Web-based expert system to determine digital forensics tool using rule-based reasoning approach

E Ramadhani*, H R Pratama, E G Wahyuni
Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia

Corresponding author: erika@uii.ac.id

Abstract. Digital forensics is a method to trace the digital evidence using knowledge of science. There are several stages in the method of digital forensics. Each stage has their own way to use the method collaborate with the tool of digital forensics. Nowadays, there are tools that we can use in digital forensics. Therefore, not all the tool coming with the help document on how to use the tool. This situation makes the investigator have to check the feature of the tool one by one in order to suit which one is the best tool to use in some stage. To overcome this problem, we made a system to determine the right tool in digital forensics using rule-based reasoning approach. The result of this paper is web-based system to determine the right tool in digital forensics. The system shows that only 40% in suitability to help the investigator to determine the right tool. This cause by lacking of the rule consists in the reasoning approach.

1. Introduction
Today we find the huge integration of Artificial Intelligence (AI) in several technologies. AI is one of the technology that rise rapidly growing in adoption of techniques by industries and technologies. The example today we always use everyday is such as Google Maps. Another example of integrating AI in other technologies are cybersecurity, healthcare, and smart cities [1-3]. Digital forensics also explores the use of AI required for analysis and computing. It is because the rapid rise of volumes in digital data [4]. In the future, AI approach could have a role in assisting investigators. The use of AI successfully applied in the field of digital forensics. The use of AI also implemented as a framework in the form of digital forensics process [5-6].

A few studies have taken place to understand the practical and challenging aspects in digital forensics [7-9]. However, the challenge is not necessarily meant for the investigator to focus upon. According to [10], tools in digital forensics is very important, because digital forensics is wholly reliant on software application. The tool designed for the acquisition and interpretation of digital data in order to support the establishment of fact allowing in criminal justice proceedings. The princip is while using digital forensics tools, we have to notice that the data collected should not be altered. The investigator used the forensics tool to document all the activity. Overall, the main purpose of digital forensics tools is to protect against cybercrimes [11].

The problem in digital forensics tools is sometimes the investigator applies a particular tool not because it is an effective tool. The investigator chose the tool because it’s available, cheap, and familiar with it. Hence, this may lead to use of unreliable digital forensics tools which may lead to...
unreliable results [12]. Today, there are several tools of digital forensics such as open and close tools. Every tool sometimes not provided with the manual that makes the investigator must check all the tools to find the appropriate tool. The result is an investigator need some time to find the effective tools.

The purpose of this paper is to build a web-based system to help investigators determine the tools in digital forensics by using a rule-based reasoning approach. The aim of making the determination system to ease the investigator to provide the less time in choosing the right tools in digital forensics. Before building the system, we start first looking at requirements that need to be considered in the evaluation process, defining what characteristics and functional type that relate to the tools that are needed by the investigator. We make use of a rule-based reasoning to model the result of knowledge from the expert to determine the right tools. Inference model that we use is forward chaining to get the result of the choosing tools.

The remainder of this paper is organized as follows: in Section II, we present the method that we use in this paper. In Section III, we present design and implementation. In Section IV, we present the evaluation. In Section V, we present discussion then last, Section V, we present the conclusion and future work.

2. Method

We use two methods to build the web-based system. The first method is a rule-based approach and the second method is forward chaining. Those methods functioning to give the result as a conclusion of recommended tools according to the premise such a tool characteristics, then the premise will be appropriated with the facts that has been determined from the expert according to the related rule.

The first we observe to an expert to determine the tools that are usually used for investigators. We give questionnaires to a practitioner expert, and the result is 22 tools selected with 11 functionality and 6 characteristics. Every functionality that is used in this paper is the result of the observation process with an expert. Characteristics is according to the paper [9] which is a general category because it is available on each tool.

![Figure 1. Flow work developing web-based system](image)

Figure 1. Flow work developing web-based system

Figure 1. is the flow work on how to develop a web-based system to determine the right tool for investigators. The first stage is observation and analysis, followed by the second stage that relates to the method that we use on how to collaborate with the result. Rule-based approach that is used is to get the result on how to execute the rule that has been made in the inference engine such as forward chaining. This rule is made according to the expert. The next step is to design the system and implement it. Last, the system will be evaluated to determine the result. In the process of evaluation, the result of the system will be compared to the result from an expert.

3. Design and Implementation

In this section we discuss the usecase diagram and user interface of a web-based system. Usecase diagram is a diagram that relates to who will use the system. According to Figure 2. the system consists of two actors i.e. admin and user. Admin act as an administrator of the system, which is managing the system such as user, functionalities, application, characteristic, rule, history, and new
fact. Therefore, users act as a person that will interact with the system such as an investigator or expert.

Furthermore, the implementation of the system depicted in Figure 3, the user interface as a home login menu that is supposed to be used as a user or administrator. There should be an authentication process by input the username or email address and the password. Then, the system will automatically check the login information, if the login system is approved, then the system will direct to the dashboard page of the user or administrator as depicted in Figure 4 and Figure 5.

According to the paper [13] that we used to design, we have two important variables i.e. list characteristics tool and list of the tool name. We provide 22 tools with 6 characteristics. For the decision making, we use a table decision. The result after the implementation is, we have 25 rules. The format of the rule is IF-THEN with the result the name of the application. The system will check all the rules, in this case the characteristics of the rule. Characteristics of the rule include: storage, processing speed, format output, ease of use, cost, and the focus of examination. The output of the
application influde: Autopsy, Encase, Foremost, FTK/LAB, F-Response, FTK Imager, IEF, Volatility, X-Ways, DEFT, Paladin, SANS, AFLogicalOSE, Laron, Andriler, UFED, XRY, and MOBILedit.

4. Evaluation
In this section, we present the evaluation of the web-based system. The evaluation consists of two stages, i.e. the evaluation for the expert and the system. The first scenario of the evaluation is we choose the tool according to the functionality and the characteristics in manual way and system way. The result of the expert will be compared to the result of the system. If the system gives the same result accordingly the system is appropriate to use. The evaluation uses all the rule data and chooses one functionality that consists of every tool. The result of evaluation to the expert is 100% related to the system.

The second scenario is we give a questionnaire to experts and to students of digital forensics as a tester to use the system. We conclude that the second scenario gives the result 100% appropriate to the data of application, functionality, characteristic, and rule. The result grouped in three aspect:

- Functionalities aspect gives the result average to 80% from the result of expert, therefore, 87,5% average from the result of the user.
- From the data aspect, the result from the expert gives an average 60% between the result from the user that gives average to 86,7%.
- For the compatibility result of the selection tool to help the investigator, the result of the expert is 40% and the user is 85%.

5. Discussion
According to the evaluation, the compatibility result has a small result i.e. 40% from the eye of expert. It is because of the lack of the data of rules that can be processed in the inference engine. The administrator needs to update the data rule if there is a new rule appearing in the process of choosing the characteristic. We can say that the system gives a good result in the feature and functionality in the system by giving the 100% result.

Three main components in rule-based approach are acquisition and maintenance, explanation, and reasoning. In maintenance, rule-based approach in an expert system means that using the rule in the domain of expert. It always maintains the rules rather than the program for the tool. In explanation, how to represent the knowledge by the system to reason how they came to a conclusion. In a simple example the system will follow the chain of inference, lead to a result and use the facts. In reasoning, the engagement of knowledge in the inference engine. The conclusion system developed from the data set that the initial development [14], [15].

6. Conclusion
According to the discussion and evaluation, we concluded that this web based system to determine tools for digital forensics has 25 rules according to the fact include characteristics by using the rule-based reasoning approach and forward chaining method to collaborate the tool selection process. We evaluate the system with user and expertise for the feature and functionalities. The result of evaluation is 100% appropriate with the data. For further research, we can add some new rules in the database in order to get the appropriate result in the selection tool. It also needs to add the priority result for the selection if there is the same tool name in the same rule after the selection process. The process selection of characteristics and functionalities in the system may change by selecting the condition one by one.

References
[1] McKee D et al., 2018 CAAI Trans. Intell. Technol. 3(2)75–82.
[2] Jiang F et al.2017 Stroke Vasc. Neurol. 2(4) 230
[3] Li J hua 2018 Front. Inf. Technol. Electron. Eng 19(12) 1462
[4] Alghamdi M I 2020 *Period. Eng. Nat. Sci.* 8(3) 1321
[5] Al Fahdi M, Clarke NL and Furnell SM 2013 *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference.*
[6] Rughani P H and Rughani Ph D P H 2017 *Int. J. Adv. Res. Comput. Sci.* 8(8) 10
[7] Rogers M K and Seigfried K 2004 *Comput. Secur.* 23(1) 12
[8] Kumari N and Mohapatra A K 2016 *International Conference on Computational Techniques in Information and Communication Technologies, ICCTICT 2016 - Proceedings* p. 243–250.
[9] Richard J and Kiper R 2018 *Pick a Tool, the Right Tool: Developing a Practical Typology for Selecting Digital Forensics Tools SANS Institute: Reading Room - Tools.*
[10] Horsman G 2020 *Forensic Sci. Int. Reports* 2 100076.
[11] Ghazinour K, Vakharia D M, Kannaji K C and Satyakumar R 2018 *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017* 3136
[12] Kogeda O and Dimpe P 2017 *Proceedings of the World Congress on Engineering and Computer Science 2017*
[13] Ramadhani E, Wahyuni E G and Pratama H R 2020 *IOP Conf. Ser. Mater. Sci. Eng.* 852 012137.
[14] Naser S SA, Alamawi W W and Alfarra M F 2016 *ITEE::Rule Based System for Diagnosing Wireless Connection Problems Using SL5 Object.*
[15] Masri N et al. 2019 *Int. J. Acad. Inf. Syst. Res.*3(7) 1