Open Source Tools for Digital Forensic Investigation: Capability, Reliability, Transparency and Legal Requirements

Isa Ismail[1,2], and Khairul Akram Zainol Ariffin[2*]
[1] Pharmacy Enforcement Division, Malaysia
[2] Center for Cyber Security, Universiti Kebangsaan Malaysia, Malaysia
[E-mail: p108044@siswa.ukm.edu.my, k.akram@ukm.edu.my]
* Corresponding author: Khairul Akram Zainol Ariffin

Received February 14, 2024; revised June 2, 2024; accepted July 26, 2024; published September 30, 2024

Abstract

Over the past decade, law enforcement organizations have been dealing with the development of cybercrime. To address this growing problem, law enforcement organizations apply various digital forensic (DF) tools and techniques to investigate crimes involving digital devices. This ensures that evidence is admissible in legal proceedings. Consequently, DF analysts may need to invest more in proprietary DF hardware and software to maintain the viability of the DF lab, which will burden budget-constrained organizations. As an alternative, the open source DF tool is considered a cost-saving option. However, the admissibility of digital evidence obtained from these tools has yet to be tested in courts, especially in Malaysia. Therefore, this study aimed to explore the admissibility of digital evidence obtained through open source DF tools. By reviewing the existing literature, the factors that affect the admissibility of the evidence produced by these tools in courts were identified. Further, based on the findings, a conceptual framework was developed to ensure the admissibility of the evidence so that it will be accepted in the court of law. This conceptual framework was formed to outline the factors affecting the admissibility of digital evidence from open source DF tools, which include; 1) The Availability and Capability of open source DF tools, 2) the Reliability and Integrity of the digital evidence obtained from open source DF tools, 3) the Transparency of the open source DF tools, and 4) the Lack of Reference and Standard of open source DF tools. This study provides valuable insights into the digital forensic field, and the conceptual framework can be used to integrate open source DF tools into digital forensic investigations.

Keywords: Digital forensic, tools, readiness, open source, conceptual framework, legal

http://doi.org/10.3837/tiis.2024.09.012 **ISSN : 1976-7277**

1. Introduction

Digital forensics (DF) is a relatively new field for Malaysian law enforcement agencies. The rise of digital-related crimes is a new challenge for these agencies to investigate and prosecute criminals. Cyber Security Malaysia (CSM) reported that there were 10,106 cyber-related incidents in Malaysia for the year 2020. The high number of cyber-related cases signifies the need for certified and trained DF first responders who are necessary to preserve and collect digital evidence at crime scenes. Then, this digital evidence will be analyzed in DF labs, and the results will be presented in the form of reports to be used by the relevant investigator and prosecutor.

The first edition of the Digital Forensics Research Workshop defines DF 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 to facilitate or further the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations [1]. This definition covers all aspects of DF methodology requirements to ensure digital evidence can be legally presented in a court of law.

The National Institute of Standards and Technology (NIST) defines digital forensics (DF) as applying a scientific methodology to identify, collect, examine, and analyze digital evidence while preserving integrity and maintaining a strict chain of custody of the data. Thus, DFs consist of four generic phases: i. Collection: The process of identifying, labelling, recording, and acquiring data from the investigated digital evidence while preserving the integrity of the data. ii. Examination: The process of forensically examining the collected data using both automated and manual methodologies to assess and extract data related to a case while preserving the integrity of the data. iii. Analysis: analyzing the data using legally proper procedures and techniques to derive relevant information that answers the questions that prompted collecting and examining digital evidence. iv. Reporting: The process of presenting the findings of an investigation, which may include describing the actions taken, explaining how tools and procedures were chosen, determining what additional actions are required, such as presenting digital forensic findings in court, and could also suggest making recommendations for improvements to policies, procedures, tools, and other aspects of the forensic process.

From the perspective of digital evidence, today, it is not limited to data retrieved from computers. Other digital devices that can store data, such as smartphones, cameras, USB flash drives, and network-related devices, are crucial digital evidence to be collected and secured at crime scenes. However, technological development over the past ten years has resulted in new challenges in the field of DFs. New technologies such as cryptocurrencies, Internet of Things (IoT) devices, and Big Data, which contain new sets of data, software, and hardware, will pose a problem that must be addressed by DF analysts [2]. Through this development, DF analysts need to further their knowledge to keep up and combat digital crimes.

DFs aim to comprehensively examine digital evidence to identify, retrieve, analyze, and present facts and opinions on the information gathered from the evidence. For this purpose, DFs utilize various specific DF tools and techniques to investigate digital crimes. The DF tools help DF analysts identify, collect, preserve, and examine digital evidence. These tools can be grouped into computer forensics, mobile device forensics, software forensics, and memory forensics.

DF analysts have long relied on specialized DF tools to acquire and analyze data from digital evidence. The study by Reedy [3] reported that the DF market is expected to grow from USD 4.62 billion in 2017 to USD 9.68 billion by 2022. The DF market's expected growth shows demand due to the rising trend of digital-related crime. Proprietary or commercial DF tools are primarily utilized in DF laboratories. Unfortunately, these proprietary tools are costly and usually require annual license renewal, burdening budget-constrained organizations. Alternatively, reliable open source DF tools are readily available for free and have seen an increase in their numbers and options in recent years. Over time, much debate has been regarding the advantages and disadvantages of proprietary and open source DF tools. This is especially true for the accuracy and performance of the tools used. Furthermore, the admissibility of digital evidence derived from the preservation, acquisition, or analysis of open source DF tools is still very vague worldwide, particularly in Malaysia.

Additionally, the cost of maintaining the DF lab will continually rise due to the increasing cost of DF tools owing to the complexity of developing new DF tools as one of the challenges facing DF experts in the future [4]. As new technologies emerge and existing technologies are updated, DF analysts may need to invest in new hardware and software to keep their lab up-to-date and maintain their ability to analyze and recover 65 digital evidences [5]. Therefore, the DF organization must adopt open source DF tools as an alternative to save costs and maintain operations.

The acceptance of open source DF tools in the court of law and the admissibility of digital evidence derived from these tools are yet to be fully explored. From the perspective of Malaysia, digital evidence results from proprietary tools such as EnCase are readily applied in any court of law due to well-documented and accepted methodologies and validations. In comparison, open source tools in the courts of law in Malaysia still need to be proven reliable and relevant. Therefore, this study aimed to identify the factors related to the admissibility of open source DF tools and outline a conceptual framework from these factors for the usage during investigations. The factors were identified through a systematic literature review (SLR) of DF tools. Three research questions were designed for the SLR:

- How capable are open-source DF tools compared with proprietary DF tools?
- What are the available open-source tools and frameworks that can facilitate the DF analysis?
- What are the legal requirements that affect the use of open-source DF tools?

The SLR was conducted to retrieve the studies from 2011 to 2022 and two databases available in Universiti Kebangsaan Malaysia: (1) Scopus and (2) Carian Bestari@UKM. The explanation of the overall systematic literature review process is highlighted in **Fig. 1**.

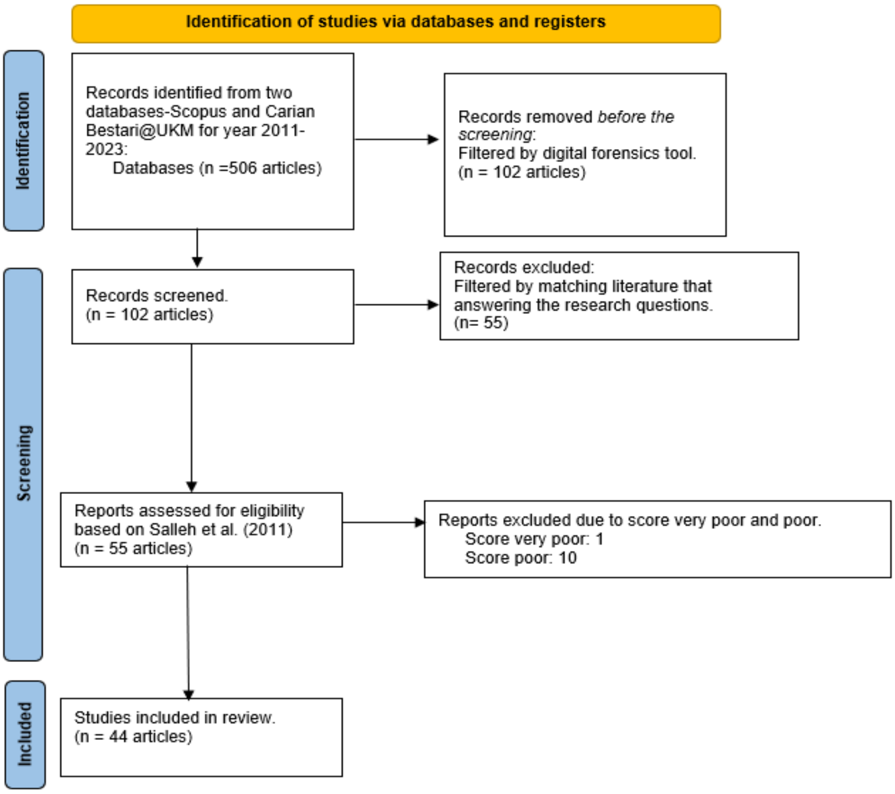
Identification of studies via databases and registers
Identification
Screening
Included
Records identified from two databases-Scopus and Carian Bestari@UKM for year 2011-2023:
Databases (n =506 articles)
Records removed *before the screening*:
Filtered by digital forensics tool.
(n = 102 articles)
Records screened.
(n = 102 articles)
Records excluded:
Filtered by matching literature that answering the research questions.
(n= 55)
Reports assessed for eligibility based on Salleh et al. (2011)
(n = 55 articles)
Reports excluded due to score very poor and poor.
Score very poor: 1
Score poor: 10
Studies included in review.
(n = 44 articles)

Fig. 1. PRISMA flowchart for systematic literature review.

The remainder of the paper is structured as follows: Section 2 highlights proprietary vs open-source digital forensic tools, and Section 3 describes the systematic literature review methodology. Section 4 outlines the result and discussion of the SLR, covering the research questions. Next is Section 5, which covers the reliability and integrity of digital evidence produced by open source DF tools. Section 6 discusses the transparency of the open source DF tool, while Section 7 outlines the lack of references and standards. Then, Section 8 proposes the conceptual framework and readiness for open source DF tools. Finally, conclusions are presented in Section 9.

2. Proprietary vs Open Source Digital Forensic Tools

Paid and licensed DF or proprietary tools were purchased from DF-related providers. Not only do these tools need to be purchased, but providers also usually charge a license renewal fee annually. Yearly, an incremental cost will burden DF agencies in continuing their operations and maintaining the investigative laboratory. The study by Lee et. al [6] listed several examples of proprietary tools and their cost in dollars, such as EnCase, a multi-function DF tool that Guidance Software developed, costs $2995, and Forensic Explorer, a multifunction DF tool that GetData developed, costs $1247.95.

In comparison, open source tools can be defined as free software that does not limit users' usage [7]. Wu et al. [8] outlined 62 different DF tools that were readily available. However, only 33 were open source DF tools, and most needed to be appropriately maintained after their development. Such open source DF tools include Autopsy, Sleuth Kit, Fiwalk, Bulk Extractor, and Foremost, which can be used in digital forensic investigations and present digital evidence in court [9]. Sonnekus et al. [10] conducted a study comparing open source DF tools with proprietary DF tools, involving the open source tools, Autopsy and SIFT and proprietary tools such as EnCase and FTK. Two hard disk samples were provided with Windows 7 and Linux OS, respectively. The result outlined that open source tools produce the same accuracy as proprietary tools. It also stated that the open source DF tool must be validated and verified in DF investigations. Additionally, Wu et al. [8] highlighted several risks involved in using open source DF tools, such as the lack of support, documentation and updates or safety features. The study showed that 33 open source tools needed to be more adequately commented on or had limited associated documentation to support their use. It also proposes a centralized repository specifically for the tested open source tools. The centralized repository contains compilations of results and data produced during DF investigation using open source DF tools. It can be a standard or reference for DF analysts to validate and verify their tools. The centralized repository provides DF analysts with documented and tested tools that the community can widely accept and validate.

Most of the studies that can be found show that the results between open source and proprietary tools demonstrate unique and variable capabilities and limitations. In addition, the DF analyst's strength and knowledge are essential in understanding the features and capabilities of each tool. However, many past and present studies have mainly focused on the problem of data accuracy but need more result validation tests and adherence to legal requirements.

3. Methodology

This review aimed to discern, assess, and discuss all available studies to answer research questions on open-source and proprietary digital forensic (DF) tools. Study documents such as journals, articles, conference papers, and other materials were collected and assessed based on Kitchenham [11] and Salleh et al. [12] methods.

It started by designing the research questions to thoroughly explore and discuss matters relating to open-source and proprietary digital forensic tools, such as (1) the capabilities of open-source DF tools when compared to proprietary DF tools, (2) the available open-source DF tools and frameworks in studies of overcoming current and future technology challenges, and (3) exploring the legal issues or other challenges related to the use of open-source DF tools. This review will finally identify any knowledge gap on this topic and propose a framework to solve the problem. Therefore, the following research questions were selected for this review:

- RQ 1: How capable are open-source DF tools compared to proprietary DF tools?
- RQ 2: What are the available open-source tools and frameworks that can facilitate the DF analysis?
- RQ 3: What legal requirements affect the use of open-source DF tools?

The search process for the study began by creating a combination of search strings to aid in the search for relevant literature through the following steps:

- Identifying primary keywords and terms used to address the research questions. The important keywords are ideas and subjects essential to defining a topic of interest. Identifying the correct keywords is critical to avoid any difficulty in searching for related literature in the SLR. Keywords were identified by correlating the main concepts of the research questions.

- List keywords from previously published articles. Searching previous studies will aid in listing the most used keywords. However, not all keywords in previous studies were beneficial to SLR. Therefore, it is crucial to filter out keywords unrelated to the subject matter and select the ones that best answer the research questions.
- Search for available synonyms and alternative keywords. Merrian-Webster [13] defines synonyms as one of several words or phrases from the same language with similar meanings. The incorrect use of synonyms may cause the search to be incorrect because of the change or broader meaning of the keyword. To avoid this problem, synonyms were searched using a thesaurus, a set of word databases to provide standardized synonyms.
- Boolean 'AND' was used to link primary keywords.
- Using the Boolean 'OR' in the search string to include alternative spellings and synonyms.

The following primary keywords were identified as relevant to the research question:

- Digital Forensic OR Digital Forensic Tools.
- Open-Source OR Freeware.
- Proprietary OR Commercial OR Licensed.

By considering all relevant keywords, a search in the databases was performed using the following search string:(Digital Forensic OR Digital Forensic Tools) AND ((Open-Source OR Freeware) OR (Proprietary OR Commercial OR Licensed)). According to Salleh et al. [12], multiple databases from different sources were used in the search to avoid bias in the review process. Two (2) online databases were used in the search process of existing studies to be scrutinized and reviewed. The online databases selected were Scopus and Carian Bestari@UKM. Both are reliable online databases of extensive scholarly studies, provided and subscribed by Universiti Kebangsaan Malaysia. The results of the search using the search string are summarized in **Table 1**.

Table 1. Summary of database search

Digital library	Years	Number of articles
Scopus	2011-2023	272
Carian Bestari@UKM		233

The results compiled in the search table include all relevant and non-relevant topics related to the research questions. The following inclusion and exclusion criteria were applied to narrow the relevant literature related to this review:

Inclusion criteria

- Scholarly publications match the search string.
- Scholarly publication from 2011 to 2023 (12-year period).
- Scholarly publications discussing research questions.

Exclusive criteria

- Scholarly publications are not subscribed to or provided by the UKM.
- Scholarly publications were not written in English.
- Articles not published and peer-reviewed, such as those from websites, magazines, and lecture notes.
- Evaluated scholarly publications that scored very poor (score= 0-2) or poor (score= 2-3) based on literature quality assessment.

To remain relevant to current and future issues, only studies published within 12 years, from 2011 to 2023, were selected for this review. Additionally, the studies collected must be related to the comparison between open-source and proprietary DF tools. Kitchenham [11] explains the importance of assessing the quality of reviewed studies. Therefore, in this review, the quality of the studies was evaluated and assessed using a checklist by Salleh et al. [12] and adapted to its reviewing process. The checklist consisted of seven (7) general questions to assess the quality of the literature. Using the following ratio scale: Yes=1, Probably=0.5, No=0; the score was tallied and resulted in the quality score for each study, which ranged from 0 (very poor) to 7 (very good). Each of the selected studies was evaluated using the evaluation process described above to aid data extraction. Studies that scored very poor (score = 0-1) or poor (2-3) were excluded, as they were deemed too low in quality to address the issues relating to this review process. The questions are as follows:

1. Was the article referred to by other scholars studying open source DF and proprietary DF tools?
2. Were the aim(s) of the study clearly stated? For example, to compare the advantages and disadvantages of open source DF tools to proprietary DF tools in terms of capabilities and legal aspects?
3. Were the study participants or observational units adequately described? For example, the type of DF tools, DF tools capabilities etc., used in the study.
4. Were the data collection carried out very well? For example, a discussion of procedures used for collection during a DF tool testing and how the study setting may have influenced the data collected.
5. Were potential confounders adequately controlled for the analysis? For example, type of digital evidence, operating system, workstation, etc.
6. Were the approach to the discussion and interpretation of the analysis well conveyed? For example, a description of the data comparing DF tools or the rationale for choosing a method/tool/sample in a DF tool experiment.
7. Were the findings credible? For example, the study was methodologically explained so that we can trust the findings; findings/conclusions are related to this study's objective of determining the admissibility of digital evidence from open source DF tools.

4. Result and Discussion

Through the search process, as shown in **Fig. 2**, multiple studies were found discussing matters relating to the application of open source and proprietary tools of interest. A total of 505 scholarly studies were screened and scrutinized during the search process, leaving 55 articles. These 55 articles were further narrowed down by filtering, screening related titles, and reading the abstracts. Finally, the quality of the literature was assessed, and inclusion and exclusion criteria were applied. During this phase, the first author (Ismail) was responsible for reading, extracting content, and evaluating each article based on the checklist. The findings from this exercise were then presented in a meeting for validation. Additionally, the second author reviewed the selected articles (55 articles) and compared the findings in the meeting. If there were any contradictions in the findings, but the difference remained at most 10-20 %, it was discussed until a consensus was reached. This practice aimed to reach an absolute consensus on the selected studies for this SLR.

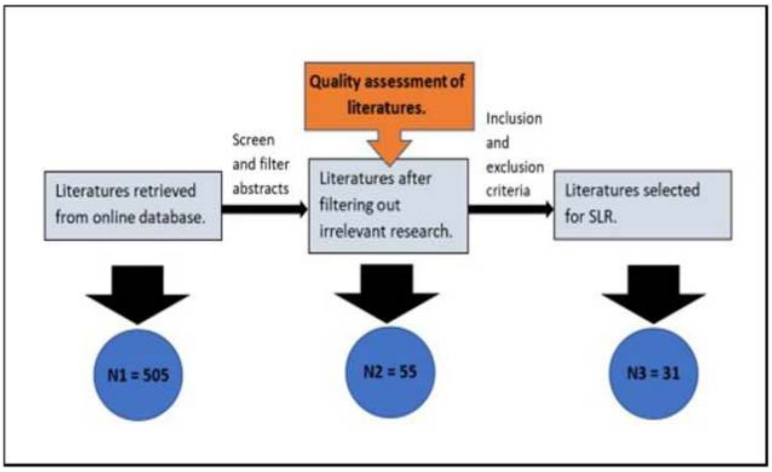
Quality assessment of literatures.
Screen and filter abstracts
Inclusion and exclusion criteria
Literatures retrieved from online database.
Literatures after filtering out irrelevant research.
Literatures selected for SLR.
N1 = 505
N2 = 55
N3 = 31

Fig. 2. Literature review process and result.

Table 2 shows the quality scores for all the primary studies after the meeting. From the initial filtering and validation, it was determined that 44 studies (80%) achieved above-average quality; 23 studies (42%), and 21 studies (38%) were deemed good and excellent quality, respectively. However, from the 39 studies that scored good to very good, eight (8) were removed from the analysis phase after applying the inclusion and exclusion criteria. In addition, 11 studies attained very poor to poor quality and were deemed unreliable. Thus, only 31 studies were included in the SLR.

Table 2. Quality score for articles

Quality score	0 – 3	3 – 4	4 – 6	6 - 7
Number of articles	1	10	23	21
Percentage	2%	18%	42%	38%

4.1 RQ1: How capable are open-source DF tools compared with proprietary DF tools?

This research question aims to determine the capability and reliability of open source DF tools compared to proprietary DF tools. Comparisons between open source and proprietary DF tools have been widely debated regarding accuracy, capabilities, functionality, and cost-effectiveness. The work by Agarwal et al. [14] described the basic process and procedure during the DF investigation. Three of the phases involve the usage of forensic tools, and it can be summarized as follows:

- Preservation: This phase focuses on creating an image from digital media while preserving the chain of custody.
- Collection: Data or information are extracted from the created image or digital media using an accepted method during this phase.
- Examination and Analysis: These phases involve an in-depth evaluation of the collected data to be reviewed and scrutinized by the analyst. Additionally, deleted, or hidden data are recovered from digital media, and data validation is performed by calculating the hash value of the acquired artefacts.

Through this review, it was found that the experimentation or focus of the studies pinpoints the capabilities of open source and proprietary tools during the process of preservation, collection, examination, and analysis. Seventeen studies specifically compared open source and licensed tools during the DF process, as highlighted in **Table 3**.

Table 3. Mapping studies to digital forensic process

Digital forensic process	Studies
Preservation	[10, 15, 16]
Collection	[10, 17-25]
Examination and Analysis	[10, 20, 21, 24, 26]

Eight (8) studies focused on the comparison of computer forensic tools [10, 15-17, 23-26], seven (7) on mobile forensics tools [18-22, 25, 27], and two (2) studies highlighted the challenges and advantages of open source tools over proprietary tools [28, 29]. While some studies compared more than one tool for each open source and proprietary tools, such as in Sonnekus [10] and Sharif et al. [26], others only choose to compare one tool to another [16, 18, 19]. There was a risk of bias because of the low sampling represented in the review if the studies were viewed individually. However, this SLR can better represent the population by comparing several studies using multiple sets of open source and proprietary tools in the existing studies.

Most studies shared a common objective in comparing these tools to several factors, such as cost, accuracy, capability, and efficiency. Studies by Leopard [23] and Cervellone et al. [24] highlight the cost of proprietary tools as a significant obstacle for law enforcement agencies. Cervellone et al. [24] specifically performed a cost analysis for each tool tested in the study. It was found that proprietary tools such as EnCase cost $8,284 per examiner, and FTK will cost upwards of $12,114. The open source tool SIFT Workstation 3.0 will cost $5979 to purchase FOR508 (online course) if needed, or it is free. Most law enforcement agencies have little or no budget to purchase and maintain yearly license renewals for these proprietary tools. Therefore, most of the literature reviewed recommended open source tools with zero to little cost as an alternative for DF investigations. However, to convince law enforcement agencies to use open source tools, most studies have aimed to demonstrate that they are comparable to their proprietary counterparts in accuracy, capability, and efficiency. Most of the reviewed studies showed that open source tools are accurate and reliable for acquiring images or data from digital media, as shown by Delgado et al. [15]. In addition, artefacts produced by open source tools are mainly similar to those produced by proprietary tools.

Even when some experiments showed less accuracy than the tested proprietary tool, the accuracy result of the tested open source tools was high enough to be considered for utilization in field investigations [16]. A study by Sharif et al. [26] demonstrated the accuracy of open source tools in their study by comparing Recuva, an open source tool, to three (3) other proprietary tools, which include Blade v1.9, Encase, FTK, and Recover My Files. The results from the experiment showed that Blade v1.9 was the most successful tool for recovering the deleted data (86.44 %). However, Recuva's open source tool showed a preferable result to the other proprietary tools (73.44 %). Delgado et al. [15] exemplified open source tools such as dd (Unix-like operating command) and EwfAcquire, which created an image from digital media similar to that of the proprietary tool EnCase. The results were validated by showing that all three (3) produced the same image with the calculated hash value.

Another critical factor to be considered is the capability or functionality of the open source DF tools. Adding features such as cloning, data recovery, hash calculator, and many others are crucial considerations in selecting a DF tool and its ease of use [10]. The studies by

Padmanabhan et al. [20] and Carvaja et al. [25] evaluated the capabilities of open source and proprietary tools to obtain digital evidence from Android smartphones. Both studies concluded that most features present in proprietary tools can also be found in open source tools.

In contrast, some studies state that proprietary DF tools have more functionalities than open source DF tools, such as the capability to automate certain functions, which reduces the processing time. However, some functionalities were also found to be lacking in these proprietary DF tools could be found in open source DF tools [10, 16, 17]. Some open source tools offer a multi-user environment and the option to utilize a GUI-based program or a command-line interface. Therefore, instead of selecting only one tool, combining proprietary and open source tools to complement one another in the DF investigation process is recommended. Also, it was found that open source tools can be used to acquire and collect digital evidence from several digital media (computers and smartphones) or different operating systems such as Windows, Linux and MacOS [10, 23].

Several studies have shown that open source tools have poorer efficiency in completing their processes than proprietary tools. Most of the tested proprietary tools demonstrated faster processing times than open source tools. The study by Himanshu et al. [16] highlighted that FTK has a faster processing time of 33 minutes to complete the data acquisition process compared to the 37 minutes taken by the open source tool Pro Discover. Although the difference in the experiment was only 4 min, it is theorized that with an increasing amount and size of data, the efficiency of the open source tool will be more affected when compared to proprietary tools.

The study by Roussey [28] addressed the scalability issue. Data scalability has been discussed as an issue faced by all the DF tools. Open source tools like TSK, Autopsy, and DFF were developed without addressing data scalability. The increasing size of the available hard disks containing terabytes of data could affect old and poorly maintained open source tools. Additionally, the cost of maintaining these open source tools could be increased significantly by acquiring custom components to develop the tool further.

A study by Patterson [29], however, argued for using open source tools by highlighting several advantages. The literature discusses that the open source tool gives users more control and freedom of use. The transparent nature of open source tools may lead to higher legal arguments reliability than the closed unknown codes of proprietary tools. It also found that updates for specific open source tools with solid community support are more frequent and readily available compared to the scheduled release of patches or updates for proprietary tools.

This review showed that through several studies compiled, open source tools are viable options, especially for budget-constrained law enforcement agencies. It demonstrated that open source tools have comparable accuracy and capability to other proprietary tools. However, the efficiency of these open source tools might be an issue, mainly because of data scalability, which can lengthen the overall workload. Therefore, law enforcement agencies must balance cost efficiency when determining which DF tools to use and implement in their DF investigations. Proper selection and use of both open source and proprietary tools are recommended, as both tools can complement one another to help balance the cost-effectiveness of the overall DF process.

4.2 RQ2: What are the available open-source tools and frameworks that could facilitate DF analysis?

This research question aims to demonstrate the availability of different types of open source tools for different DF investigations. By answering the research question, law enforcement agencies can choose and select open source tools for use in different situations. It has identified a list of multiple tools for all DF domains, such as computer, memory, mobile, digital image/photo, blockchain, and IoT DF investigations. It was found that 50% of the listed open source tools are used in computer forensics, followed by 20% for memory forensics, 14% for image forensics, 12% for mobile forensics and 2% each for blockchain and IoT forensics, as shown in **Fig. 3**.

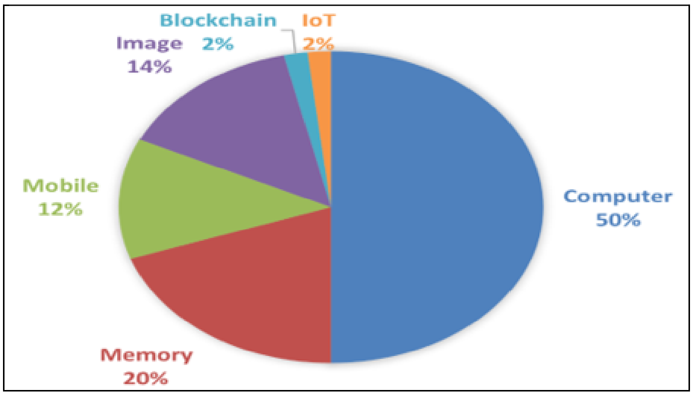

Fig. 3. Usage of open source tools in DF domains.

Statistics show plenty of options for computers, memory, images, and mobile open source forensic tools with capabilities and functions comparable to proprietary tools. All primary forensic phases during a DF investigation, such as preservation, collection, examination, and analysis, can be completed using one or combined with other open source tools.

Furthermore, most tools can be readily used and downloaded from multiple resources. Most of these tools can be found in GitHub, which is a renowned resource for open source software. Only three (3) of the listed tools (automated Python-based tool, Izitru, and TUX4N6) were not available for utilization, as there are no readily available resources. Himanshu et al. [16] stated that the ease with which open source tools can be found and readily used with zero upfront cost is one of its main advantages compared to proprietary tools. Studies on the availability of open source tools for blockchain and IoT forensics are lacking. The only studies on Blockchain and IoT open source tools were by Zollner et al. [30] and Clark et al. [31]. Both studies only cover a portion of Blockchain and IoT technology, as there is a multitude of blockchain currency and IoT devices available in the market today. In addition, no literature was found on open source tools for other newer technologies, such as big data, cloud, or artificial intelligence (AI). The list of tools can be grouped as follows:

Computer forensic

- dd (Unix Program): Create low-level image and conversion of raw data. [15]
- Ewfacquire: Create image data from various storage devices from floppy, Zip, memory card, or MP3 player. [26]
- Automated python-based tool: Automated image metadata analysis to detect coordinate and geolocation from images and Win 7 Recycle Bin analysis to analyze deleted files. [32]

- Paladin: A live Linux system based on Ubuntu that can be used to create forensic images. It also has write-blocker features. [10]
- SANS Investigative Forensic Toolkit: A forensic workstation with a suite of free and open-source incident response and forensic tools for DF investigations in multiple environments such as computer, memory, mobile and image forensics. [10, 20, 24]
- Enhanced Write Filter (EWF): A Linux-based tools that is used to create forensic images. [10]
- Sleuth Kit (TSK): A set of command-line tools and a C library for analyzing images and file recovery. Often used with Autopsy. It also covers memory, mobile and image forensics. [10, 17, 20, 28, 33]
- Autopsy: A DFs platform with a GUI used in conjunction with TSK and other DFs tools to analyze forensic images. It also covers memory, mobile and image forensics. [10, 33-35]
- Foremost: A console program used for data carving for Linux systems. [10,34]
- Scalpel: File carving for Linux and Mac operation systems. [10]
- RegRipper: Use to extract and analyze information such as keys, values, and data from the Window Registry. [10]
- HxD: A hex editor program used for data carving for the Windows system [10]
- Bless: A hex editor program used for data carving for the Linux system. [10]
- Digital Forensics Framework: A forensic workstation to collect, preserve and analyze digital evidence from Windows and Linux systems. Offer a GUI to aid the investigation. [8, 17, 25, 28]
- Live View: Creates a VMware virtual machine from a physical drive or a raw disc image. [17]
- Helix/ Helix3: Network analysis tool to use as live forensics, incident response and e-discovery from a bootable live CD. [17, 23]
- PyFlAG: A general forensic workstation for disk forensics, memory forensics and network forensics. It also covers memory forensics. [28]
- Open Computer Forensics Architecture (OCFA): An automated digital media analysis tool for the Linux System. [28]
- ProDiscover: An in-depth forensic workstation to collect, preserve, filter, and analyze digital evidence. [16]
- Browser History Viewer: A forensic program for extracting and analyzing internet history from web browsers (Chrome, Firefox, Internet Explorer, and Edge). [36]
- Wireshark: Widely used for network and malware analysis for Unix and Windows systems. [36]
- Cyboorg hawk Linux OS: Network analysis tool used to collect and analyze digital evidence. [37]
- Fiwalk: Collect, analyze, and recover deleted data from the disk image and integrate it into TSK. [34]
- Bulk extractor: Scans disk images, files, or a directory of files and extracts useful information to be further analyze by other tools. [34]
- Field Search: A live tool to conduct a fast and reliable search of the target's computers in the field. [35]
- TUX4N6: Automatically discover and grant read-only access to the suspect's computer's file systems, such as compressed files, media files and document files. [35]

Memory forensic

- memdump: Use to obtain volatile memory from Linux and Linux-based devices, such as Android-powered devices. [10]
- Dumpit: Provides a simple way to get a memory image of a Windows system. [10]
- ProcDump: Can be used to generate dump files that contain all the process memory of the Windows or Linux system. [10]
- Automated python-based tool: Automated image metadata analysis to detect coordinate and geolocation from images and Win 7 Recycle Bin analysis to analyze deleted files. [32]
- OSXPmem: It is used to acquire and collect data from the physical memory of the Mac operating system. [23]
- Win32dd: Use to dump physical memory to a file for Windows 2000 and Windows 7. [23]
- Nigilant32: Imaging RAM memory for Windows 2000, XP, and 2003. [23]
- Memoryze: Acquire and analyze memory images and live systems for Windows and Mac systems. [23]
- Computer Online Forensic Evidence Extractor (COFEE): A live tool that helps investigators collect data from a target computer. Contains tools for password decryption, Internet history recovery and other data extraction. [35]

Mobile forensic

- Andriller: A workstation with multiple forensic tools for the preservation and collection of data from smartphones. It is able to acquire data forensically from the Android system. [17, 25]
- AFLogical OSE: Mobile forensic tool to collect CallLog Calls, Contacts Phones, MMS messages, MMSParts, and SMS messages from Android devices. [21]
- SuperOneClick and BusyBox App: it is used in combination with wireless network analysis for Android devices. [38]
- Libimobiledevice: It is used to collect data from iDevices such as iphones, ipads and others. [22]

Image forensic

- FotoForensics: Web based digital picture analysis. Includes error level and metadata analysis. [39]
- JPEGsnoop: Use to investigate the origins of an image in order to determine its legitimacy. [39]
- Ghiro: An image forensic tool to search any analysis data, geolocation, administer users, and view all images in the system. It is able to analyze images in a huge number and can be automated. [39]
- Forensically: A web base image forensic tool which includes magnifying functions, clone detection, error level analysis, noise analysis, level sweep, and others. [39]
- Izitru: A web-based image forensic tool used to verify the authenticity of an image. [39]

Blockchain forensic

- Internet Evidence Finder (IEF) \& BTCscan: To locate and extract Bitcoin information, such as private or public key, address log or other traces of Bitcoins in a system. [30]

IoT forensic

- DRone OS Parser (DROP): Able to parse licensed DAT files extracted from the drone's non-volatile internal storage for further analysis. [36]

4.3 RQ3: What legal requirements affect the use of open-source DF tools?

One of the significant challenges for law authorities when considering open source tools is the related legal implications [22]. Hence, this research question aimed to identify the related legal factors and solutions to justify the use of the open source tool in DF investigations. It was found that ten studies conducted extensive research or discussed the legal argument for using open source tools [10, 15, 18, 20, 29, 40].

The first is the reliability of the open source tools used in the DF investigation. Wu et al. [8] and Sonnekus [10] stated that a reliable forensic tool should produce results that are accurate, repeatable, reproducible, and authentic for acceptance in any court of law. As discussed in RQ1, open source tools can be as reliable as proprietary tools in DF investigations because the reliability and capability of these tools are comparable with their proprietary counterparts. Most experiments comparing both tools showed acceptable accuracy, which can be repeated and reproduced using different tools. Additionally, Delgado et al. [15] showed that hash values can be used to calculate and compare the accuracy of results generated by open source tools.

Additionally, the issue relates to the integrity of the digital evidence from open source tools. Digital evidence should not be altered in any shape or form before, during, or after the investigation. Any changes in digital evidence could compromise the integrity of the evidence and its acceptance in court. The risk of open source tools compromising digital evidence has been highlighted by Ahmed et al. [22] and Leopard et al. [23]. It was shown that the open source tool, Libimobiledevice comprises three (3) files from the extracted data. In addition, the open source tool Helix3, in extracting data from physical memory, left 150mb of data residue during the operation, which could risk deleting previously stored data in the RAM.

Leopard et al. [23] also highlighted that proprietary tools may compromise digital evidence. Therefore, both sets of tools may pose a risk in maintaining the complete integrity of digital evidence during the DF investigation process. However, there is a lack of data in determining which tools may compromise the integrity or accuracy of digital evidence, as most of the literature is limited to one set of tools that cannot represent the entire set of other DF tools available today. The DF analyst can implement necessary steps and measures, such as tools or result validation and verification, to avoid the aforementioned problem.

Another issue concerns the transparency of DF tools. Delgado et al. [15] states that it is critical to determine whether forensic tools comply with the legal requirements determining evidence admissibility. Therefore, any forensic tool should be transparent, unbiased, and neutral during the DF investigation. open source tools have an advantage over proprietary tools in transparency, whereby the source code for open source tools can be readily available to scrutinize in court, compared to the close-guarded nature of proprietary tools [29]. The source code for the open source can be publicly viewed and altered by other experts. However, the security of open source tools comes into question, as any individual may intentionally or unintentionally alter the codes, which could affect the neutrality of the said open source tools [8].

Finally, using open source tools for DF investigations is an unproven process. In court proceedings, unproven scientific forensic techniques are heavily condemned [40]. Currently, there are no accepted or established guidelines for the use and testing of open source tools. As proprietary tools are well documented for criminal case investigations, the judiciary body is more accepting of them and has proven to be used in court proceedings. Charpentier et al. [35] is the only study to provide evidence of open source tool use during judiciary proceedings.

Two of the tested tools, Field Search and TUX4N6, have documented cases with convictions in the United States.

5. Reliability and Integrity of Digital Evidence produced by Open Source DF Tools

Reliability and integrity of digital evidence refers to the trustworthiness and accuracy of digital data collected and used as evidence in legal or investigative contexts. It refers to the consistency and dependability of digital evidence. Reliable digital evidence is evidence that has been properly collected and preserved, and that is not corrupted or altered. This means that digital evidence should remain unmodified and unchanged from when it was collected to when it is used as evidence [41]. Integrity refers to the completeness and accuracy of digital evidence. Digital evidence must be authentic and represent a true and accurate representation of the original data. This means that the digital evidence should not be tampered with or altered in any way and should provide a complete and accurate representation of the original data [42].

Reliability and integrity are critical considerations in digital forensics, as the accuracy and credibility of digital evidence can significantly impact the outcome of legal or investigative proceedings. To ensure the admissibility of digital evidence, the open source DF tool used while collecting, preserving, and analyzing digital evidence must be accurate without compromising the integrity of the digital evidence.

6. Transparency of Open Source DF Tools in DF Investigation

Transparency refers to the openness and accessibility of information about a digital forensic tool's design, implementation, and functioning. In the context of open source DF tools, transparency refers to the availability of the source code, documentation, and other information related to the tool [15].

Open source DF tools are digital forensic tools with publicly available source code, allowing anyone to view, use, modify, or distribute the code. This level of transparency makes it possible for digital forensic practitioners, researchers, and other stakeholders to understand exactly how the tool works, which can increase trust and confidence in the tool's results [7].

Further, it is an essential consideration in digital forensics, as it helps ensure that the methods and techniques used in a digital forensic investigation are transparent and open to scrutiny. It helps avoid potential biases or inaccuracies in the results and can increase the reliability and credibility of the digital evidence obtained. The advantage towards open source DF tools, such as Autopsy and ProDiscover, is that source code is readily available to be scrutinized without bias. Contrast to their proprietary counterpart, whereby the source code of the tools is often a closely guarded business secret [10]. Additionally, the documentation must clearly explain and detail the tools' functionality.

The transparency of the documentation of these open source DF tools also demonstrates the update frequency and available technical support for the tools. As with other open source software, the updates and technical support for open source DF tools are mostly community-driven. Most documentation and support could be retrieved from GitHub and other public forums. Wu et al. [8] stated that open source DF tools often lack proper support, documentation and safety updates to the software. Therefore, it is integral to the DF investigation to properly review the open source DF tools documentation to determine the selection and tool validation.

7. Lack of Reference and Standard relating to the Use of DF Tools in DF Investigation

The lack of references and standards relating to open source DF tools can potentially challenge DFs. The absence of well-established and widely recognized guidelines and best practices for the use of open source DF tools may make it difficult for DF analysts to determine the most appropriate tool to use for a specific investigation and to determine the reliability and validity of the results obtained to be presented in court [40]. These challenges can significantly impact the credibility and reliability of the results obtained using open source DF tools. For example, the absence of established protocols and methodologies can make it difficult for DF analysts to ensure that the results obtained are accurate and that the evidence obtained is admissible in a court of law. Thus, specific legal and technical standards must be met for digital evidence to be admissible in a court of law. Taylor et al. [43] discussed the five (5) general rules of evidence that determine the admissibility of digital evidence:

- Relevance: Evidence must be relevant to the facts of the case in order to be admissible. The evidence must directly affect the litigated issue and help prove or disprove a fact in dispute.
- Authenticity: Evidence must be authentic to be admissible where it must be outlined to be what it purports to be and must not have been altered or tampered with.
- Completeness: Evidence must be complete to be admissible, provide a full and accurate picture of the facts of the case, and not be misleading in any way.
- Reliability: Evidence must be reliable where it must have been collected, preserved, and processed to ensure its accuracy and integrity and that the methods used to collect and analyze the evidence are reliable and trustworthy.
- Credibility: Evidence must be credible to support a reasonable belief or conclusion and must not be based on speculation, conjecture, or unreliable sources.

The rules of evidence are a set of legal principles that dictate what evidence is admissible in a court of law. These rules ensure that the evidence presented in court is reliable, relevant, and credible and that the legal process is fair to all parties involved. These rules of evidence are essential because they help to ensure that the legal process is fair and that decisions are based on the best and most trustworthy evidence available. They also protect the rights of all parties involved and ensure that the legal system operates efficiently and effectively [44].

In the Malaysian judiciary system, there is yet an acceptable reference or standard relating to using the open source DF tool to produce admissible evidence. Currently, the admissibility of digital evidence is governed by the Evidence Act 1950 and the Rules of Court 2012. These laws and regulations provide digital evidence collection, preservation, and admissibility guidelines in legal proceedings.

Under the Evidence Act 1950, digital evidence is admissible if it is relevant to the matter in question and is not excluded by any act provision. Digital evidence can be admitted in the form of electronic records, printouts, or other electronic storage devices. Section 90A Evidence Act and Order 24 Rules of Court 2012 also provide guidelines for the admissibility of digital evidence. These rules require that digital evidence be accompanied by a certificate of authenticity, a written statement certifying the authenticity of the digital evidence. The certificate of authenticity must be endorsed by the person who collected and preserved the digital evidence and specifies the method used to collect and preserve the evidence. Therefore, DF analysts must prepare and equip themselves with the proper knowledge and expertise on the open source DF tool used in the DF investigation.

8. Conceptual Framework and Digital Forensic Readiness

A conceptual framework is a structured approach for organizing and analyzing ideas, concepts, and theories in a specific subject area. It visualizes the relationships between concepts and theories and helps clarify and organize a complex topic's understanding [45]. The conceptual framework can be represented in different ways, such as a figure, flowchart, or matrix. This should be based on a comprehensive review of the existing literature in the field. It states that a conceptual framework should be characterized as follows:

- Clear and concise, using simple and understandable language.
- Consistent, with a logical and coherent structure.
- Relevant and aligned with the research questions and objectives of the study.
- Testable, providing a basis for empirically validating the concepts and theories.

Through the SLR, we identified four (4) factors that affect the admissibility of digital evidence produced by the open source DF tools. The factors include:

- Availability and Capability: The capability and availability of open source DF tools can impact the ability of investigators to collect and analyze digital evidence effectively and efficiently. Numerous open source DF tools are available with various applications in DF investigations. However, a DF analyst must determine the tools that suit the needs and wants of an investigation.
- Reliability and Integrity: To be admissible, digital evidence must be relevant, reliable, and authentic. The reliability and integrity of digital evidence produced by open source DF tools can be affected by factors such as the methods used to acquire and preserve the evidence, the quality of the tools used, and the expertise of the investigators. Thus, open source DF tools should be able to produce repeatable results without compromising the integrity of the digital evidence.
- Transparency: Transparency is essential when using open source DF tools to ensure that the source code and methods used to collect and analyze digital evidence are clearly understood and can be easily validated.
- Lack of Reference and Standard: The lack of reference and standard for using open source DF tools can make it challenging to evaluate the reliability and validity of the open source DF tool. This can impact the admissibility of digital evidence produced in legal proceedings.

Fig. 4 presents a conceptual framework based on the four factors affecting the admissibility of digital evidence from open-source tools. In this framework, the capability and availability of open source DF tools form the foundation for successful digital forensic investigation. The reliability and integrity of the digital evidence produced by these tools and the tool's transparency are essential factors that impact the admissibility of digital evidence in legal proceedings. Finally, more references and standards related to DF tools must be considered when validating these tools.

Based on this conceptual framework, a new standard operating procedure (SOP) was developed to validate the results obtained from open source DF tools, as shown in **Fig. 5**. The preliminary SOP integrates the proposed SOP into the current DF investigation procedure in a typical DF laboratory. The new addition to the SOP requires DF analysts to validate at least three (3) results to ensure the accuracy and repeatability of the digital evidence presented to the court.

The conceptual framework combines three (3) phases in a DF investigation process. The L1 phase is where basic DF processes such as preservation, collection, examination, and analysis are done. L2 is the phase that validates the results obtained from open source DF tools.

Finally, L3 is the DFR plan for implementing open source DF tools. R1 is when an analyst decides to use any open source DF tools during the preservation, collection, examination or analysis process in L1. During L2, the analyst will use open source tools to fulfil their forensic objectives. The results obtained from those tools are then repeated at least three (3) times and validated by comparing the accuracy and repeatability of the results. R2 is the point if the validation process passes, and the analyst will continue with the process in L1. Alternatively, if the validation process fails, proceed to point R3, and the result will be considered inadmissible. In this case, the analyst should consider other tools or methods. The L3 phase describes the readiness requirements for an organization to start implementing open source DF tools in DF investigations.

Digital forensic readiness (DFR) is an organization's competence in gathering, maintaining, safeguarding, and analyzing digital evidence for use in legal proceedings, disciplinary proceedings, employment tribunals, and courts of law [4]. [2] described DFR as a continuous activity to ensure that DF operations and infrastructure inside the organization can support an investigation effectively before and after any case.

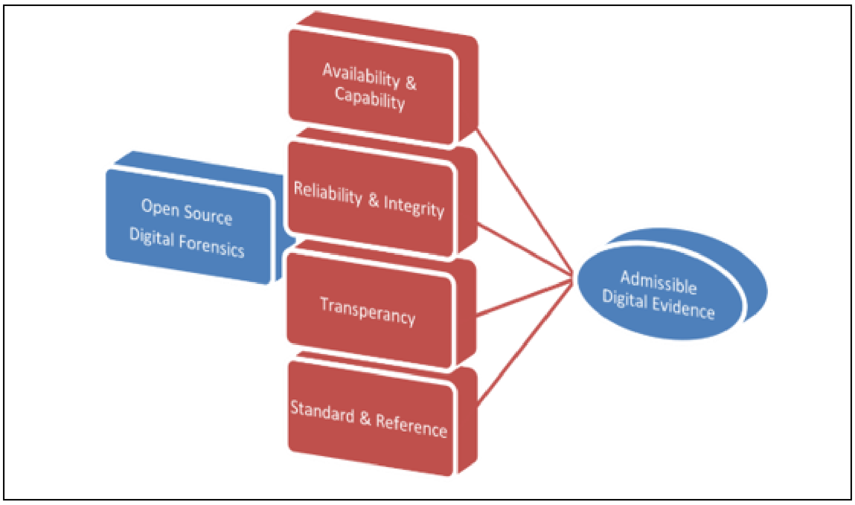
Availability & Capability
Open Source Digital Forensics
Reliability & Integrity
Transperancy
Standard & Reference
Admissible Digital Evidence

Fig. 4. Conceptual framework for admissibility of digital evidence from open source DF tools.

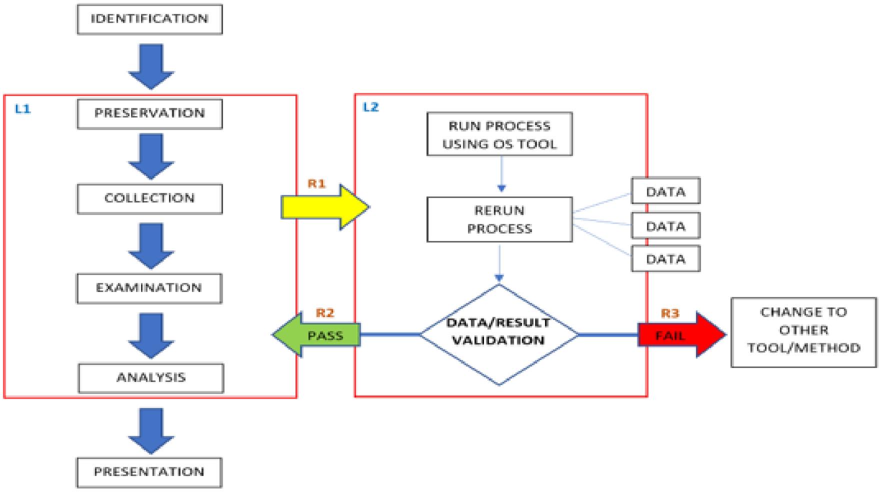

Fig. 5. Preliminary open source DF Standard of Procedure.

Open source tool DFR is the preparation an organization needs to effectively use open source DF tools in DF investigations. Therefore, the objective of DFR for open source tools includes:

- To obtain legally admissible evidence without interfering with organization processes.
- To allow investigations to be carried out at a cost appropriate to the severity of the incidence.
- To ensure that evidence has a favourable influence on the result of any court proceeding.
- To avoid disruption of services by keeping investigations at a minimum but effective manner.

As shown in L3, four (4) core components are critical toward the DFR, which includes people, organization policy and technology. The people component encompassed the training and hiring of skilled analysts, segregation of roles, and security training and awareness campaigns. DFR requires the establishment of a competent and expert analyst to securely acquire legally admissible evidence using an open source DF tool. The second component, policy, details the organization's policies, including policies on DF processes, training, and legal requirements to assist in using open source DF tools in the organization's DF investigation. The final component technology includes determining the best open source tool to use in order to avoid and detect any related issues to facilitate the organization's DF activities. Therefore, DF organizations must develop DFR plans by introducing open source tools today and in the future. Hence, this work introduced ten approaches for DFR planning, as shown in **Table 4**.

One of the main reasons the DFR plan is essential is that technologies are evolving tremendously with little consideration for the digital forensic process. From the literature search, it was clear that the DFR of these technologies is vital for the future of cyber security, which will protect not only the consumer but also the technology provider. DFR of these technologies can be achieved if serious support is collectively given by the digital forensic community, technology provider, lawmaker, and standard organization to harmonize DF with the new technology environment and architecture.

9. Conclusion

The determining factor for law enforcement agencies to consider when using open source tools compared to proprietary tools is cost. As mentioned in several studies, proprietary DF tools cost thousands of dollars to purchase and maintain. Agencies with budget constraints could not afford these proprietary tools and had to find alternative tools to complete their DF investigations.

In this SLR, we identified factors such as accuracy, capability, availability, and legal requirements when selecting the open source tools. Through this review, it was shown that open source tools are comparable to proprietary tools in terms of accuracy and capability. However, open source tools may suffer from lower efficiency, particularly when facing data scalability, and could prolong the investigation process. This review also demonstrated the variety and availability of multiple open source tools that can be used in different situations. The lists in RQ2 above may serve as a reference point for law enforcement agencies to view and select appropriate open source forensic tools. Finally, several legal requirements and issues are discussed. Factors such as tool reliability, integrity, transparency, and documentation were found to affect the admissibility of the open source DF tool in a court of law.

Through this SLR, we identified gaps in the current study. Although open source tool validation has been discussed, the admissibility of the digital evidence produced by these tools has yet to be proven and well-researched. Issues such as digital evidence authenticity, integrity, and admissibility resulting from the use of open source tools have not been satisfactorily addressed. The need for a proper guideline or framework to validate evidence from open source tools was also nonexistent. Therefore, in this study, we aim to close the gap related to these issues and outline the conceptual framework for admissibility of digital evidence from open source tools in DF investigation. For future work, this conceptual framework will be evaluated further and validated to enhance the acceptance of use of open source tools in the legal proceedings.

Table 4. Ten approaches for Digital Forensic Readiness plan for open source Tools

Components	Steps	Description
Policy	Identify the business scenarios that required the use of open source tools.	Recognize the capability of the DF organization to collect and process digital evidence using open source tools. The decision to utilize an open source tool can be made by identifying the risks and benefits to the organization.
Technology	Locate available sources and various possible open source tools.	Identify potential open source tools to be applied in the current DF investigation process. All information regarding the data, such as format, function, size, security, and others, must be fully understood. It is critical to recognize the way the tools operate.
Policy and Technology	Determine the requirement of the open source tool.	Define the open source tool requirement. This may involve identifying the type of data, software, hardware, cause and effect of data processes, storage of evidence, and others. It is encouraged to provide a plan for cost-effective when applying the open source tools.
Policy	Create a capability of obtaining legally admissible evidence when applying open source tools (in terms of security).	Ensure the collected digital evidence is confidential, maintains its integrity and is always available for the court of law. It is important to ensure the collection process does not hinder any other processes.
Policy	Create a policy for storing and handling potential evidence produced by open source tools.	Develop a policy to manage and store digital evidence produced by open source tools for an extended period by securing its integrity and maintaining the chain of custody.
Policy	Ensure monitoring is focused on detecting and preventing major issues or events.	Besides ensuring the admissibility of digital evidence produced by open source tools, this step involves monitoring and auditing process to detect and prevent any potential incident. It is critical to record and document any event related to open source tools.
Policy	Specify the situation when a complete formal investigation should be undertaken and considered when utilizing open source tool.	The decision to escalate the investigation should weight on the risks and benefits.

People	Training, education, and awareness in applying the open source tools.	Plan training and awareness programs to educate and upskill the analysts in preparing for utilizing the open source tools. The awareness should include the risks in applying the tools to ensure the analyst understands the legal implications of their actions.
People	Create a record of the evidence-based case that describes the incident and its consequences.	Record and maintain case files related to the use of open source tool as a document to be presented to the court of law. The result of the investigation contains findings related to the case should be detailed and understood by the stakeholders.
Policy and People	Conduct a legal assessment concerning the use of open source toll to expedite response to the incident.	Case files and other relevant records are to be maintained and made available to be reviewed and audited. Legal advice could also be obtained internally or externally.

Acknowledgement

The authors would like to thank the Ministry of Higher Education through Fundamental Research Grant Scheme, FRGS/1/2023/ICT07/UKM/02/3. Additionally, the authors also would like to show gratitude to Frontier Network Technology research group, Center for Cyber Security Malaysia and Universiti Kebangsaan Malaysia for their support.

References

[1] DFRWS, A Road Map for Digital Forensic Research, DFRWS Technical Reports, 2001. Article(CrossRefLink)

[2] K. A. Z. Ariffin and F. H. Ahmad, “Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0,” Computers & Security, vol.105, Jun. 2021. Article(CrossRefLink)

[3] P. Reedy, “Interpol review of digital evidence 2016 - 2019,” *Forensic Science International: Synergy*, vol.2, pp.489-520, 2020. Article(CrossRefLink)

[4] S. L. Garfinkel, “Digital forensics research: The next 10 years,” *Digital Investigation*, vol.7, pp.S64-S73, 2010. Article(CrossRefLink)

[5] M. A. Majid and K. A. Z. Ariffin, “Model for successful development and implementation of Cyber Security Operations Centre (SOC),” *PLoS ONE*, vol.16, no.11, 2021. Article(CrossRefLink)

[6] J.-U. Lee and W.-Y. Soh, “Comparative analysis on integrated digital forensic tools for digital forensic investigation,” *IOP Conf. Ser.: Mater. Sci. Eng.*, vol.834, 2020. Article(CrossRefLink)

[7] B. Carrier, Open Source Digital Forensics Tools, The Legal Argument, 2003. Article(CrossRefLink)

[8] T. Wu, F. Breitinger, and S. O’Shaughnessy, “Digital forensic tools: Recent advances and enhancing the status quo,” *Forensic Science International: Digital Investigation*, vol.34, 2020. Article(CrossRefLink)

[9] V. O. Waziri, O. N.O., A. Isah, O. S. Adebayo, and S. M. Abdulhamid, "Cyber Crimes Analysis Based-On Open Source Digital Forensics Tools," *International Journal of Computer Science and Information Security*, vol.11, no.1, pp.30-43, 2013. Article(CrossRefLink)

[10] M. H. Sonnekus, "A Comparison of open source and proprietary digital forensic software," *Theses*, 2014. Article(CrossRefLink)

[11] B. Kitchenham, Procedures for Performing Systematic Reviews, Joint technical report, 2004. Article(CrossRefLink)

[12] N. Salleh, E. Mendes, and J. Grundy, "Empirical Studies of Pair Programming for CS/SE Teaching in Higher Education: A Systematic Literature Review," *IEEE Transactions on Software Engineering*, vol.37, no.4, pp.509-525, 2011. Article(CrossRefLink)

[13] Merriam-Webster, Synonym, Merriam-Webster.com dictionary, 2024. [Online]. Available: https://www.merriam-webster.com/dictionary/synonym

[14] R. Agarwal and S. Kothari, "Review of Digital Forensic Investigation Frameworks," in *Proc. of Information Science and Applications*, Lecture Notes in Electrical Engineering, vol.339, Springer, pp.561-571, 2015. Article(CrossRefLink)

[15] M. Delgado, M. Aparicio, and C. Costa, "Using open source for forensic purposes," in *Proc. of OSDOC '12: Proceedings of the Workshop on Open Source and Design of Communication*, pp.31-37, 2012. Article(CrossRefLink)

[16] Himanshu, S. Bhatt, and G. Garg, "Comparative analysis of acquisition methods in digital forensics," in *Proc. of 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, pp.129-134, 2021. Article(CrossRefLink)

[17] S. Yadav, K. Ahmad, and J. Shekhar, "Analysis of Digital Forensic Tools and Investigation Process," in *Proc. of High Performance Architecture and Grid Computing: International Conference, HPAGC 2011*, Communications in Computer and Information Science, vol.169, pp.435-441, 2011. Article(CrossRefLink)

[18] M. Raji, H. Wimmer, and R. J. Haddad, "Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools," in *Proc. of SoutheastCon 2018*, pp.1-6, 2018. Article(CrossRefLink)

[19] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative Analysis of Android Mobile Forensics Tools," in *Proc. of 2020 IEEE Conference on Computer Applications (ICCA)*, pp.1-6, 2020. Article(CrossRefLink)

[20] R. Padmanabhan, K. Lobo, M. Ghelani, D. Sujan, and M. Shirole, "Comparative analysis of commercial and open source mobile device forensic tools," in *Proc. of 2016 Ninth International Conference on Contemporary Computing (IC3)*, pp.1-6, 2016. Article(CrossRefLink)

[21] S. C. Sathe and N. M. Dongre, "Data acquisition techniques in mobile forensics," in *Proc. of 2018 2nd International Conference on Inventive Systems and Control (ICISC)*, pp.280-286, 2018. Article(CrossRefLink)

[22] M. J. Ahmed, U. Khalid, and B. Aslam, "iDevice forensics - Data integrity," in *Proc. of 17th IEEE International Multi Topic Conference 2014*, pp.260-265, 2014. Article(CrossRefLink)

[23] C. B. Leopard, N. C. Rowe, and M. R. McCarrin, “Memory Forensics and the Macintosh OS X Operating System,” in *Proc. of Digital Forensics and Cyber Crime: 9th International Conference, ICDF2C 2017*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol.216, pp.175-180, 2018. Article(CrossRefLink)

[24] A. Cervellone, R. Price Jr., J. Brunty, and T. Fenger, A Comparison of Computer Forensic Tools: An Open-Source Evaluation, pp.1-30, 2015. Article(CrossRefLink)

[25] L. Carvajal, C. Varol, and L. Chen, “Tools for collecting volatile data: A survey study,” in *Proc. of 2013 The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE)*, pp.318-322, 2013. Article(CrossRefLink)

[26] S. Al Sharif, M. Al Ali, N. Salem, F. Iqbal, M. El Barachi, and O. Alfandi, “An Approach for the Validation of File Recovery Functions in Digital Forensics' Software Tools,” in *Proc. of 2014 6th International Conference on New Technologies, Mobility and Security (NTMS)*, pp.1-6, 2014. Article(CrossRefLink)

[27] A. K. Kubi, S. Saleem, and O. Popov, “Evaluation of some tools for extracting e-evidence from mobile devices,” in *Proc. of 2011 5th International Conference on Application of Information and Communication Technologies (AICT)*, pp.1-6, 2011. Article(CrossRefLink)

[28] V. Roussev, “Building Open and Scalable Digital Forensic Tools,” in *Proc. of 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp.1-6, 2011. Article(CrossRefLink)

[29] F. M. Patterson, The Implications Of Virtual Environments In Digital Forensic Investigations, Electronic Theses and Dissertations, STARS, 2011. Article(CrossRefLink)

[30] S. Zollner, K.-K. R. Choo, and N.-A. Le-Khac, “An Automated Live Forensic and Postmortem Analysis Tool for Bitcoin on Windows Systems,” *IEEE Access*, vol.7, pp.158250-158263, 2019. Article(CrossRefLink)

[31] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, “DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III,” *Digital Investigation*, vol.22, pp.S3-S14, 2017. Article(CrossRefLink)

[32] T. Mehrotra and B. M. Mehtre, “An automated forensic tool for image metadata and Windows 7 Recycle Bin,” in *Proc. of 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, pp.419-425, 2014. Article(CrossRefLink)

[33] J.-N. Hilgert, M. Lambertz, and S. Yang, “Forensic analysis of multiple device BTRFS configurations using The Sleuth Kit,” *Digital Investigation*, vol.26, pp.S21-S29, 2018. Article(CrossRefLink)

[34] D. R. Kamble, N. Jain, and S. Deshpande, “Cybercrimes Solutions using Digital Forensic Tools,” *International Journal of Wireless and Microwave Technologies*, vol.5, no.6, pp.11-18, 2015. Article(CrossRefLink)

[35] H. M. Charpentier, “Computer forensics and law enforcement: The need for inexpensive, reliable, fast and easy to use forensic tools in the field,” *Utica College ProQuest Dissertations & Theses*, 2013. Article(CrossRefLink)

[36] K. K. Sindhu and B. B. Meshram, “Digital Forensic Investigation Tools and Procedures,” *International Journal of Computer Network and Information Security*, vol.4, no.4, pp.39-48, 2012. Article(CrossRefLink)

[37] N. P. Tmienova, O. Ilarionov, and N. Ilarionova, "Exploring Digital Forensics Tools in Cyborg Hawk Linux," *International Conference on Intelligent Tutoring Systems*, 2017. Article(CrossRefLink)

[38] P. Andriotis, G. Oikonomou, and T. Tryfonas, "Forensic Analysis of Wireless Networking Evidence of Android Smartphones," in *Proc. of 2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp.109-114, 2012. Article(CrossRefLink)

[39] A. Parveen, Z. H. Khan, and S. N. Ahmad, "Classification and evaluation of digital forensic tools," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol.18, no.6, pp.3096-3106, 2020. Article(CrossRefLink)

[40] H. Arshad, A. B. Jantan, and O. I. Abiodun, "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," *Journal of Information Processing Systems*, vol.14, no.2, pp.346-376, 2018. Article(CrossRefLink)

[41] R. Stoykova, S. Andersen, K. Franke, and S. Axelsson, "Reliability assessment of digital forensic investigations in the Norwegian police," *Forensic Science International: Digital Investigation*, vol.40, 2022. Article(CrossRefLink)

[42] S. K. Taylor, M. S. M. Omar, N. Noorashid, A. Ariffin, K. A. Z. Ariffin, and S. N. H. S. Abdullah, "People, Process and Technology for Cryptocurrencies Forensics: A Malaysia Case Study," in *Proc. of Advances in Cyber Security: Second International Conference, ACeS 2020*, Communications in Computer and Information Science, vol.1347, pp.297-312, 2021. Article(CrossRefLink)

[43] S. Taylor, S. H.-y. Kim, K. A. Z. Ariffin, and S. N. H. S. Abdullah, "A comprehensive forensic preservation methodology for crypto wallets," *Forensic Science International: Digital Investigation*, vol.42-43, 2022. Article(CrossRefLink)

[44] A. Antwi-Boasiako and H. Venter, "A Model for Digital Evidence Admissibility Assessment," in *Proc. of Advances in Digital Forensics XIII: 13th IFIP WG 11.9 International Conference, Digital Forensics 2017*, IFIP Advances in Information and Communication Technology, vol.511, pp.23-38, 2017. Article(CrossRefLink)

[45] A. C. Jozkowski, Reason & Rigor: How Conceptual Frameworks Guide Research, 2nd Edition: by Sharon M. Ravitch & Matthew Riggan, SAGE Publications, 2017. Article(CrossRefLink)

Isa bin Ismail holds a Bachelor of Pharmacy (Honors) from the MARA University of Technology (UiTM), which he completed in 2008. He furthered his education by earning a Master's Degree in Cybersecurity from The National University of Malaysia (UKM) in 2022. Isa began his professional career in 2009, completing his provisional registered pharmacy at Hospital Selayang. Since 2009, Isa has been a dedicated officer of the Pharmacy Enforcement Division under the Ministry of Health (MOH). His role has included working as an analyst in the digital forensic lab at the Pharmacy Enforcement Division headquarters in Petaling Jaya. Throughout his tenure, Isa has earned several certifications in digital forensics, including CSM ACE Certified Digital Forensic for First Responder, MSAB XRY, and XAMN Certification. Isa's unique combination of expertise in both pharmacy and cybersecurity has been instrumental in advancing the capabilities of the Pharmacy Enforcement Division, particularly in the realm of digital forensics.

Khairul Akram Zainol Ariffin earned his Bachelor`s and Master`s degrees with First Class Honours in System Engineering with Computer Engineering from the University of Warwick, the United Kingdom, in 2008 and 2009. He later joined Universiti Teknologi PETRONAS (UTP) in 2010 to pursue his journey toward academic research and teaching courses to earn his Ph.D. in Information Systems. During his time at UTP, many journal articles and conference papers have been produced and published internationally. Then, he was appointed as a Researcher in the Digital Forensic Department, CyberSecurity Malaysia, and was entrusted with the research on embedded systems and live forensics. Currently, he is a member of the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, to pursue his passion in research towards cybersecurity, digital forensics, algorithms, and embedded system. He is GCFA certified and a member of both IEEE and IET.