FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG
TECHNISCHE FAKULTÄT

Department Informatik

Technical Reports / ISSN 2191-5008

Andreas Dewald, Felix C. Freiling

From Computer Forensics to Forensic Computing: Investigators Investigate, Scientists Associate

Technical Report CS-2014-04

May 2014

Please cite as:
Andreas Dewald, Felix C. Freiling, “From Computer Forensics to Forensic Computing: Investigators Investigate, Scientists Associate,” Friedrich-Alexander-Universität Erlangen-Nürnberg, Dept. of Computer Science, Technical Reports, CS-2014-04, May 2014.

Friedrich-Alexander-Universität Erlangen-Nürnberg
Department Informatik

Martensstr. 3 · 91058 Erlangen · Germany

www.cs.fau.de

From Computer Forensics to Forensic Computing: Investigators Investigate, Scientists Associate

Andreas Dewald Felix C. Freiling
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

***Abstract*—This paper draws a comparison of fundamental theories in traditional forensic science and the state of the art in current computer forensics, thereby identifying a certain disproportion between the perception of central aspects in common theory and the digital forensics reality. We propose a separation of what is currently demanded of practitioners in digital forensics into a rigorous scientific part on the one hand, and a more general methodology of searching and seizing digital evidence and conducting digital investigations on the other. We thereby mark out the route for computer forensics to turn into a true forensic science. To illustrate the feasibility of the proposed path, we supply a couple of practical examples, as well as a list of exemplary questions that should be answered by digital forensic scientists.**

I. Introduction

Like in other forensic sciences, the emergence of computer forensics was mainly driven by practitioners trying to satisfy immediate needs within concrete digital investigations. This has left the area in a rather immature state. Rogers and Seigfried [2] identified "a disproportional focus on the applied aspects of computer forensics, at the expense of the development of fundamental theories." Even though many universities have started to establish degree programs and research labs in this area, Garfinkel [3] projects a "crisis" of digital forensics, Casey [4, p. xxxiv] states that "the field [of computer forensics] must become more scientific in its approach", and Cohen [5] questions the "science" in digital forensics.

In this report, we reconsider computer forensics as a forensic science. We do this by framing computer forensics in the context of other forensic sciences and their underlying fundamental theory of the "origin of evidence" [6]. We argue that only specific parts of computer forensics satisfy the definition of forensic science in this sense. We therefore propose to separate computer forensics into two largely distinct parts: (1) a very rigorous forensic science that attempts to establish associations between (data) objects, and (2) a more general methodology of searching and seizing digital evidence and conducting digital investigations. This separation has several advantages:

1) It structures the methodologies of computer forensics into classes that require different skills and rigor and therefore helps to separate concerns in practice.
2) It places computer forensics onto a firm theoretical basis and clarifies its relation to other forensic sciences.

This report ist structured as follows: In Section II, we first explain the fundamental theories of traditional forensic science. In Section III, we give a short overview over the field of computer forensics and its various facets in current investigations. Within Section IV, we argue that computer forensics as described in the previous section can hardly be called a forensic science and suggest ways to turn computer forensics into a forensic science in Section V by applying the described theories known from traditional forensics as a central aspect in digital investigations. In Section VI, we give examples to illustrate how those principles can be applied as proposed. Finally, we conclude with a short summary of our results and give an outlook for further development in computer forensics in Section VII.

II. Forensic Science

The American Academy of Forensic Sciences (AAFS) defines forensic science as the application of science to the legal system [7]. The definition is as broad as the range of sciences organized within AAFS, which range from physics, engineering, biology, psychiatry to linguistics. Historically, forensic sciences evolved from the need to analyze evidence found at a crime scene. In public perception, the analysis of biological evidence, impression evidence, firearms and tool marks still dominate

A previous version of this report appeared in the proceedings of the 5th MPICC Interdisciplinary Conference on Current Issues in IT Security 2012 [1].

the image of forensic scientists [8], and we too, in this report, focus on the "applied science" aspect of forensic science in the tradition of experimental natural sciences [9, p. 7f]. Following Groß and Geerds [10], researchers have commonly termed this branch of forensic science *criminalistics* [9, 11]. While not excluding branches like forensic psychology, they lie not in the focus of our argument.

One of the most fundamental notions in criminalistics is *transfer*. In its original meaning [12], transfer refers to the fact that during criminal activities, a perpetrator usually comes into contact with objects at the crime scene and therefore (often unwillingly) brings something to the crime scene and takes something from it. The basis for Locard's observation was that criminal activities usually involved the application of force to humans or materials. As a result, blood, fibers, splinters or discharge residues could be found on both, the victim and the perpetrator, giving rise to a specific form of evidence with a high probative value. It is in this context that advances in science, for example blood classification tests or DNA analysis, formed the basis for specific forensic sciences to evolve.

However, Locard's transfer was always physical transfer, i.e., the *transfer of matter*. Such transfer could not explain other types of evidence, such as tool marks, tire marks or foot imprints. Inman and Rudin [6] generalized Locard's observation to further cover the *transfer of traits*. This transfer of traits is an additional kind of transfer, that might occur even without transfer of (physical) matter. For example, traits of a perpetrator's rifle on the bullet that was found in the victims body are the result of such kind of transfer. However, both types of transfer can occur in combination with each other, too. As an example for such a combination, consider a perpetrator both leaving his foot imprint in the garden of a victim, and carrying particles of soil with him. As another example for the sole transfer of traits, Inman and Rudin [6] mention a piece of paper that is torn into two pieces. Both pieces show a very individual edge that exactly matches that of the other piece. The contact between those two pieces of paper is obvious, but only due to traits instead of physical traces. Based on the established literature, such as Kirk [13] and Lee and Harris [14], Inman and Rudin [9] embedded these principles into a theory underlying criminalistics, the most advanced and mature theory of forensic science that we are aware of.

Roughly speaking, in this theory, evidence is always the result of transfer. A forensic scientist therefore always seeks to prove that two objects A and B were in contact. One of the two objects, e.g., a blood stain or a tool mark, is usually found at the crime scene. Analyzing this object A helps to find the other object B. During this process, four steps are usually taken:

1) (Identification) In a first step, the object A needs to be identified as potential evidence. If an object, such as a patch of flat soil below a window, for example, is not recognized as a potential source of evidence, it will not be used for proving contact with the perpetrator. As it is not possible to analyze every particle of a physical crime scene, it is obvious that there is no alternative to the step of identification such as just seizing everything to not miss anything.
2) (Classification) In a second step, object A is usually analyzed for class characteristics, i.e., characteristics that distinguish it from other classes of objects and that especially allow for reducing the set of potential objects B that were in contact with A. The characteristics considered within this step usually stem from a known and controlled creation process. For example, the patch of flat soil could be classified as a shoe imprint of size 9.
3) (Individualization) Class characteristics only point to a class of objects to which object B belongs. The goal, however, is to narrow down this set to the size of one. This is performed in a third step where individual characteristics are taken into account. Such characteristics result from individual and random processes, in contrast to the classifying characteristics mentioned within the previous step. In our example, the shoe imprint could exhibit a characteristic type of wear at the heel (a crack for example).
4) (Association) Individualization points to the specific object B in question. If several candidate objects have been seized with object B among them, the forensic scientist uses scientific methods to establish the association between object A and object B. A detailed comparison between the individual wear of a particular shoe and the marks in the shoe imprint, for example, could lead the scientist to the conclusion that this particular shoe left the imprint. The result is the association between object A (shoe imprint) and object B (specific shoe). A possibly more obvious example of the application of scientific methods to prove an association is DNA typing, where a forensic

scientist checks whether the DNA that was found at the crime scene (object A) matches the sample (object B) that was taken from a suspect using the RFLP analysis, for example.

Such association is just about one event (contact between two objects) within a possibly much more complex sequence of events that made up the crime. Inman and Rudin [9] argue that the reconstruction process of a crime can be broken down into many such associations. It is the task of the forensic scientist to prove them and also to quantify the probability of error using scientific knowledge.

III. Computer Forensics

Computer forensics (sometimes called *cyber-*, *digital* or *IT forensics*) is a branch of forensic science pertaining to *digital* evidence, i.e., any legal evidence that is processed by digital computer systems or stored on digital storage media [4]. Computer forensics aims at identifying, preserving, and analyzing digital evidence after a security incident has occurred.

Examples of typical tasks in computer forensics are

- the quick assessment of the security incident by looking at log files or applying other live response techniques,
- the imaging of physical storage media using specific hard- and software,
- the recovery of deleted data using file system information or file carving techniques,
- the creation of time lines of actions based on file system meta data,
- the bypassing of protection mechanisms of a digital system in order to obtain data, or
- the extraction of cryptographic keys from snapshots of physical memory.

Today, many practical problems in computer forensics also stem from the necessity to process enormous amounts of digital data, both in terms of physical processing (efficiently storing and retrieving data), as well as identifying data items of probative value in large data sets (image databases, email folders, etc.).

In most cases, computer forensics professionals either guide or are at least deeply involved in the investigation process. They assess first evidence, draw conclusions within the context of the case and determine further steps. By doing so, the expert's experience and knowledge of functional principles in a digital system come into play. This is especially valid for activities in the context of corporate *incident response* [15] where responsibility lies in the hands of Computer Emergency Response Teams (CERTs). But also many investigations conducted by law enforcement are directed by specially trained experts. *All* of these activities fall under the heading of "computer forensics" (see Casey [4], Mandia et al. [15], Garfinkel [3]).

IV. Computer Forensics is not a Forensic Science

Comparing computer forensics and the theory of forensic science sketched above, there is an obvious disproportion between the type of questions answered in both areas. Whereas in the theory of Inman and Rudin [9], the notion of *transfer* is the central aspect of any forensic question, computer forensics seems to have a much broader scope. Carrier and Spafford [16] explain this "historically" by the "much more involved process where the investigator must trace user activity and cannot provide a simple yes or no answer". But if the theories of transfer cannot be applied to most questions in computer forensics, can computer forensics be called a forensic science?

One indication of a starting alienation within the research community of computer forensics is Böhme et al. [17] who state that "multimedia forensics is not computer forensics". Multimedia forensics is centered around specific types of digital evidence: images, videos or other forms of digital recordings. It is argued that such pieces of multimedia are captured from the real world using sensors and not *entirely* generated within a digital system (as is the case with emails, text-documents or log files for example). Consequently, the existence of artifacts that are left by the physical capturing unit within the digital data are the distinguishing feature. Böhme et al. [17] define the field of *digital forensics* to cover both computer forensics and multimedia forensics. However, the relation of digital forensics to other forensic sciences is not discussed in detail.

There already have been some approaches to unify computer forensics with classical theories of forensic science. Most notably, Carrier and Spafford [18] define the *digital crime scene* in analogy to the physical crime scene and propose to investigate both with similar methodological processes. However, Carrier and Spafford [18] base their suggestions on books [19, 11] that focus more on enumerating techniques than explaining unifying theories. Casey [4] bases his model mainly on Carrier and Spafford [18]. Similarly, Carrier and Spafford [16] map event reconstruction in the digital world to the same concept in the physical world. The

concept of transfer is only implicitly used within state transitions of automata.

To our knowledge, Pollitt [20] was the first to adapt the theory of Inman and Rudin [9] to computer forensics. Pollitt [20] already identifies the need for applying common forensic theory to the field of computer forensics and draws a sketch of how Inman's and Rudin's process of association could look like in the digital world. The underlying concept of transfer, however, is outside of Pollitt's scope. More recently, Cohen [21, 5] and Cohen et al. [22] have also placed digital forensics research within the context of Inman and Rudin [9] but rather focus on the concept of transfer than the concept of association.

V. Making Computer Forensics a Forensic Science

We believe that computer forensics should relate itself much more closely to classical forensic sciences and their fundamental theories. This means that the notions of *association* and *transfer* should be at the core of any endeavor. We show below, that the theory and concepts of Inman and Rudin [9] can be mapped to the handling of digital evidence too. However, not all aspects of computer forensics can be covered in this way.

We therefore propose to distinguish two aspects of computer forensics and separate the relevant methodologies into two domains:

1) The first domain contains a very focused set of questions and methods that deal with the search and establishment of associations at its core. We give examples for such questions and methods below in Section VI. Sharing a common basic theory with other forensic sciences, this part of computer forensics turns it into a forensic science.
2) The second domain comprises the entire process of conducting a digital investigation, e.g., searching for evidence, recovering deleted documents, managing large volumes of data, etc.

The latter domain can be roughly equated with what today is called computer forensics or digital forensics. It can be executed by personnel specially trained to perform *digital investigations*. The former domain, however, requires more scientific background and should be performed by scientists in a digital crime laboratory. To emphasize the scientific aspect of the former domain and to distinguish it more clearly from the latter, we propose to call it *forensic computing*.

We emphasize that both aspects of computer forensics are equally important and we explicitly do not intend to establish any two-class society in the area, especially because it is impossible to cleanly delineate both areas from each other. However, we believe that the general field of computer forensics will be able to mature better if such a separation of duties is established more strongly, the basic point being that people focus on what they are good at: *Investigators investigate, scientists associate*.

In order to illustrate the benefit more clearly, we give some examples where strict forensic reasoning must be applied within the next section.

VI. Transfer and Association in the Digital World

We now elaborate on the concept of transfer and association in the context of digital evidence and give several examples for questions and methods where the theory of Inman and Rudin [9] clearly applies. We supply some examples to illustrate how the concept of association can be applied in the digital world, beginning with the most comprehensible example and ending with the most abstract one.

We start with two examples, where physical objects are involved. Thus, in those examples, association is reasonably intuitive, although the actual association already takes place in the digital world. The next example is a less obvious one, in which association is established solely between digital objects. Our last example is a very abstract one, which is reduced to the minimum core of a digital association. Allthough this final example might be difficult to understand for people without a computer science background, it clearly demonstrates the core of what association is based on in the digital world: the clear statement of assumptions, rigorous scientific reasoning, and critical quantification of error. The challenge lies in formulating assumptions that on the one hand are sufficiently weak so that they cover reality and are assessable by law, but on the other hand are sufficiently strong to allow for quantifiable scientific reasoning.

A. Multimedia Forensics

We begin with the field of multimedia forensics. Recall that the digital evidence in multimedia forensics is data that is captured from the real world using sensors. Artifacts left by the sensors in this data can be used to answer questions regarding consistency and origin. The establishment of origin, i.e., the statement "image file A was taken by digital camera B", is a quite obvious example for the establishment of an association, here between some digital media object and the sensor that originally captured it.

Identification: Object A in this example is a file found on a seized hard disk or on a particular server on the Internet. Assume that the case in question is about the possession of illegal pornography. Therefore the existence of the file is sufficient to identify object A as potential evidence.

Classification: Subsequently, the file is examined for class characteristics, resulting in the findings that object A is an image of certain size in a particular image format (for example JPEG). Brief analysis of the file (e.g., by visual inspection) results in the conclusion that the image was probably produced by a digital camera, our object B. Using further class characteristics (here small but systematic deviations in the light sensitivity of single sensor elements) is often possible to determine the class (manufacturer) and model of the camera [23] from a single image only.

Individualization: Having several digital cameras at hand that were seized at a suspects home, it is now possible to investigate the detailed sensor noise characteristics of the individual cameras. This is done by taking a number of pictures with each camera in a controlled way and extracting their individual sensor noise characteristics [23, 24].

Association: Using the individual characteristics of each camera it is possible to associate the found image (object A) with a particular camera (object B) with high confidence.

B. USB Storage Devices

The next example we consider is the association between a removable storage device and a particular computer. Storage devices today are most commonly connected to a computer system via *Universal Serial Bus* (USB). It is well known that operating systems collect information about the storage devices that were used in the past. More specifically, the device drivers use individual characteristics of the storage device, for example, to select the appropriate device driver within the operating system [25]. This can help to make a statement like "USB storage device A was previously connected to computer system B", again an obvious example of an association in the sense of Inman and Rudin [9].

Identification: Object A is a small plastic object with a metal end found at a crime scene. Assume that the case in question is about data theft. This should be sufficient to identify object A as potential evidence.

Classification: Further investigations, looking at the *class characteristics* of the device, reveal that object A is indeed a USB mass storage device of a certain brand. The class of objects B to which A may be associated now comprises the set of all computer systems having a USB interface.

Individualization: Assume a set of computer systems of different suspects has been seized as well and these systems run the Microsoft Windows operating system. When a USB storage device is attached to a Windows system, the operating system creates a *device instance identifier* from different values that are present on the device. Most storage devices provide a serial number that is unique to that device. These identifiers are stored in the Windows registry key

```
HKEY_LOCAL_MACHINE\System\
  CurrentControlSet\Enum\USBStor
```

and can be extracted using appropriate tools (see Carvey and Altheide [25]). Further individualizing characteristics could consist of a particular set of files found both on object A and object B.

Association: Under the assumption that the suspect is not able to manipulate this particular evidence, finding the unique identifier of a USB storage device in certain locations on a computer system is a strong indication that in the past, that particular storage device (object A) was connected to that particular computer (object B).

C. Browser Cache

For performance reasons, web browsers usually store copies of visited websites in cache files on the computer. These files can be used to answer the question which website has been visited by the user of a particular computer in the past. It therefore allows to associate a computer (object A) with a particular website (object B). The process of association can (and in most cases implicitly is already) applied in the following way.

Identification: From a first visual analysis, the forensic scientist may find files in a file system path that is known to be used by a particular browser for storing cached files. For example, with Microsoft Internet Explorer this is the following directory:

```
%systemdir%\Documents and Settings\
  %username%\Local Settings\Temporary
  Internet Files\Content.ie5
```

Thus, in this step he may come to the conslusion that these files might potentially belong to the browser cache and therefore are identified as potential evidence.

Classification: In the next step, the scientist typically has to use some kind of tool in order to draw further conclusions. Depending on the browser that produced the cache files, a special parsing tool for this particular cache file format is needed to verify that the identified files indeed belong to the browser cache. This evidence stems from a known and controlled creation process, as the browser is known to always create cache files within this particular path and file name in this particular format. This is an important criteria for the distinction between the steps of classification and individualisation. The result of this step is that those files indeed are cache files of this particular web browser.

Individualisation: Finally, the actual contents of the identified files are investigated, again using tools, like an image viewer for visualizing cached images or a web browser to render HTML files. In this step, the scientist tries to find out, which particular content was cached. Depending on the cache file format and operating system, timing information, as well as the user that caused the caching of those files, and their origin might be available, too. This type of evidence is typically subject to an unintentional or even random creation process, because the fact that a user with this particular user name caused caching of that specific website with those contents at that time is very individual and it is very unlikely that there is another computer with exactly (and only) that evidence. As a result of the individualisation step, the forensic scientist would state, that on the investigated system, this particular browser at the specified time displayed and thus cached these contents.

Association: As a result of the previous steps, the forensic scientist is able to establish an association between a user on the system and a website, together with the time of visiting that website and the delivered contents.

D. Copy/Move in Computer Memory

The previous examples always alluded to some (faint) form of "physical contact", be it visual like in the first example or over a network link like in the third example. In our last example, we would like to show that even the sole *transfer of traits* in the form of a copy/move machine operation on a computer system can be cast into the process of association, although many assumptions about the environment need to be made to conclude an association without doubt. Therefore, the last example is rather artificial and less intuitive without practical relevance at a first glance. However, it is intentionally reduced to the minimal essentials and illustrates the possibility of associating one region (object A) with another region (object B) of main memory.

In contrast to real world computers, the regarded automaton allows for 3 different values for each storage location, instead of only two. This is because in addition to the bit values `0` and `1`, we introduce an explicit NIL value $\perp$. Our automaton is equipped with a 2-bit read-only memory (ROM): The first bit, which we call `A`, stores the value `0`, while the second storage position `B` stores the value `1`. Further, the automaton operates on a 1-bit random access memory (RAM) `R` , which is initialized with the value $\perp$. We call the current assignment of values to those three storage positions the state of the automaton.

The only command that can be executed by this machine is the move command `mov`, that copies the value of a source storage location to a destination storage. The syntax of this command is as follows: `mov` ⟨`source`⟩, ⟨`destination`⟩. As a source location, each of the automaton's 3 bits (`A`, `B`, and `R`) can be used. However, as a target location, obviously only the RAM `R` can be used, as ROM storage contains fixed values and can not be written. Finally, we assume that there exist no external influences (such as radiation), that could change the state of the machine without the execution of a command. Figure 1 illustrates the initial state of the automaton, as well as the state after the execution of the command `mov B, R`.

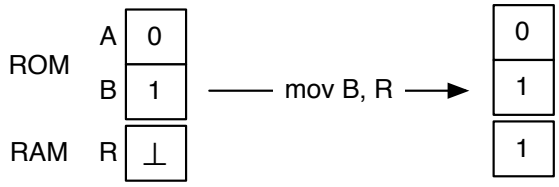

Figure 1. State of the 3-bit Automaton before and after the execution of a `mov` command

As an example, we now consider we are given the state after the execution of this command, as shown in the right part of Figure 1, to discuss the steps of association.

Identification: When examining the given state, we can first observe that in contrast to the known initial state of the system, the RAM does not contain $\perp$. Thus, we draw the conclusion that there is some evidence (of some event within the system).

Classification: In the next step, we might classify the identified evidence as a bit $\texttt{R} \in \{\texttt{0},\texttt{1}\}$ and conclude that it is a copy of some storage location that is not $\perp$.

This is a classifying property of that evidence, since we know that there is always a bit stored in `R`, whenever a `move` command is executed in our system. However, this is not yet an individual property, as we neither know the exact command that was executed, nor the storage location this particular value originates from.

Individualisation: Within the step of individualisation, we take a look into the RAM's content and notice that it contains the particular value `1`, for example. Hence, we know that this evidence can only have been copied from another storage location that contains this value.

Association: From the knowledge about our 3-bit automaton, we can conclude that the bit stored in `R` can only originate from ROM `B`, as it is the only storage that contains a `1`, besides `R`. Thus, we are able to state that the operation `mov B, R` has been executed (which is the event we just reconstructed) and caused this evidence. We can further specify the quantity of error to be `0` in this model, as there are no external influences and the only way to change the value in the RAM is to execute the `mov` command.

VII. Conclusion and Outlook

We believe that large parts of computer forensics can be founded on the same basic theory as other forensic sciences. This, however, makes it necessary to rethink methods and procedures of computer forensics in terms of this theory, i.e., using the notions of transfer and association. In this report, we have argued that this is indeed possible. It also forces the forensic investigator to formulate precise statements about the findings he makes. We feel that such statements, as well as their implications, are also easier to understand by non-technical persons involved in the prosecution of the crime (e.g., judges) because the notion of transfer is so fundamental. In our view, this is supported by our examples where the statements were:

1) Picture A was taken by digital camera B.
2) USB device A was attached to computer B.
3) Computer A visited website B.
4) Data in location A was copied from storage location B.

Prosecutors often formulate these statements as questions that should be answered by forensic scientists. Many more such questions can be asked in digital investigations, for example:

- Has email A been composed and sent on computer B?
- Was file A copied/downloaded to computer B?
- Does a particular keyword A occur in documents on computer B?
- Are there movies with content A stored on computer B?
- Was software A installed/used on computer B, for example some particular filesharing-, wiping-, or VoIP-software?
- Was computer A compromised by malicious software B, such as a banking trojan, for example?
- Using computer A, has an instant messaging/VoIP communication with user/computer B taken place?

Proving or disproving similar statements are at the core of what a forensic scientist in computer forensics should do. Answering any of these statements requires a high amount of specialization to establish the level of certainty necessary in court. This is the true "forensic science" part of computer forensics that we call *forensic computing*.

Guiding an investigation and formulating such questions in the process of an investigation is the "digital investigation" part of computer forensics. This can be performed by police officers and trained prosecutors who need proper knowledge of the crime (modus operandi, criminology, etc.) and a basic training in computers, but do not need the level of expertise of forensic scientists in forensic computing. We believe that this separation of concerns is the core of making computer forensics more scientific and reaching standards that are normal in other branches of forensic science: Investigators investigate, scientists associate.

Partly, the distinction between computer forensics and forensic computing is already common in practice. For example, the German police already distinguishes roles of *expert witnesses* ("Sachverständiger") and *investigative support* ("IT-Beweissicherung", "Digitale Beweismittel"). But even expert witnesses often lack a particular area of specialization and have to delve into concrete topics (like application analysis, computer architecture, reverse engineering) anew for every new case they have to deal with. While they do this using scientific methods, the efficiency of such undertakings can be much improved with an increased focus on concrete technical areas. The examples above argue strongly for the fact that *associations* can help us to identify these areas.

References

[1] A. Dewald and F. Freiling, "Is Computer Forensics a Forensic Science?" in *5th MPICC Interdisciplinary Conference on Current Issues in IT Security*, 2012.

[2] M. K. Rogers and K. Seigfried, "The future of computer forensics: a needs analysis survey," Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University, Tech. Rep. 2003-30, 2003.

[3] S. L. Garfinkel, "Digital forensics research: The next 10 years," in *Proceedings of the Digital Forensics Research Conferencs (DFRWS)*, 2010.

[4] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press, 2011, 3. Auflage.

[5] F. Cohen, *Digital Forensic Evidence Examination*. ASP Press, 2011.

[6] K. Inman and N. Rudin, "The origin of evidence," *Forensic Science International*, vol. 126, pp. 11–16, 2002.

[7] American Academy of Forensic Science, "AAFS," [Accessed October 28, 2011] Available from World Wide Web: http://www.aafs.org/, 2011.

[8] J. Toobin, "The CSI Effect: The truth about forensic science," *The New Yorker*, May 2007.

[9] K. Inman and N. Rudin, *Principles and Practice of Criminalistics: The Profession of Forensic Science*. CRC Press, 2000.

[10] H. Groß and F. Geerds, *Handbuch der Kriminalistik*. Verlagsgesellschaft Manfred Pawlak, 1977, vol. 1.

[11] R. Saferstein, *Criminalistics: An Introduction to Forensic Science*, 10th ed. Pearson, 2010.

[12] E. Locard, *L'enquete criminelle et les methodes scientifique*. Ernest Flammarion, Paris, 1920.

[13] P. L. Kirk, *Crime Investigation*. John Wiley & Sons, 1974, herausgegeben von John I. Thornton, 2. Auflage.

[14] H. C. Lee and H. A. Harris, *Physical Evidence in Forensic Science*. Lawyers and Judges Publishing, 2000.

[15] K. Mandia, C. Prosise, and M. Pepe, *Incident Response & Computer Forensics*. McGraw-Hill, 2003, 2. Auflage.

[16] B. D. Carrier and E. H. Spafford, "Defining event reconstruction of digital crime scenes," *Journal of Forensic Science*, vol. 49, no. 6, 2004.

[17] R. Böhme, F. C. Freiling, T. Gloe, and M. Kirchner, "Multimedia forensics is not computer forensics," in *Proceedings of the 3rd International Workshop on Computational Forensics*, ser. IWCF '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 90–103. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-03521-0_9

[18] B. D. Carrier and E. H. Spafford, "Getting physical with the digital investigation process," *IJDE*, vol. 2, no. 2, 2003.

[19] S. H. James and J. J. Nordby, Eds., *Forensic Science: An Introduction to Scientific and Investigative Techniques*, 3rd ed. CRC Press, 2009.

[20] M. Pollitt, "Applying traditional forensic taxonomy to digital forensics," in *Advances in Digital Forensics IV*, I. Ray and S. Shenoi, Eds. Springer Verlag, 2008, ch. 2, pp. 17–27.

[21] F. Cohen, "Toward a science of digital forensic evidence examination," in *IFIP Int. Conf. Digital Forensics*, ser. IFIP, K.-P. Chow and S. Shenoi, Eds., vol. 337. Springer, 2010, pp. 17–35.

[22] F. Cohen, J. Lowrie, and C. Preston, "The state of the science of digital evidence examination," in *IFIP Int. Conf. Digital Forensics*, ser. IFIP Publications, G. L. Peterson and S. Shenoi, Eds., vol. 361. Springer, 2011, pp. 3–21.

[23] M. Chen, J. J. Fridrich, M. Goljan, and J. Lukás, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, 2008. [Online]. Available: http://dx.doi.org/10.1109/TIFS.2007.916285

[24] J. Lukás, J. J. Fridrich, and M. Goljan, "Digital "bullet scratches" for images," in *ICIP (3)*, 2005, pp. 65–68. [Online]. Available: http://dx.doi.org/10.1109/ICIP.2005.1530329

[25] H. Carvey and C. Altheide, "Tracking USB storage: Analysis of windows artifacts generated by USB storage devices," *Digital Investigation*, vol. 2, no. 2, pp. 94–100, 2005. [Online]. Available: http://dx.doi.org/10.1016/j.diin.2005.04.006