Discussion of Basic Concepts of digital Forensics on the example of Volatility and Manipulability.

Johannes Fähndrich[1], Lars Mechler[2]

Abstract: Digital forensics has many properties of evidence, which need to be defined formally. The goal of this paper is to formalize the properties of evidence with the application of digital forensics. The contribution is a discussion of the current definitions of volatility and manipulability. The analysis starts the discussion on the application of those concepts to the application of ontological definitions to digital forensics. With that, we want to discuss the trust and the need to understand complex AI models.

Keywords: cyber forensics, computer forensics

1 Introduction

The basic terms used in a scientific discussion need to be well-defined. Well-defined technical terms help to reduce misapprehension, which leads to different interpretation. Different interpretations lead to misunderstanding, which leads to different reasoning. With this argument, the basis of our scientific discussion is a common ground on the technical terms used. The technical terms are given by the definitions of the field of study. This idea of defining a category has been subject to research [Ka55]. The idea here is the discussion of objects themselves, their quality, quantity, modality, and relations.

Most definition of a chain of custody for digital forensics have similar steps [PS15]. For such a chain of custody, we analyze definitions of ontology and with that the definition of basics terms used in digital forensics.

The contribution of this paper is to collect the state-of-the-art of basic terms used in digital forensics and discuss their value. In cases where a new definition could be helpful, we suggest an updated formulation.

2 State of the Art

First, we look at the requirements of how a description of a definition is done in the academic discussion. Scholars have a discourse about a term of interest, and a prevailing opinion is

[1] Hochschule für Polizei Baden-Würtenberg, Fachgruppe für Digitales Spuren und Künstliche Intelligenz, Sturmbülstr 250, 78054, Germany johannesfaehndrich@hfpol-bw.de

[2] Hochschule für Polizei Baden-Würtenberg, Fachgruppe für Digitales Spuren und Künstliche Intelligenz, Sturmbülstr 250, 78054, Germany larsmechler@hfpol-bw.de

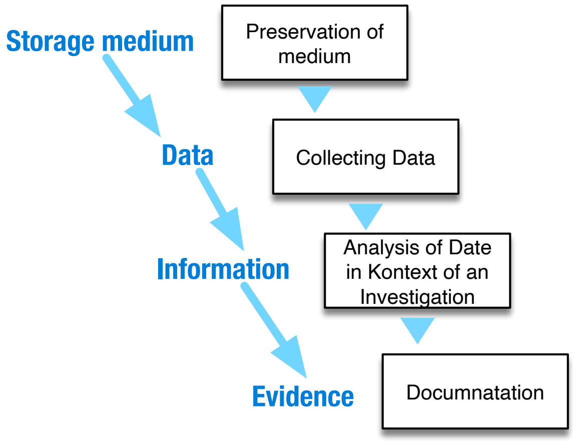

Abb. 1: Abstract description of the chain of custody for digital forensics.

reached. This process is repeated for each term used. This includes, e.g., the discussion of relationships. Making the result of such a discussion, an ontology, a model. Some structuring of the domain has been done [Al21]. Therefore, we look at the description of an ontology. Some discussion done here is taken from [Fä18][3] with the adaption to the discussion context (Digital Forensics).

A quite general description of ontologies has been given by Gruber, with "*an explicit specification of a conceptualization*" of entities of concern and their relationships[4]. This definition is quite abstract and does not formalize the notion of an ontology but rather explains what is done to create an ontology, which can be done by a multitude of modeling techniques.

To grasp the definition of ontology ready to hold up in court, we want a formal description of ontologies. At least more formal than the definition of Gruber. To find a fitting formalization, we need to look at similar terms first, to distinct them from ontologies:

Model: A model can be seen as an abstraction of an entity. Containing the relevant information regarding a given context. Favre [Fa04a; Fa04b] would describe it as "a system that enables to give answers about a system under study without the need to consider directly this system under study." [Fa04b, p. 3] and further Miller [MM01, p. 3] describes a model as "... a model is a formal specification of the function, structure and/or behavior of a system". This should be distinguished from a machine learning model [MRT18].

[3] for more details see `https://shorturl.at/iCVZ6`

[4] `http://www-ksl.stanford.edu/kst/what-is-an-ontology.html` last visited 2017.09.01

Epistemology: Epistemology can be seen as "*the field of philosophy which deals with nature and source of knowledge*" [Nu87] (cited in [SKR07, p. 6]). This sounds like a good starting point on describing knowledge for the use in criminal court. But the problematic areas like the use of AI in investigations is part of this discussion. Regarding AI research, the knowledge is interpreted as consisting of propositions and logical reasoning upon those propositions to create new knowledge in the form of formal structures [Gu95]. With that, Epistemology can not be used to describe digital evidence, since the evidence can be created by software (including use of Machine learning and AI).

Taxonomy: A Taxonomy is the science of classification of entities into classes. Putting them into a category. Thus identifying common properties and properties which differential the entities. Taxonomies structure entities into an order which can hierarchical [SL97]. Further, Euzenat and Shavaiko [ES07, p. 27] define a taxonomy as "a partially ordered set of taxons (classes) in which one taxon is greater than another one only if what it denotes includes what is denoted by the other." For digital investigations, a taxonomy is mostly not the discussion point. As part of structural science, computer science as well-defined terms which are mostly part of a taxonomy. It is the conceptual designing of how an ontology is created, which aspects are abstracted, and which are designed following a certain view point, which pose a problem.

The definition of a model is too general to be used in forensics, since the abstract way entities and relationships are discussed, seems unnecessary for forensics. Euzenat and Shavaiko [ES07] define an ontology as a conceptual model with features of an entity-relation model. The ontology is thereby seen as a logical theory with model theoretic semantics.

A Taxonomy seems too restricted for entities of digital forensics, since the classification of entities is not enough ("is-a" relationship). This is needed if we want to formalize relationships like "part-of" e.g., a message is part of a conversation under investigation.

A scoping review [MFH22] has extracted the projects of the state-of-the-art of ontologies in digital forensics. The projects UCO [Sy16] and CASE [CNH19] are two projects to design a united ontology out of the discussion of experts in digital forensics.

Figure 2 illustrates a simple taxonomy using the "has" relation, which describes the storage of data in a file system. This gives us an example of how an ontology can capture part of our beliefs and knowledge, depending on the viewpoint of the ontology creator.

This example of Fig. 2 shows how an ontology represents the view of the author. Many of the described entities and their relations can be seen differently. E.g., emphases can be given to the abstraction: Metadata can be further separated into internal and external meta-data.

However, first, we have to look at a different kind of formalization. There are two well-researched theories to formalize ontologies: Set theory and Mereology [Sm98]. We will

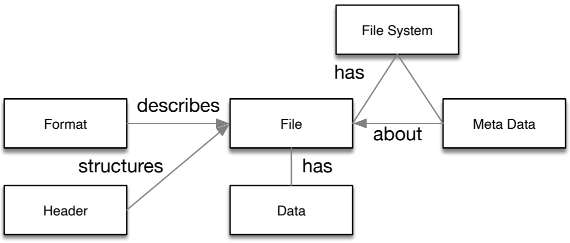

Abb. 2: An example ontology of data in a files

have a short look at both. Applications of such formalization are UCO [Sy16] another one is CASE [CNH19].

Mereotopology The theory of Mereology which became popular in the early 20^{th} century. Mereology is based on the principle of parthood [Sc03] which is similar to the idea of a subset relation in set-theory. The fundamental element in Mereology is called "Object" and is separated into *thin* and *thick* objects. Where thick objects undergo change and, in consequence, are volatile, and the thin objects are invariant. For that reason, a thick object can be identified over time by its set of thin objects which are its parts. This leads to the question of identity: How much change can an Object undergo before becoming another object?. An example in a digital forensic investigation is the use of a refurbished Smartphone. The MAC-Address (thin object) might be the same, but the "thick" object might have changed.

Set-theoretic Ontologies A second and more common formalization of an ontology is a set-theoretic view [Sm98]. Set-theory as one of the basic concepts in mathematics is made up of entity in called *elements* which are joint to a group of entities called *sets* by using the *element relation* ($\in$). With the *subset* ($\subset$) relation, one can declare a hierarchy of sets. More formal approaches model set-theoretic ontologies as category[5] like in the work of Patterson [Pa17], e.g., allows only relations between two sets of concepts.

The argument against Set-theoretic Ontologies models for formal ontologies is that they are inadequate since, e.g., we are not modeling any continuous universe [Sm98]. We argue that in computer science, every data is discretized. Thus, continuous models are approximated.

There are many drawbacks to set theory, which can be resolved with additional abstraction. One of them is that relations are basic entities. Building a taxonomy over each relation allows us to define, e.g., a hierarchy in relations like the "is-a" or "is-part" relations. The definition of an ontology by Maedche und Staab [Ma01] or Euzenat and Shavaiko [ES07]

[5] Category theory formalized structures in directed graphs with labels on edges and nodes.

or of Pickert[6] are described in [Fä18]. As well as the here used **Model of Conception** by Mahr [Ma97].

The definition of a model of conception of Mahr [Ma97] describes an abstract view on a conceptualization. This maps to natural language, where each concept can be described by a set of concepts [MP87]. With that, we can describe, e.g., the relation “is created by X” in “File created by user X” which in itself is a set of concepts which might be called “author” or might be a relationship between a file and a person ”authored-by”.

The idea here is, that in en investigation, even if the investigative team tries to be objective, there is always a conceptualization including a point of view [7].

Formally we defined an ontology similar to Euzenat and Shavaiko [ES07] but now we should even consider the mind set of the Model of conception from Mahr [Ma97] as shown in Figure 3.

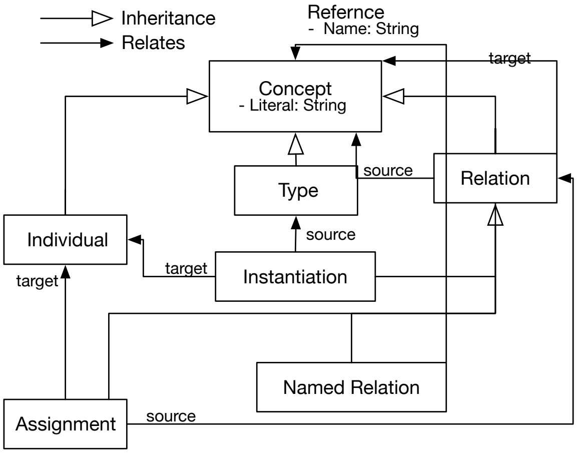

Abb. 3: Type graph of an ontology definition.

Figure 3 describes that everything is a concept. Especially, relations are concepts. We have specified three example relationships:

Named Relation: are relationships with a name like a ”send from” or “IP-Adderess”.

Instantiation: a relationship which relates concepts to individuals like ”192.168.1.1” or ”127.0.0.1”.

Assignment: a relationship which assigns concrete individuals to the sources or targets of a relationship. E.g. ”send form” and ”192.168.1.1”.

[6] Taken from a technical report from `http://www.dbis.informatik.hu-berlin.de/dbisold/lehre/WS0203/SemWeb/artikel/2/Pickert_Ontologien_final.pdf`

[7] e.g., the history of each person in the team.

We can see that this definition is more practical and is meant for the comparison of ontologies, since there is an explicit difference between classes and instances as well as between an instantiation and an assignment. Furthermore, Euzenat and Shavaiko declare data types and data values as part of the ontology, which is a kind of relations and entities with the purpose of comparing the individuals of an ontology.

The idea is similar to OWL [Ma04] with some extensions from Mahr: Everything is a concept. This means every relation is a concept. Meaning a relation can be seen as a concept, thus can have relationships with other concepts or relationships. This gives us the ability to further describe every aspect of the ontology without redefining its overall structure.

2.1 Conclusion

Like UCO [Sy16] another one is CASE [CNH19] the selection of OWL as ontology description language can be supported. The ontology with a model-theoretic semantics after Tarski [Ta44] which need a formal representation and a history of existing tools. Tools like in UCO and CASE, the existing of tools like reasoners allows a faster application into investigative processes. An interpretation allows us to define the meaning of an expression formulated in the language defined by the ontology. Tarski, e.g., does this for atomic well-formed formulas and defines that if A is a fell-formed formula, so is $notA$.

All these formalizations have entities which might have some kind of relation with other entities or themselves. The relations are quite general and might differ depending on the language used to describe the ontology. The basic concepts are still subject to discussion and the ontological semantics and pragmatics need to be described. Discussion of such properties, their classification and how they can be related and described in a formal way, is part of the here presented contributions.

In general, we want to describe evidence as something which is not true or false, since both are impossible to prove. We rather formulate probabilities on a spectrum.

The idea of Fig. 4 is to describe evidence (or a hint) in Locard's Exchange principle [Sa12]. The idea is to bring the theory from the physical evidence described by Locard to the digital evidence [Po21]. The evidence is taxonomies with regard to properties in digital investigations.

3 Analysis of Definitions

With the definition of digital evidence, we analyze the two properties of evidence, volatility and Manipulability. Ruffly speaking, the meaning of the two therms are: **Volatility** is how long evidence preserver in a given environment. And **Manipulability** is the resources needed to manipulate evidence.

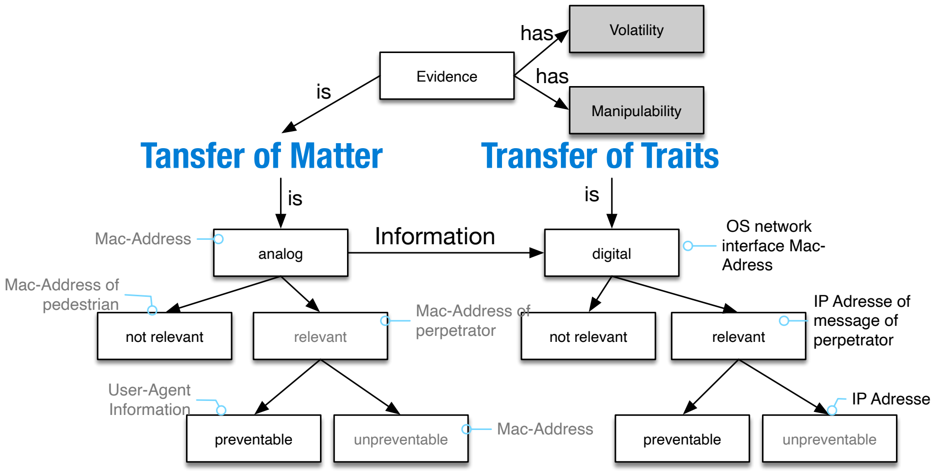

Abb. 4: Ontology representation of evidence of the perspective of digital forensics.

We discuss these two since other properties like preventability or relevance need additional discussion. Preventable e.g., is difficult since digital evidence can be not preventable like an IP-Address to send a request. But with enough manipulation afterward, the evidence can be tampered with. E.g., by deleting log files. Thus, even though we categorize a digital evidence a non-preventable, it might still unavailable for the investigation[8]. Additionally, we do not discus “red herring” or feint evidence, with a similar argument: The creation of dummy evidence can be seen as manipulation of the evidence, e.g., by rewriting log files in a system to point to other IP-Addresses.

3.1 Volatility

Volatility is defined by the Cambridge Dictionary[9] with: ”the quality or state of being likely to change suddenly”. For digital forensics, this is transferred to memory. Memory can change its state from one bit to another. Corrupting the information stored in the memory. Corruption of information can lead to the loss of data. The loss of data can lead to the loss of evidence.

The definitions we want to discuss are the definitions of properties of digital forensics from [DF15]. They differentiate between persistent evidence (evidence which is conserved over a ”relatively big time span” without power.) and volatile evidence, which needs power to be preserved. They further categorize volatile ”in a broader sense” evidence if the evidence

[8] One question here is: Does the preventability then influence the volatility? Since the information needed to be there for the system to work, e.g., the TCP/IP communication. But the manipulation of evidence, e.g., deadlines for deleting of data might destroy them.

[9] `https://dictionary.cambridge.org/dictionary/english/volatility` visited: 30.6.2023

preserver with powered devices. Without power, they are lost. Evidence with volatility ”in a strict sense” is evidence which is not persistent even though the power to the system is provided. Here we get into a gray area of definitions, using the ”power on” as part of the definition. The problem here is, that even evidence volatile in a strict sense can be differently volatile. Fig. 5 shows examples of different evidence and its classification of a volatility as a spectrum.

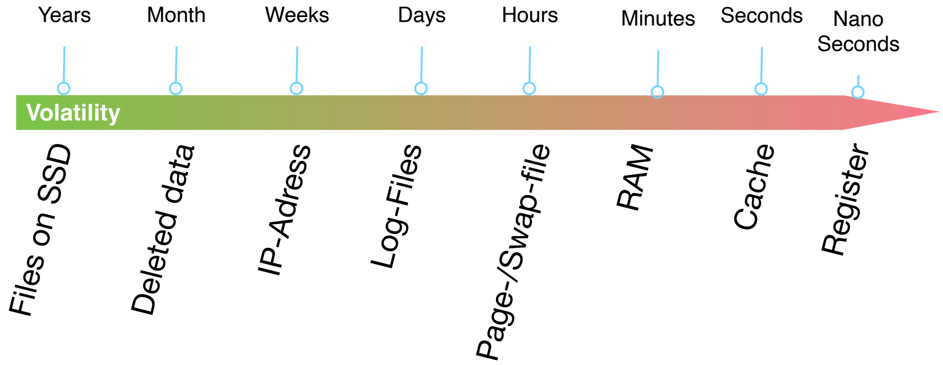

Abb. 5: Volatility as a spectrum.

Our model of volatility does take into account, that there are different reasons why evidence is at a certain level of volatility. The idea is that the evaluation of a piece of evidence can be volatile for many reasons. E.g., circular log files or ring buffer are overwritten after a reach a maximum of time or capacity. This classification of a volatility of log files therefore (because they could be written to a persistent memory) is still volatile, depending on how much is written in them, or how much time has elapsed.

Additionally, the volatility is dependent on the evidence collection process shown in Fig. 1. Depending on how the Preservation and analysis of data is done, the volatility of the evidence changes. One example here could be the analysis of Page-/Swap files. If a running system is analyzed, the page file might contain persistent versions of the data held in the RAM. If during the collection of efficient a laptop lit is closed, or the memory management of the system evacuates additional data from the ram, the page file is altered.

This example shows, that the definition of ”something is stored as long as there is power to the system” does not apply here. The definition by [DF15] includes this with the notion of ”strict sense” but does not quantify this idea.

Volatility: The time information is available for reading depending on the context.

$$volatility(D)_\theta \propto P(chage(D))_\theta, \tag{1}$$

with D being the data looked at and C the context. The function $chage(D)_\theta$ Likelihood of change

$$P(chage(D)_\theta = \mathcal{L}(\theta|D) \tag{2}$$

With a fixed θ, this is a likelihood given the observed data D. For digital investigation, the question is how to act on this information. The basic concept of likelihoodist statics is the ratio of likelihoods. Thus, depending on the context, the ratio of different contest can be calculated:

$$A(\theta_1 : \theta_2|D) = \frac{\mathcal{L}(\theta_1|D)}{\mathcal{L}(\theta_2|D)} \tag{3}$$

This means for two contexts $\theta_{1,2}$ the possible context can be asses and decisions can be based on the ratio of likelihoods. E.g. if the operating system is known, and the amount of RAM memory in proportion to the available System memory. The likelihood of a write in a page-/swap file can be asses and help with further investigative decisions.

This kind of model for volatility opens the theory up to the use of further statistical analysis, e.g., the use of a survival model [Ow01] like the Cox proportional hazard model [Co72] With survival models we can estimate the expected duration of time until an event occurs. The event being, e.g., the writing of some data from RAM to the page-/swap file. An alternative here would be to use Bayesian statistics.

In our application of digital forensics, with such an analysis, the chain of custody could be time boxed, to maximize the evidence collected as well as critical decision points could be learned with every collection. Making the system learn for every one. E.g., there could be the system features stored in a database including successfully used modules. Thus showing if a Windows Build version changed something in the implementation of memory management for RAMA dress space layout randomization so that memory acquisition does no longer work and tools need adaption.

3.2 Manipulability

Manipulation in digital forensics has been discussed by, e.g., [DF15]. They state that the manipulation of digital evidence might not leaf evidence at the level of digital evidence itself. The idea here is, that some evidence can be manipulated with ease and some is more difficult to manipulate. But first, we define manipulation in the context of digital forensics.

Manipulation: The change of information with a purpose of creating misinterpretation.

The definition of manipulation as a type of change seems logical, since a manipulation without change would result in no change in the evidence. Thus, for manipulation of digital evidence, changes in the information or in its interpretation needs to be done.

The second part, changing the interpretation, is more complex. An interpretation of evidence includes its presentation before court. With that, standards like the change of custody for information processing need to be fulfilled. The chain of custody is needed, so that manipulation of the digital evidence can be minimized. The interpretation of the evidence can be chanced, if the chain of custody is corrupted. Which might conclude in an exclusion of the evidence at trail. To formalize this kind of manipulation, some additional publications are needed.

Therefore, we concentrate on the first part of manipulation of the information which makes up the evidence. Fig.6 shows different qualities of manipulability.

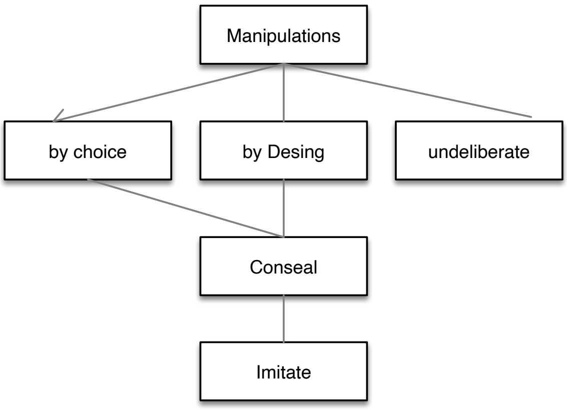

Abb. 6: Qualities of Manipulability.

Manipulation can have many reasons, which we classified in three categories:

by choice: the changes making up the manipulation have been done with intend. E.g., deleting Event-logs.

by design: the changes are done by the system itself, e.g., for privacy reasons in autonomous cars using cameras with ring buffers, which are overwritten after a defined time.

undeliberate: without intend, the information used as evidence can change. E.g., with an error in the transmission protocols.

For the manipulation, there can be different purposes. We classified them in two classes: To conceal information. This could be a simple deletion of information. The lack of information created by the deletion is evidence again. Thus, the second class inheriting concealing information is imitated. By imitate, we mean imitating evidence. Imitating of evidence is harder to identify manipulation and might lead to false evidence.

The problem with a formal definition of manipulability is, that the time it takes to manipulate something, is dependent on the skills and tools of the manipulator. Furthermore, the quality of the evidence can be correlated to the manipulability. For Example, DNS Caches in a browser is specific to the system user (Easy to manipulate but specific). DNS-Caches of wireless LAN Router are specific to all users in Network. Meaning that the evidence is less useful, and it is harder to manipulate the DNS Cache of a Router. Even less specific is the DNS Cache of the ISP. It can be interpreted as: one of the customers of the ISP used the DNS Entry. This is even less specific to the use, and in general even harder to manipulate.

Without knowledge of the skills and tools or access of the manipulator, we define manipulability as a spectrum as well. Even though the in Fig.7 presented examples might be placed differently by others, we want to show, that each part of the spectrum can be used.

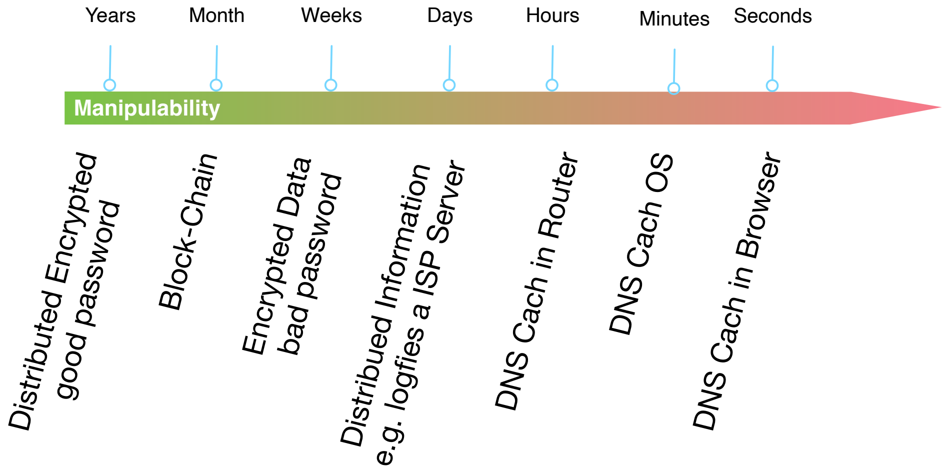

Abb. 7: Manipulability as a spectrum.

Fig. 7 depicts green as hard to manipulate and read as easy. Ranging from a 51% attack on a blockchain to the deletion of a browser history in the browser. In our future work, we want to discuss the other basic terms of digital forensics and correlate them. Correlation of properties of digital forensics[10] needs to be shown by evidence. We want to collect evidence with experiments on manipulation of information, the possibility to identify and revoke a manipulation.

[10] like done in the correlation of expressiveness and manipulability.

3.3 Future Work

With the beginning of seeing volatility and manipulability as a spectrum, we are able to classify digital evidence to their degree of volatility and manipulability. Furthermore, we are looking forward to the scientific discourse on the definition of basic forensics terms in the application of digital forensics. Next on our research agenda is to integrate the idea in first responder software, so that information about the analyzed systems might be collected and used to improve the collection of digital evidence.

Literatur

[Al21] Al-Dhaqm, A.; Ikuesan, R. A.; Kebande, V. R.; Abd Razak, S.; Grispos, G.; Choo, K.-K. R.; Al-Rimy, B. A. S.; Alsewari, A. A.: Digital forensics subdomains: the state of the art and future directions. IEEE Access 9/, S. 152476–152502, 2021.

[CNH19] Casey, E.; Nelson, A.; Hyde, J.: Standardization of file recovery classification and authentication. Digital Investigation 31/, S. 100873, 2019.

[Co72] Cox, D. R.: Regression models and life-tables. Journal of the Royal Statistical Society: Series B (Methodological) 34/2, S. 187–202, 1972.

[DF15] Dewald, A.; Freiling, F. C.: Forensische informatik. BoD–Books on Demand, 2015.

[ES07] Euzenat, J.; Shvaiko, P.: Ontology Matching. Springer-Verlag Berlin Heidelberg, 2007, ISBN: 3-540-49611-4.

[Fa04a] Favre, J.-M.: Towards a basic theory to model model driven engineering. In: Workshop in Software Model Engineering, WiSME. S. 262–271, 2004, URL: http://scholar.google.com/scholar?q=related:pZ-67HCYDo4J:scholar.google.com/&hl=en&num=20&as_sdt=0,5.

[Fa04b] Favre, J.-M.: Foundations of meta-pyramids: languages vs. metamodels. In: Episode II. Story of Thotus the Baboon, Procs. Dagstuhl Seminar. 2004.

[Fä18] Fähndrich, J.: Semantic Decomposition and Marker Passing in an Artificial Representation of Meaning. Technische Universitaet Berlin (Germany), 2018.

[Gu95] Guarino, N.: Formal ontology, conceptual analysis and knowledge representation. International Journal of Human-Computer Studies 43/5-6, S. 625–640, 1995, URL: http://www.sciencedirect.com/science/article/pii/S107158198571066X.

[Ka55] Kant, I.: Critique of pure reason, tr. by JMD Meiklejohn. 1855.

[Ma01] Maedche, A.: Ontology Learning for the Semantic Web. English, IEEE Intelligent systems 16/2, S. 72–79, 2001, URL: http://books.google.de/books?id=Hm4jFCxk5VYC&printsec=frontcover&dq=intitle:Ontology+Learning+for+the+Semantic+Web&hl=&cd=1&source=gbs_api.

[Ma04] Martin, D.; Paolucci, M.; McIlraith, S.; Burstein, M.; McDermott, D.; McGuinness, D.; Parsia, B.; Payne, T.; Sabou, M.; Solanki, M.; Srinivasan, N.; Sycara, K.: Bringing Semantics to Web Services: The OWL-S Approach. In: Semantic Web Services and Web Process Composition. Springer Berlin Heidelberg, Berlin, Heidelberg, S. 26–42, 2004, ISBN: 978-3-540-24328-1, URL: http://link.springer.com/10.1007/978-3-540-30581-1_4.

[Ma97] Mahr, B.: Gegenstand und Kontext - Eine Theorie der Auffassung. In (Eyferth, K.; Mahr, B.; Posner, R.; Wysotzki, F., Hrsg.): Prinzipien der Kontextualisierung. Technische Universität Berlin, 1997.

[MFH22] Morgenstern, M.; Fähndrich, J.; Honekamp, W.: Ontology in the Digital Forensics Domain: A Scoping Review. INFORMATIK 2022/, 2022.

[MM01] Miller, J.; Mukerji, J.: Model Driven Architecture (MDA), Techn. Ber., 2001.

[MP87] Mel'čuk, I.; Polguère, A.: A Formal Lexicon in the Meaning-Text Theory (or How to Do Lexica with Words). Computational Linguistics 13/3-4, S. 261–275, 1987, URL: http://dl.acm.org/citation.cfm?id=48166.

[MRT18] Mohri, M.; Rostamizadeh, A.; Talwalkar, A.: Foundations of machine learning. MIT press, 2018.

[Nu87] Nutter, E.: Epistemology. Encyclopedia of Artificial Intelligence 1/, S. 460–468, 1987, URL: http://scholar.google.com/scholar?q=related:-HhWKsfaAhoJ:scholar.google.com/&hl=en&num=20&as_sdt=0,5&as_ylo=1987&as_yhi=1987.

[Ow01] Owen, A. B.: Empirical likelihood. CRC press, 2001.

[Pa17] Patterson, E.: Knowledge Representation in Bicategories of Relations, Techn. Ber., 2017, URL: https://arxiv.org/abs/1706.00526.

[Po21] Povalej, R.; Rittelmeier, H.; Fähndrich, J.; Berner, S.; Honekamp, W.; Labudde, D.: Die Enkel von Locard: Analyse digitaler Spuren in der forensischen Informatik. Informatik Spektrum 44/, S. 355–363, 2021.

[PS15] Prayudi, Y.; Sn, A.: Digital chain of custody: State of the art. International Journal of Computer Applications 114/5, 2015.

[Sa12] Sammons, J.: The basics of digital forensics: the primer for getting started in digital forensics. Elsevier, 2012.

[Sc03] Schneider, L.: How to Build a Foundational Ontology. In: Agents and Computational Autonomy. Springer Berlin Heidelberg, Berlin, Heidelberg, S. 120–134, 2003, ISBN: 978-3-540-20059-8, URL: http://link.springer.com/10.1007/978-3-540-39451-8_10.

[SKR07] Sharman, R.; Kishore, R.; Ramesh, R.: Ontologies: A Handbook of Principles, Concepts and Applications in Information Systems. Springer Science + Business Media, LLC, New York, 2007, ISBN: 978-0387-37019-4.

[SL97] Shanks, D.; Lamberts, K.: Knowledge, Concepts, and Categories. Psychology Press, 1997.

[Sm98] Smith, B.: Basic Concepts of Formal Ontology. Formal Ontology in Information Systems/, S. 19–28, 1998, URL: http://philpapers.org/rec/SMITBT.

[Sy16] Syed, Z.; Padia, A.; Finin, T.; Mathews, L.; Joshi, A.: UCO: A unified cybersecurity ontology. UMBC Student Collection/, 2016.

[Ta44] Tarski, A.: The Semantic Conception of Truth: and the Foundations of Semantics. Philosophy and phenomenological research 4/3, S. 341, 1944, URL: http://www.jstor.org/stable/2102968?origin=crossref.