LEGAL EYE: AN INNOVATIVE TOOL TO COLLECT ONLINE E-EVIDENCE

Michele Della Marina / Dario Tion

Network and Security Engineer, M.D. Darnet UK LTD
152, City Road, EC1V 2NX London, UK
dellamarina@darnetltd.co.uk / dellamarina@gmail.com; www.darnetltd.co.uk

CEO, legalEYE srl
Via Vittorio Cadel 9, 33100 Udine, IT
tion@legaleye.it; www.legaleye.it

Keywords: ***Cybercrime; E-evidence; Safer Internet; Illegal online content; cyberbullying; Cloud Forensics; IPR infringements & forgery***

Abstract: *EU statistics show a steady increase in online cybercrime. There isn't an international standard procedure to acquire evidence from Internet in a forensically sound way. The Legal Eye™ project is an innovative web-based SaaS solution in the area of fight against cybercrime. It addresses specifically the process of gathering and storing the evidence of an online crime. Legal Eye™ provides an innovative solution to acquire online e-evidence, using an automated procedure admissible in court.*

1. Cybercrime

We have entered an era where digital technologies and the Internet are becoming the key enablers of prosperity and freedom, creating a foundation for our society and the economy. At the same time, these key enablers are becoming a feeding ground for criminal activities (online) that are becoming bigger, more frequent and more complex.

Cybercrime is, by its nature, a borderless, evolving and continuously advancing problem of global society. The effective fight against online criminal activities is pivotal to assure a high level of information security and secure business and consumer confidence required to keep the online economy striving. New technologies create new criminal opportunities such as online defamation, stalking, harassment, cyberbullying, identity theft, online fraud and forgery, unauthorised access, illegal online content.

According to the International Press Institute [IPI, 2015], the number of convictions for criminal defamation and insult in the EU vary between the countries, with Germany being the strictest country in this respect (21,963 convictions in 2013). The average number of defamation per capita (EU in 2013) is at the level of 3.22 cases for 100'000 citizens. The average annual growth of defamation cases is at the level of 5%. Based on the «Report on EU customs enforcement of intellectual property rights» [European Commission, 2014], in 2014 the total number of IPR infringement cases in the whole EU reached 95,194 level, an increase of 10% from 2013. When looking at the growth rate of the IPR infringements, we can see steady growth since 2007 at the average level of ca. 10.2% per year reaching 95'194 cases in 2014 (on the EU28 level) [Eurostat, 2017].

Many cybercrimes have gone unpunished as evidence of crime has been deleted before the collection process could start. The digital evidence requires to be forensically sound in order to be admissible in court proceedings.

2. Forensically Sound Evidence

«Forensically sound» is a term used extensively in the digital forensics community to qualify and, in some cases, to justify the use of a particular forensic technology or methodology. Despite the variations in the use

of «forensically sound,» there remains one universally consistent objective for a digital forensic process – the need to ensure that the end product does not lose its evidentiary weight and, therefore, its admissibility as evidence [McKemmish, 2008].

In the absence of specific guidelines and standards recognized at an international level, «forensically sound» is proposed and four criteria are provided for determining whether or not a digital forensic process for acquiring online content may be considered to be «forensically sound» [Costantini, 2016].

Defining the «environment» as the environment within which the acquisition is performed by the operator, the «operator» as the one who performs the evidence collection procedure, «malware«[1] as a software which is specifically designed to disrupt, damage, or gain authorized access to a computer system, «server» as a computer program or a device that provides functionality/data for other programs or devices, the four criteria are defined as follows. (1) The «environment» needs to be clean and free from any kind of «malware»; (2) a secure connection has to be established between the «environment» and the «server» containing relevant data; (3) the «operator» collecting data cannot have any kind of control on the «environment»; (4) the process has to be transparent. The first criterion states that in case where a malware is present in the environment, since it can cause unpredictable behaviours, the evidence collected may be altered therefore it is not genuine and differs from the original. The second criterion states that the digital communication between the environment and the server containing the relevant data must be protected. Protecting the digital communication means that there is no way to introduce any device to alter the data between the two end points. The third criterion states that the operator must be prevented from altering the environment, otherwise it could affect the integrity of the collected data. The fourth criterion states that the forensic process has to be accurate and reliable. It is of paramount importance that the forensic process is transparent and capable of being independently verified. Transparency can be achieved by documenting all the steps, identifying the tools and procedures used, detailing the analysis environment. All these elements have to be technically certified in order to become evidence and fulfil not only the requirements of data transparency, but their final purpose, which is to allow an unbiased discussion and a fair decision.

3. Current state-of-the-art and methodologies

In order to guarantee that the collected evidence has not been modified or altered, even if only partially, at a time after its first issue, it is important to have techniques that are highly secure and robust, and which do not allow substantially in any way the intentional, and in some cases fraudulent, modification of the aforementioned collected evidence.

People wrongly think that printing online evidence such as e-mail, website pages or taking the picture of the screen (screenshot) is enough as evidence. It is generally possible, and not extremely complex, to take a picture of a website (screenshot) and then edit the acquisition date directly on the electronic document (for example, a previous date at the effective date of acquisition) or modify the content of the electronic document itself, for example using a photo-editing software program, by altering reference or a relevant link, or deleting a text field, or by changing the URL address of the website by rewriting it and / or disguising it [McKemmish, 2008].

According to our professional experience, more and more digital forensic experts are using software-based products for evidence collection, which need to be installed on a computer. Most of the time, such software products simply help and guide to download the online content (rather than forcing the operator to follow a manual procedure) and they do not guarantee that the collected data conforms to the original (referring to the criteria listed in the previous chapter). These software products are not reliable as they depend on other parts of the computer (hardware and other software installed on the computer).

[1] Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of harmful or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. Malware is defined by its malicious intent, acting against the requirements of the computer use (https://en.wikipedia.org/wiki/Malware).

In fact, it is possible to modify and alter the environment where the evidence collection takes place by installing tampering devices, or simply the computer being used to collect the online evidence might be affected by virus or malware. This approach has significant security issues and disqualifies the collected evidence as it proves to be different from the original.

Some Digital Forensic experts adopt procedures more rigorous than software or a screenshot, in fact the current state-of-the-art in terms of forensic tools to collect online evidence is represented by Forensic «Linux Live»[2] distributions. Forensic Linux Live distribution is based on the Linux Operating System tailored for Forensic Analysis, with the purpose of running live on systems without corrupting the devices connected to the PC where the boot process takes place. The Linux Live distributions still have some disadvantages: they may not comply with the 4 criteria discussed in the previous chapter, require extended manual activity subject to human error, they are not standardised and involve a long analysis by the other party in order to accept their validity. Moreover, since the environment where the data collection takes place might have been altered by the operator (by negligence or on purpose) who still has control over it, there is no guarantee that the collected evidence is identical with the original [McKemmish, 2008].

In the face of all these possibilities of alteration and modification of digital data, the known certification methods discussed so far generally do not offer high security and guaranteed parameters.

4. Legal Eye™

The Legal Eye™ project is an innovative web-based SaaS[3] solution which addresses directly the biggest challenge faced during the process of gathering and storing the evidence of an online crime that is admissible in court proceedings. The Legal Eye™ solution highly innovates the current state-of-the-art where the e-evidence, to be admissible in a court, needs to be collected by digital forensic experts in a lengthy and manual procedure and even then, human error can disqualify the collected evidence from being used in court [Horizon 2020 Call, 2015].

Specifically, Legal Eye™ meets the need to acquire the Internet online content via a web browser running inside the Legal Eye™ infrastructure located in a protected cloud environment. There is no need to install any software since the evidence collection procedure is being performed in a controlled and highly secure cloud environment (network data traffic inspected by Application Layer firewalls and infrastructure controlled by 24/7 monitoring systems). In order to access the Legal Eye™ infrastructure, the user is required to enter username and password, once the authentication procedure completes successfully, the user is presented with a «browser within a browser». Therefore, Internet browsing does not take place on the user's device (which is vulnerable to malicious software and potential tampering, result of negligence or done on purpose) but in a protected and constantly monitored infrastructure. In particular, the Internet browsing takes place in a «read-only» virtual machine (which means that the virtual machine and all the included elements cannot be altered at all, not even by mistake) which is automatically generated from scratch by a certified standard template and automatically destructed once the acquisition procedure is complete. The virtual machine is free from malware or virus and, since is protected and locked, the user does not have any control on it. The only feature available in the virtual machine is the browser which is being used to collect online evidence only; any other standard functionality offered by the browser is locked and unavailable to the user. The whole Internet navigation is automatically recorded into a video file, manual screenshots are available to the user who might require

[2] A live CD (also live DVD, live disc, or live operating system) is a complete bootable computer installation including operating system which runs directly from a CD-ROM or similar storage device into a computer's memory, rather than loading from a hard disk drive. It allows users to run an operating system for any purpose without installing it or making any changes to the computer's configuration (https://en.wikipedia.org/wiki/Live_CD).

[3] Software as a service (SaaS; pronounced /sæs/ [Horizon 2020 Call, 2015]) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted (https://en.wikipedia.org/wiki/Software_as_a_service).

to collect specific information displayed on the web pages such as images or text which are of interested. Once the Internet browsing is complete, the whole digital content acquired (evidence of interest alongside the technical data such as log files, metadata and so on) is compressed into an encrypted archive protected by a password chosen by the user and known by the user only. No-one else is able to access the archive (neither the Legal Eye™ system administrators).

To summarise, the output of the whole Legal Eye™ procedure is an encrypted archive available to the user only, based on the collected evidence accompanied by a whitepaper (Technical Report) based on a set of technical and legal documents with which Legal Eye™ is compliant. The whole archive generated is validated via a Hash[4] function, which is reported in the Technical Report, and a Timestamp[5] is applied, compliant with the standard procedures used for forensic copies. The encryption method being used is SHA-256 for the Hash and AES256 for the encrypted archive.

Legal Eye™ acquires several technical data such as log files and metadata to certify that the collected online evidence conforms to the original. Some of those data are reported as follows, in a non-exhaustive manner: detection of current date and time, system time synchronization with the server «time.ien.it», entire recording of the network traffic generated during the session, video recording of the whole activities carried out, screen-shots of web pages visited containing elements of interest, acquisition of web pages using GNU Wget , data related to the Domain Name System, several system commands such as ipconfig, route, arp, tcpdump, tracert, win32tm, nslookup, whoisCL.

We can argue that Legal Eye™ meets the requirements and fulfils the four criteria detailed in the previous chapter [Costantini, 2016]. (1) The environment needs to be clean and free from any kind of malware has been proved to be true, since Legal Eye™ is a protected cloud based infrastructure providing with self-destructing virtual machines automatically generated based on a standard template; (2) a secure connection has to be established between the environment and the server containing relevant data is also a fulfilled criteria: in fact, the Legal Eye™ infrastructure cannot be altered since cannot be accessed neither tampered, because self-contained in the cloud; (3) the operator collecting data cannot have any kind of control on the environment is another met requirement since the virtual machine provided to the user is entirely locked and inaccessible a part from the web browser being used for the evidence collection; (4) the process has to be transparent, it is proven by the fact that Legal Eye™ generates a Technical Report providing with all information regarding the acquisition methodology, evidence collection and a video recording the whole acquisition procedure.

Legal Eye™ is compliant with specific regulatory requirements in terms of acquisition of digital data which respond promptly to current standards, established and widely recognized by the technical-scientific community[6] at national and international level in terms of Network Forensics and Cloud Forensics.

5. Towards the future of the e-evidence collection in the European Union

The digital era and the Internet have facilitated the growth and the sharing of digital information thanks to the Web technologies, Blogs and Social Networks. This is the reason why concepts such as «digital identity» and «digital reputation» are acquiring more and more importance.

---

4 A cryptographic hash function is a special class of hash function that has certain properties which make it suitable for use in cryptography. An important application of secure hashes is verification of message integrity. Verifying the authenticity of a hashed digest of the message is considered proof that the message itself is authentic (https://en.wikipedia.org/wiki/Cryptographic_hash_function).

5 Trusted timestamping is the process of securely keeping track of the creation and modification time of a document. Security here means that no one – not even the owner of the document – should be able to change it once it has been recorded provided that the timestamper's integrity is never compromised (https://en.wikipedia.org/wiki/Trusted_timestamping).

6 ISO, 2012; IACIS, 2015; Chauhan/Panda, 2015; Meyer/Stander, 2015; NIST, 2014; Shipley/Bowker, 2014.

Considering how the mobile technology is evolving alongside the digital data, we believe that the forensic acquisition tools should be developed accordingly. Legal Eye™ is committed to developing easy-to-use plugins and applications in order to facilitate the evidence collection on mobile devices and from social networks such as Twitter™, Facebook™, LinkedIn™ and so on. We believe that an interesting challenge for the future will be designing and developing easy-to-use application for evidence collection, tailored for each type of potential users, so that everyone will be able to collect valid evidence by himself tackling efficiently the growing cybercrime.

We are also willing to develop collaborative research projects such as the Evidence Project[7].

6. Conclusion

We are witnessing a dramatic grow of cybercrime activities in EU such as online defamation, stalking, harassment, cyberbullying, identity theft, online fraud and forgery, unauthorised access, illegal online content. These cybercrime actions cannot be resolved via technical solutions; moreover the volatility of the online data requires that a solution has to be put in place to acquire online evidence of these crimes, in order to protect the rights during the court proceedings.

Four criteria are identified for determining whether or not a digital forensic process for acquiring online content may be considered to be «forensically sound». As mentioned previously, the four criteria are: (1) «Environment» free from malware; (2) Untampered connection between the «environment» and the «server»; (3) «operator» unable to alter the acquisition process; (4) transparent process suitable to third party verification.

A solution that complies with these four criteria has been designed and implemented, it has been called Legal Eye™ and it allows acquiring online content using a procedure which is not contestable. Since the Legal Eye™ solution will be available «as a service» to each type of potential user (private individuals or companies) and it is aiming at improve the rights during the court proceedings, the impact on the society in the EU countries will be subject of further analysis.

7. References

Sudhanshu Chauhan/Nutan Kumar Panda, Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques, Syngress 2015.

Federico Costantini, Digital forensics in the European Union: theoretical background, current issues, future perspectives, paper presented at JURIX2016.

European Commission, Report on EU customs enforcement of intellectual property rights – Results at the border (https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/customs/customs_controls/counterfeit_piracy/statistics/2015_ipr_statistics.pdf), 2014.

Eurostat, Statistics explained (http://ec.europa.eu/eurostat/statistics-explained/index.php/Main_Page/de), 2017.

Horizon 2020 Call, H2020-SMEInst-2016-2017 «Open Disruptive Innovation Scheme» (http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-smeinst-2016-2017.html), 2015.

International Association of Computer Invastigative Specialists (IACIS), IFI Training Program, Internet Forensics and Investigation (https://www.iacis.com/training/internet-forensics-and-investigations/), 2015.

International Organization for Standardization (ISO), ISO/IEC 27037/12: Information technology – Security Techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence (https://www.iso.org/standard/44381.html), 2012.

International Press Institute (IPI), Out of Balance: Defamation Law in the EU (https://ipi.media/out-of-balance/), 2015.

Rodney McKemmish, When is digital evidence forensically sound?, in: Indrajit Ray/Sujeet Shenoi (Eds.), Advances in Digital Forensics IV – Conference proceedings DigitalForensics 2008, New York 2008.

[7] Evidence Project: www.evidenceproject.eu.

Gertreuida Meyer/Adrie Stander, Cloud Computing: The Digital Forensics Challenge, in: Eli Cohen/Elizabeth Boyd (Eds.), Proceedings of Informing Science & IT Education Conference (InSITE) 2015, Informing Science Institute 2015, p. 285–299.

National Institute of Standards and Technology (NIST), Interagency Report 8006 – NIST Cloud Computing Forensic Science Challenges (https://csrc.nist.gov/csrc/media/publications/nistir/8006/draft/documents/draft_nistir_8006.pdf), 2014.

Todd G. Shipley/Art Bowker, Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace, Syngress 2014.