ProCAVE: Privacy Preserving Collection and Authenticity Validation of Online Evidence

Efthymios Lalas[1], Lilian Mitrou[2,3], and Costas Lambrinoudakis[1]

[1] Department of Digital Systems,
University of Piraeus,
GR-18534, Greece
lalas@webmail.unipi.gr, clam@unipi.gr
[2] Department of Information & Communication Systems Engineering,
University of the Aegean,
GR-83200, Greece
l.mitrou@aegean.gr
[3] Department of Informatics,
Athens University of Economics and Business,
GR-10434, Greece

Abstract. It is an undisputable fact that nowadays many different types of crime are conducted by utilizing some type of electronic device - communication. To address this new situation, modern forensics tools evolved, becoming sophisticated enough to handle almost all kinds of digital content. However, surprisingly enough, collecting and validating the authenticity of online content remains, until now, a problem to resolve. The common practice is to capture (screen-shot) or save a web page, the authenticity of which is usually validated in a judicial process by an expert's testimony. In this paper, we introduce *ProCAVE*, a simple software architecture with a set of accompanying procedures, and we argue that their combined use can deliver evidence from online sources in the court, in a sound and privacy-preserving manner.

1 Introduction

The web today is used by billions of people, facilitating business, communication and exchange - dissemination of information. However, this new reality also has a "dark side" [5], since a series of crimes are committed through and with the use of it. Such crimes are known as: (a) *"Computer Crimes"* i.e. those posing a direct threat to data, information systems and networks, (b) *"Computer Related Crimes"*; i.e. crime perpetrated by means of a computer such as computer fraud, property rights infringements, and (c) *"Content-related Crime"*; such as child pornography, defamation via internet, etc.

In the legal system of most countries, guilt in a criminal proceeding is the summation of *means*, *motive* and *opportunity* [4]. However, the presence of those three elements is often not sufficient to convict someone; appropriate evidence must be presented that will prove that the opportunity was indeed taken by the accused for the crimes that he/she is charged (a U.S. example is stated in [4]).

S. Furnell, C. Lambrinoudakis, and J. Lopez (Eds.): TrustBus 2013, LNCS 8058, pp. 137–148, 2013.

Nevertheless, legal systems are mostly tailored to traditional types of crime. Any information obtained from the Internet has to convince the truth of a deed, which means that it must have all the attributes of conventional evidence. It has to be "irrefutable authentic", i.e. it must be possible to positively tie evidentiary material to the incident [5] and collected in accordance with formal requirements to establish its reliability [13] and admissibility. As for conventional crime, in order to prove the guilt and convict a person for having committed an offense, it is required to recognize, recover, reconstruct and present the digital evidence in a way that it renders it admissible in legal proceedings [11].

World Wide Web has become not only a crime scene, but also a breeding ground for primary and secondary sources of evidence. However, internet evidence, as internet content, is ex natura ephemeral and volatile, since it can be easily altered or deleted. Even though it should be stressed that, in general, with the advent of European digital signature legislation (Directive 2000/31/EC on electronic commerce), electronic material has gained a comparable legal status as paper material.

Considering crimes in which online content plays a crucial role, the main challenge is its collection, preservation and admissible presentation. In order to achieve its goal, i.e. allow and assist the court to form and pass a judgment, this online content has to be properly collected and its authenticity validated.

To this end, a number of different procedures have been employed around the world. Perhaps the most common one is taking a screenshot of a web site, printing it and validating its authenticity in the court by a witness' testimony [2,6]. The same procedure is followed with web pages that have been saved using the "Save As" function of the browser, or with other means of web page downloading. Recently, there are some tools that have also been proposed, mainly for forensics purposes, that save online content locally and perform some hashing and/or apply the current timestamp to the downloaded content [26].

There are cases where the aforementioned procedure, based on a witness' testimony, is not enough [3]. Furthermore, it is possible the content in question to be removed, so an expert from a certain company (usually WebArchive) is being called to provide evidence of what a web page looked like at a certain point of time. When this is not feasible, then the owner of the web site in question is called to testify, in order to provide evidence of the online content [3].

It is well known among the people involved in judicial processes, that the approaches described above cause too many controversies and concerns which often result in non-admissibility of the digital evidence. Some examples are: "The witness altered/photoshoped the screenshot", "The witness changed the html code of the saved web page before signing it", "The web page was not publicly available at that time", "The site's administrator/owner is in another country and cannot testify". Such statements demonstrate that the key element for online content admissibility is the validation of its authenticity; as stated in [7], once the authenticity of the electronic evidence has been validated, all other evidentiary problems are the common problems lawyers face all the time.

This paper proposes a novel way for collecting online evidence and validating its authenticity so as to be acceptable for evidentiary purposes. Our approach is based on the notion of web proxy, which has never been used before in collecting and validating the authenticity of web site content. It is argued that, as soon as someone identifies online content related to a crime, he/she can pass the request through a web proxy (belonging to a trusted authority) that will "freeze" the content, apply current timestamp and signatures and deliver the evidence to the user (a natural person, an organization or a public authority). Moreover, the same request can be simultaneously performed by other web proxies in order for the evidence to be securely stored in more than one servers. To demonstrate the applicability of the proposed solution, *ProCAVE* has been implemented and tested extensively with various web sites.

The rest of the paper is organized as follows: Section 2 reviews the current legal and technological status regarding the collection and validation of authenticity of online content. An overview of the proposed software solution is presented in Section 3. The experimental evaluation and results are discussed in Section 4 whereas Section 5 refers to some technical and other considerations.

2 Current Status and Motivation

Evidence has been present in legal systems since the first trial in the human history. All countries have incorporated rules and procedures that are deemed to be appropriate and legally robust for validating the authenticity of evidence in the court. Judge Grimm [14] has codified the rules governing the validation of the authenticity of web page evidence under the US Law. According to this categorization the most common rules for web pages are the following:

- 901(b)(1): witness with personal knowledge,
- 901(b)(3): expert testimony,
- 901(b)(4): distinctive characteristics of a web site,
- 901(b)(7): public records - usually from government web sites,
- 901(b)(9): system or process capable of producing a reliable result, and
- 902(5): official publications.

The important part of validating the authenticity (and thus admissibility) of the evidence is that one cannot rely on a simple method, since the degree of foundation which is appropriate in any given case is in the judgment of the court [14]. Thus, if multiple methods are used it is more likely that a court will deem the online content as authentic [9]. This is the main reason that all of the solutions that are currently used fail to produce undisputable results.

First of all, the authenticity of printed copies or captured images of a web site has to be validated by the witness in order to be admitted [20], a procedure that many times is still questionable especially when the witness is not independent (e.g. is not a police officer). Moreover, the exact time that the specific content was accessible online cannot be proven, since standard time-signing techniques cannot be applied [10].

Certain commercial tools [6,26] claim that they support a sound mechanism for collecting online evidence; the time issue may be resolved, however once again the user needs to validate the authenticity of the evidence in the court. The cost is another drawback, and of course when someone comes across online content that needs to be collected for legal purposes, no one expects him to buy a software only for saving an instance of a page!

Expert testimony (as is usually the case with Web Archive) is always an option. However companies that archive web pages do not store dynamic or personalized content, and there are also cases that some content has been removed before the page was archived. Moreover, it is surely very difficult (nearly unfeasible) for experts from Web Archive to testify in another country.

The last option is to have the web site's owner testify about the web site's content at a certain date/time. But this is very rarely done and of course even if such a testimony exists, it is still necessary to employ third party tools to prove the existence of the content.

Another essential feature missing from all above online content preservation techniques, and which has partially motivated our work, is the notion of privacy. More specifically, as described in [11], the use of forensics methods may itself constitute a violation of citizens' fundamental right to privacy; that's why digital evidence must - among others - comply with the respective provisions guaranteeing data privacy.

Finally, as extensively documented over the past few years [8,11,16], forensics, in general, lack standardization of methods and formats, a fact that causes many procedural problems. In terms of collection of online content, this is impossible with existing techniques, since they are proprietary, diverse and depend on each user's technical knowledge regarding evidence acquisition.

The above-described needs for a privacy-preserving, standardized method of independent collection of online content nurtured the seeds of our current work. To this end, our paper makes the following contributions:

- The first privacy-preserving web-based tool for collecting evidence from web pages, namely *ProCAVE* , is presented. It is demonstrated that it fulfills all the aforementioned requirements.
- A prototype of *ProCAVE* has been implemented and together with a dataset of known web sites has been used for the evaluation of its effectiveness and accuracy.

3 Solution Overview

This Section unravels the logic behind the proposed *ProCAVE* software solution. To accomplish its goals, *ProCAVE* is practically comprised of two elements: the *Web Proxy* and the *Collection and Validation of Authenticity (CVA) Engine*.

3.1 Web Proxy

As soon as a user discovers a web site, e.g. *www.abc.com*, whose content can be used as evidence, he/she visits the web site *www.xyz.com*, which serves as the

Web Proxy of *ProCAVE*. There he/she is presented - among other options - with an address field, where he/she can enter the url that he/she wants to navigate to. He/she enters *www.abc.com* and the *Web Proxy* receives the request, forwards it to *www.abc.com* and receives and forwards back the result. This procedure is depicted in Figure 1.

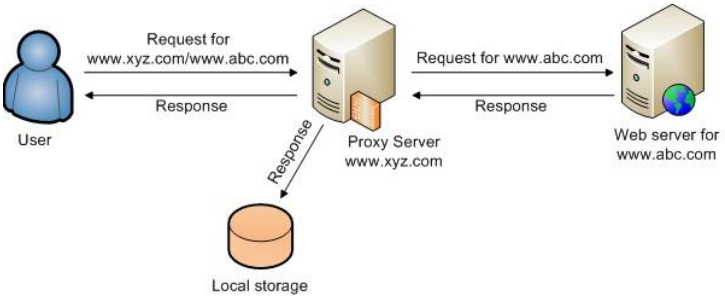

Fig. 1. Proxy HTTP request

Therefore, the user requests url *www.xyz.com\www.abc.com*, and he/she is presented with the contents of url *www.abc.com*. However, contrary to a conventional HTTP request, this specific request passes through the *ProCAVE Web Proxy* that keeps a copy of the response (i.e. HTML code, CSS, images, scripts etc.) locally. This means that whenever the user wishes, and provided that the content is the one that he/she wants to collect, he/she can proceed to the next step which is the *Collection and Validation of Authenticity* described next.

3.2 Collection and Validation of Authenticity (CVA)

Currently the user possesses content (a response), which is stored locally in the *Web Proxy*. He/she can now proceed with the validation of the authenticity of the stored content. This will be done, as shown in Figure 2, with the help of privacy, hashing and digital signing modules.

As soon as the user selects the CVA option, the id of the response is sent to the *Web Proxy*, along with some other parameters. These parameters reflect the privacy level that the user is requesting and correspondingly the confidentiality level for the collected content. To this end, if the user decides to use the privacy option, a blacklist/whitelist option is adopted; i.e. the user is allowed to choose some content and scramble all the other, or scramble some content and leave all the other intact. This scrambling is accomplished by sending the chosen HTML element ids, together with the selected option, to the *Web Proxy*, that modifies the content accordingly. The scrambling process engages the public key of the user, and is represented in Figure 2 with a dashed rectangular due to its optional use.

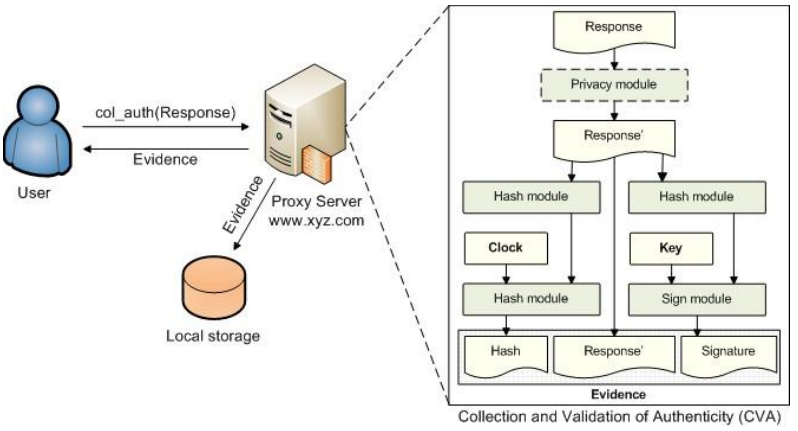

Fig. 2. Collection and Validation of Authenticity (CVA) Workflow

Next, a hashing of the (scrambled or unscrambled) content is performed, producing the "digest", which will be later utilized for the verification of the content. A timestamp (which has been produced at the time of the request) is concatenated to the digest, in order for the date and time to be bind to it, according to [10]. The concatenated "digest + timestamp" is fed once more to the hash module, producing the final hash value.

Up to now the proposed mechanisms ha maintained the original message while a message digest has been produced. In the final step of the CVA procedure, the original message is signed with the engine's private key, thus validating the authenticity of the evidence's creator, which is the engine itself. The final (signed) elements will be grouped together, forming the evidence of the online content. This evidence will be returned to the user, and it will be also stored locally for future reference.

3.3 Multiple Requests

As already discussed in previous sections, a single copy of digital evidence is not necessarily sufficient to prove a crime. It may be necessary to prove how the specific web site was visible to various locations around the world. Moreover, it may be necessary to store the evidence in various, geographically spread, locations.

The design of *ProCAVE* satisfies the above requirement. When a certain *Web Proxy* receives a request, it creates a copy of this request and forwards it to other Web Proxies. As a result, each one of these Web Proxies will collect and validate the authenticity of the *www.abc.com* web site's content, returning the resulting evidence. The returned evidence may be different from one *Web Proxy* to another, since the content of the same web site may differ from country to country. Nevertheless, the collection of online content from different locations

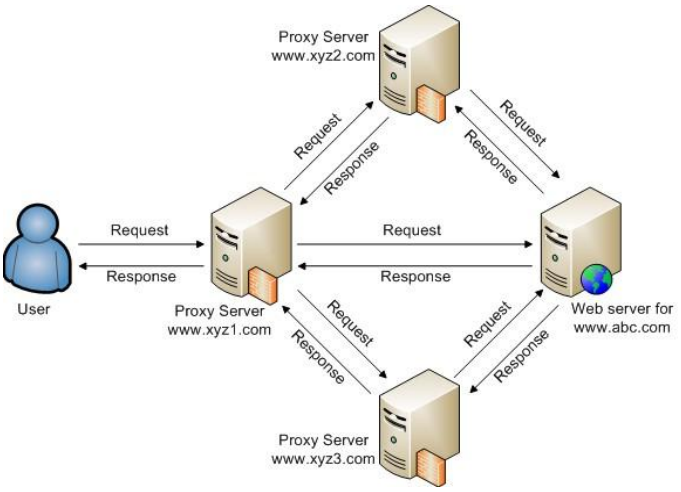

Fig. 3. Performing multiple requests

serves the purpose of: (a) storing evidence multiple times for security reasons and (b) depicting how a web site was appearing to the users around the world. Figure 3 illustrates this procedure.

3.4 Putting It All Together

Let's consider a simple use case scenario for *ProCAVE*.

Scenario. *The web site www.abc.com contains content that can be presented as evidence in a judicial process. It must be properly collected and its authenticity must be validated.*

Procedure. The user visits web site *www.xyz.com* (the *Web Proxy*) and through that proxy performs a request to the web site *www.abc.com*. The result of the latter request is shown on his/her browser. If this is the content that, according to the user, is related to a crime, then the user selects the content that he/she wishes (or does not wish) to be anonymized. Consequently, he/she chooses to store the content, and the website returns the evidence from multiple locations, along with validation of its authenticity.

The above procedure addresses all the problems related to evidence from online content. Specifically, the user has a fully-functional html file that can be presented to the court as its authenticity is proved. Moreover, the user can prove the exact date and time that the evidence was created and by which engine. Therefore if someone questions the initial evidence, he/she can take a copy from the corresponding engine to see if something has changed. In addition, there is evidence from multiple locations, something that provides the user with the opportunity to prove that this content was visible from around the world.

The way *ProCAVE* handles digital evidence covers more than one of the requirements stated by [14,24]; they can be admitted to court by a witness, an expert (administering the local copy of *ProCAVE*) can testify in the court regarding the locally stored content and this content can also fall under rule 901(b)(7) as public record, if *ProCAVE* is run by a governmental organization [15].

Last but not least, the entire procedure respects the privacy of the user, since he/she is given the option to scramble all the content that he/she wants to be invisible or not accessible to third/not authorized persons.

4 Implementation and Experimental Evaluation

4.1 Implementation

To evaluate the effectiveness and applicability of the proposed solution, *ProCAVE* was implemented as a PHP/MySQL software tool [22]. The implementation was based on a simple web proxy, described in [17], extended to include the collection and authenticity validation functions described in the previous sections.

More specifically, each time a request for a web site is performed through the *Web proxy*, a random 6-digit hex number is assigned to it and to the subsequent requests made for downloading the other components of the page (stylesheets, images, scripts, etc.). Thus, when the viewed page needs to be stored, the CVA engine uses this number to group all these files together (response). In terms of hashing, the standard `hash_file()` php function, with the 320-bit version of the RIPEMD algorithm, is utilised. On the other hand, digital signing is performed with the SHA-1 algorithm for hashing, followed by encryption with a private-key generated with the help of OpenSSL [23].

4.2 Results

ProCAVE was tested with various web sites of diverse content (news, academics, entertainment). For each of those web sites, evidence was collected through the proposed tool and was then compared to the content resulted from the usual "Save As" procedure supported by the browsers. The comparison was performed with the Similarity Analyzer [19], which examines two web pages and computes the percentage of HTML similarity and Text Similarity. The results for 10 web pages are depicted in Table 1.

It can be noticed that in most cases, HTML Similarity is close to 90%. This is an expected result, since both *ProCAVE* and the browser's "Save As" function change the links in the downloaded HTML code to point to local locations, which is different for those two methods. On the other hand, Text Similarity is close to 98%, which means that what someone can see through the browser is very close to what is saved through *ProCAVE*. The 2% difference on average is mainly due to text parts that are downloaded/altered in the browser, with standard or asynchronous scripting and not in the content saved through *ProCAVE*.

A graphical representation of the results, together with their mean values, is depicted in Figure 4.

Table 1. Results of the comparison between *ProCAVE* and the "Save As" function

Hex	Web page	HTML Similarity	Text Similarity
298168	inria.fr	99,86%	99,98%
558404	ssl.ds.unipi.gr	100%	100%
20d62f	news.yahoo.com	93,23%	96,72%
337ec6	spiegel.de	94,68%	99,38%
408faa	behind-the-enemy-lines.com	48,56%	90,59%
418f7e	maawg.org	94,57%	98,75%
75a048	ansa.it	97,31%	98,05%
79031e	bbc.co.uk	87,58%	95,79%
7a777b	slashdot.org	96,14%	99,13%
82400b	xkcd.xom	84,03%	100%

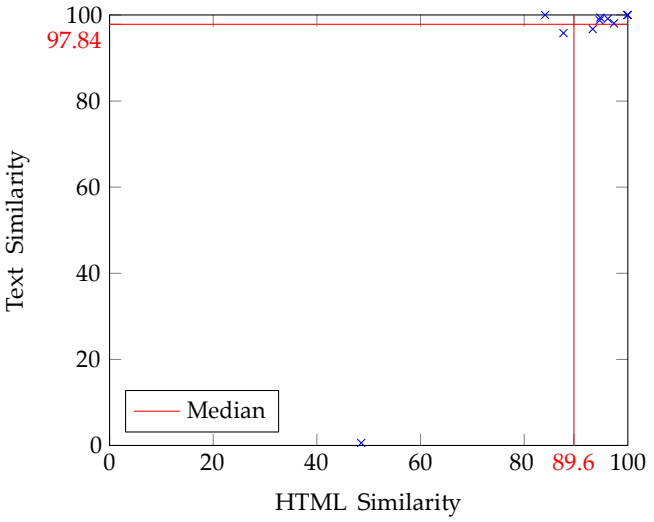

Fig. 4. Graphical representation of the results and their mean values

5 Anti-forensics and other Considerations

As stated in [1], from the very first day that digital computers and networks appeared, data hiding was, and continues to be, an issue. Since it is not expected that *ProCAVE* will be an exception to that, this section refers to technical and other issues that have mainly to do with anti-forensics.

Considering that *ProCAVE* will run in centralized locations (servers), a perpetrator could find all the domain names and ip addresses used by the tool and deny all requests originating from them - or, even worse, present legitimate content to them. A simple solution to that would be the use of a dynamic ip

address pool for the server's outgoing traffic, or the use of ip proxy servers that periodically change ip address.

Another anti-forensic technique would be the use of programming tools to present content to the user in a way not supported by *ProCAVE*, e.g. synchronous/asynchronous scripts. However, this is something that can be easily addressed through minor modifications of the way *ProCAVE* works. For instance, in the current implementation a javascript/ajax request would produce a false result, since it would modify content locally without making the correct changes in the saved copy. A solution would be to support listening of local events and simulating them to the remote end (with the use of a scriptable Web browser, like in [18]). Especially for the AJAX case, it is not a major issue since according to [25] only 3.2% of all web sites use this technology.

There are certain applications that do not fall under the above mentioned case; those would be flash-based web sites, specific chatting technologies etc. We believe that those services are out of this work's scope, since they represent instantly available content which does not resemble the traditional online content that *ProCAVE* deals with.

Since the functionality of *ProCAVE* will be publically available, it will be also vulnerable to attacks like denial-of-service (DOS), abusing etc. To that end, standard techniques for protecting a web site must be adopted, like firewalls, intrusion prevention systems, etc. Moreover, access to the website can be limited to registered users (perhaps owning a digital certificate), who will be able to perform a certain number of requests per minute.

Furthermore, regarding the use of digital certificates in *ProCAVE*'s privacy option, a Public-Key Infrastructure (PKI) must be used for their creation, management and revocation. However, the level of trust that is achieved depends heavily on the chosen Certificate Authority (CA). Simple implementations can make use of open source tools, like OpenSSL [23], but for large-scale use a commonly trusted entity must be employed.

Last but not least, an important issue refers to the authority which could be considered as being trustworthy enough to be held responsible for running this tool and keeping local copies of evidence. We argue that this issue has to be handled in accordance to the legal framework and the jurisdiction of the Forensics Department of each Country or Region; however, the distributed design of our tool and the fact that multiple requests can be performed (and multiple copies of the evidence can be saved) by remote servers, makes it easy for every individual or organization to run an instance of *ProCAVE*. In any case, we may assume that if more *ProCAVE* instances are involved, the integrity and acceptability of evidence and the procedure is better served and preserved.

6 Conclusions and Future Work

In this paper a simple software solution, namely *ProCAVE*, that can collect and validate the authenticity of content from online sources has been presented. To the best of our knowledge, *ProCAVE* is the first system that avoids the usual

local copies or screenshots of web sites (and the resulting dispute). Instead, it is based on an online architecture that collects evidence from multiple locations at the same time and, most importantly, in a privacy-preserving manner.

To verify it's correctness, a simple implementation of *ProCAVE* was employed for conducting a series of representative tests. The results of the tests have proved that the resulting evidence was of great resemblance to the content that the user was presented through his/her browser and thus that *ProCAVE* can produce acceptable digital evidence in real-time; i.e. during the time that the user sees the content on his/her screen, without involving him in any complicated procedures.

Future work will include modifications of the software so as to implement currently unsupported features, like listening to local events and modifying remote content accordingly, grabbing videos etc. The employment of *ProCAVE* by Forensics Departments around the world would also be of great importance, since it would provide valuable feedback from real-life scenarios.

Acknowledgements. The first author would like to thank Stavros Niarchos Foundation (*www.snf.org*) for supporting this work.

References

1. Berghel, H.: Hiding data, forensics, and anti-forensics. Communications of the ACM 50(4) (April 2007)
2. CanProve - Capture Online Evidence, http://canprove.com (last visited: March 2013)
3. Careless, J.: Collecting and authenticating online evidence, CBA Practicelink, (last visited: March 2013)
4. Commonwealth vs. Michael M. OLaughlin: Burglary, armed assault in a dwelling, assault and battery by means of a dangerous weapon, practice, criminal, required finding, Appellate Court Decision, No. 04-P-48 (2005)
5. Council of Europe (CoE), Explanatory Report to the Convention on Cybercrime, ETS 185 (2001), http://conventions.coe.int/Treaty/en/Reports/Html/185.htm
6. DVers - Digital Verification Services, http://www.dvers.gr (last visited: March 2013)
7. Fenner, M.G.: Evidentiary Problems Associated with the Introduction of Web-Based Evidence, LSN: Evidence (Public Law) (Sub-Topic) (December 2010), Available at SSRN: http://ssrn.com/abstract=1722714
8. Garfinkel, S.L.: Digital forensics research: The next 10 years. Digital Investigation: The International Journal of Digital Forensics & Incident Response 7, S64-S73 (2010)
9. Gibson, J.: A Primer on Admitting Web Page into Evidence, Nevada Lawyer Magazine, http://nvbar.org/articles/content/primer-admitting-web-pages-evidence (last visited: March 2013)
10. Hosmer, C.: Proving the Integrity of Digital Evidence with Time. International Journal of Digital Evidence 1(1) (2002)
11. Karyda, M., Mitrou, L.: Internet Forensics: Legal and Technical issues. In: 2nd Annual Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), Samos, Greece (August 2007)

12. Kerzner, M.: Evidence Authentication: Web Site Content, Atkison Baker, http://www.depo.com/E-letters/TheDiscoveryUpdate/2008/October/Articles/website_authentication.html (last visited: March 2013)
13. Leroux, O.: Legal Admissibility of Electronic Evidence. International Review of Law Computers and Technology 18(2), 193–220 (2004)
14. Lorraine, J.R., Mack, B.: Plaintiffs v. Markel American Insurance Company, Defendants. Civil Action No. PWG-06-1893, United States District Court for the District of Maryland (2007)
15. Mylonas, A., Meletiadis, V., Mitrou, L., Gritzalis, D.: Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition. In: Proceedings of the 27th IFIP International Information Security and Privacy Conference. AICT, vol. 376, pp. 249–260. Springer (2012)
16. Nixon, R.: Plug-In PHP: 100 Power Solutions: Simple Solutions to Practical PHP Problems. McGraw-Hill Education (2010)
17. PHP Scriptable Web Browser, http://www.simpletest.org/en/browser_documentation.htm (last visited: March 2013)
18. Similarity Analyzer, http://tool.motoricerca.info/similarity-analyzer.phtm (last visited: March 2013)
19. Sommer, P.: Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Adviders and Lawyers, 3rd edn. Version 3.0, Information Assurance Advisory Council (March 2012)
20. Tanenbaum, A.S.: Computer Networks, 4th edn. Prentice Hall Professional Technical Reference (2002)
21. ProCAVE Tool. Access available upon request
22. The OpenSSL Toolkit, http://www.openssl.org (last visited: March 2013)
23. U.S.Courts, Federal Rules of Evidence (December 1, 2010), http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/2010%20Rules/Evidence.pdf
24. Web Statistics - Key data of the Web, http://www.scriptol.com/web/statistics.php (last visited: March 2013)
25. X1 Social Discovery, http://www.x1discovery.com/social_discovery.html (last visited: March 2013)