Design and Evaluation for Digital Forensic Ready Wireless Medical Systems

Ar Kar Kyaw, Zhuang Tian(✉), and Brian Cusack

Digital Forensic Research Laboratory, School of Engineering, Computer and Mathematical Science, Auckland University of Technology, 55 Wellesley Street East, Auckland, New Zealand
{arkar.kyaw, zhuang.tian, brian.cusack}@aut.ac.nz

Abstract. This paper reports research into mitigating security vulnerability in IoT medical devices by inserting forensic readiness states into the network system and preparing mitigation for security failure. A design is built and tested, and then validated by expert feedback. The contribution of this research is to present a novel conceptual design for a digital forensic readiness framework for WMedSys, which can be easily implemented and integrated into existing IoT and wireless networks in the healthcare sector.

Keywords: IoT · Wireless · Medical · Forensic · Readiness · Framework

1 Introduction

Internet of things (IoT) have become a critical part of the way people live and work. In the last of few years, IoT devices have started playing more important roles, and even providing vital services to companies, enterprises, government departments, healthcare and public sectors [1]. However, security incidents are rapidly increasing along with the benefits provided by IoT. In expectations of information system (IS) security incident response (Request for Comments: RFC 2350), Brownlee and Guttman [2] define security incidents as "any adverse event which compromises some aspect of computer or network security" (p. 17). Hence, a security or cyber security incident is commonly associated with the compromise of the pillars of network security such as confidentiality, integrity, availability, authentication, and the like. For example, the manipulation or alteration of patient data from the personal health record (PHR) or electronic medical record (EMR) of a hospital or a clinical network in the healthcare sector is one of the compromises of network security. Currently, the approach deployed, or action taken by organisations or government departments to mitigate cyber security incidents is oriented to disaster recovery and business continuity to lessen the impact on business processes [3]. But, the impact on business processes can also be reduced by having a digital forensic readiness (DFR) system. Having a DFR system in an organisation is "having an appropriate level of capability in order to be able to preserve, collect, protect and analyse digital evidence so that this evidence can be used effectively: in any legal matters; in security investigations; in disciplinary proceeding; in an employment tribunal; or in a court of law" [4, p. 3]. In fact, the DFR

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2020
Published by Springer Nature Switzerland AG 2020. All Rights Reserved
N. M. Garcia et al. (Eds.): HealthyIoT 2019, LNICST 314, pp. 118–141, 2020.
https://doi.org/10.1007/978-3-030-42029-1_9

system can help an organisation not only to properly acquire and preserve digital evidence (DE), but also to simplify the digital forensic investigation (DFI) process after a security incident happens. In addition, the DFR system can help an organisation to reduce cost, optimise the time and have digital evidence that could be acceptable by a court of law.

Over the last decade, the number of cyber incidents in the healthcare environment including hospitals that deployed wireless medical networks (WMedSys) and wireless medical devices (WMedDs) have significantly increased due to malicious internal and external attacks. For instance, Quinn [5] reported that Hancock Health Regional Hospital from Greenfield (Indiana, United States) paid a small ransom ($55,000.00) to the hackers to regain access to its computer systems due to over 1,400 files being encrypted by ransomware. Similarly, one recent cyber incident was when an authorised employee stole 28,434 patients' related data and their sensitive records from the Centre for Health Care Services in San Antonio in December 2017 [6]. Such incidents are occurring and becoming part of any organisation or healthcare environment that claim to invest in the best technology and resources to provide unfeasible 100 percent security for its information system. In fact, there are many security threats and risks (such as human errors, DDoS and MITM attacks) to the WMedSys and WMedDs [7–12]. Therefore, it is essential to have a proper DFR system for investigating security incidents [13]. As a result, different researchers have proposed theoretical frameworks for forensic readiness of cloud computing [14–18], a theoretical forensic model for acquiring digital evidence in the Internet of Things (IoT) [19] and a theoretical network forensic readiness framework for generic enterprise networks [20]. Moreover, some researchers [21] introduce a generic DFR model for Bring-Your-Own-Device (BYOD) to capture potential (DE by utilising Honeypot while others propose a mobile DFR model [22] and a DFR framework for small to medium-sized enterprise (SME) environments [23]. Similarly, Ngobeni, Venter, and Burke [24] present a prototype implementation of a forensic readiness model for WLANs whereas Rahman, Ahmad and Ramli [25] designed a DFR for WBAN based on the previous proposed research [26]. However, to the best of our knowledge, none of the previous research focuses on the DFR of a hospital wireless network (WMedSys) that deploys WPA2-Enterprise for handling security attacks (such as MITM, patient data manipulation, etc.). Consequently, we extend our proposed DFR of WMedSys [26] to address the research gap. Therefore, the main contribution in this paper is to design and evaluate a novel DFR framework for WMedSys. Hence, the structure of this paper is as follows. Section 2 provides the background of DF, DFR and the significance of DFR. Sections 3 and 4 present the research methodology and the conceptual design of the proposed DFR framework for WMedSys, respectively. Section 5 explains the conceptual design of the proposed DFR framework artefact, which is followed by findings and discussion in Sect. 6. Finally, we discuss limitations and future work in the conclusion (Sect. 7).

2 Background

Any information system including WMedSys is susceptible to cyber-attacks or incidents due vulnerabilities such as technical flaws and weakness of users who use those systems. For example, different researchers have demonstrated attacks in wireless networks as a result of the technical flaws in wireless security protocols (WEP, WPA or WPA2). Thus, any malicious person or adversary can exploit these vulnerabilities in order to destroy, manipulate or steal confidential data of an organisation. In such situations, the impact of cyber-attacks can lead the organisation to have financial and reputation losses. In a severe case scenario, the life of a patient or a person who uses a WMedD (e.g. continuous wireless glucose monitoring system or wireless implantable medical device) could be in serious danger if the patient's physiological data from WMedSys or WMedD is compromised. As a consequence, the DF investigator has to investigate the cyber incident by applying DFI processes in order to answer questions related to the case under investigation. Ieong [27, p. S33] describes six categories of questions in the "FORZA (FORensics Zachman framework)" paper, including "Why (the motivation), What (the data), How (the procedures), Where (the location), Who (the people), and When (the time)" that are related to the eight DF investigator roles. However, the time taken (cost) to perform the investigation and the possibility of failure to collect DE related to the cyber indent or crime could be high if a proper DFR system is not in place. Therefore, this section provides a brief introduction to digital forensics, digital forensic readiness (DFR) and its significance, the requirements of DFR, and attacks in WMedSys and WMedDs.

2.1 Digital Forensics

DF is an emerging area and has many definitions. DF is defined as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." In NIST Special Publication (800-86: Guide to Integrating Forensic Techniques into Incident Response), Kent et al. [29, p. E-11] defines DF as computer and network forensics that apply "science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data or digital information". Similarly, other researchers describe DF as "a branch of forensic science focusing on the recovery and investigation of raw data residing in electronic or digital devices (p. 8)". Nonetheless, DF necessitates a high level of attentiveness and accuracy to ensure the evidential data is uncompromised, reliable and verifiable during the course of investigation. As a result, it is essential to have a DFR system in WMedSys for preserving the integrity potential digital evidence that can be admissible in a court of law. The following sub-sections explain DFR and the significance of having a DFR system in organisations.

2.2 Digital Forensic Readiness

Unlike digital forensic investigations (DFI), DFR is a proactive measure that healthcare providers such as clinics or hospitals have to enforce and implement in order "to comply to DFI with sufficient forensic preparedness" [18, p. 25]. The main objective of DFR is to achieve maximum capability of any healthcare provider in collecting potential digital evidence related to cyber incidents or digital crimes while reducing the cost of DFI during investigations [14, 16, 23, 31–33]. Similarly, ISO/IEC 27043 highlights DFR as a process that focuses on pre-incident investigation [2014, cited in 21]. DFR can be defined as "the achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal matters, disciplinary matters, employment tribunal or court of law" [CESG, Good Practice Guide No. 18, cited in 3, p. 1; 35, p. 1]. Some researchers [18, 21, 22] state that DFR is the dynamic process in which an organisation requires forensic planning and preparation for collecting, accumulating and processing incident response data. In fact, a forensic readiness plan can help organisations not only to fulfil a compliance requirement, but also to provide potential evidence during DFI as part of internal investigation [35]. Other researchers [36] describe DFR as one of the metrics that organisations can use to measure its ability to thwart cybercrimes. Moreover, DFR's goal is to maximise the utilisation of preserved digital evidence if any information security incident happens within the organisation [16, 37]. In addition, Carrier and Spafford [2003, cited in 9] define DFR as "pre-incident plan within the digital forensic (DF) lifecycle that deals with DF identification, preservation, and storage whilst minimising the costs of a forensic investigation (p. 1)". The pre-incident plan of pro-active DF can also empower an organisation to be DFR and provide DFR as an integral component of an information system's best practice [32]. Hence, DFR of a WMedSys can be defined as a mechanism or system that can provide the capability to collect potential digital evidence related to cyber incidents or digital crimes while reducing the cost of DF during investigations.

2.3 Significance of Digital Forensic Readiness

The significance of having a DFR system in organisations has been stated by many researchers. A DFR system can be usually implemented as a pre-incident mechanism to collect and preserve potential DE while reducing the DF investigation cost by promptly and effectively responding to a cyber incident [24, 39–41]. Regiani [3] mentions that a DFR system can help organisations to simplify activities and reduce the process or step for collecting the DE during DFI. In applying a DFR framework, the authors [38] discuss that a DFR can complement the information security policy of an organisation by proactively practising its forensic capability in DE collection. In addition, any organisation with a DFR system deployed will be complying with legal preparedness when it comes to dealing with cybercrime or digital crime cases [18, 20, 33], as the organisation can rapidly collect, inspect, analyse and report the credible DE related to the cybercrime case under investigation. Due to the advances in technology, Pooe and Labuschagne [42] and Rowlingson [33] also state that there is a need to review and

enhance DF models and processes, which can support organisations in finding DE quickly and allow the validation of DE easily. Similarly, other researchers [23] point out that having a DFR system can benefit organisations in collecting DE without disruption or minimising the effect to the operation of organisations during investigation and ensure the collected DE has an impact on the outcome of any legal progress. Therefore, the organisation will be well prepared to get the reliable DE at a lower cost [14, 31, 33, 40] and will have the best response [37, 43] when a cyber incident happens. In fact, the DFR system must be capable of logging or preserving the digital footprints linking to users' activities including authorised (internal) or unauthorised (external) malicious actions within the organisation's IT environment. The digital footprints should disclose details of the malicious person or user account, the source (such as originated IP and MAC addresses), the type or technique used, and date and time of an attack [9, 44]. Moreover, Rowlingson [33] introduced "a ten-step process for forensic readiness", in which the importance of having a DFR system is evidently stated. Therefore, DE is admissible in a court of law, organisations can appreciate the significance of the "legal sensitivities of evidence [33, p. 1]", and the organisation can maximise "ability to collect credible digital evidence and minimise the cost of an internal investigation during an incident response (p. 3)". Likewise, Rowlingson highlights the DFR can help organisations in utilising it "as a deterrent to insider threat", demonstrating "due diligence and good corporate governance of the company's information assets", signifying "regulatory requirements have been met", improving "the prospects for a successful legal action", or resolving "a commercial dispute", and lessening "interruption to the business from any investigation" (pp. 6–9). Previous researchers [17] also raised the importance of having proactive DFR system in the cloud computing environment for gathering potential evidence or valuable data pertaining to cyber incidents for saving time and money during DFI. However, other researchers [20] raise the point that the DFR is a resource intensive answer to DFI even though the DFR can reduce the incident response cost and provide "the basis for security awareness training throughout the enterprise (p. 6)". Nonetheless, the DFR can safeguard against security attacks or breaches by adding appropriate security controls, ensure good corporate information security (IS) governance is in practice to effectively verify possible sources of any security attacks, and provide the IS strategy enhancement of an organisation [32, 34]. Furthermore, having a DFR system in any organisation or in the WMedSys of a healthcare provider can fulfil not only the requirements of DE preservation [33, 34, 45], but also the prevention of a cyber incident from happening within an organisation [15, 34].

3 Research Methodology

3.1 Design Science Research Paradigm

The design science (DS) is a paradigm "for developing scientific knowledge about the problem domain, including artefact, and engineering knowledge about carrying out design" [46, p. 134]. However, Fleming [46] claims that the DS paradigm provides the way in which the process of research should progress and what is required to be

addressed in the research to assure its quality instead of giving the direction on how the artefact should be designed. Moreover, Fleming [46] also argues that the research rigour requirements are commonly in conflict with a major requirement of DS, which is related to real business problems. As a result, a DS paradigm should provide a framework that addresses the problems related to research rigour rather than specifying rigour requirements.

3.2 Design Science Research Methodology

Design science research methodology (DSRM) is proposed by Peffers et al. [47, p. 1] in order to achieve "a commonly accepted framework for DSR" by integrating "principles, practices, and procedures required to carry out DSR" in information systems. To provide a proof of concept, the proposed DSRM is evaluated by using four IS case studies. There are six process elements in the proposed DSRM (see Fig. 1) which are based on well- accepted elements and are derived from previously published papers.

The first process of the DSRM is the "problem identification and motivation" as it is important to define the particular research problem that will be employed in the development of an artefact, which can present a solution effectively. However, the value of such a solution can be achieved by motivating "the researcher and the audience of the research to pursue the solution and to accept the results and it helps to understand the reasoning associated with the researcher's understanding of the problem [47, p. 55]". Hence, the knowledge of the state of the problem and the importance of its solution are required resources in this process stage.

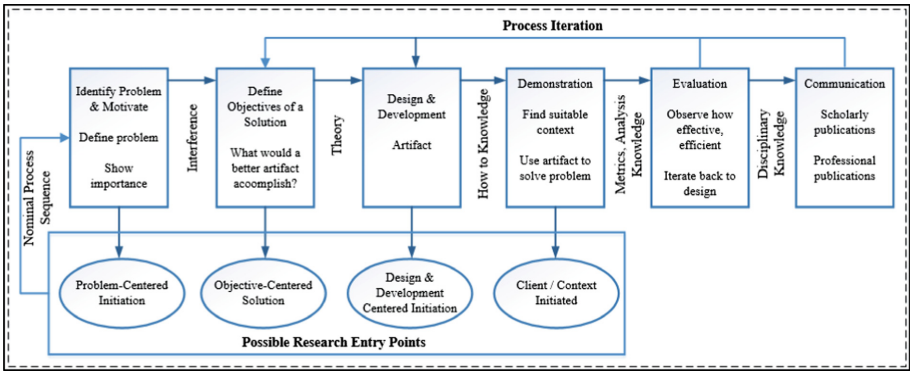


Fig. 1. Design science research methodology process model [47, p. 54]

The second process of DSRM is to "define the objectives for a solution" from the definition of the problem and knowledge of feasibility. The objectives should be deduced from the problem specification and could be quantitative or qualitative. For

instance, the quantitative objective can be "a desirable solution would be better than current ones [47, p. 55]". Similar to the first process stage, the knowledge of the state of problems and current solutions, if any, and their efficacy are required as resources in this process stage.

The third process is to "design and develop" the artefact, which can be "constructs, models, methods, or instantiations" or "new properties of technical, social or informational resources [Jarvinen, 2007, p. 49 cited 48, p. 55]. According to Peffers et al. [47] a conceptual DS artefact is an artefact in which a research contribution is embedded in the design. The architecture and desired or required functionality of the artefact is indispensable for creating the tangible artefact, and therefore theory knowledge is an essential resource that can bring in a solution.

The fourth process is the "demonstration" of the artefact application in order to answer one or more cases of the problem by using "experimentation, simulation, case study, proof or other appropriate method [47, p. 55]". Thus, the effective knowledge for utilising the artefact to answer the problem is an important resource in this process stage.

The fifth process is the "evaluation", in which how well the artefact provides a solution to the problem (effectiveness and efficiency) can be observed and measured by evaluating "the objectives of a solution to actual observed results from the use of artefact in the demonstration" [47, p. 56]. As a result, the knowledge of relevant metrics and analysis methods are necessary in this stage. However, the artefact evaluation may be different depending upon the nature of the problem context. For instance, the evaluation may be done by comparing the functionality of the artefact with the solution objectives from the second process of the DSRM process model in addition to other quantitative evaluation methods such as surveys, client feedback, or simulations [47]. Nevertheless, the evaluation should conceptually consist of any suitable empirical or pragmatic evidence or plausible proof. After completing the evaluation process, the researchers can make a decision on whether to iterate back to the third process phase "to try to improve the effectiveness of the artefact or to continue on to communication and leave further improvement to subsequent projects" [47, p. 56]. Moreover, the feasibility of iteration will be based on the nature of the research in the problem context.

The final process of the DSRM process model is "communication" according to previous researchers. Thus, the problem, the significance of the problem, the artefact designed, the utility and novelty, the rigor of the artefact design and its effectiveness should be communicated "to researchers and other relevant audiences such as practicing professionals, when appropriate" [47, p. 56]. Similarly, the outcome of DSR could be communicated in scholarly research publications (Fig. 2).

Fig. 2. Design science research methodology process model [47, p. 54]

3.3 Artefact Evaluation Criteria

According to March and Smith (1995), the main purpose of evaluation in Design Science Research (DSR) is to ensure the goal that an artefact design aligns with the solution of an identified problem and controls the progress of design development and deployment of an artefact. To systematically review whether the progress has been accomplished or completed, evaluation criteria should be formulated. Hence, March and Smith suggest a set of evaluation criteria for DSR artefacts.

Nonetheless, researchers not only need to focus on academic interest, but also more importantly need to consider the industry application and adoption of an artefact. Such an implication is the essential goal of DSR. For example, on the one hand, industry is more concerned with how easy an artefact can be used, how well it can be adopted and how efficient it can be. On the other hand, researcher is more interested in how reliable the artefact is and whether or not it is adequate. Therefore, when selecting the evaluation criteria and subsequently formulating evaluation questions, a researcher must satisfy both needs and only ask relevant and appropriated questions to ensure the process will be conducted thoroughly and rigorously.

In addition, another set of evaluation criteria has been developed by Rosemann and Vessey [9]. These criteria focus on whether or not an artefact can be applicable to an industry practitioner. These criteria include importance, suitability and accessibility of an artefact. Further, Prat et al. (2014) have recommended a new set of criteria based on March and Smith [1] for evaluating information systems (IS) artefacts which is comprised of three major components including system dimensions, evaluation criteria and sub-criteria. The new set of evaluation criteria introduces more categories and further divides March & Smith's criteria into a hierarchical set. Thus, it provides more precise and balanced evaluation result against an artefact. Table 1 shows artefact evaluation criteria based on a systematic approach derived from Prat et al. (2014).

Table 1. Expert evaluation criteria

System dimensions	Evaluation criteria	Sub-criteria	Questions
Goal	Efficacy		Q1: Overall, for preserving potential digital evidence, how effective do you think the proposed DFR Framework artefact would be in the production environment?
	Validity		Q2: Are the defined components of the proposed DFR Framework artefact clear and relevant to what you observe? Q3: Do you think the provided requirements helpful and adequate in designing DFR Framework artefact for WMedSys?
Environment	Consistency with people	Utility	Q9: Do you think the proposed DFR Framework is effective and efficient in capturing security attacks on a WMedSys? Q10: Do you think the proposed DFR Framework is effective and efficient in determining security attacks on a WMedSys? Q11: Do you think the proposed DFR Framework is effective and efficient in addressing to improve patient/user safety? Q18: How effective do you think the proposed DFR Framework could be if IT managers/security engineers of clinical and hospital networks start using it in their WMedSys?
		Understandability	Q6. What was an approximate time for you to follow all components of proposed DFR Framework artefact? Was it easy to understand?

(*continued*)

Table 1. (*continued*)

System dimensions	Evaluation criteria	Sub-criteria	Questions
			Q15. Were the information provided related to the artefact logical and helpful?
		Ease of use	Q5: How easy or difficult do you think it is to implement and integrate the proposed DFR Framework artefact in an existing WMedSys? Q12: Please provide your comments on the usability and ease of operation
	Consistency with organization	Utility	Q4: Do you think the proposed artefact is useful and realistic in improving/addressing user/patient safety? Q16: Is the proposed DFR Framework artefact cost effective and efficient? Q17: Is the proposed artefact likely to be widely adopted and implemented in WMedSys?
Structure & Activity (Dynamic, the operations and functionalities of the artefact)	Completeness		Q7: Do you think there is any area of improvement in the proposed artefact? If so, please give your suggestion Q8: Is there any modification that should be made to any component of the proposed DFR Framework? Q13: Can you list the weaknesses and strengths of the proposed DFR Framework artefact for WMedSys? Q14: Regarding the completeness of the DFR Framework artefact for WMedSys, how do you think?

4 Conceptual Design of the Proposed Framework Artefact

The proposed DFR Framework artefact for WMedSys (see Fig. 3) is composed of several components such as Pi-drone, Wireless Forensic Server (WFS), Remote Authentication Dial-In User Service (RADIUS) Server, Wireless Access Point (WAP) Controller,

Integrity Checking/Hashing Server (OSSEC), Intrusion Detection/Prevention System (Bro-IDS) Server, Web Server (XAMPP), and a centralised Syslog Server (Splunk).

Pi-drone: It uses the Kali Linux ARM version to act as a forensic wireless drone. Kali Linux is Debian-based Linux distribution which contains many tools designed for penetrating testing and security audits. A TP-link Wi-Fi USB was connected to the Raspberry Pi to use to scan the Wi-Fi signal on 2.4 GHz. Pi-drone also utilises Kismet application which can sense any wireless network device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework. By using Kismet as drone mode, Pi-drone can scan and capture the wireless signal coming from any Wi-Fi devices then all the information collected will be sent to a Wireless Forensic Server for analysis.

Wireless Forensic Server (WFS): It uses the Kali Linux operating system and runs Kismet application as a wireless intrusion detection system (WIDS) server. The Kismet server receives, categorises and analyses the information sent by Pi-drones. The server lists the wireless access points (APs) based on the service set identifiers (SSIDs) and their associated Media Access Control (MAC) addresses. Moreover, it also presents all clients including clients' MAC addresses connected to the same SSID (Kismetwireless, 2019). WFS server hosted a database which stores all the legitimate APs and clients' MAC addresses. The server will then forward all the logs with different information (e.g. timestamps, clients' MAC address, brute force attack timestamps). WFS can identify different brute force attacks on the wireless client as soon as it detects the attacks. In addition, the source code of Kismet can be modified to add new capabilities to detect different wireless attacks. Then, all the information will be forwarded to the Syslog server for further investigation.

Remote Authentication Dial-In User Service (RADIUS) Server: The main purpose of a RADIUS server is to provide the authentication service for user's network connection requests and return appropriate configuration information, accordingly. By using a Microsoft Windows Server 2008R2 for RADIUS server, RADIUS controls devices and user's authentication based on the username and password stored on the Domain Controller server. In this proposed DFR Framework, all the information and log (including username, timestamp, client MAC address) of the RADIUS server will be forwarded to the Syslog server as soon as a wireless client is successfully or unsuccessfully connected to the legitimate AP.

Access Point Controller (Unifi controller): A Microsoft Windows Server 2008R2 hosts the UniFi Controller software. This software controls and monitors all the Unifi APs on the network, decides the SSID on each APs based on different VLAN. It also monitors clients connected to each APs and SSIDs. In this proposed DFR Framework, the server will forward all the logs (e.g. AP MAC address a client connected to, timestamp, and client MAC address) to the Syslog server.

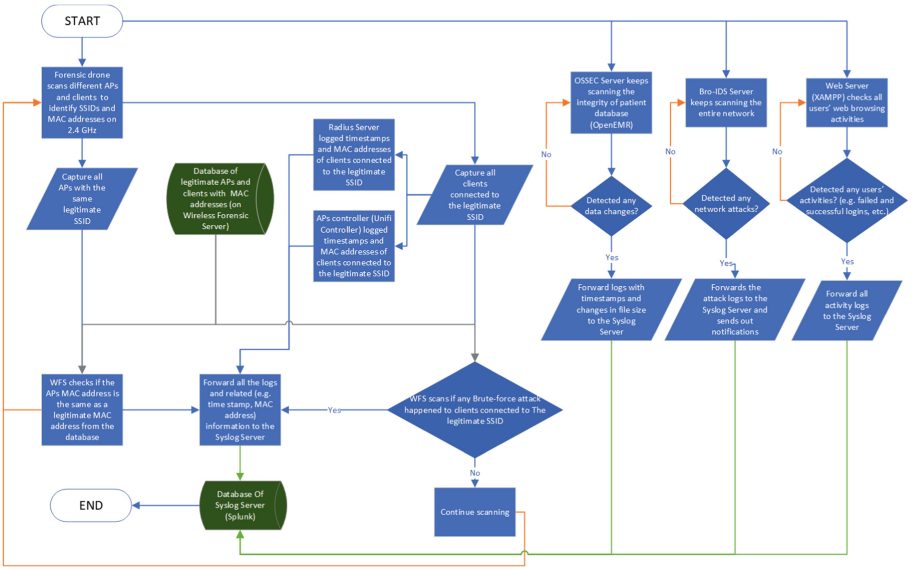


Fig. 3. Digital forensic readiness framework for WMedSys

Integrity Checking/Hashing Server (OSSEC) Server: OSSEC is a widely used scalable open-source application for the Host-based Intrusion Detection System (HIDS), which can run on different operating system platforms. It provides extensive features such as file integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response. The security requirements can be tailored through configuration options and customised rules can be added. For example, OSSEC scripts can be written to perform actions responding to security alerts. In addition, the source code of OSSEC can be modified to add new capabilities. In this proposed DFR Framework, OSSEC is used to check the integrity of the patient's database (need to specify where that database is located, e.g. OpenEMR runs on which machine). Any change in patient-related data will be logged. Those logs comprise of timestamps, hash values, and changes in file sizes. Then, all information is configured to be forwarded to the Syslog server.

IDS Server (Bro-IDS): The IDS server runs Bro-IDS on top of Ubuntu OS. Bro-IDS is a passive, open-source network traffic analyser. Its primary function is to provide security monitoring and inspection of all traffic for signs of suspicious activity. Furthermore, it supports various traffic analysis tasks including performance measurements and helping with trouble-shooting (Zeek, 2019). In this proposed DFR Framework, Bro-IDS continues scanning the entire network to identify any attacks on the network such as a Distributed Denial-of-Service (DDoS) attack, and network scanning. All the information collected by the server will be forwarded to the Syslog server.

Web Server (XAMPP): It is a compilation of free software (comparable to a Linux distribution) (Apachefriends, 2019). XAMPP provides a web server platform which

allows the hosting of any website or web service in low cost. This server hosts OpenEMR which provides patient related electronic medical records (OpenEMR, 2018) and provides a platform for users to use a different function from OpenEMR. In this proposed DFR Framework, all the users' activities (e.g. user success and failure logins, setting changes, and timestamp) will be logged by XAMPP and then forwarded to the Syslog server.

Syslog Server (Splunk): Splunk is a commercial software which is designed to collect and analysed data from different devices, and software on the network system. The Splunk server will be run on a Windows Server 2008R2 and in this proposed DFR Framework, this server will collect all the logs and information from different components of the framework. This server allows the forensic investigator to select a specific timestamp and create a report including detailed information from all servers in the network. It also supports search functions to help the forensic investigator to search specific information.

5 Evaluation of DFR Framework Artefact

The proposed artefact was evaluated by the subjective method (i.e. by a group of experts).

5.1 Preparation for Evaluation

Based on the evaluation criteria, 18 questions were created and provided to all experts with the proposed framework artefact, descriptions of all system components' functions and supplement reading of related material. In order to thoroughly evaluate the proposed artefact, the following six experts from related fields with exclusive knowledge and work experience were selected and requested to conduct the evaluation of the proposed artefact against the suggested evaluation criteria [48].

5.2 Evaluation of the Artefact

The following group of experts participated in the artefact evaluation.

Expert 1 has specialised in areas such as Health Information Technology (HIT), Wireless Networks, Internet of Things (IoT), and Software Defined Networks (SDN) for more than 25 years. He was a researcher and the head of the management section of Ministry of Science and Technology, Iraq. Currently, he is a senior academic staff member of an Institute of Technology in New Zealand as well as being a certified instructor of Cisco Networking Academy for 14 years.

Expert 2 has been a senior field service engineer for GE Healthcare and Siemens Private Limited (Pte. Ltd) specialising in medical equipment including X-Ray systems, Digital Mammography, Digital Angiography, Computed Tomography (CT) and Magnetic Resonance Imaging (MRI) systems for more than 19 years in the Healthcare Industry.

Expert 3 has extensive knowledge and work experience as a digital forensic investigator and a researcher of more than 7 years. He has also been a lecturer in Information Security, Risk Management, Microsoft Windows Servers based Networks at both graduate and post-graduate level for more than 4 years. Moreover, Expert 3 has published and presented several research papers closely related to the new emerging research areas in Digital Forensics and Network Security at internationally well-recognised conferences and journals.

Expert 4 has more than seven year experience as a Digital Forensic Analyst in the IT Industry. He has worked on hundreds of investigations looking for electronic evidence on a wide range of devices including computers, mobile devices, global positioning system (GPS) units, and other storage devices. For the last two years, Expert 4 has worked as a Penetration Tester, working on a number of security reviews, including web application reviews, mobile application testing and hardware reviews of embedded devices. He has also written a Master's thesis on forensic data collection of Apple iPhones and recently presented a number of disclosed vulnerabilities found in modern routers.

Expert 5 specialises in wireless networks and security, cloud computing, network architectures and protocols and SDN. He is an assistant professor and also a reviewer for many prestige international journals and conferences. Expert 5 used to work as a head of telecommunications and computer networks group for a university.

Expert 6 has extensive experience in Medical Information Systems, Digital Forensics, Cyber Security, Risk Management and Standards of more than 20 years. He is not only a full-professor at a University in New Zealand, but also has been a negotiator representing New Zealand in the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) for 14 years. Moreover, he is a board member of Information Systems Audit and Control Association (ISACA, Auckland Chapter).

6 Findings and Discussions

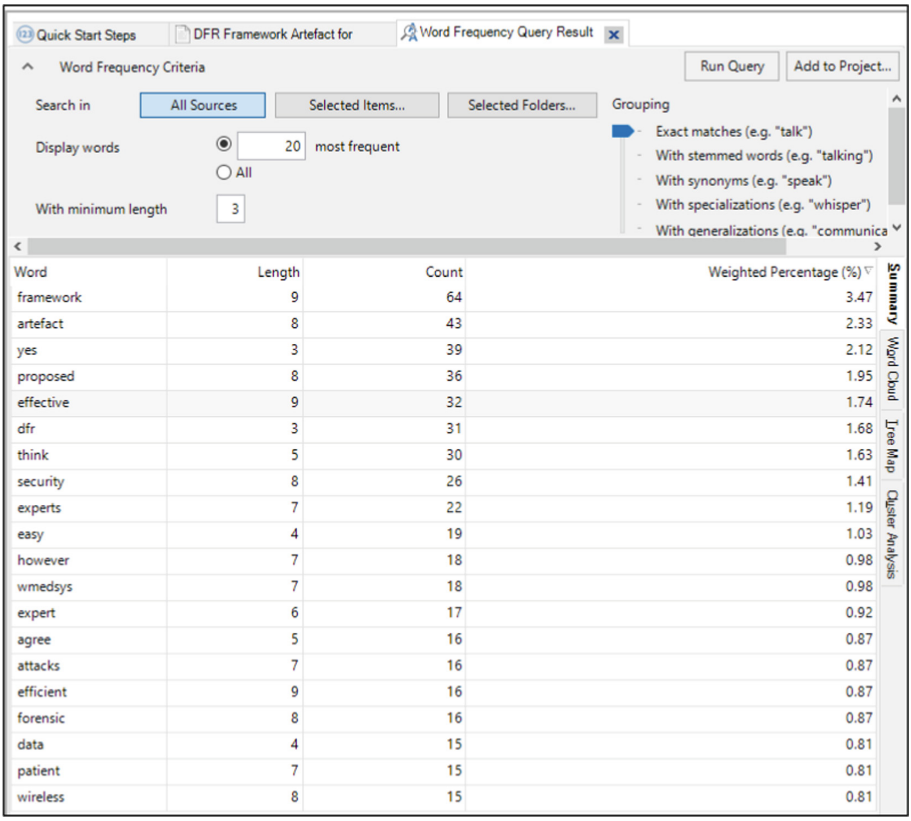
The evaluated artefact is further analysed using a thematical approach in NVIVO. Thematic analysis is a commonly used approach in conducting qualitative data analysis in DS research. Qualitative methodologies aim to explore complex phenomena [48]. They accept multiple realities and have a commitment to identifying an approach to in-depth understanding of the phenomena, a commitment to participants' viewpoints, conducting inquiries with the minimum disruption to the natural context of the phenomenon, and reporting findings in a literary style rich in participant commentaries. Thematic analysis is a process for encoding qualitative information [49]. This type of analysis looks mainly at "what and how" the data say and aims at identifying patterns within the data.

Feedback received from expert evaluations, a central theme was established first which is the DFR framework. The central theme is then categorised into three areas for further analysis against evaluation criteria discussed in Sect. 3 in three system dimensions, which are "Goal", "Environment" and "Structure/Activity". "Goal" is to analyse whether or not the DFR framework has achieved its design goal. "Environment" is to

analyse whether or not the DFR framework has been consistent with an organization and its people. "Structure/Activity" is to analyse the artefact's dynamic of operations and its functionalities. Each of these three areas is divided into smaller areas of prospects for in-depth analysis. For example, "Goal" is divided into two smaller areas of prospects of "Efficacy" and "Validity". "Environment" is divided into two smaller areas of prospects of "Consistency with organization" and "Consistency with people". "Consistency with people" is then classified into "Utility", "Understandability" and "Ease of use". "Activity" is divided to "Completeness".

6.1 Word Frequency Analysis Results

Word frequency queries in NVIVO provides researchers with a list of the most frequently occurring words or concepts of referenced material. This can help the researcher in not only identifying possible themes, particularly in the early stages of the project; but also finding the most frequent words occurring in a particular referenced material. Figures 4 and 5 show top 20 most frequent exact word matches and stemmed word matches.

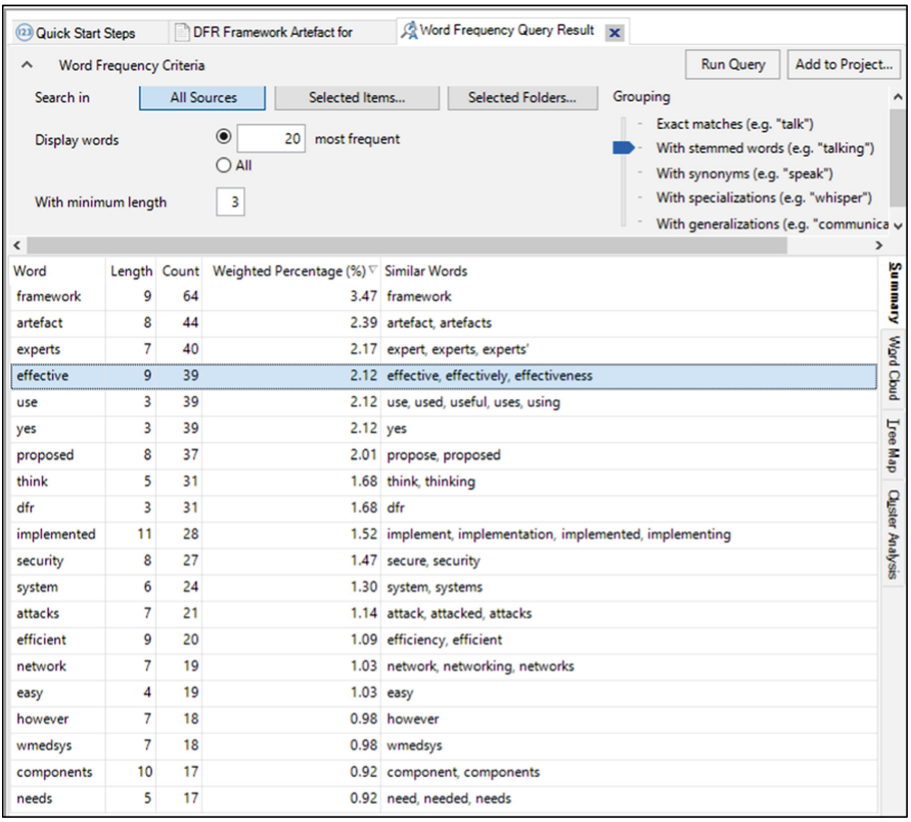


Word	Length	Count	Weighted Percentage (%)
framework	9	64	3.47
artefact	8	43	2.33
yes	3	39	2.12
proposed	8	36	1.95
effective	9	32	1.74
dfr	3	31	1.68
think	5	30	1.63
security	8	26	1.41
experts	7	22	1.19
easy	4	19	1.03
however	7	18	0.98
wmedsys	7	18	0.98
expert	6	17	0.92
agree	5	16	0.87
attacks	7	16	0.87
efficient	9	16	0.87
forensic	8	16	0.87
data	4	15	0.81
patient	7	15	0.81
wireless	8	15	0.81

Fig. 4. Top 20 most frequent exact word matches

Comparison is made after running both features to provide more in-depth and broad analysis. Noticeably, "effective" goes up to fourth place on the stemmed word match table (see Fig. 5) from the fifth place on exact word match table (see Fig. 4). Also, "implemented" has gone up. This is consistent with overall experts' comments that emphasize implementing the artefact. Moreover, "use/useful", "efficient/efficiency" and "easy" are also at the top of the table. Thus, analysis shows that experts agree that the proposed DFR framework is "effective", "efficient", "useful" and "easy" to implement and utilise.

After conducting the "word frequency query", a "text search query" is used to understand the meaning of these most frequently appearing words in the content. This can provide the researcher with better understanding of the implication and interpretation of these words in context and with a more meaningful context for reasoning. Based on the results provided from "word frequency query" and evaluation criteria in Sect. 3, the following words are used, which are "effective", "efficient", "useful", "strength", "weakness", "easy", "security", "safety" and "evidence" showed in Figs. 6, 7, 8, 9, 10, 11, 12, 13 and 14 (see Appendix).



Word	Length	Count	Weighted Percentage (%)	Similar Words
framework	9	64	3.47	framework
artefact	8	44	2.39	artefact, artefacts
experts	7	40	2.17	expert, experts, experts'
effective	9	39	2.12	effective, effectively, effectiveness
use	3	39	2.12	use, used, useful, uses, using
yes	3	39	2.12	yes
proposed	8	37	2.01	propose, proposed
think	5	31	1.68	think, thinking
dfr	3	31	1.68	dfr
implemented	11	28	1.52	implement, implementation, implemented, implementing
security	8	27	1.47	secure, security
system	6	24	1.30	system, systems
attacks	7	21	1.14	attack, attacked, attacks
efficient	9	20	1.09	efficiency, efficient
network	7	19	1.03	network, networking, networks
easy	4	19	1.03	easy
however	7	18	0.98	however
wmedsys	7	18	0.98	wmedsys
components	10	17	0.92	component, components
needs	5	17	0.92	need, needed, needs

Fig. 5. Top 20 most frequent stemmed word matches

Since the goal of this research is to design and develop a cost-effective DFR framework; hence, "effective" and "efficient" are essential characteristics to evaluate whether or not a such goal has been achieved. The analysis result shows that most of these expert feedbacks provides very positive comments. Thus, the artefact is considered as "effective" and "efficient" in preserving digital "evidence". Consequently, the goal of the study has been achieved. In addition, the artefact is considered as "useful" and realistic in improving and addressing patient "safety" and overall medical system "security" in health clinical environment against attacks. Thus, patient safety is protected and ensured. Additionally, according to the experts, the artefact is easy to implement, understand and use. "strength" and "weakness" analysis show that the proposed DFR framework design is suitable for security risk coverage, has several benefits of "easy" implementation, "easy" to use, low cost resources, and competitive prices. It can also access HL7 and DICOM format. However, the proposed framework does not consider 5 GHz and residual risk management. Otherwise, all experts agree the proposed framework is good in preserving digital evidence and recommend integrating the DFR framework into existing networks in a controlled laboratory environment to prove the concept.

7 Conclusion

The main contribution of this research is to present a novel conceptual design of a DFR framework for WMedSys, which can be easily implemented and integratedlxd to existing wireless networks in the healthcare sector. Thematic expert evaluation analysis shows that the proposed artefact is efficient and effective in providing better security for patient safety. The proposed artefact uses Pi-drones to collect any user's successful and unsuccessful wireless login attempts to WMedSys and forward them to a centralised logging system in order to preserve digital forensic evidence. In addition, it has low resource requirements, is cost-effective and provides customisation benefits by adapting free open-source software. Hence, it is suitable for security risk coverage. Nevertheless, it also has several limitations. Although experts believe that the proposed framework is only designed for WMedSys in 2.4 GHz band, the proposed framework can easily be applied to both 2.4 GHz and 5 GHz by replacing the hardware of the Pi-drone. For future study, experts suggest that the proposed DFR framework needs to be implemented and tested in a controlled laboratory environment to prove this conceptual design of a DFR framework for WMedSys.

Appendix

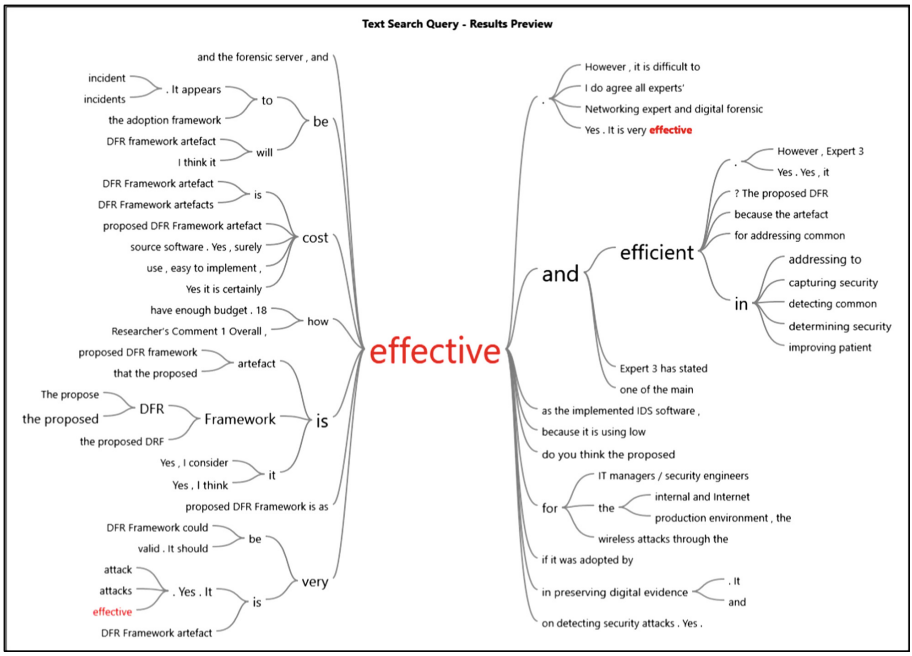


Fig. 6. Text search query result for "effective"

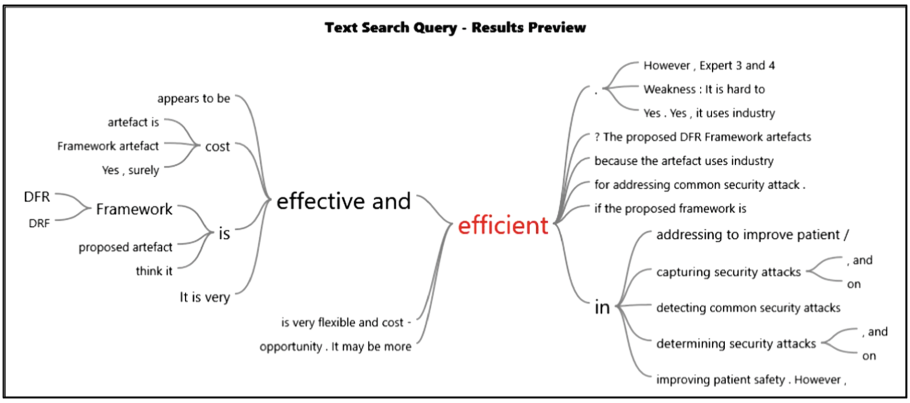


Fig. 7. Text search query result for "efficient"

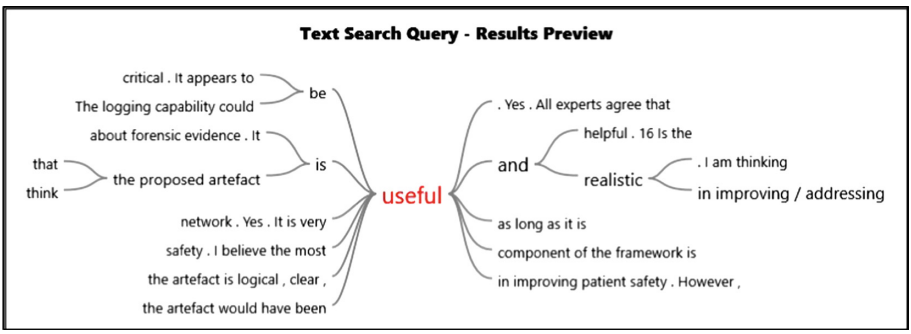


Fig. 8. Text search query result for "useful"

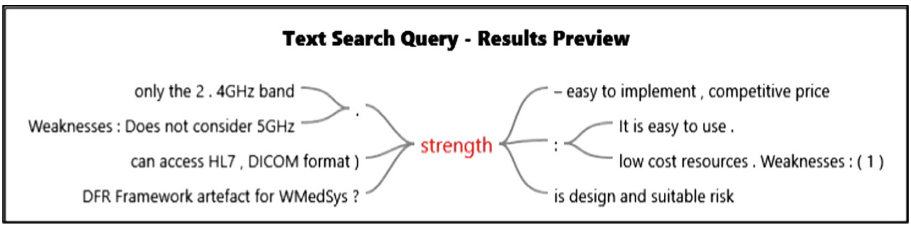


Fig. 9. Text search query result for "strength"

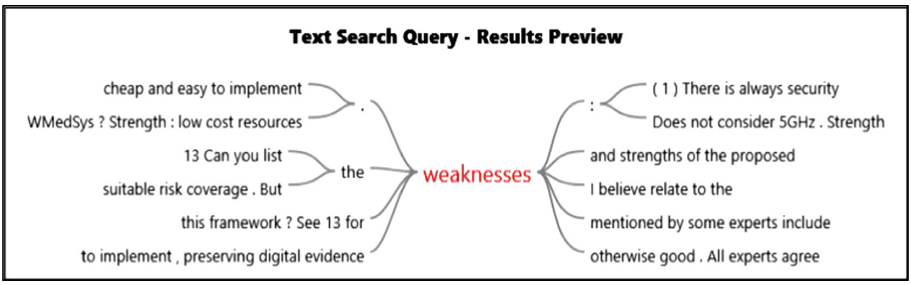


Fig. 10. Text search query result for "weakness"

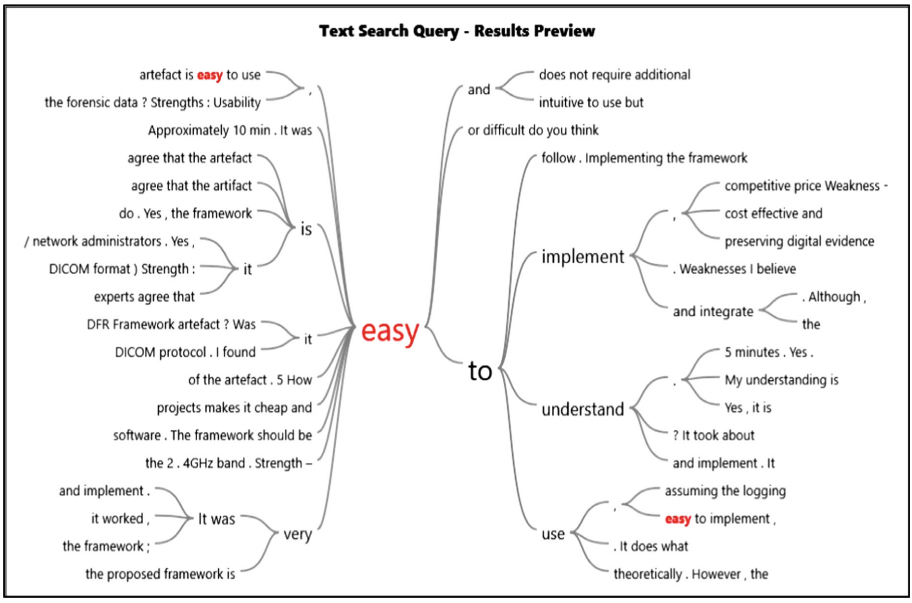


Fig. 11. Text search query result for "easy"

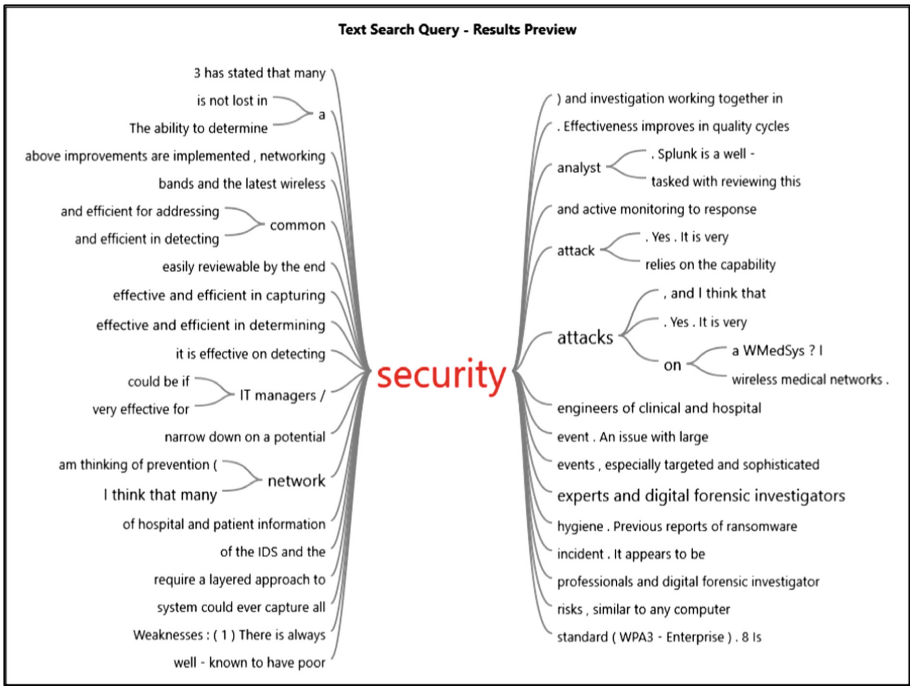


Fig. 12. Text search query result for "security"

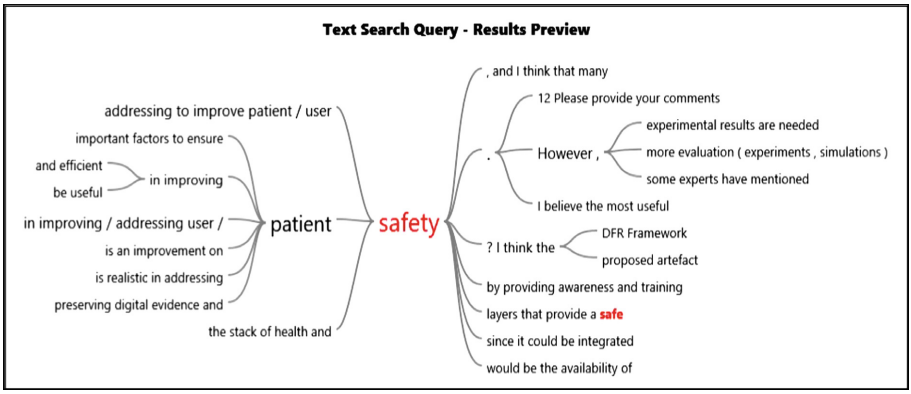


Fig. 13. Text search query result for "safety"

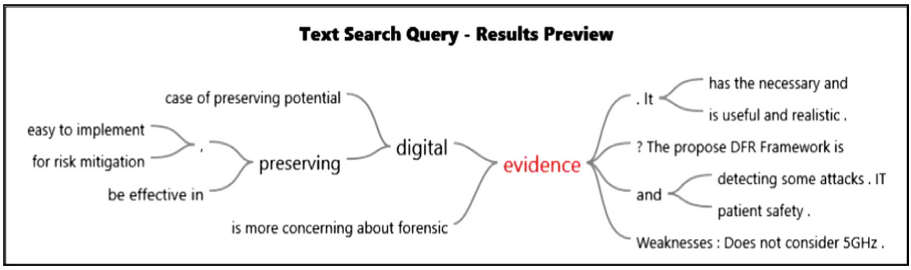


Fig. 14. Text search query result for "evidence"

References

1. Baldoni, R., Montanari, L.: Italian Cyber Security Report 2015 - A national framework. Capienza Università di Roma and CINI Cyber Security National Lab, Roma (2016)
2. Brownlee, N., Guttman, E.: Expectations for Computer Security Incident Response. The Internet Society, Reston (1998)
3. Reggiani, M.: A brief introduction to Forensic Readiness (2016). http://resources.infosecinstitute.com/a-brief-introduction-to-forensic-readiness/#gref. Accessed 13 Mar 2019
4. Napier, J.: NICS forensic readiness guidelines (2011). http://studyres.com/download/4392801. Accessed 14 Mar 2019
5. Quinn, S.: Hospital pays $55,000 ransom; no patient data stolen (2018). http://www.greenfieldreporter.com/2018/01/16/01162018dr_hancock_health_pays_ransom/. Accessed 14 Mar 2019
6. Ehlinger, S.: Former employee reportedly steals mental health data on 28,434 Bexar County patients (2017). https://www.expressnews.com/business/local/article/Former-employee-reportedly-steals-mental-health-12405113.php. Accessed 14 Mar 2019
7. Halperin, D., et al.: Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In: IEEE Symposium on Security and Privacy, Oakland (2008)

8. Radcliffe, J.: Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System (2011). https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf. Accessed 14 Mar 2019
9. Li, C., Zhang, M., Raghunathan, A., Jha, N.K.: Attacking and defending a diabetes therapy system. In: Burleson, W., Carrara, S. (eds.) Security and Privacy for Implantable Medical Devices, pp. 175–193. Springer, New York (2014). https://doi.org/10.1007/978-1-4614-1674-6_8
10. Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., Fu, K.: They can hear your heartbeats: non-invasive security for implantable medical devices. In: ACM SIGCOMM 2011 Conference, New York, NY (2011)
11. Clark, S.S., Fu, K.: Recent results in computer security for medical devices. In: Nikita, K.S., Lin, J.C., Fotiadis, D.I., Arredondo Waldmeyer, M.-T. (eds.) MobiHealth 2011. LNICST, vol. 83, pp. 111–118. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29734-2_16
12. Burleson, W., Clark, S.S., Ransford, B., Fu, K.: Design challenges for secure implantable medical devices. In: 49th ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco (2012)
13. Hermans, J., Tinholt, H.W., de Wit, J.: Achieving digital forensic readiness (2015). https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/Achieving-Digital-Forensic-Readiness-12-9-2015.pdf. Accessed 13 Mar 2019
14. Alenezi, A., Hussein, R.K., Walters, R.J., Wills, G.J.: A framework for cloud forensic readiness in organizations. In: 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), San Francisco (2017)
15. Rahman, N.H., Glisson, W.B., Yang, Y., Choo, K.K.: Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Comput. **1**(3), 50–59 (2016)
16. Raju, B.K., Geethakumari, G.: An advanced forensic readiness model for the cloud environment. In: International Conference on Computing, Communication and Automation (ICCCA), Noida, India (2016)
17. De Marco, L., Ferrucci, F., Kechadi, M.: Reference architecture for a cloud forensic readiness system. In: EAI Endorsed Transactions on Security and Safety, pp. 1–9 (2014)
18. Kebande, V.R., Venter, H.S.: A cloud forensic readiness model using a Botnet as a Service. In: International Conference on Digital Security and Forensics (DigitalSec2014), Ostrava, Czech Republic (2014)
19. Harbawi, M., Varol, A.: An improved digital evidence acquisition model for the Internet of Things forensic I: a theoretical framework. In: 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania (2017)
20. Endicott-Popovsky, B., Frincke, D.A., Taylor, C.A.: A theoretical framework for organizational network forensic readiness. J. Comput. **2**(3), 1–11 (2007)
21. Kebande, V.R., Karie, N.M., Venter, H.S.: A generic digital forensic readiness model for BYOD using honeypot technology. In: IST-Africa Week Conference, Durban, South Africa (2016)
22. Kebande, V.R., Karie, N.M., Omeleze, S.: A mobile forensic readiness model aimed at minimising cyber bullying. Int. J. Comput. Appl. **140**(1), 28–33 (2016)
23. Barske, D., Stander, A., Jordaan, J.: A digital forensic readiness framework for South African SME's. In: Information Security for South Africa (ISSA), Sandton, Johannesburg, South Africa (2010)
24. Ngobeni, S., Venter, H., Burke, I.: A forensic readiness model for wireless networks. In: Chow, K.-P., Shenoi, S. (eds.) DigitalForensics 2010. IFIPAICT, vol. 337, pp. 107–117. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-15506-2_8

25. Rahman, A.F.A., Ahmad, R., Ramli, S.N.: Forensic readiness for wireless body area network (WBAN) system. In: 16th International Conference on Advanced Communication Technology, Pyeongchang (2014)
26. Cusack, B., Kyaw, A.K.: Forensic readiness for wireless medical systems. In: 10th Australian Digital Forensics Conference, Perth, Western Australia (2012)
27. Ieong, R.S.C.: FORZA – digital forensics investigation framework that incorporate legal issues. Digit. Invest. **3S**, S29–S36 (2006)
28. Reggiani, M.: A brief introduction to Forensic Readiness (2016). https://resources.infosecinstitute.com/a-brief-introduction-to-forensic-readiness/#gref. Accessed 14 Mar 2019
29. Kent, K., Chevalier, S., Grance, T., Dang, H.: NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology, Gaithersburg (2006)
30. Given, L.: The SAGE Encyclopaedia of Qualitative Research Methods. SAGE Publications, London (2008)
31. Kebande, V.R., Venter, H.S.: A functional architecture for cloud forensic readiness large-scale potential evidence analysis. In: 4th European Conference on Cyber Warfare and Security (ECCWS), Hertfordshire, Hatfield (2015)
32. Grobler, C.P., Louwrens, C.P.: Digital forensic readiness as a component of information security best practice. In: Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (eds.) SEC 2007. IIFIP, vol. 232, pp. 13–24. Springer, Boston, MA (2007). https://doi.org/10.1007/978-0-387-72367-9_2
33. Rowlingson, R.: A ten step process for forensic readiness. Int. J. Digit. Evid. **2**(3), 1–28 (2004)
34. Sule, D.: Importance of forensic readiness. ISACA J. **1**(2014), 1–5 (2014)
35. CYFOR: Specialists in Organisational Forensic Readiness Planning and Implementation (2018). http://cyfor.co.uk/digital-forensics/forensic-readiness-planning/. Accessed 13 Mar 2019
36. Makutsoane, M.P., Leonard, A.: A conceptual framework to determine the digital forensic readiness of a Cloud Service Provider. In: Portland International Conference on Management of Engineering & Technology (PICMET), Kanazawa, Japan (2014)
37. Reddy, K., Venter, H.: A forensic framework for handling information privacy incidents. In: Peterson, G., Shenoi, S. (eds.) DigitalForensics 2009. IFIPAICT, vol. 306, pp. 143–155. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04155-6_11
38. Mouhtaropoulos, A., Dimotikalis, P., Li, C.T.: Applying a digital forensic readiness framework: three case studies. In: IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA (2013)
39. Kebande, V.R., Ntsamo, H.S., Venter, H.S.: Towards a prototype for achieving digital forensic readiness in the cloud using a distributed NMB solution. In: 15th European Conference on Cyber Warfare and Security (ECCWS), Munich (2016)
40. Kebande, V.R., Venter, H.S.: Requirements for achieving digital forensic readiness in the cloud environment using an NMB solution. In: 11th International Conference on Cyber Warfare and Security, Boston (2016)
41. Mouhtaropoulos, A., Li, C.T., Grobler, M.: Digital forensic readiness: are we there yet? J. Int. Commer. Law Technol. **9**(3), 173–179 (2014)
42. Pooe, A., Labuschagne, L.: Cognitive approaches for digital forensic readiness planning. In: Peterson, G., Shenoi, S. (eds.) DigitalForensics 2013. IFIPAICT, vol. 410, pp. 53–66. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41148-9_4
43. Ngobeni, S.J., Venter, H.S.: The design of a wireless forensic readiness model (WFRM). In: Information Security South Africa Conference, Johannesburg, South Africa (2009)

44. Lalla, H., Flowerday, S., Sanyamahwe, T., Tarwireyi, P.: A log file digital forensic model. In: 8th International Conference on Digital Forensics (DF), Pretoria, South Africa (2012)
45. Alrajeh, D., Pasquale, L., Nuseibeh, B.: On evidence preservation requirements for forensic-ready systems. In: 11th Joint Meeting on Foundations of Software Engineering, Paderborn (2017)
46. Fleming, R.F.: Towards the analysis of information environment resilience for real enterprises (Doctoral thesis). The University of New South Wales, Canberra, Australia (2010)
47. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A design science research methodology for information systems research. J. Manag. Inf. Syst. **24**(3), 45–77 (2007)
48. Vaismoradi, M., Turunen, H., Bondas, T.: Content analysis and thematic analysis: implications for conducting a qualitative descriptive study. Nurs. Health Sci. **15**(1), 398–405 (2013)
49. Boyatzis, R.: Transforing Qualitative Information: Thematic Analysis and Code Development. SAGE Publications, Thousand Oaks (1998)