Procedure for Obtaining and Sharing the Digital Evidence

Tomas Marques-Arpa, Jordi Serra-Ruiz
Universitat Oberta de Catalunya, Barcelona, Spain

Abstract

The proposals presented in this paper have been realized to solve one of the main problems in the analysis of Digital Chain of Custody (CoC) in computer forensics, that is: the traceability of the procedure of evidence. Usually, the Evidence is obtained by scene investigators, which is examined and analyzed by forensic information experts. At the time of obtaining the proof has been cited as the most critical moment in the CoC, because it is the most vulnerable point. If that initial moment is contaminated, the CoC will be invalid and the evidence could be invalided for a judicial process. Once the evidence has been obtained, it must be treated with all security guarantees. Sharing the evidence with correct treatment will be required for the validity of the process. On the other hand, to obtain the exact capture position and time, Global Positioning Satellite (GPS) has been proposed to be used by some authors. GPS has been demonstrated vulnerable but this is the only solution nowadays. The current technology could allow the automation of tasks and routines as to capture proofs and to start the chain. Then, a tool as Android application is proposed for testing (running on a smartphone device). Once it is analyzed on a mobile, it is proposed for integration in a new device based on very low cost personal computer. In this work, a procedure and a tool are proposed to guarantee the Chain of Custody.

1. Introduction

If the programs of interest for the European Union in area of security are studied in detail in the past and in the coming years, it could be possible to detect the importance in the study of the evidence. The development of management frameworks and the creation of tools and artifacts that provide aid in the fight against crime are widely demanded.

In relation to this interest, some examples are mentioning:

- Development of a Common European Framework for the application of new technologies in the collection and use of evidence [1].
- European toolbox, focusing on procedures, practices and guidelines for CBRN forensic aspects [1].
- Framework and tools for (semi-) automated exploitation of massive amounts of data for forensic purposes [1].
- Tools and infrastructure for the extraction, fusion, exchange and analysis of big data including cyber-offenses generated data for forensic investigation [2].
- Advanced easy to use in-situ forensic tools at the scene of crime [2].
- Mobile, remotely controlled technologies to examine a crime scene in case of an accident or a terrorist attack involving CBRNE materials [2].
- Advanced easy to use in-situ forensic tools at the scene of crime [3].
- Internet Forensics to combat organized crime [3].
- Develop novel monitoring systems and miniaturized sensors that improve Law Enforcement Agencies evidence-gathering abilities [3].

In this paper, as it has already been proposed by the authors [4], concepts such as geolocation and timestamp of the evidence via satellite signal have been introduced. At the same time, some classical methods of secure communication such as the use of 3G/4G networks have been used up to now. In addition, the possibility of using a certification company (public or private) to ensure the veracity of the process, as well as storing evidence in a safe place (judicial court), have been proposed.

Additionally, a digital secure CoC in security forensics has been proposed in [4]. So, it is seen as a set of bidirectional chain links. In case of chain attack could be possible an investigation on the backups of each step through search the difference between evidence that follow and which should have been followed.

With the new proposed method, the Chain of Custody is more complicated to manipulate with bad intentions of the major threats, for instance, spoofing the satellite signal, man-in-the-middle, wire-tapping, collision and preimage. Therefore, the evidence could be followed and consulted by the judges and all parties concerned in the process.

Having established a clear procedure, the second proposal is exposed in this paper: to create an artifact which it is capable to accomplish the procedure and that it must take into account a set of items such as:

digital evidence acquisition and the metadata associated with this new digital evidence (e.g. video, audio, pictures or regular files), probe localization, timestamp and secure communication capabilities.

Finally, some conclusions and future work are presented.

Therefore, the requirements of the European Union on security of information technologies and telecommunications have been considered, as well as future research in this area, as the industrial development and legislation in Spain as full member of the European Union.

Consequently, proposals are perfectly suited to the principles of market development, security and sector regulation.

2. State of the art

2.1. Computer forensics

As reference, standards of investigation process classes and activities proposed by the International Standard Organization [5] have been considered, showed in Figure 1.

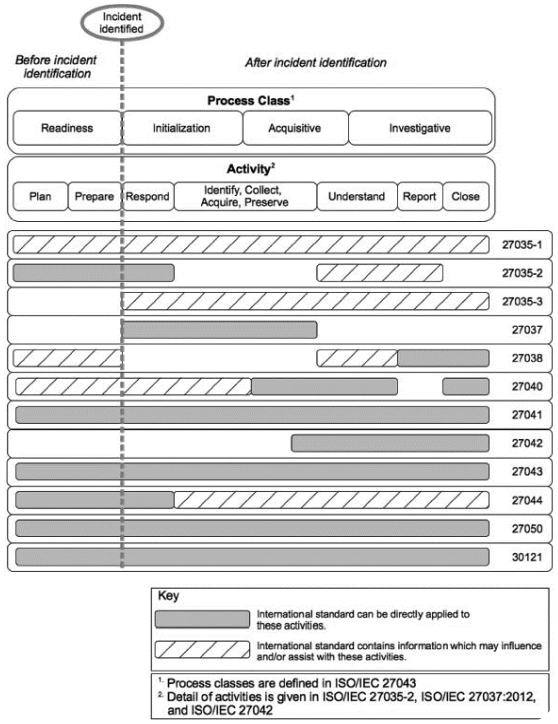

Figure 1. Applicability of standards to investigation process classes and activities as it is defined by ISO/IEC 27042:2015 [5]

Initially, proposal of secure "Digital Chain of Custody" to warrant digital evidence (information or data), stored or transmitted in binary form has been determined through the process of analysis. Been relevant to the investigation could be accepted in court proceedings and the principles of identification, preservation, securing and posterior analysis are guaranteed [5].

2.2. Chain of Custody

Bradford and Ray [6] define the CoC as: "*A chain of custody is a detailed account documenting the handling and access to evidence. The information is preserved about the data and its changes that shows specific data was in a particular state at a given date and time. Data that is non-predictable, widely distributed, verifiable stored, and time sensitive is socially bound data"*.

Chain of Custody is defined by The Office of Justice Programs (OJP) of U.S. National Institute of Justice (NIJ) as: "*a process used to maintain and document the chronological history of the evidence*". This means control over the individual's names collecting evidence and each person or entity subsequently has custody of it, the dates and the items were collected or transferred, the agency and case number, the victim's or suspect's name, and a brief description of each item [7].

For validate the CoC, all details on how evidence was handled in every point of the method of obtaining evidence must be known. The old formula used by police, journalists and researchers: Who, What, When, Where, Why, and How (it is known as "Five Ws and one H") must be applied in digital forensic investigation, presented in [8], [9].

2.3. Digital Evidence Management Framework (DEMF)

As is shown in Figure 2, other questions could be presented like a function of secure management depending on a few factors [10]:

```
DEMF = f {fingerprint _of _file,          //what
          biometrics_characteristic,      //who
          time_stamp,                     //when
          gps_location,};                 //where
```

According to the proposal of Ćosić and Bača presented in [9], [10]:

- What: a fingerprint of evidence could be used and it must be a SHA2 hash function instead of SHA0/SHA1 because of cryptographic attacks like as Collision and/or Preimage.

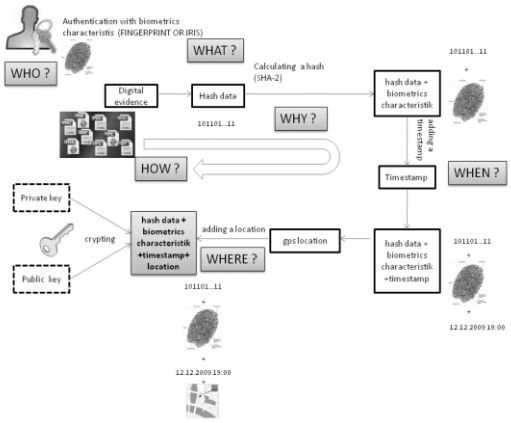

Figure 2. High defition view of DEMF [9]

- Who: an authentication on process system must be performed to identify "who was handled the evidence? A good method is to use biometric for: first responders, forensic investigators, curt expert witness, law enforcement staff and police officers (crime inspectors), i.e for all members who need access to the evidence.
- When: the method applied for this phase could be a "trusted time stamping". RFC 3161 standard define that trusted time stamp is a time stamp issued by a Trusted Third Party (TTP) acting as Time Stamping Authority (TSA) [11]. In this kind of "time system", it must be "external auditors" acting as witness.
- Where: Some authors as Strawn [12] have recommended the use of a GPS, because this system can be used for determination of accurate location as where digital evidence is discovered. And where it has been handled later.

Therefore, according to the process showed in [9], a SHA2 hash value of digital evidence is obtained at the first instant, with biometrics characteristics, time stamp and GPS location. For stronger security, asymmetric encryption is proposed. Digital evidence and obtained value will be encrypted with private key received from Certification Authority (CA) and it will be stored for further use. All processes are presented on Figure 2.

In addition, the methods proposed by Alfonso Muñoz et al [13] have been considered, concerning to improve the security of ETSI (European Telecommunications Standards Institute) about LI (Lawful Interception) and management of digital evidence: The Digital Wiretap Warrant (DWW) proposal guarantees confidentiality, integrity, timeliness and authenticity of the exchanged information end-to-end, by means of public key cryptography and digital signatures (i.e. PKI and TSA). The Monitoring Station (MS) is able to check whether the DWW is valid (i.e. signed by an authorized judge) before it starts capturing any data. Also, a forensic expert can certify the source MS of any evidence during a test. Therefore, the DWW

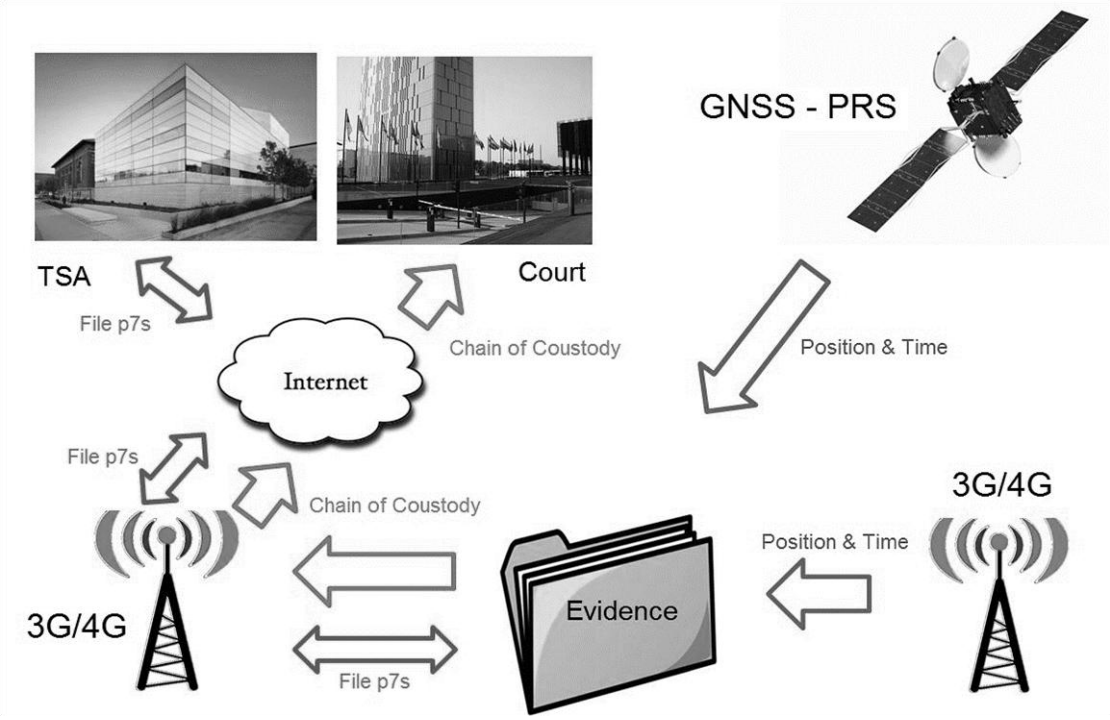

Figure 3. DEMF proposed

proposal defines security mechanisms against all general security attacks specified by ETSI, including denial of service and hacking, as analysed later. Furthermore, the DWW proposal also considers advanced attacks that are specific to LI platforms, such as evidence elaboration or tampering, even in confabulation scenarios. Moreover, since the global Time Stamping Authority (TSA) is a third party that oversights all messages exchanged by the LI platform, including the data plane ones, it may be also employed for improved LI auditing. Nowadays Lawful Interception is subject to public scrutiny by requiring the Judicial System to publish periodically the number of wiretap requests by how many agencies, affecting how many suspects, etc.

3. Digital Evidence Management Framework (DEMF)

The DEMF proposed in this paper is based on the Ćosić and Bača proposal described in [9]. The main idea is based on the paradigm described above named "the five Ws and one H".

They explained their proposal in response to several questions. A set of conclusions has been considered:

- Why: a crime has been committed.
- Who: the use of biometry for authentication purposes of all people related to the investigation.
- What: A footprint or hash function (SHA-2) of Evidence.
- When: Adding a secure timestamp.
- Where: using GPS location.
- How: Using Asymmetric encryption for the Evidence.

When a digital evidence is generated (a photo, a video, usually a file), time and the geographical position of the acquisition is added in the file metadata. In outdoor cases, the geolocalization of the Evidence can be done safely by using 3G/4G mobile communication or GPS (or Galileo PRS, when this particular coded signal will be available). This is useful in outdoor localizations, but in indoor cases, the geolocalization using satellite can be used at the street (at the entrance of the building) or in the roof if it is accessible. However, when place is outdoor or remote location, the accuracy and security provided by Galileo-PRS will be excellent, However, right now,the coded signal og Galileo satelite system is not operative. The GPS system is the unique one that is operational.

The treatment of the evidence and the associated metadata is described in Figure 3. Following the bidirectional line started at evidence, a footprint or symbol function SHA-2 of 256 bits is sent securely from the device to a Time Stamp Authority (TSA), which returns a small encryption file in p7s format (based on Public-Key Cryptography Standard PKCS # 7 Signature, as it is defined in section 4, RFC 2311 [14]) and this file could serve to demonstrate the instant that the evidence was sent to TSA, in this case, the metadata of the evidence is not altered in this process. The device with the evidence, the p7s file and a control document of changes could be packaged and sent to the court by a secure channel, following the Chain of Custody.

From another point of view and considering the functionality of the proposal of DEMF, the Figure 4 shows this proposal. The cloud described in the

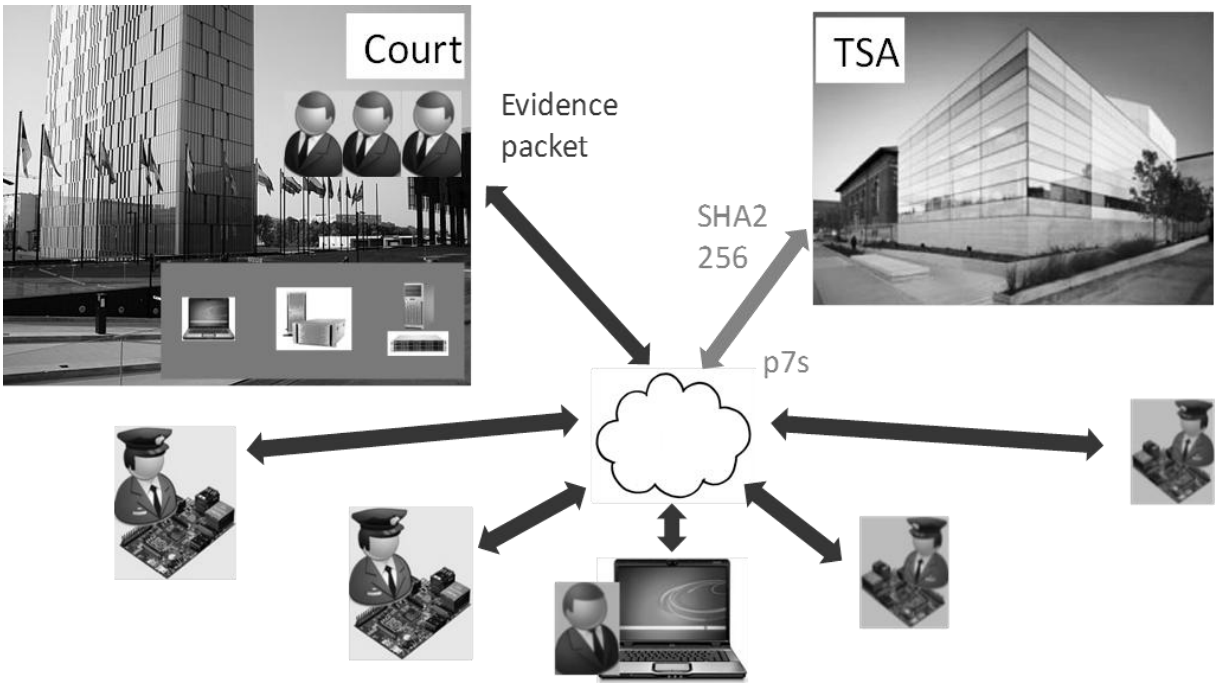

Figure 4. Functionality of DEMF

Figure 4 must be understood as an unsafe exchange space. This means that safety measures for this communication between all members of the process must be implemented. In this particular case, a VPN and encoded communication have been implemented between each device and the servers which preserve the evidence. The external units are responsible for capturing the evidence, later obtaining the time certificates (p7s files via TSA) and finally, they are sent packaged to a secure storage place (Court).

Subsequently, the document of changes must be digitally signed by all the people who participate in the process. This document will also be included in the package.

4. Device for obtaining digital Evidence.

The most critical point in the chain of custody has been found as the capture of evidence or the starting point. This is so because any contamination at the beginning of the chain could cause the invalidation of the proof, as it not possible to check the level of contamination.

The main idea is creating a device that could be made on different platforms: very low cost small computer (Raspberry Pi or similar) or a mobile phone with an application that obtains the localization, the user and can create a new secure CoC. On the other hand, laptop computers are needed to verify that the system works and packages can be accessed by authorized people, and to control de CoC process. And finally, a server for storing package with evidences is necessary.

The new specific device for the process must be able of:

- To identify the user by means of a code, a certificate or biometric authentication.
- To capture the evidence (in case of photo, video, audio, etc.) and to generate a file with all associated metadata.
- To determine position and time: GPS (or Galileo-PRS), and 3G/4G networks.
- To calculate a footprint SHA-2 hash of a file with metadata.
- To create a zip file adding the evidence file, control document text file and p7s file.
- To communicate via 3G/4G/Wireless with secure Internet access by Virtual Private Network (VPN).

Thus, a device with all security measures in ICT to capture the evidence is designed with these characteristics:

- For its location and time: device authentication and data encryption.
- In order to secure access to the device and application: access code PIN, IMEI and SIM (Personal Identification Number, International Mobile system Equipment Identity and Subscriber Identity Module card), mobile application with password and biometry control access.

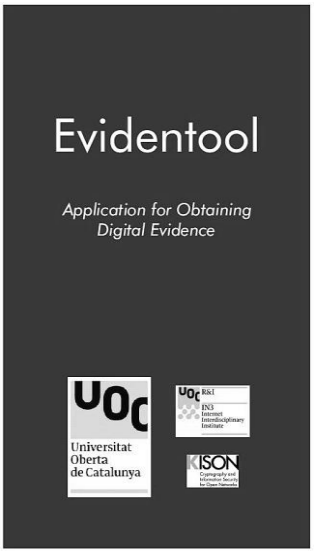

Figure 5. Evidentool application.

- For a footprint of the evidence: cryptographic function Secure Hash Algorithm 256 or 512 bits (SHA2-256 or SHA2-512). The advantage found with this method is the obtaining of a small single code file, so if any modification is made in the image or metadata, a different hash code is generated. Furthermore, the function is not reversible.
- For shipping to the TSA the SHA-2 code, it has decided to do this via Secure File Transfer Protocol (SFPT) using the algorithm of Rivest, Shamir and Adleman (RSA) on Secure SHell. The TSA generates a file extension p7s based on PKCS # 7 Signature as it is defined in section 3.2, RFC 2311.
- For shipping p7s file from TSA to device it is done by Secure File Transfer Protocol using the algorithm RSA on Secure SHell.
- For document change control, RSA 2048-bit key using Pretty Good Privacy (PGP).
- Finally, for sending the zip package and general connections between devices, computers and the server Virtual Private Network must be used.

With the main idea of satisfying the above requirements, an experimental application for Android operating system has been developed, named “Evidentool”. The principal screen of the tool is shown in Figure 5.

For the access to the application, the fingerprint (or PIN code) of mobile phone is required. In addition, it does not work without 3G/4G network connectivity, so it is imperative the IMEI code of

terminal owner and SIM code of phone user. This guarantee the indoor localization.

Figure 6. Using the application.

Users registered in the application and in the server as authenticated user, will be able to access it. A list of these users can be seen in the Users option in the Figure 6. When this option is selected, a list (without passwords) of all the people who have previously registered appear as: detailed name of the person acquiring the evidence and his position. In case of a new user not registered a form must be filled and authenticated by server.

If the user has accessed to app then it will be able to get new evidences. It may be by a picture, a video or an audio file. So respectively, the user will have direct access to the photo camera, video camera or audio recorder. It is possible to generate as many files as necessary.

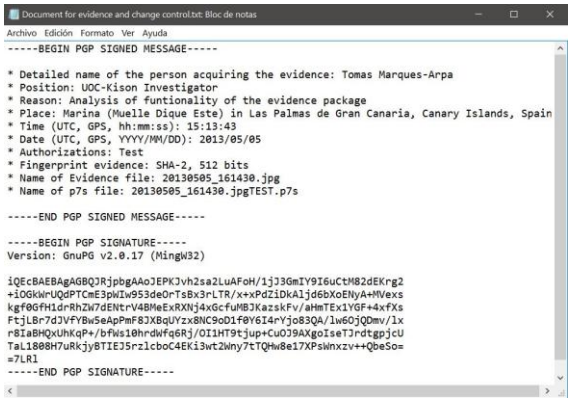

Figure 7. Document for evidence and change control.

Once finished the first step or obtaining proofs, the next step is started with the generation of witnesses using p7s files. When the p7s button is selected, a small file with the footprint of the original file of the evidence, or a folder with more than one evidences, is obtained using the SHA2-512 application. This file is shown in Figure 7. In order to obtain the p7s file, a secure communication between Evidentool application and TSA is stablished via Secure File Transfer Protocol (SFPT) on SSH. Therefore, a SHA2-512 file is sent to TSA and a p7s file is received from TSA.

The next step is to create a zip package with all information obtained during the process. For this purpose and using a file browser, the evidence file or folder and its corresponding p7s file are chosen.

In addition, a text file is automatically added to the zip package as third file. The text file is the "Document for evidence and change control" as is shown in Figure 7. This document is obtained by the user data (detailed name of the person acquiring the evidence, position and reason) and Exif metadata file of the Evidence (as it can be seen in the Figure 8).

Analysing GPS data of Fig 8, it is possible to detect that position and UTC time provided by the satellite is available. This information will be used to locate the evidence in exact position and time.

For security reasons, the text document must be digitally signed. Therefore, the GnuPG program with RSA 2048-bit encryption key is used. This program is a complete and free implementation of the OpenPGP standard as defined by RFC4880 [15].

From here, anyone involved in the judicial process should digitally sign in case of adding information. But the original zip file will be saved as unaltered containing the evidence, the p7s file and the original text document.

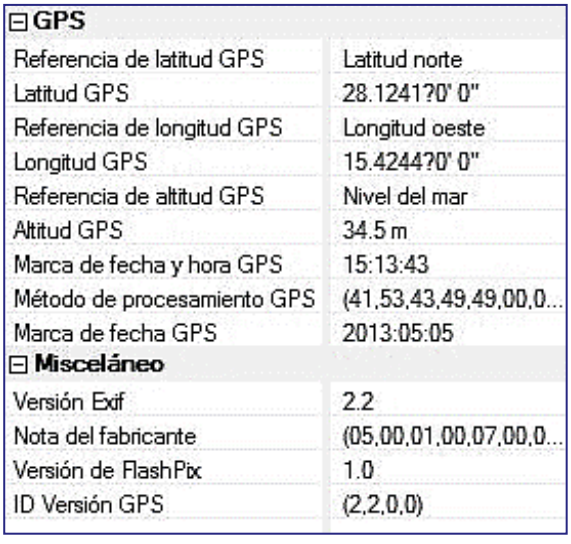

Figure 8. Exif metadata file

Finally, the last step is to send the zip file (in Figure 6) mentioned in the previous paragraphs. For this action a Virtual Private Network must be used.

This VPN has been configured at the first time of device acquisition. The information will be sent from the tool to a server located in a secure place (usually in a judicial court). In order to improve the security, the communications must be established using 3G or 4G.

Figure 9. Example of an evidence.

For experimental results and serving as example of Evidentool application, an image was captured in a marina of Canary Island (Figure 9 upper picture). The exact position of the capture was a bench as Figure 9 (bottom image).

The exact capture localization of our test evidence was translated to a google Maps application using GPS satellite constellation (Figure 10). The error in the location was less than 0.5 meters, which is excellent in terms of positioning of evidences in outdoor case.

3. Conclusions and future work

This work has been developed with the intention of creating a valid method of CoC and a tool that manages this new digital CoC. The main idea was to create the digital Chain of Custody, but later it was detected that the Chain must have a starting point, which is: the generation of the evidence, the weakest point of this process.

Therefore, does a hand written script be followed in the evidence acquisition in order to ensure that it proceeds correctly? The answer is no. The current technology can allow the automation of certain tasks and routines, which is the main proposal of this work by creating a tool that automates the process on the weaker part of the chain which is the correct acquisition of evidence. As result, a new tool has been proposed.

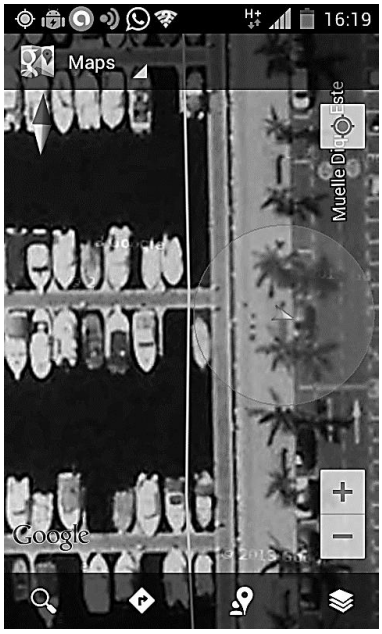

Figure 10. Locating the Evidence.

Subsequently, the evidence should be protected from greater threats that have been detected: spoofing, man-in-the-middle, wiretapping, collision and preimage. To avoid this and above all, it cannot be easily modified without trace the evidence. For this reason, this method has been proposed.

The results demonstrate that is it possible to develop a new method for Chain of Custody and implement in a mobile device.

The improvement work can focus on the following aspects:

- Upgrading of Android app as proposed.
- Designing of a device made on a low cost small computer that supports connecting peripherals as well as provide other possibilities in the creation of the CoC using images instead of tracks. This avoids the disqualification of the evidence by degeneration of physical support that it contains its.
- Using biometric identification as authentication of users according to technical progress.
- Realization of cyberattacks to the proposal in order to demonstrate their weakness or their strength.
- Using of geolocation as accurate and safe as possible with the incorporation of positioning data Galileo encrypted PRS data. Whose main objective would be to prevent from the possibility of a malicious spoofing

or jamming attack when Evidence is being captured, even the possibility of a combined attack [4].

4. Acknowledgements

This work was partly funded by the Spanish Government through grant: TIN2014-57364-C2-2-R "SMARTGLACIS".

References

[1] European Commission Decision C 4536 (2012), "7th Framework programme. Work programme for 2013", *Cooperation, theme 10, security*. European Commission, July 2012.

[2] European Commission Decision C 4995 (2014), "Horizon 2020. Work programme 2014-2015", *Theme 14, secure societies, protecting freedom and security of Europe and its citizens*, European Commission, July 2014.

[3] European Commission Decision C 6776 (2015). "Horizon 2020. Work programme 2016-2017", *Theme 14, secure societies, protecting freedom and security of Europe and its citizens*, European Commission, October 2015.

[4] T. Marques-Arpa and J. Serra-Ruiz, "PRS signal in acquiring Evidence of Digital Chain of Custody", *In Proceedings of the 11th International Conference for Internet Technology and Secured Transactions (IEEE-ICITST-2016). Barcelona 5-7, 2016. pp. 273-278*. Infonomics Society, London, UK. ISBN: 978-1-908320-74-2.

[5] ISO/IEC 27042:2015 (E). "Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*", pp. vii, June 2015*.

[6] P.G. Bardford and D.A. Ray, "An online algorithm for generating fractal hash chains applied to digital chains of custody", *IEEE-ISI (Intelligence and Security Informatics Conference), pp. 8 – 15, June 2007.*

[7] National Institute of Justice of USA (NIJ), Office of Justice Programs, "Crimes scene guides": *http://nij.gov/topics/lawenforcement/investigations/crime-scene/guides/Pages/welcome.aspx* (22 January 2017).

J. Tallim, " Deconstructing web pages", Media Awarenes Network:http://mediasmarts.ca/lessonplan/ deconstructing-web-pages-lesson (22 January 2017).

[8] J. Ćosić and M. Bača, M. "A framework to (im)prove "chain of custody" in digital investigation process", *Proceedings of CECIIS-2010, 21st Central European Conference on Information and Intelligent Systems, Faculty of Organization and Informatics, Varazdin, Croatia, pp. 435 – 438, September 22-24 2010*.

[9] J. Ćosić and M. Bača, "Do we have a full control over integrity in digital evidence life cycle", *Proceedings of ITI-2010, 32nd International Conference on Information Technology Interfaces, Dubrovnik, pp. 429-434, 2010*.

[10] S.Vanstone, P. Van Oorschot and A. Menezes, *Handbook of Applied Criptografy*, CRC Press, 1997.

[11] C. Strawn, "Expanding the potential for GPS evidence acquisition", *Small Scale Digital Evidence Forensic Journal, Vol.3, No1., 2009*.

[12] A. Muñoz, M. Ureña, R. Aparicio and G. Rodríguez de los Santos, "Digital wiretap warrant: improving the security of ETSI lawful interception", *Digital Investigation no. 14, pp. 1-16*, Elsevier, 2015.

S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade and L. Repka, "S/MIME version 2 message specification", 1998.https://www.rfc-editor.org/rfc/pdfrfc/rfc2311.txt.pdf (22 January 2017).

[13] J. Callas, L. Donnerhacke, H. Finney, D. Shaw and R. Thayer, "OpenPGP Message Format", *The Internet Engineering Task Force (IETF®), 2007.* https://tools.ietf.org/html/rfc4880 (22 January 2017).

