Forensic in information technology: A redefinition

M K M Nasution
1
1Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Padang Bulan 2055 USU, Medan, Indonesia
E-mail: mahyuddin@usu.ac.id

Abstract. The foundation for the development of theory is the definition. In a scientific culture, definitions force a scientific field to be present. However, the term and meaning always present a different framework for definition. This paper aims to redefine computer forensic science based on the existence of forensic terms and the relationship between these terms. A new definition is completed based on the reciprocal function of this field, a definition related to information technology.

1. Introduction
The virtual world has become a shadow of the real world [1, 2, 3, 4, 5]. An event will be recorded slowly or quickly into the information space as a marker of the existence of the related object [6]. The virtual world stores events that can be recognized, thought out, done, written, and manipulated through technology that makes it easy [7], while a technology is always like a double-edged knife: it is possible to be used to improve or to undermine human well-being [8].

The use of technology can apply to the good side or the bad side [9]. On the bad side, sometimes unwittingly by technology users, or directly or indirectly intentionally carried out for unilateral gain either personally, a group of people, or organizations, including certain governments [10, 11]. On the good side, technology besides being used to reveal crime, also primarily aims to improve the welfare of human life [12]. Of course, in the case it cannot be separated from the use of information technology [13]. Meanwhile, to see the abuse and use of information technology requires forensic science that applies specifically, and this requires a special definition of forensic science [14]. Many definition about forensic related to information technology, including forensic computers, digital forensic, computational forensic, forensic (aerial) photography, and so on [15]. Therefore, this paper intends to redefine a forensic science related to information technology. This paper will be elaborated by involving a review based on several related definitions, outlining possible approaches, and discussing related matters so that a definition is produced.

2. A review towards definition
The term forensic has long been used in medicine recognized as physiological, i.e. (T1): *a branch of biology that focuses on organisms and organ systems either physical or chemical for functioning the investigation related to law* [16]. A definition of forensic in a dictionary is a term

1 https://en.wikipedia.org/wiki/Physiology
that holds as (T2): an implication of scientific knowledge to legal problems whereby it used in, belonging to, or suitable to courts of judicature or to public discussion and debate [17, 18, 19].

The knowledge is not only science, but also about engineering [20, 21]. Based on function of legal issues on the application of both in the user communities, by considering the pure side of science from ones and zeros mathematically and its implementation in physics [22], the term forensic in computer is stated as the computer forensic, it is defined as (T3): the application of science and engineering to the legal problem of digital evidence [23]. Specifically, for example, if it involves the information technology like the storages such as memory, compact disk, hard disk, and others, the binary images are immediately made when the forensic examination is carried out [24]. However, to do forensic for getting the digital evidence is needed computation. Computing is based on a formula and functions to analyze based on the identified tasks. In this case, forensic computing is (T4): the process of identifying, preserving, analyzing and presenting digital evidence in a way that is legally acceptable. However, the involvement of hardware alone is not enough to clearly state it. Therefore, forensic computers can also be stated as (T5): the collection of techniques and tools used to find evidence in a computer [25].

In addition, the definition of forensic related to information technology involves many different terms. The digital forensic is related to the recovery of data from electronic media that is directly in contact with a computer laboratory [26]. Interpretation involving computers on photos, for example, is related to the term forensic photography [27]. While the term forensic intelligence involves the process of data collection, integration of results, and crime analysis [28]. Therefore, the definition of forensic involves information technology from two sides: it uses or use it. This is the reason that triggers the change in the definition of forensic which is stated explicitly with a computer forensic science.

3. An approach
Defining something precisely is not only to achieve an understanding of something, but it is the first step in giving the appropriate meaning [29, 30]. In the scientific world, definition is the basis for developing related theories [31]. In scientific development, the approach is based on a review of several existing definitions, then redefining them according to needs [32].

In theory the redefinition requires additional information. Additional information related to the existence of something [33], and then this existence is supported by data or other information that is interconnected [34]. Based on several definitions of forensic, a number of terms are considered and a number of other terms are ignored based on the repetition of the terms used [35]. The term is also compared to its meaning based on information space in order to produce an interpretation as the socialization of the definition of the term. Comparisons are based on the percentage (%) of two related values. Furthermore, considering the completeness term especially related to the term to express the focus of science, based on several definitions of related terms are evidence, for example. Based on that, the existence of any other related terms is revealed from the information space, including the methods involved in science. The terms that are felt to support science are proven by their existence in addition to the relationship between them so that the study related to science is deemed necessary. Relationships are formed for example through the concept of similarity measurement

\[ s = 2|ab|/(|a| + |b|) \in [0, 1] \]

whereby \( a \) and \( b \) are vectors in information space [36].
4. Design for a definition

The presence of computer forensic science from the beginning is directly related to the field of legal studies with which legal problems need to be resolved or get a decision. Legal problems can involve anyone individually, a group of people, or an organization as a result of an inability to resolve a dispute. When the law is created, the law needs to be enforced and applied, because culture is built on habits and habits formed from compulsion, while welfare is produced from a cultured life based on the law. The law force the growth of a culture. With that choice, the law requires evidence to be able to resolve any dispute. Law does have a close relationship to evidence. It is based on a review of forensic definitions related, from T2 to T5. Evidence is the main focus of forensic definition (i.e., there are 3 words for only 3 documents). Evidence related to legal problems as expressed by the emphasis on the review of the definitions of T2 to T5 through a word legal (in 2 definitions) and a word problem (in 2 definitions).

Dispute resolution that is directly or indirectly related to consideration zero and one is to present evidence that requires a more in-depth study, both in using tools, technology, methods, hardware and software or mining data. An overview of the forensic definitions of T2 to T5 emphasizes this with 2 definitions use a word digital. On the one hand, the involvement of information technology such as computer machines and its equipment in order to find evidence also involves methods that are scientifically reduced, like Fig. 1. On the other hand, the involvement of information technology for itself in order to find evidence that is capable of resolving disputes is caused by the impact of information technology both on hardware, software, data, information, and knowledge generated. It also requires the 10 methods. The method described in Fig. 1.

Forensic as a science does not tend to favor those associated with disputes, because science is

---

2 https://www.merriam-webster.com/dictionary/forensic
3 https://pdfs.semanticscholar.org/2b86/6f239f498d7d0c9a0ebc3622a9e6719755e7.pdf
4 https://en.wikipedia.org/wiki/Forensic_science
not directly related to value. When science is applied or involves technology, the course is related to value, the presence of value will affect the method used, because the application involves people who will be affected by other external factors. Thus, forensic has a role in determining the validity of evidence. Because the method as a process tool applies correctly, but incorrect the method will cause inappropriate results, or the data entered is not in accordance with the method causing the evidence to be at least inappropriate or incorrect. Therefore, from the point of view, computer forensic science in the early stages of defining it raises a problem that questions the validity of computer forensic users in the court system. However, the court system that requires evidence, it can be explained as evidence must come from legal studies. Data is valid evidence if it meets the requirements for collection, processing and presentation. Information is valid evidence if it does not come from issues developed for certain purposes. Whereas, evidence knowledge that determines if not sidedly misused. Therefore, computer forensic science or forensic science involves information technology as knowledge is defined based on keys that become the supporter of its presence.

An example of understanding is expressed in Fig. 1. Some methods are expressed as having an explanation. This explanation is a definition for several methods that require a deeper understanding through several words arranged so that information is easily accessible to them. Likewise, access to this information is given a value based on the information space that supports it. A term that has been stated is directly related to the forensic term that requires redefinition. All terms related to those methods have an understanding of them, and support socialization of the term is expressed as a percentage value. There are several methods that are not supported by social scientific understanding such as the terms: collection, identification, and presentation, while the term extraction of scientific socialization support is more than necessary. As a comparison between the definitions, expressed some calculations based on Eq. (1), where is the term information technology is lower with some terms: law, evidence, forensic, and forensic science. This is also expressed by the relationship between a term and other terms such as Fig. 2. The relationship between the term information technology semantically with other terms requires the expansion of linkages including the term forensic science, so more in-depth studies are needed, and in order to be the basis of the study whereby the computer forensic as a science, the following definition is expressed.

Information technology (computer) forensic science is a science that is developed based on the principle of zeros and ones to be applied in engineering the actual digital evidence for legal problems that involve technology, system, or not.

5. Conclusion
Redefining a scientific field requires special attention so that its development can be carried out properly. Definition of the computer forensic science is based on the collaboration of several conceptual terms which can express semantically the meaning of the related field of science whereby based on information space that computer forensic science requires a more in-depth scientific study. Furthermore, this requires the studies in several aspects, which is the task of
further work.

References
[1] Wellman B, Salaff J, Dimitrova D, Garton L, Gulia M, and Haythornthwaite C 1996 Computer networks as social networks: Collaborative work, telework, and virtual community Ann. Rev. Social 22.
[2] Nasution M K M, and Noah S A 2011 Extraction of academic social network from online database 2011 International Conference on Semantic Technology and Information Retrieval, STAIR 2011.
[3] Nasution M K M, and Noah S A 2012 Information retrieval model: A social network extraction perspective Proceedings - 2012 International Conference on Information Retrieval and Knowledge Management (CAMP’12).
[4] Nasution M K M, Syah R, and Elvida M 2018 Information Retrieval Based on the Extracted Social Network Advances in Intelligent Systems and Computing 662.
[5] Elveny M, Syah R, Elvida M, and Nasution M K M 2018 Information Retrieval on social network: An Adaptive Proof IOP Conference Series: Materials Science and Engineering 300(1)
[6] Nasution M K M, Syah R, and Elveny M 2017 Studies on behaviour of information to extract the meaning behind the behaviour Journal of Physics: Conference Series 801(1).
[7] Nasution M K M 2011 Web: Teknologi yang mengubah aliran informasi Renungan
[8] Nasution M K M 2012 Information retrieval model: A social network extraction perspective Proceedings - 2012 International Conference on Information Retrieval and Knowledge Management (CAMP’12).
[9] Nasution M K M 2013 Superficial Method for Extracting Academic Social Network from the Web Ph.D Dissertation, Universiti Kebangsaan Malaysia (UKM), Bangi, Malaysia.
[10] Nasution M K M 2014 Ontologi: Ontologi dan Taksonomi 1.
[11] Nasution M K M 2015 Digital forensics research: The next 10 years Digital Investigation 7.
[12] Nasution M K M 2016 Principles, practices, and procedures: An approach to standards in computer forensics Forensic Science Investigation 216(1-3).
[13] Nasution M K M 2017 Forensic intelligence Forensic Science International 156(2-3).
[14] Nasution M K M 2018 Semantic interpretation of search engine resultant IOP Conference Series: Materials Science and Engineering 300(1).
[15] Nasution M K M 2019 Ontology Journal of Physics: Conf. Series 1235(2019) 012106 doi:10.1088/1742-6596/1235/1/012106.
[31] Nasution M K M, and Sawaluddin 2018 Redefining the magic square on numerical characters *IOP Conference Series: Materials Science and Engineering* **308**(1).

[32] Nasution M K M, Sitepu R, Rosmayati, Siregar M F G, Syam B, Sihombing L, Farhat, Rambe A S, Ginting B, Hasanuddin, Maulina S, Ramli, Boel T, Agustono B, Sebayang K, Amin M, Yustina I, Masfria, Zulkarnain, Setiawan, Sitompul O S, Latifah S, Sibarani R, Munir E, Tulus, Putra I B, Tala Z Z, Sari D K, Saidin, Hasibuan P M, Leviza J, Hanum H, Ginting J, Supriana T, Tarigan J, Syahrizal, Irvan, Lumbanraja P, Siregar H S, Lubis A N, Pintaui S, Nasution R O, Zulkarnain M, Purba M, Dewi H, Nasution I, Pasaribu N, Bangun P, Gea S, Thamrin H, Nasution M A, Harahap H, Nurmaini, Chahaya S I, Santosa H, Hasibuan P A Z, Khairunnisa, Marianne, Ginting E D J, Novliadi F, Eliana R, Wahyuni S E, Siregar C T, Nasution S S, Zamzami E M, Syahputra M F, Lidya M S, Hartono R, Samsuri, Iswanto A H, Suryanto D, Lubis S, Wibowo R P, Husni M, Siregar G A W, Sitorus E, Bangun H, Bukit R, Sinulingga E P, Fadli, Bakti D, Hanum C, Marsaulina I, Ambarita H, Herawati E, Onrizal, Muda I, Yuandani, Eyanoer P C, Tambun R, Rahmat R F, Siregar R, Hasugian J, Chalil D, Nasution T I, Surya I, Rosmalinda, Muchtar M A, Nasution T H, Efida M 2018 Talenta *Journal of Physics: Conference Series*.

[33] Nasution M K M 2018 Singleton: A role of the search engine to reveal the existence of something in information space *IOP Conference Series: Materials Science and Engineering*

[34] Nasution M K M 2018 Doubleton: A role of the search engine to reveal the existence of relation in information space *IOP Conference Series: Materials Science and Engineering*

[35] Nasution M K M 2011 Kolmogorov complexity: Clustering objects and similarity *Bulletin of Mathematics* **3**(1).

[36] Mahyuddin K M N, Sitompul O S, Nasution S and Ambarita H 2017 New similarity *IOP Conference Series: Materials Science and Engineering* **180**(1).