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).

