Collecting evidence in the «Information Society»: theoretical background, current issues and future perspectives in «Cloud Forensics»

Collecting Evidence in the «Information Society»: Theoretical Background, Current Issues and Future Perspectives in «Cloud Forensics»

Autoren/Autorinnen: Federico Costantini / Marco Alvise De Stefani
Kategorie: Beiträge
Region: Italien
Rechtsgebiete: Sicherheit und Recht
Sammlung: Tagungsband IRIS 2017, Top 10 – Peer Reviewed Jury LexisNexis Best Paper Award des IRIS2017
DOI: 10.38023/6ed3ae5b-6079-498a-8006-7a1b1555a21d
Zitiervorschlag: Federico Costantini / Marco Alvise De Stefani, Collecting Evidence in the «Information Society»: Theoretical Background, Current Issues and Future Perspectives in «Cloud Forensics», in: Jusletter IT 23. Februar 2017

The increased adoption of «cloud computing» – allowing a partial or complete «virtualization» of computing resources – requires a particular method of investigative analysis of data, called «cloud forensics». In this paper we tackle technical and legal issues concerning its theoretical and practical aspects. After a short explanation of «Philosophy of Information» – taken as theoretical model – we introduce the issues pertaining «digital forensics» and then we propose some criteria in order to assess a cloud acquisition. In conclusion we provide an example and offer our final remarks.

Table of contents

1. Introduction: the challenges of «Cloud computing» in the legal field

[1] If the appearance of our «Information Society» can be described as distributed networks,[1] data are its substance and computation is its form. Indeed, current technologies allow not only to access huge and pervasive amounts of information, but also to handle «virtualized» computing resources.

[2] The cutting-edge trend in ICT is brought about by «cloud computing».[2] In it, such «virtualization» can be provided in very different ways,[3] yet the most common are known as «Infrastructure as a Service» (IaaS),[4] «Platform as a Service» (PaaS),[5] and «Software as a Service» (SaaS).[6]

[3] These technologies are spreading at a very fast pace not only in the legal, but also the illegal economy. Indeed, nowadays cybercrime is scattered in transnational networks capable of sudden attacks with severe damages and often irreversible consequences.

[4] The key issue is that, day by day, it becomes more and more difficult for investigating authorities to collect evidence. The main challenge is that, with such technologies, criminal activities don't leave any trace on the servers, so prosecutors have neither hard disks to access, nor a network to analyse or a data stream to intercept[7].

[5] In this paper we address legal and technical issues of «cloud forensics» in order to offer, on the one hand, the theoretical framework in which they are placed and, on the other hand, to detect criteria suitable to contribute to solving practical difficulties. To do so, we focus on three different profiles that can be expressed in the following answers: (1) from a philosophical-epistemical perspective, in which sense an «information» can be considered as «evidence»? (2) in a legal-theorical sense, how «information» can be introduced in legal proceedings? (3) forensically, what requirements should «digital evidence» gathered from a cloud fulfil in order to become affordable? In the next paragraphs, after discussing these issues, we provide an example of a peculiar technology developed according to the identified criteria and then we express some final remarks.

2. Theoretical framework: «Philosophy of Information» and «Onlife Manifesto»

[6] As «information» is not a material entity, many issues arise in contemporary legal thought. Among them, some are afflicting the concept of «proof», which needs to be redefined in order to include, on one hand, the idea of «information» in itself and, on the other hand, evidence collected with digital support[8].

[7] In order to provide a background explanation for the concept of «information», it is useful to recall the epistemical perspective better known as the «Philosophy of Information»,[9] which has been taken into consideration in the «Onlife Manifesto»,[10] a document promoted under the auspices of the European Union. In this regard, we focus on three main topics: (1) the ontological *status* of the «information», (2) the «Level of Abstraction» (LoA) and (3) the Multi-Agent System (MAS).

[8] Starting with the *first*, we may say that the «Philosophy of Information» shapes a metaphysical perspective from the cybernetic[11] vision, identifying three ontological *statuses* of «information»: (1) «Information *as* reality», for example the electrical signal, which is transmitted regardless of the message contained, (2) «Information *about* reality», that is information about natural phenomena, (3) «Information *for* reality», which conveys instructions or algorithms to one or many recipients. The evolution of the contemporary concept of «information» is represented in the following table[12].

Information theory[13]	**Cybernetics**	**Philosophy of Information**[14]
Technical information	Technological information	Information *as* reality
Semantic information	Natural information	Information *about* reality
Influential information	Cultural information	Information *for* reality

Table 1: Three ontological statuses of «information»

[9] Considering the *second* aspect, since the «Philosophy of Information» aims to overtake the

traditional distinction between «reality» and «representation», on the one hand, and between «object» and «subject», on the other hand, «information» is conceived within its «Level of Abstraction» (LoA) that represents the perspective adopted by the observer in gathering information. Precisely, a LoA is a formalized model of the observer's expectations concerning the inputs of the observation. [15]

[10] As regards the *third* profile, since in the «Philosophy of Information» every aspect of reality can be represented and thus formalized in «information», a LoA can contain many observers sharing resources and exchanging data in different ways.

[11] According to such perspective, the concept of legal system in itself can be redefined: political, institutional, economic, legal and also personal interactions can be conceived as MASs [16]. Thus, by means of legal rules it is possible to set LOAs in which not only the difference between *hardware* and *software* becomes irrelevant, but also between technological protocols and procedural regulations, or even people and machines. [17]

3. Legal Theory: legal proceedings as LOA and MAAS

[12] We can implement the vision brought by the «Philosophy of Information» into the legal system not only from a comprehensive view, as done in the previous paragraph, but also focusing on the workflows in which law actually is enforced. In such terms, a legal procedure can be generally arranged on a LoA defined as a given set of technological processes – natural and artificial, bureaucratic and technical in a strict sense – managed by a MAS including very heterogeneous figures (judges, lawyers, policemen, parties, witnesses, expert witnesses, court clerks, etc.) each pursuing its own strategy in gathering data and interacting with others. [18]

[13] If the structure of a legal proceeding can be shaped in a LoA and if its functions can be modelled in a MAS, then we can develop a vision in which each kind of «information» finds a correspondence in traditional legal concepts: (1) «Information *as* reality» includes «evidence», (2) «Information *about* reality» corresponds to procedural rules»; (3) «Information *for* reality» is represented by the judicial decision [19].

4. Forensic Sciences: a theoretical framework for digital and cloud forensics

[14] Provided that evidence has to be considered as «information *about* reality», additional issues arise concerning the «quality of information» collected. [20] Indeed, precautions have to be adopted in the process of abstracting information from facts so as to guarantee the affordability of data to be presented as evidence and discussed by parties in the proceedings. Historically, we can say that this is the purpose of all forensic disciplines, which have evolved and developed criteria, methods and standards to allow expert witnesses to contribute with their findings to the debate among non-experts (defendants, prosecutors, judges). [21]

[15] In «digital forensics», [22] two important features need to be identified. *Firstly*, since «information» becomes the very subject of inquiry, the technological factor needs indeed to be considered, so the continuous and fast evolution of ICTs requires endless forensic methodologies and *best practices* updates. *Secondly*, it becomes critical for expert witnesses to

be trusted in their findings as well as to have the most widespread technological *know-how* or to cope with elevated scientific understanding.[23] In this field «information quality» hangs on different factors, the most relevant of which are «data security» (confidentiality of investigative information), «data privacy» (discretion of personal matters) and «data transparency» (reviewability of procedures).[24] *Best practices*, acknowledged by international treaties and implemented by state legislations aim to establish a «chain of custody» of the physical support in order to safeguard the transparency of the operations performed on it.[25]

[16] Digital forensics, of course, has specialized in a sub-field of inquiry concerning «cloud forensics»[26] where «information quality» is even a more challenging task.

[17] The overall approach to this suite of technologies, methods and criteria is qualified as «hybrid» since it involves «technology» (different technologies, such as remote, virtual, network, live, large-scale, thin client, thick client), «organization» (different roles, such as cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) and «legislation» (multijurisdictional and multi-tenant situations). Each aspect presents various challenges, which have been discussed by scholars[27] and explored by governments.[28] Besides technical details cloud forensics is a very elusive concept, in fact, the contents of the cloud, by their nature, are extremely volatile and thus relevant data can be changed or no longer be available at the time of trial, due to several factors: for example, voluntary deletion, fortuitous event, data obsolescence, damaged infrastructure, database corruption. Furthermore, as said above, the cloud does not keep any trace of such modification[29]. Given these facts, it is mandatory to acquire evidence that can be considered identical to the source, even if original data is no longer available at the time of the trial, as in other branches of digital forensics (i.e. «forensics images» of hard disks).

[18] Unlike digital forensics, in cloud forensics there are still no specific standards or clear guidelines recognized at an international level. Hence, in this field to guarantee the «quality of information» – precisely: to ensure that the collected data are identical to the original even if those are missing – the only method is to adapt the current procedures (such as ISO/IEC 27037:2012).

[19] We argue that «information quality» in «cloud forensics» can be guaranteed designing an *ad hoc* clean and transparent virtual «forensics capture environment» fulfilling at least the following four criteria: (1) a secure connection has to be established between said environment (which is used by the forensics operator) and the web server containing relevant data (the information to be acquired), in the absence of devices that could tamper the content of the network traffic; (2) said environment has to be guaranteed to be clean from any kind of malware; (3) the data collector cannot have any kind of control on the platform and its processes; (4) the process has to be transparent and any alteration after the data collection has to be prevented.

5. The example of LegalEYE™

[20] Many commercial tools perform some of the previously mentioned criteria without any warranty on the fact that data cannot be subsequently modified or that data has not been altered before reaching the capture environment (intentionally, for incompetence or due to third parties)[30].

[21] This guarantee is provided instead by the LegalEYE™ platform (www.legaleye.it), supported by the Departments of Computer Science and of Legal Sciences in the University of Udine.

[22] LegalEYE™'s solution consists in an innovative procedure, based on ISO/IEC 27037:2012[31] but greatly improved and adapted to an online environment.

[23] The first part of the innovative approach is the change of the acquisition environment, which is now based on a monitored and protected cloud environment with an encrypted «evidence recording» service available for the forensics operator – or user – only. The user has no administration rights on this environment and is not able to alter the evidence collected or the network connection. The acquisition environment is not the user's device anymore, which can be affected by a virus or a malware that would alter/destroy the evidence and make it useless in front of the court.

[24] Another outcome of this approach is that the network connection between the acquisition environment and the web server containing the relevant data is the one between the target webserver and the LegalEYE™ monitored infrastructure, and not the user's Internet connection, which can be altered by a network device.

[25] The LegalEYE™ cloud environment relies on virtual machines. Every time a user starts an acquisition, a new virtual machine is powered up using a standard and certified template. The virtual machine template gets the current time and date from NTP servers, captures network traffic, records the video of the browsing activity, takes screenshots of the visited websites, gets data from the Domain Name System and uses other tools/commands such as ipconfig, route, arp, tcpdump, tracert, win32tm, nslookup, whoisCL, etc.[32]

[26] Thanks to this innovative approach and to other procedures, the collected evidences cannot be altered with errors, malice, malware or concealed network devices because the user has no way to modify the LegalEYE environment. All the collected evidences are automatically stored in an encrypted container, which is digitally signed using a timestamp and a strong Hash algorithm.

[27] From the user's perspective, LegalEYE™ is an online tool (rather than a software) accessible via a web-interface. The user logs into the LegalEYE™ website, starts the acquisition and is able to browse the Internet via the LegalEYE™ web interface, collecting evidences that are automatically checked, recorded, hashed, marked, encrypted and directly stored in a secure cloud environment and cannot be altered by any third party (including the user). The LegalEYE™ process of evidence collection is in compliance with the regulations and standards required by the law.

[28] When the user has completed his evidence collection he can download an encrypted archive with all the evidence and a whitepaper that describes the LegalEYE™ environment and outlines the set of technical and legal documents which LegalEYE™ is compliant with[33].

6. Final Remarks: from current issues to future opportunities

[29] *Cloud forensics* are very promising tools to be used in tackling the challenges of cybercrime.

[30] In order to be suitable for this aim, not only technological procedures have to be standardized, but also theoretical premises need to be clarified and legal framework has to be enforced accordingly.

[31] Provided that we intend to proceed in the following paths of research: (1) deepen the representation of the legal procedures in terms of LOA, according to the approach developed in the «Philosophy of Information»; (2) define the role of the «information quality» not only in forensic science (information about reality), but also as regards the procedural rules (information as reality) and court decision (information for reality); (3) improve the understanding of cloud forensics; (4) represent in terms of «second-order» systems the strategic behaviour of each agent within a legal procedure.

7. References

ASSOCIATION OF CHIEF OFFICERS POLICY, Good Practice Guide for Digital Evidence, Version 5, ACPO, 2012.

ATTANASIO, ANTONINO/COSTABILE, GERARDO (eds.), IISFA Memberbook 2012. Digital Forensics. Knowledge sharing among members of the IISFA Chapter, Experta, Forlì 2013.

ATTANASIO, ANTONINO/COSTABILE, GERARDO (eds.), IISFA Memberbook 2013. Digital Forensics. Knowledge sharing among members of the IISFA Chapter, Experta, Forlì 2014.

BARABÁSI, ALBERT-LÁSZLÓ, Network science, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 2013, Vol. 371, Issue 1987.

BARAN, PAUL, On Distributed Communications Networks. RAND Corporation papers, RAND 1962.

BATESON, GREGORY, Mind and nature: a necessary unity, Dutton, New York 1979.

BIRK, DOMINIK/PANICO, MICHAEL (eds.), Mapping the Forensic Standard ISO / IEC 27037 to Cloud Computing CSA (Cloud Security Alliance), 2013.

BORGMANN, ALBERT, Holding on to reality. The nature of information at the turn of the millennium, University of Chicago Press, Chicago 1999.

COUNCIL OF EUROPE, Electronic evidence guide – A basic guide for police officers, prosecutors and judges Version 1.0, 2013.

FLORIDI, LUCIANO, The Ethics of Information, Oxford University Press, London 2013.

FLORIDI, LUCIANO (ed.), The Onlife Manifesto. Being Human in a Hyperconnected Era, Open Access Springer, Berlin-Heidelberg 2015.

FLORIDI, LUCIANO, The Philosophy of Information, Oxford University Press, Oxford 2013.

FLORIDI, LUCIANO/ILLARI, PHYLLIS, The Philosophy of Information Quality, Synthese Library, 358, Springer, Berlin-Heidelberg 2014.

GETTIER, EDMUND, Is Justified True Belief Knowledge?, Analysis 1963, Vol. 23, Issue 6, pp. 121–123.

HARJINDER SINGH, LALLIE/ LEE, PIMLOTT, Challenges in applying the principles in ACPO cloud forensic investigations, the Journal of Digital Forensics, Security and Law 2012, Vol. 7, Issue 1, pp. 15–28.

IACIS, Internet Forensics and Investigation Training Program, 2015.

ILLARI, PHYLLIS/ALLO, PATRICKBAUMGAERTNER, BERT/D'ALFONSO, SIMON/FRESCO, NIR/GOBBO, FEDERICO/GRUBAUGH, CARSON/ILIADIS, ANDREW/KERR, ERIC/GIUSEPPE, PRIMIERO/RUSSO, FEDERICA/SCHULZ, CHRISTOPH/TADDEO, MARIAROSARIA/TURILLI, MATTEO/VAKARELOV, ORLIN/ZENIL, HECTOR, The Philosophy of Information – a Simple Introduction. Society for the Philosophy of Information, 2012.

KOHN, M. D./ELOFF, M. M./ELOFF, J. H. P., Integrated digital forensic process model, Computers & Security 2013, Vol. 38, pp. 103–115.

LUHMANN, NIKLAS, Soziale Systeme. Grundriss einer allgemeinen Theorie, Suhrkamp, Frankfurt am Main 1984.

MATURANA, HUMBERTO R./STAFFORD BEER, ANTHONY/VARELA, FRANCISCO J., Autopoiesis and cognition: the realization of the living, Boston Studies in the Philosophy of Science, 42, D. Reidel Pub. Co., Dordrecht 1972.

MELL, PETER/ GRANCE, TIMOTHY, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, U.S. Department of Commerce, Gaithersburg 2011.

NIST Cloud Computing Forensic Science Working Group, NIST Cloud Computing Forensic Science Challenges, 2014.

OLIVEIRA, JOSÉ ANTONIO MAURILIO MILAGRE/CAIADO, MARCELO BELTRÃO, Cloud Forensics. Best practice and challenges for process efficiency of investigations and digital forensics, Proceedings of the Eight Conference in Computer Science ICOFCS, Brasilia, 2013.

PALMER, GARY, A Road Map for Digital Forensic Research. Report From the First Digital Forensic Research Workshop (DFRWS), New York 2001.

PICHAN, AMEER/LAZARESCU, MIHAI/SOH, SIE TENG, Cloud forensics: Technical challenges, solutions and comparative analysis, Digital Investigation 2015, Vol. 13, pp. 38–57.

POVAR, DIGAMBAR/GEETHAKUMARI, G., A Heuristic Model for Performing Digital Forensics in Cloud Computing Environment. In: Mauri JaimeLloret, Thampi SabuM, Rawat DandaB, Jin Di (eds.), Security in Computing and Communications, Communications in Computer and Information Science, Springer, Berlin-Heidelberg 2014, pp. 341–352.

RUAN, KEYUN/CARTHY, JOE/KECHADI, TAHAR/BAGGILI, IBRAHIM, Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results, Digital Investigation 2013, Vol. 10, Issue 1, pp. 34–43.

RUAN, KEYUN/CARTHY, JOE/KECHADI, TAHAR/CROSBIE, MARK, Cloud forensics, Advances in digital forensics VII Springer, Berlin-Heidelberg 2011, pp. 35–46.

SCHAFER, BURKHARD, Information Quality and Evidence Law: A New Role for Social Media, Digital Publishing and Copyright Law? In: Floridi Luciano, Illari Phyllis (eds.), The Philosophy of Information Quality, Synthese Library, 358, Springer, Berlin-Heidelberg 2014, pp. 217–238.

SHARMA, SUGAN, Evolution of as-a-Service Era in Cloud. https://arxiv.org/abs/1507.00939v1, 2015.

SIMON, JUDITH, Distributed Epistemic Responsibility in a Hyperconnected Era. In: Floridi Luciano (ed.), The Onlife Manifesto, Springer, Berlin-Heidelberg 2015, pp. 145–159.

SIMOU, STAVROS/KALLONIATIS, CHRISTOS/KAVAKLI, EVANGELIA/GRITZALIS, STEFANOS, Cloud Forensics: Identifying the Major Issues and Challenges. In: Jarke Matthias, Mylopoulos John, Quix Christoph, Rolland Colette, Manolopoulos Yannis, Mouratidis Haralambos, Horkoff Jennifer (eds.), Advanced Information Systems Engineering, Lecture Notes in Computer Science, Springer, Berlin-Heidelberg 2014, pp. 271–284.

VAN BEEK, H. M. A./VAN EIJK, E. J./VAN BAAR, R. B./UGEN, M./BODDE, J. N. C./SIEMELINK, A. J., Digital forensics as a service: Game on, Digital Investigation 2015, Vol. 15, pp. 20–38.

WEAVER, WARREN, The Matemathics of Communication, Scientific American 1949, Vol. 181, Issue 1, pp. 11–15.

---

1 BARAN, On Distributed Communications Networks; BARABÁSI, Network science, Philosophical Transactions of the Royal Society A.

2 *Cloud computing* has been defined as «*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*». MELL/GRANCE, The NIST Definition of Cloud Computing, p. 6.

3 SHARMA, Evolution of as-a-Service Era in Cloud.

4 In IaaS «*the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client*

interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings». MELL/GRANCE, The NIST Definition of Cloud Computing, p. 7.

5 In PaaS «*the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment*». Ibid.

6 In SaaS «*the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)*» . Ibid.

7 In other words, to understand if and how, for example, a specific file stored on a cloud can be considered legally as «evidence», it has to be legally granted the relationship among the circumstances as such (the historical fact as it happened), their knowledge (the legitimacy of the belief built upon it) and their representation in trial (its meaning in that given context).

8 As for the first aspect, networked data produce results expressed in terms of statistical probability which cannot be qualified neither as empirical finding, nor as full presumption or legal argument. Regarding the second profile, «digital evidence» is neither an empirical medium (a physical «thing»), nor a witness» statement (an intangible «word»), thus it is complicated, according to traditional legal science, to validate the veracity of a source, the accuracy of an analysis or the integrity of a results.

9 FLORIDI, The Philosophy of Information.

10 FLORIDI (ed.), The Onlife Manifesto. Being Human in a Hyperconnected Era.

11 *See* BATESON, Mind and nature: a necessary unity; MATURANA/STAFFORD BEER/VARELA, Autopoiesis and cognition: the realization of the living, Boston Studies in the Philosophy of Science.

12 It is important to observe that only one of the three concepts detected, the «information *about* reality», can be «true» or «false». In other words, it can be qualified by an «alethic» value. Therefore, we can state that the concept of «evidence» can be included only in this genre.

13 WEAVER, The Matemathics of Communication, Scientific American, pp. 11–15 (p. 11).

14 BORGMANN, Holding on to reality. The nature of information at the turn of the millennium.

15 From such perspective, the outcome of an analysis – its «meaning» – requires: (1) the preliminary definition of a LoA; (2) a rigorous epistemic strategy in qualifying the findings as observable «objects», *see* ILLARI ET AL., The Philosophy of Information – a Simple Introduction; FLORIDI, The Ethics of Information, p. 29.

16 Law in itself becomes a kind of social technology – maybe the most efficient one – since legal rules are designed with the specific purpose of controlling interactions among people. More precisely, laws contribute in determining the ecosystem of technological processes where MASs are operating.

17 This perspective is very similar to that envisioned by Luhmann, *see* LUHMANN, Soziale Systeme. Grundriss einer allgemeinen Theorie.

18 Some scholars argue that each agent in a MAS is charged with an «epistemic responsibility», assuming the duty – qualified almost as an ethical obligation – to gather, organize and share valuable information to enable others making rational decisions and obtain effective results from their interactions. SIMON, Distributed Epistemic Responsibility in a Hyperconnected Era, pp. 145–159.

19 We can qualify a juridical proceeding as a kind of system exchanging information with its environment: on the one hand it receives certain inputs (evidences and procedural rules) just, on the other hand, it generates certain outputs (decisions and other minor outcomes). In this sense, in terms of «information about reality» we can build an abstract and general definition of evidence regardless of its empirical nature (a written document or a witness hearing) and its physical support appearance (a physical media or an electronic device).

20 FLORIDI/ILLARI, The Philosophy of Information Quality.

21 As an example, we can mention the illustrative factors considered by U.S. jurisprudence in order to

assess an expert witness' opinion, expressed in form of a check-list according to decision Daubert / Merrell Dow Pharmaceuticals (1993): «*(1) whether the expert's technique or theory can be or has been tested – that is, whether the expert's theory can be challenged in some objective sense, or whether it is instead simply a subjective, conclusory approach that cannot reasonably be assessed for reliability; (2) whether the technique or theory has been subject to peer review and publication; (3) the known or potential rate of error of the technique or theory when applied; (4) the existence and maintenance of standards and controls; and (5) whether the technique or theory has been generally accepted in the scientific community*» (*see* Federal Rules of Evidence, art. VII, Rule 702).

22 Digital forensics have been defined as «*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*». PALMER, A Road Map for Digital Forensic Research, p. 23. Scholars classified in different taxonomies the activities performed in digital forensics and developed various models. KOHN/ELOFF/ELOFF, Integrated digital forensic process model, pp. 103–115.

23 SCHAFER, Information Quality and Evidence Law: A New Role for Social Media, pp. 217–238.

24 VAN BEEK/VAN EIJK/VAN BAAR/UGEN/BODDE/SIEMELINK, Digital forensics as a service: Game on, pp. 20–38.

25 CoE «Budapest» Convention on Cybercrime of 23 November 2001 (STE n. 185), art. 19 par. 3: «*Each Party shall adopt such legislative and other measures […]. These measures shall include the power to: a) seize or similarly secure a computer system or part of it or a computer-data storage medium; b) make and retain a copy of* those *computer data; c) maintain the integrity of the relevant stored computer data […]*».

26 Cloud forensics have been defined as «*the application of computer forensics principles and procedures in a cloud computing environment*». POVAR/GEETHAKUMARI, A Heuristic Model for Performing Digital Forensics in Cloud Computing Environment, p. 341–352 (p. 344).

27 PICHAN/LAZARESCU/SOH, Cloud forensics: Technical challenges, solutions and comparative analysis, pp. 38–57; RUAN/CARTHY/KECHADI/CROSBIE, Cloud forensics, pp. 35–46; RUAN/CARTHY/KECHADI/BAGGILI, Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results, pp. 34–43. Said challenges are «unique» to the cloud environment, or «exacerbated» by it. Some scholars propose a different taxonomy in forensics» process – i) Identification, ii) Preservation, Collection, iii) Examination, iv) Presentation – and classify challenges according to the phases afflicted by them. SIMOU/KALLONIATIS/KAVAKLI/GRITZALIS, Cloud Forensics: Identifying the Major Issues and Challenges, pp. 271–284 (p. 275).

28 NIST Cloud Computing Forensic Science Working Group, NIST Cloud Computing Forensic Science Challenges.

29 From a practical perspective, we could say that, while in digital forensics usually evidence emerges only after the acquisition of the physical support or the access to the domain, in cloud forensics data are immediately detectible and readily visible, but remain difficult to fix in a definitive and univocal representation. Let us assume that we need to secure evidence from a Facebook chat. If we could analyse the physical device used, the forensic procedure would be quite easy: using a «write blocker», calculating the «hash» and generating a digital «time stamp», we would obtain a «forensic image» of the hard drive; only after that we would look for Facebook artefacts, a complex challenge indeed. If, on the contrary, we would acquire evidence directly from Facebook, the data could be easily identified, but it would be required a different process to collect them, assuming that the provider would not enable access to servers. Obviously, a printed web page or a saved screenshot are not suitable for constituting evidence, notwithstanding what many lawyers still believe.

30 Some experts use tools like Linux-live based operating system – such as DEFT (http://www.deftlinux.net/it/) or Caine (http://www.caine-live.net/) – in order to monitor network traffic (via «dump»), record the browsing activity (via video), generate various system logs and finally secure the result (with a digital «time stamp»). This laborious procedure, prone to human error due to several tasks to be performed, still does not provide any technical guarantee of the authenticity of the evidence collected.

31 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.

32 All this jobs are performed while another part of the LegalEYE™ cloud environment monitors the

infrastructure itself, guaranteeing safeguard, compliance and reproducibility. The security of the LegalEYE™ environment takes advantage of Citrix Netscaler, Layer 7 firewalls, Zabbix, and other powerful and well-known services.

33 CoE «Budapest» Convention, cit.; BIRK/PANICO (eds.), Mapping the Forensic Standard ISO / IEC 27037 to Cloud Computing CSA (Cloud Security Alliance); NIST Cloud Computing Forensic Science Working Group, NIST Cloud Computing Forensic Science Challenges; COUNCIL OF EUROPE, Electronic evidence guide; IACIS, Internet Forensics and Investigation Training Program; ASSOCIATION OF CHIEF OFFICERS POLICY, Good Practice Guide for Digital Evidence; HARJINDER SINGH/LEE, Challenges in applying the principles in ACPO cloud forensic investigations, pp. 15–28; OLIVEIRA/CAIADO, Cloud Forensics. Best practice and challenges for process efficiency of investigations and digital forensics; ATTANASIO/COSTABILE (eds.), IISFA Memberbook 2012; ATTANASIO/COSTABILE (eds.), IISFA Memberbook 2013.

0 Kommentare

Es gibt noch keine Kommentare

** Pflichtfelder*

Was ist Ihr Kommentar?

Titel:

Ihr Kommentar: *

Name: *

Federico Costantini

Senden

Ihr Kommentar wird durch eine Moderatorin bzw. einen Moderator geprüft und in Kürze freigeschaltet.

Source details

usletter IT

Scopus coverage years: from 2017 to 2019

Publisher: Weblaw AG

E-ISSN: 1664-848X

Subject area: Social Sciences: Law | Computer Science: Computer Science (miscellaneous)

View all documents > | Save to source list | Journal Homepage

CiteScore 2019
0.1

SJR 2019
0.121

SNIP 2019
0.071

CiteScore | CiteScore rank & trend | Scopus content coverage

Improved CiteScore methodology

CiteScore 2019 counts the citations received in 2016-2019 to articles, reviews, conference papers, book chapters and data papers published in 2016-2019, and divides this by the number of publications published in 2016-2019. Learn more >

CiteScore 2019

$$0.1 = \frac{18 \text{ Citations } 2016 - 2019}{356 \text{ Documents } 2016 - 2019}$$

Calculated on 06 May, 2020

CiteScoreTracker 2020

$$0.1 = \frac{19 \text{ Citations to date}}{356 \text{ Documents to date}}$$

Last updated on 10 June, 2020 • Updated monthly

CiteScore rank 2019

Category	Rank	Percentile
Social Sciences – Law	#632/685	7th
Computer Science – Computer Science (miscellaneous)	#63/64	2nd

View CiteScore methodology > | CiteScore FAQ > | Add CiteScore to your site