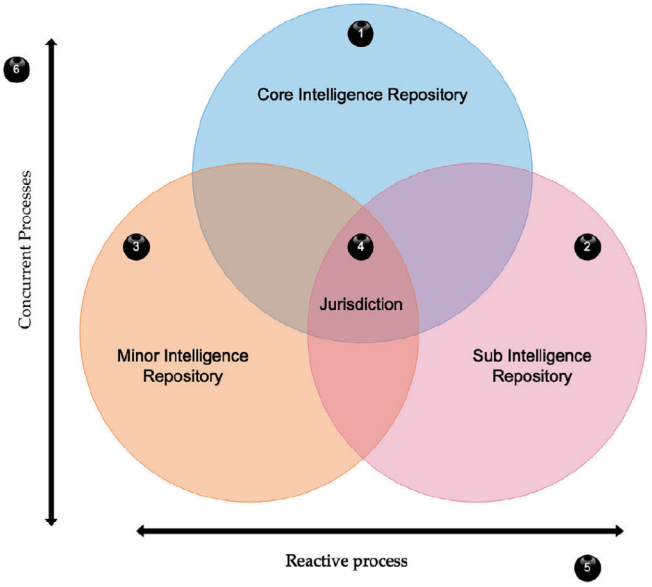
2.1 | Digital forensic readiness

Forensic readiness as defined by researchers such as Mohay[10] is the extent to which computer systems or computer networks record activities and data in such a manner that the records are sufficient in their extent for subsequent forensic purposes, and the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations. Being forensically ready can help organizations with quicker recovery, improved business continuity, compliance and an improved success rate in legal actions by having available relevant digital evidence.[11] However, the authors should not only rely on organizations to have in-place such practices.[8] There is also a need to integrate forensic-by-design principles in the design of such systems, so that they can be readily used (analogous to secure-by-design and privacy-by-design concepts).[1,2,7,9] For example, Rowlingson[12] identified key activities in implementing a forensic readiness programme, such as identifying available sources and different types of potential evidence and the establishment of a policy for secure storage and handling of potential evidence. Similarly, researchers in References 1, 2, 7, 9 have also identified several key building blocks in a forensic-by-design process.

2.2 | Forensic intelligence repositories and knowledge sharing

Forensic intelligence as broadly defined by Ribaux et al,[13] and Quick and Choo[14,15] is the accurate, timely, and useful product of logically processing forensic case data from different evidence sources, and cases/incidents (that may even be seemingly unrelated). In other words, forensic intelligence focuses on broader criminal activity, and uses data to identify patterns and connections between crimes.[14] Available information can be used to understand criminal phenomena, as well as preventing future similar activities from happening, by introducing relevant mitigation strategies. The authors posit that in our proposed DFRIR approach, the gathering of potential evidence may not necessarily be manual, since this study can also integrate/introduce forensic intelligence into existing digital forensic processes and utilize artificial intelligence (broadly defined to include machine and deep learning techniques) to facilitate the identification, collection and analysis of PDE from a broad range of sources. A forensic intelligence repository may also be explained to be some centralized locations in which data are stored and managed. In the context of this paper, an intelligence repository is a central location where digital forensic readiness intelligence data are stored. Data in the repository can be presented in different formats, including visualizing repository data with graphs.[16,17] In other words, having such a proposed repository allows one to organize, create, capture or distribute intelligence knowledge and ensure its availability for future digital forensic practitioners. This, as discussed earlier, complements other approaches such as the digital forensic knowledge sharing platform proposed in Reference 9.

FIGURE 1 High-level description of DFRIR



2.3 | Other related work

In addition to the literature discussed earlier in this paper, there have been other attempts to develop similar concepts. For example, Weiser, Biros, and Mosier[18] proposed the development of a national repository of a digital forensic Intelligence, in order to provide efficiency for examiners and DF investigators through knowledge sharing.[19-21] Also proposed a technique through which digital forensic investigations (DFI) can use knowledge management techniques to capture, manage, and analyze PDE. Kebande and Venter[20] proposed digital forensic readiness techniques that can be applied in a distributed environment, with the cloud being a focus. Other relevant research efforts include preservation of digital evidence for criminal investigations[21,22] securing reliable and secure evidence in forensic readiness approach and achieving readiness in cloud using forensic agents. In addition, Reddy and Venter[22] proposed an architecture of a digital forensic readiness management system that can be used to manage forensic readiness processes. Vidalis, Angelopoulou, and Jones[23] also developed a distributed conceptual architecture that forensic analyst can use to analyze evidence that are potentially of intelligence value.

3 | DIGITAL FORENSIC INTELLIGENCE REPOSITORY (DFRIR)

Now, this study will present our proposed DFRIR, designed to be proactive in assisting LEAs, DFIs and DF analysts to be able to share PDE across diverse jurisdictions based on the shared intelligence repositories—see both Figures 1 and 2. As shown in Figure 1, there are interactions between different components to ensure that relevant digital information that can be used as forensic intelligence is captured in a forensic repository for sharing among relevant stakeholders. Similar to the digital forensic data sharing platform,[7] one could implement DFRIR in a secure, cloud-based repository that enables relevant stakeholders (e.g., digital forensic practitioners from different agencies and jurisdictions) to access and contribute case-specific information in real-time. There are a number of components in the proposed DFRIR, and additional components can be introduced as required. In this paper, this study introduces six key components, namely: jurisdictions, core intelligence repository (CIR), sub-intelligence repository (SIR), minor intelligence repository (MIR), reactive process (5), and concurrent processes (6). Clearly, given the sensitivity of the stored information, this study should ensure that the intelligence repository can securely store and index all the different types of digital content (e.g., text, images, audio, and video). Indexing of the content in the repository allows easy accessibility of information by any authorized stakeholder from different jurisdictions. Besides, indexing is good for quick searches and filtering case-specific information.

CIR is designed to collect PDE proactively, which can subsequently be shared as forensic intelligence across different jurisdictions. Relevant intelligence is also stored in both SIR and MIR, which can be used as admissible evidence. Intelligence from other related cases can be contributed to any of these repositories in real-time, and can complement

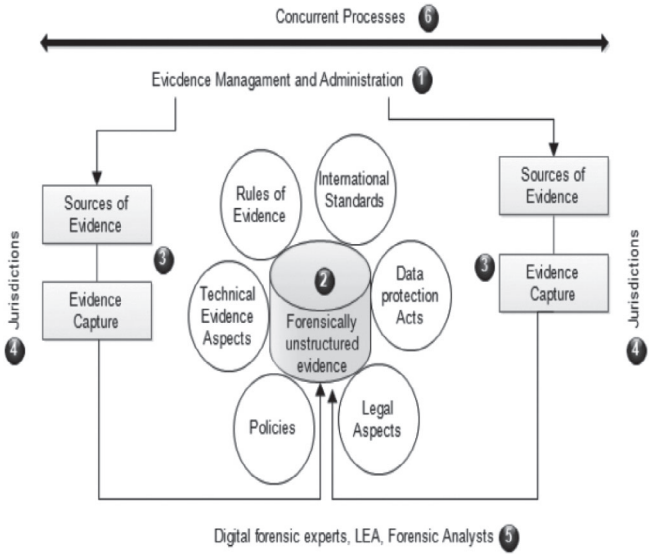


FIGURE 2 How different repositories can be linked: A simplified example

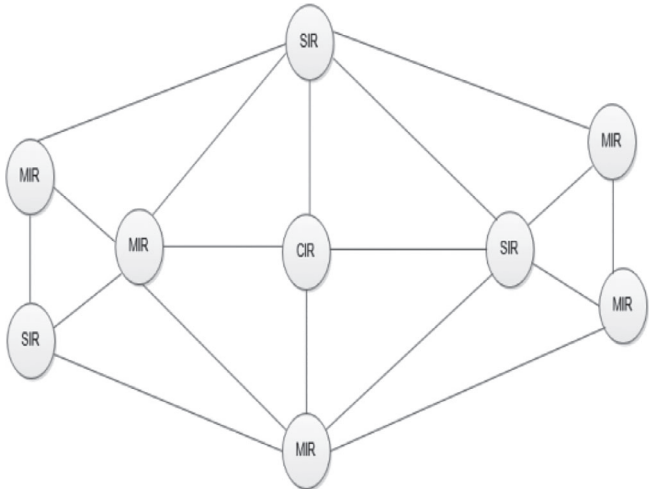


FIGURE 3 Detailed intelligence repository: An example

the concurrent reactive forensic investigations. This echoes the recommendations in the ISO/IEC 27043 international standard.[24,25]

Figure 2 presents a simplified example of how different repositories can be linked to, and interacts with each other based on different jurisdictions The CIR, SIR, and MIR repositories consists of various cloud-based databases, with different information attributes and metadata that can be used to correlate and possibly profile some perpetrators in a given jurisdiction. However, the CIR, SIR, and MIR can also be a collection of data from different digital devices (e.g., IoT devices). Beforehand, a DFRIR mining rule coupled with association rules can be used to extract the proactively collected data from multiple jurisdictions and/or multiple digital devices. A detailed view of the digital forensic readiness repository is shown in Figure 3.

We will now explain the six components in Figure 3.

- Evidence Management and Administration Digital evidence may be structured and unstructured, however, most of the captured digital forensic evidence may be unstructured (see label (2) in Figure 3), and hence there is a need to maximize the utility of such unstructured forensic evidence. In the context of this research, the evidence management and Administration (EMA) is a process that allows digital forensic investigators to initiate and track evidence in real-time from the network structure. This may include how to enter intelligence content into the repository, how to categorize as well as properly index intelligence information, and how to tag and annotate intelligence information entered into the repository. In addition, the EMA should be able to allow users to search on unstructured evidence from the different sources (see label (3)), and to send out automated notifications to, say the investigators. The latter feature is beneficial

to stakeholders such as investigators as it reduces the need for them to log into different systems or having to travel to different jurisdictions to manually gather evidence. This can be made possible by allowing the repository to have the ability to dynamically-update the content, which then allows users from different jurisdictions to quickly review new information relevant to their needs. Moreover, notifications that alert the investigators as well as other digital forensic investigators of any changes on content can quickly eliminate the need for digital forensic practitioners to repeatedly check the repository for updates or new content added.

- Unstructured Evidence NORMALLY, evidence can come in different formats, sizes, and types. For example, one may have video, images, audio, and text. Thus, given the volume, variety, velocity and veracity of the data, it can be challenging for digital forensic investigators to interpret find the meaning of the collected digital data. A forensic analyst should be able to analyze the digital data fragments that are recovered from multiple PDE sources, bearing in mind the Rules of evidence, technical aspects of digital evidence, policies and procedures, legal aspects regarding digital evidence, data protection requirements and international standards.
- Evidence Sources and Capture Identifying the many PDE sources can be challenging, particularly for inexperienced digital forensic investigators or when dealing with newer consumer technologies. Examples of PDE sources include embedded devices (and any applications—apps installed on these devices), GPS systems, removable media, mobile devices, computers, physical, and virtual resources. The PDE source identification is crucial, and should be ongoing (e.g., due to replacement/addition of devices to existing systems), in any forensic readiness and forensic-by-design strategies.[26-28]
- Jurisdiction is important to ensure that the tools and processes used are forensically sound and comply with the requirements in the respective jurisdiction. This can be challenging when dealing with newer devices and systems, or using newer tools and techniques that have not been trialed and tested. For example, a practice or process may be acceptable in one jurisdiction, but not soon in another jurisdiction due to differing rules of evidence. The need to consider jurisdictional requirement differences is also highlighted in References 26-28.
- Digital Forensic Experts, LEA and Forensic Analysts Digital forensic experts can also play an important role in the proposed approach, since they can help to ensure that the shared information comply with local requirements. The intelligence repository proposed in this paper is also designed to help the digital forensic experts, LEA and other key stakeholders to understand what tools can be used for their investigations of similar devices/systems and/or share and retrieve the information available in existing repositories. Benefits of such repositories include:

    1. Spending less time on intelligence information gathering
    2. Consolidating scattered intelligence information into a centralized intelligence repository
    3. Making informed decision-making, based on collective intelligence information from the international community
    4. Sharing of intelligence from the international community
    5. Gaining real-time understanding and actionable insights from discussion based on the collective intelligence information from the international community
    6. Reducing time and costs (e.g., manpower) associated with conducting repetitive research on information that is already present in the repository hence more focus on data analysis and finally
    7. Facilitating fruitful collaborations, for example to shared intelligence information

- Concurrent Processes have been taken verbatim from the ISO/IEC 27043[24] international standard, which are important processes that happen in tandem with the other processes. The concurrent processes include obtaining authorization, documentation, managing information flow, preserving chain of custody process, preserving digital evidence process and interaction with physical investigation process.

In the next section, this study will briefly explain how it can be deployed in practice.

Based on the discussion that has been given in the high-level description, the DFRIR further provides a common ground through which digital evidence that has facts that could be used by investigative agencies could be managed. This can also be adapted easily in a forensically ready environment while taking care of the prevailing forensic laws of a given jurisdiction. Based on that, this study consider the CIR as the prime repository, but based on the knowledge base that may be needed, this study identify common functions together with the SIR that could be integrated into digital forensic investigative models as is shown in Figure 4. Notably, an exploration of existing forensic intelligence research has explored a number of open research problems (see Table 1) coupled with key investigative techniques with relevant observations.

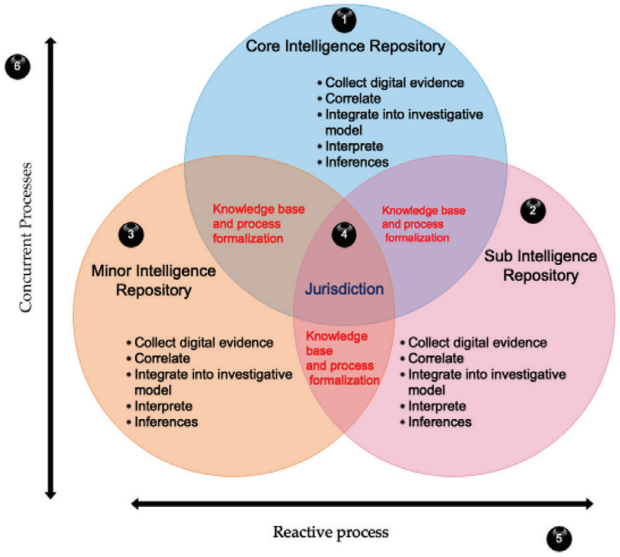


FIGURE 4 High-level description of DFRIR

Precisely, Table 1 has been used to articulate how forensic intelligence research has been leveraged to solve digital crime related scenarios.

Figure 4, which is basically an extension of the high-level description shows key indicators that cohesively work together based on the common understanding(knowledge-bases)behind the extracted evidence. Consequently, the legal aspects should be upheld based on the laws of a given jurisdiction. As a result, the CIR, MIR, and SIR achieve the following functions: Collecting and correlating digital evidence by way of interpreting through inferences. These functions can easily be used to manage the processes that were highlighted in Figure 2, and this gives a flexible approach by way of considering the requirements, standards and evidence management techniques.

4 | POTENTIAL USE CASE

The proposition for a DFRIR has shown the collection and acquisition of digital information that can be used as potential digital evidence across diverse jurisdictions is the basis for computer or digital forensics. It is possible for the DF experts and the LEAs to be able to access important forensic information captured through the CIR, SIR, and MIR through respective jurisdictions. A very important aspect that needs to be the point of concentration is the implementation of the common international law. This is important because of cross-cutting jurisdictions where the validity of evidence or investigation can be questioned. Even though a variety of forensically collected unstructured data may be collected, still it is important because there will be effective planning and preparation before potential incidents or attacks may occur. This, therefore, reduces the cost and time that is needed to conduct a digital forensic investigation (reactive process) see Figure 1. This study takes a step toward highlighting the potential use-case that could be used by DFRIR. Generally, in a smart intelligent city network, digital or smart devices are connected via ad-hoc networks and the presence of mobile devices brings about complexities when a digital incident is detected. As a result, one would allow the collection of potential digital evidence[37,38] that can be distributed across the aforementioned CIR, SIR, and MIR databases for purposes of sharing useful investigative forensic knowledge. In this smart city, forensic intelligence could easily be gathered across different connected devices and this form of forensic intelligence could easily be used to link the perpetrator to the crime. These processes could easily be achieved by conducting forensic investigation of the smart connected city based on the environment through which potential evidence is collected from References 5, 6, 8. Nevertheless, although the process of collecting digital information is tedious, it is vital to have emphasis on the collection methods, rules, technical aspects, policies, data protection acts, acceptable international standards in order to maintain the legality and admissibility that digital evidence may need. Consequently, ISO/IEC 27037: 2012 and ISO/IEC 27043: 2015[24,25] have mentioned important strategies on how digital evidence can be collected from digital sources. An important argument that may arise as a result of the implementation of DFRIR is on what may be collected as a result of the existence of voluminous "big data". Of Importance to note is that, DFRIR is still a generic approach that at a given time may need to filter and analyze the captured unstructured data, however, that stands out to be an open problem. Even though collecting digital data for dig-

TABLE 1 Key forensic intelligence research that addresses pertinent issues

Reference	Main focus	Investigative technique	Open problems	Observations
13	Forensic intelligence and crime analysis	Illustrate two-step process on the potential of forensic data to provide intelligence based on inferences	Lack of theoretical framework that is able to classify core problems focused on intelligence	Study basically provides a foundation that allows systems to be able to adapt to digital crime analysis techniques in the context of forensic intelligence. This is important aspect that allows the building of a forensic intelligence framework.
29-31	Forensic led Intelligence-for crime scene processing	(Framework that postulate how traces and remnants leads to processes on decision making)	Security oriented models not well explored	Approach presented techniques of structuring knowledge that is capable to be used in a crime scene
32	Integrating forensic information with a focus in a crime scene intelligence	Development of a forensic intelligence model by integrating forensic intelligence into crime scene intelligence in forensic databases	There is increased forensic case data based on a statistical outlook on retrospective datasets, most of these cases are detected based on this data	Based on the outcome it is easy to detect a crime based on forensic outcomes. For example, using DNA-it is possible to detect crimes. Integrating this brings out intelligence in form of patterns that can increase detection
33	Possibilities of forensic intelligence	Concepts, processes and intelligence products that are delivered in forensic casework and information repositories	Forensic analysis datasets being able to make cross-discipline based on cross offense matches. Basically, this provides a correlation of crime-scenes-similarit in offenses that are not related	There is importance of searching forensic findings and observations in an intelligence approach. By doing this information is provided for digital forensic intelligence practitioners
34	Elements of a forensic intelligence model	Scene, on-submission, triaging, digital capture, transmission and comparison	Still forensic intelligence is at infancy given that focus of forensics is directed to resolution of crimes	Forensic intelligence should be employed as a cost effective approach to solve backlogs and constraints
35	Forensic intelligence in policing Identification	Development of forensic intelligence culture	Examines organizational and cultural barriers to implementing forensic intelligence models	There is a need for a national forensic intelligence structure based international jurisdictions/or high-level forensic intelligence advisory groups
36	Generic building blocks of a forensic intelligence framework	Develop suitable forensic intelligence model in relation to policing and security and builds upon the general models by focusing on decisions	lack of evaluation systems in forensic intelligence framework and scientific decision criteria	There is a need and importance of identifying key indicators and building blocks that can be used to develop a structured and a dynamic architecture in the perspective of forensic intelligence

TABLE 2 DFRIR validation and verification metrics

Metric	Explanation
Reliability	Circumstances that may lead the suggested approach to fail[45]
Logical	How the DFRIR should be implemented for example
Completeness	Given evidence that may be pointed out from some form of existing evidence[45]
Transparency	Subjected to open audit
Neutrality	Positioned to be evaluated[45]
Extensibility	Positioned to add new specifications[45]
Applicability	Suitability of appropriateness of the suggested approach

ital forensic readiness is a sensitive issue and also there may exist other obstacles concerning the suitability of analyzing the huge amount of unstructured data, this approach of DFRIR is a promising approach that significantly ensures that there is information sharing across multiple jurisdictions, which in the long run eases the process of conducting digital forensic investigation.[39,40] Having looked at critical evaluation, in the next section a conclusion of this research is given and avenues for future work.

5 | VALIDATION AND EVALUATION OF DFRIR

Since the DFRIR is positioned to maximize the collection of PDE, through a forensic readiness approach, it is important to ensure that the validity and forensic soundness of digital evidence is maintained as a result. Based on that, a validation and verification approach has been conducted using a number of suitable metrics that can ascertain the relevance of the proposed DFRIR.

The study has allowed potential expert reviews in a qualitative manner on the suitability of the proposed approach through remote interviews for a selected sample of respondents. The choice of this approach has been motivated by the fact that qualitative approach stands to be best suited in exploratory[41] studies given that a specific sample can easily be relied upon to extract results that can be relied upon based on the experts notions, perception, and views.[42,43] Also, existing studies have shown that a range between 3 and 20 in other circumstances could be accepted and in other context 12 could also be considered as a saturated sample.[44]

In order to validate the effectiveness, the following metrics have been considered for the expert-based reviews: Reliability, Logical, Completeness, Transparency, Neutrality, Extensibility and Applicability. A summary on the representation of the aforementioned metrics is given in Table 2.

A number of experts have been involved in providing expert reviews of the DFRIR in order to verify based on the identified metrics in Table 2 whether, the proposition could be improved or whether its nature could be acceptable in the forensic community. A list of the experts through which the reviews have been collected is shown in Table 3.

Findings from the expert reviews, opinions have illustrated that digital forensic readiness still plays a significant role in digital artefact identification by maximizing the time that is needed to conduct a digital investigation during a post-event response approach. Consequently, a digital forensic intelligence repository presents a significant approach that may be of interest to multiple jurisdictions during cyber-crime investigations. Most of the experts are of the views that, there need to be established international laws that can also cater for the cross-cutting jurisdiction and access to data, for example, for cases like information disclosure, where, for example, the EU General Data Protection Regulation (GDPR) is applied. A summary of the expert opinions has been shown in Table 4.

Based on the seven metrics that have been used as a baseline for the validation and verification of the DFRIR, the expert opinion/reviews has provided opinions on the reliability, logical aspect, completeness, transparency, neutrality, extensible and the possible applicability of the DFRIR. With the prevailing digital forensic challenges, the experts finds that DFRIR to be a reasonable approach that still could be improved to address more inclusive aspects. The findings from the experts/validators (1, 2, 4) have shown that knowledge sharing in digital forensics is pertinent given the difficulty involved in locating a moving digital object or the provenance of data. This has also shown the essence of saving the time that is needed to conduct digital forensic investigation process. In addition, it is the experts point of view for the need for considering standardization recommendations in intelligence repositories. It is the authors view that this aspect could be realistic in increasing admissibility based on the recommendation for the international (common) law for digital investigation as pointed by experts (7, 2).

TABLE 3 Expert validator profiles

Expert validator	Specialization	Country	Years of expertise
1	Cyber security professional	USA	8+
2	Researcher in cyber forensics	Australia	9
3	Expert in cloud forensic readiness	Malaysia	10
4	Expert in digital forensics	Qatar	9
5	industrial expert in cyber security	South Africa	8
6	Expert in standardization approaches in incident investigation techniques	South Africa	16
7	Digital forensics in the cloud researcher	Sweden	8+

TABLE 4 DFRIR validation expert opinions

Metric	Expert opinion	Expert
Reliability	Knowledge sharing is pertinent for digital crimes when it is hard to locate data (digital objects) Intelligent repository could lead to timely conclusion of digital investigations hence saving costs	1, 2, 4
Logical	International standards could provide a standardized approach for the intelligence repository, this may define the level of it being logical and levels of acceptability Intelligent repository could be logical enough if they are leveraged within a single jurisdiction, however, they could be extended internationally based on the laws	7, 2
Completeness	Important basically because presents the pool through which newer or useful evidence could be extracted, it may apply Unstructured evidence may need to be carefully sifted in this case Privacy could be defined in the DFRIR	3, 6
Transparency	Credibility of evidence may need to be verified often and how valid it may be auditing the tool or the process is step toward transparency Could chain of custody be leveraged in this instance? How can the changing technologies interfere with the transparency	4, 8, 2
Neutrality	Changes of evidence terminologies, semantics, digital forensic terminologies, and forensic terminology heterogeneity may need new evaluation criteria Pertinent to share new forensic evaluation criteria through intelligence repositories	5, 4
Extensibility	A new jurisdiction could easily be added based on the existing CIR, MIR or SIR Jurisdiction can define how they want new specifications to be added without changing the existing functionality	4, 8, 2
Applicability	With increased cost of conducting digital forensics knowledge sharing is more pertinent and could be a game changer for the forensic environments Does this apply to the investigations in the cloud environments, it looks more applicable in cross-cutting jurisdictions	1, 2, 3

In addition, there has been a suggestion for improving the DFRIR by carefully sifting unstructured evidence as illustrated by expert (3, 6), however, still the study is marked to be important by the experts. Consequently, the experts have also stressed the need of verifying evidence credibility often, however, auditing is encouraged as a step toward transparency and being able to accommodate the changing technologies.

Other important aspects pointed by experts (4, 8, 2) include the semantics involved in digital forensics like terminal heterogeneity over which the experts recommends sharing of the evaluation criteria over intelligence repositories. In addition, experts find DFRIR worthy being extended by adding potential new specifications based on the CIR, MIR, and SIR respectively. Ultimately, the study has also been positioned to address the significant costs involved in conducting digital investigations while at the same time experts point that this study could also be applied across cloud-based environments (1, 2, 3).

The metrics that have been used to show the significance of the study has been positioned to be very important by the experts, and it is also the experts' view that forensic intelligence plays a crucial role and is very significance in various jurisdictions based on the modern connected environments. Notably, expert (3, 6) is of the view that DFRIR could be more interesting if the aspect of privacy would be addressed given the adoption of new regulations like the EU-GDPR that was enacted in 2018. While there could be more other metrics that have a potential of being included in the DFRIR, the authors consider the useful suggestions from the experts and in future work this could be considered.

6 | CONCLUSION AND FUTURE WORK

Digital forensics will be increasingly challenging, due to the constantly advancing technological and threat landscapes. Rather than reinventing the wheel, the authors argued the need for digital forensic repositories that can be used to share case-relevant forensic intelligence. Thus, this study presented our proposed DFRIR, to maximize the potential use of digital evidence collected by different stakeholders.

There are a number of future research directions for this work. For example, one can deploy the proposed approach in collaboration with some LEAs and stakeholders to evaluate its utility, and identify other features that should be included. One such feature on our radar is to filter what is collected through the identification of key attributes in order to enhance attribution. In addition, the authors consider an inclusion of privacy as future work as per the experts recommendations.

ORCID

Victor R. Kebande https://orcid.org/0000-0003-4071-4596
Nickson M. Karie https://orcid.org/0000-0001-5173-9268
Kim-Kwang Raymond Choo https://orcid.org/0000-0001-9208-5336
Sadi Alawadi https://orcid.org/0000-0002-6309-2892

REFERENCES

1. Quick D, Choo K-KR. *Big Digital Forensic Data: Volume 1: Data Reduction Framework and Selective Imaging*. Springer; 2018.
2. Quick D, Choo K-KR. *Big Digital Forensic Data: Volume 2: Quick Analysis for Evidence and Intelligence*. Springer; 2018.
3. Casey E. *Interrelations Between Digital Investigation and Forensic Science*; 2019.
4. Casey E. *Maturation of Digital Forensics*; 2019.
5. Kebande VR, Ray I. A generic digital forensic investigation framework for internet of things (IoT). In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) (IEEE, 2016), pp. 356–362.
6. Kebande V, Venter H. Towards a model for characterizing potential digital evidence in the cloud environment during digital forensic readiness process. Paper presented at: ICCSM2015-3rd International Conference on Cloud Security and Management: ICCSM 2015 (Academic Conferences and publishing limited; 2015), p. 151.
7. Le-Khac N-A, Jacobs D, Nijhoff J, Bertens K, Choo K-KR. Smart vehicle forensics: Challenges and case study. *Future Gener Comput Syst*. 2018.
8. Kebande VR, Malapane S, Karie NM, Venter H, Wario RD. Towards an integrated digital forensic investigation framework for an IoT-based ecosystem. Paper presented at: 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), (IEEE, 2018), pp. 93–98.
9. Zhang X, Choo K-KR, Beebe NL. How do i share my IoT forensic experience with the broader community? an automated knowledge sharing IoT forensic platform. *IEEE Internet Things J*. 2019;6:6850.
10. Mohay G. Technical challenges and directions for digital forensics. Paper presented at: First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05) (IEEE, 2005), pp. 155–161.
11. Pour MS, Bou-Harb E, Varma K, Neshenko N, Pados DA, Choo K-KR. Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize internet-scale IoT probing campaigns. *Digit Investig*. 2019;28:S40.

12. Rowlingson R. A ten step process for forensic readiness. *Int J Digit Evid*. 2004;2:1.
13. Ribaux O, Girod A, Walsh S, Margot P, Mizrahi S, Clivaz C. *Forensic Intelligence and Crime Analysis, Law, Probability and Risk*; 2003.
14. Quick D, Choo K-KR. Digital forensic intelligence: Data subsets and open source intelligence (dfint+ osint): A timely and cohesive mix. *Future Gener Comput Syst*. 2018;78:558.
15. Quick D, Choo K-KR. Pervasive social networking forensics: intelligence and evidence from mobile device extracts. *J Netw Comput Appl*. 2017;86:24.
16. Tassone CF, Martini B, Choo K-KR. Visualizing digital forensic datasets: a proof of concept. *J Forens Sci*. 2017;62:1197.
17. Tassone C, Martini B, Choo K-K. Forensic visualization: survey and future research directions. *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Elsevier; 2017:163-184.
18. Weiser M, Biros DP, Mosier G. *Development of a National Repository of Digital Forensic Intelligence*; 2016.
19. Karie NM, Kebande VR, Swaziland K. Knowledge management as a strategic asset in digital forensic investigations. *Int J Cyber-Secur Digit Forens (IJCSDF)*. 2018;7:10.
20. Kebande VR, Venter HS. Novel digital forensic readiness technique in the cloud environment. *Aust J Forens Sci*. 2018;50:552.
21. Kebande V, Ntsamo HS, Venter H. Towards a prototype for achieving digital forensic readiness in the cloud using a distributed nmb solution. Paper presented at: European Conference on Cyber Warfare and Security, Academic Conferences International Limited; 2016, p. 369.
22. Reddy K, Venter HS. The architecture of a digital forensic readiness management system. *Comput Secur*. 2013;32:73.
23. Vidalis S, Angelopoulou O, Jones A. Extracting intelligence from digital forensic artefacts. Paper presented at: European Conference on Cyber Warfare and Security, Academic Conferences International Limited; 2016, p. 282.
24. ISO/IEC, 27043: 2015 international standard, information technology—security techniques—incident investigation principles and processes, ISO.org 1, 1; 2015.
25. Karie NM, Kebande VR, Venter H, Choo K-KR. On the importance of standardising the process of generating digital forensic reports. *Forens Sci Int: Rep*. 2019;1:100008.
26. Ab Rahman NH, Glisson WB, Yang Y, Choo K-KR. Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Comput*. 2016;3:50.
27. Ab Rahman NH, Cahyani NDW, Choo K-KR. Cloud incident handling and forensic-by-design: cloud storage as a case study. *Concurr Comput: Pract Exp*. 2017;29:e3868.
28. Grispos G, Glisson WB, Choo KKR. Medical cyber-physical systems development: A forensics-driven approach. Paper presented at: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), IEEE; 2017, pp. 108–113.
29. Ribaux O, Baylon A, Roux C, et al. Intelligence-led crime scene processing. part i: Forensic intelligence. *Forens Sci Int*. 2010;195:10.
30. Ribaux O, Walsh SJ, Margot P. The contribution of forensic science to crime analysis and investigation: forensic intelligence. *Forens Sci Int*. 2006;156:171.
31. Ribaux O, Wright BT. Expanding forensic science through forensic intelligence. *Sci Just*. 2014;54:494.
32. Rossy Q, Ioset S, Dessimoz D, Ribaux O. Integrating forensic information in a crime intelligence database. *Forens Sci Int*. 2013;230:137.
33. Bell C. Concepts and possibilities in forensic intelligence. *Forens Sci Int*. 2006;162:38.
34. Ross A. Elements of a forensic intelligence model. *Aust J Forens Sci*. 2015;47:8.
35. Raymond T, Julian R. Forensic intelligence in policing: organisational and cultural change. *Aust J Forens Sci*. 2015;47:371.
36. Baechler S, Morelato M, Ribaux O, et al. Forensic intelligence framework. part ii: Study of the main generic building blocks and challenges through the examples of illicit drugs and false identity documents monitoring. *Forens Sci Int*. 2015;250:44.
37. Karie NM, Kebande VR. Building ontologies for digital forensic terminologies. *Int J Cyb-Secur Digit Forens*. 2016;5:75.
38. Kebande VR, Karie NM. A uml-based approach for analysing potential digital forensic evidence. *Int J Cyb-Secur Digit Forens*. 2018;7:354.
39. Kebande VR, Venter H. Requirements for achieving digital forensic readiness in the cloud environment using an nmb solution. Paper presented at: 11th International Conference on Cyber Warfare and Security, ICCWS; 2016, p. 399.
40. Kebande VR, Venter HS. A comparative analysis of digital forensic readiness models using cfraas as a baseline. *Wiley Interdiscip Rev: Forens Sci*. 2019;1:e1350.
41. Hancock B, Ockleford E, Windridge K. *An Introduction to Qualitative Research: Trent Focus Group Nottingham*. Nottingham, UK: Trent Focus; 1998.
42. Banerjee A, Chitnis U, Jadhav S, Bhawalkar J, Chaudhury S. Hypothesis testing, type i and type ii errors. *Ind Psychiatry J*. 2009;18:127.
43. Grant JS, Davis LL. Selection and use of content experts for instrument development. *Res Nurs Health*. 1997;20:269.
44. Guest G. Using guttman scaling to rank wealth: integrating quantitative and qualitative data. *Field Methods*. 2000;12:346.
45. Flandrin F, Buchanan W, Macfarlane R, Ramsay B, Smales A. Evaluating digital forensic tools (dfts). Paper presented at: 7th International Conference: Cybercrime Forensics Education & Training; 2014, pp. 1–16.

How to cite this article: Kebande VR, Karie NM, Choo K-KR, Alawadi S. Digital forensic readiness intelligence crime repository. *Security and Privacy*. 2021;4:e151. https://doi.org/10.1002/spy2.151