proceedings

MDPI

Proceedings

Development of an Open Source Tool and a Multi-Platform for Generation of Forensic Reports †

Mireia Martí Vilas [1,*], Pilar Vila Avendaño [1,2] and José M. Vázquez-Naya [1,3]

1 Departamento de Computación, Facultad de Informática, Universidade da Coruña, Grupo RNASA-IMEDIR, Elviña, 15071 A Coruña, Spain; pilar.vila@forensic-security.com (P.V.A.); jose.manuel.vazquez.naya@udc.es (J.M.V.-N.)
2 Forensic & Security C/Copérnico, 3, 2ª planta, local A3, oficina 2, 15008 A Coruña, Spain
3 Centro de Investigación CITIC, Universidade da Coruña, Elviña, 15071 A Coruña, Spain
* Correspondence: mireia.marti@udc.es
† Presented at the 3rd XoveTIC Conference, A Coruña, Spain, 8–9 October 2020.

Published: 27 August 2020

Abstract: Computer Forensics is a science that is part of computer security and focuses on identifying, preserving, analyzing and presenting electronic evidence that has been found on a device. This process has to be thoroughly documented by the expert who carries it out, and must be adapted to standards such as UNE 197010:2015 or ISO/IEC 27042:2015. However, there are no tools to facilitate this task. Therefore, in this work, a multiplatform and open source tool is developed to facilitate the expert's elaboration of the report, and the management of the documentation related to the case, while keeping this information safe.

Keywords: computer forensics; forensic reports; cyber security; multi-platform; open source; forensics tool

1. Introduction

Computer forensics is a science that takes parts of informatics security and focuses on identifying, preserving, analyzing and showing electronic evidence that has been found in a device [1]. This process has to be carefully documented by an expert witness in order to describe the starting stage, check that evidence has not been manipulated, record the process followed and finally to write a conclusion. The documentation has to be in a report that, in this case, has to be carried to the court. For this reason, it is important that it is adapted to specific standards like rule UNE 197010:2015 ("General judgements for the production of reports and forensic expert opinions about Information Technologies and Communications") and the guide ISO/IEC 27042:2015 that lists specific instructions that must include the forensic report [1].

However, the legislation does not specify which tool or tools the expert witness has to use neither for the report redaction nor for the relative documentation management. Typically, the expert witness will make use of different tools to achieve this goal (word processor, file system of the OS itself to store the information, encryption tools to protect such information, etc.). However, this process is tedious, partly repetitive and prone to error. To automate this process, as far as possible, would be of great help to the expert witness, while providing greater certainty and more guarantees as to the correct wording of the report.

Due to the absence of specific tools for producing expert witness reports, this work is based on the development of a desktop, multi-platform, open-source application, which makes it easier for the expert witness to produce the report, while keeping the information safe.

2. Development

To achieve this development, an incremental development methodology has been followed, in which new functionalities have been added in each iteration. For the implementation we used the Python 3.0 language and the GTK+ library, allowing the result to be a multi-platform application.

The analysis and design deals with the corresponding use cases of each iteration, considering in each case the corresponding design decisions. Using the Balsamiq tool, the respective prototypes were created for each iteration.

The most basic functionalities of the application consist of adding and editing the expert cases. This process allows the user to fill in the fields corresponding to each phase of the expertise process (complying with the ISO/IEC 27042 guide), and also saving the case. For the storage, the user is offered the possibility of choosing the folder in which to store the case. Subsequently, a folder is created with the name of the case, in which all the documentation belonging to the case will be stored. The report will be stored in XML format to offer flexibility when exporting it to other formats.

A highlight of the storage process is the encryption of the information. Hybrid cryptography is used to store the encrypted report. This consists of using symmetric cryptography to encrypt the document (using a random key for each) and asymmetric cryptography to encrypt the random key (see Figure 1).

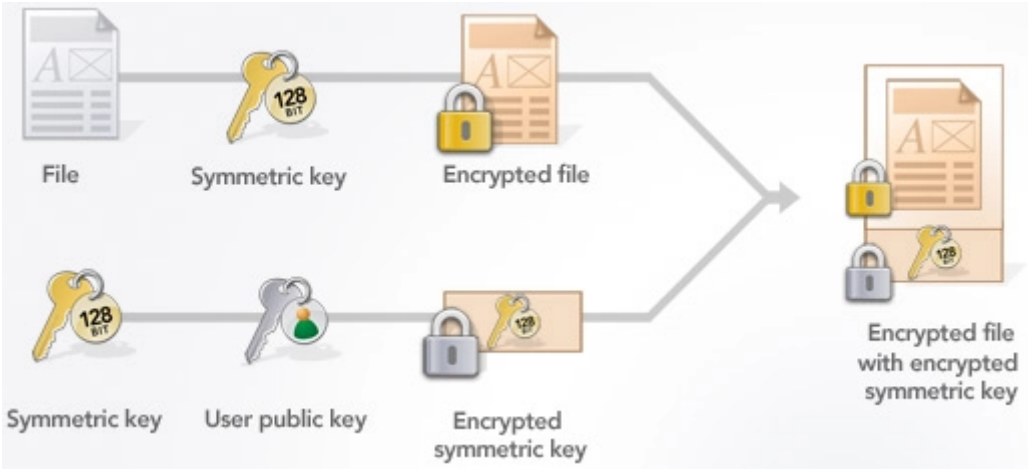

Figure 1. Hybrid cryptography scheme.

Another functionality of the tool is evidence management. To store the evidence in a folder within the case, the user can drag it into the application. These will be stored encrypted, and the name will be displayed for easy reference.

The main data of the expert should always go at the beginning of the report. Since these will not vary from one case to another, the tool allows the insertion (and editing) of the data independently of the case. In this way, the user will only have to introduce them once, and it will be the tool itself that will attach them to the beginning of each generated report.

Finally, the application implements authentication to be able to access the reports already generated. During the first access a new password is requested and the key pair (public and private) is generated. This password will be valid to store the private key in a safe way. This way, the password will be necessary to decrypt a report and be able to edit it. If for any reason the user forgets the password, it is possible to revoke it and create a new one (with its respective key pair), leaving the cases generated so far inaccessible.

3. Results and Conclusions

The drafting of the expert's report is one of the most important phases of the expertise. This tool offers functionalities such as password access, a clear and simple interface, the secure storage of

the report through encryption and exporting the report to different formats, among others. In short, it offers the user an easy way to manage the report and all the documentation pertaining to an expert case, complying with the aforementioned standards.

Author Contributions: Conceptualization, M.M.V.; Methodology, M.M.V., P.V.A. and J.M.V.-N.; Software, M.M.V.; Investigation, M.M.V., P.V.A. and J.M.V.-N.; Resources, P.V.A. and J.M.V.-N.; Writing–original draft preparation, M.M.V.; Writing–review and editing, M.M.V., P.V.A. and J.M.V.-N.; Supervision, P.V.A. and J.M.V.-N. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the "Collaborative Project in Genomic Data Integration (CICLOGEN)" PI17/01826 funded by the Carlos III Health Institute from the Spanish National plan for Scientific and Technical Research and Innovation 2013-2016 and the European Regional Development Funds (FEDER)—"A way to build Europe". This project was also supported by the General Directorate of Culture, Education and University Management of Xunta de Galicia ED431D 2017/16 and "Drug Discovery Galician Network" Ref. ED431G/01 and the "Galician Network for Colorectal Cancer Research" (Ref. ED431D 2017/23), and finally by the Spanish Ministry of Economy and Competitiveness for its support through the funding of the unique installation BIOCAI (UNLC08-1E-002, UNLC13-13-3503) and the European Regional Development Funds (FEDER) by the European Union. Additional support was offered by the Consolidation and Structuring of Competitive Research Units—Competitive Reference Groups (ED431C 2018/49), funded by the Ministry of Education, University and Vocational Training of the Xunta de Galicia endowed with EU FEDER funds.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Avendaño, P.V. *Técnicas de Análisis Forense informático para Peritos Judiciales profesionales*; 0xWord: Madrid, Spain, 2018; pp. 15–27.