
# Developing an IoT Forensic Methodology. A Practical Concept Proposal

By:
Juan Manuel Castelo Gómez, Javier Carrillo Mondéjar, José Roldán Gómez and José Luis Martínez Martínez

*From the proceedings of*
The Digital Forensic Research Conference
**DFRWS EU 2021**
March 29 - April 1, 2021

Forensic Science International: Digital Investigation 36 (2021) 301114

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

Extended Abstract

# Developing an IoT forensic methodology. A concept proposal

Juan Manuel Castelo Gómez*, Javier Carrillo Mondéjar, José Roldán Gómez, José Martínez Martínez. *Universidad de Castilla-La Mancha, Albacete Research Institute of Informatics, Investigación 2, Albacete, 02071, Spain*

*E-mail addresses:* juanmanuel.castelo@uclm.es (J.M. Castelo Gómez), javier.carrillo@uclm.es (J. Carrillo Mondéjar), jose.roldan@uclm.es (J. Roldán Gómez), joseluis.martinez@uclm.es (J. Martínez Martínez).

*Keywords*
Cybersecurity
Digital forensics
IoT forensics
Internet of things
Forensic methodology

A B S T R A C T

The adaptation of digital forensics solutions to the requirements and characteristics of the Internet of Things (IoT) is an ongoing process which has turn out to be quite demanding due to the novelty of this environment. The differences between the IoT and conventional scenarios in which forensic investigations used to took place, namely the desktop and the smart phone, are too great to be able to address IoT examinations by following a common approach. However, developing brand new solutions does not seem the best approach to follow either, since there are not many IoT-centered tools, and a drastic change might hinder the use of this new proposals in a court of law. Therefore, the development of solutions to ensure that IoT investigations are carried out in a complete and efficient manner might need to be performed by adapting the widely-accepted conventional ones to this new scenario. In this sense, this article proposes a concept methodology for conducting IoT investigations which uses a generic forensic model as a reference.



* Corresponding author.

*E-mail addresses:* juanmanuel.castelo@uclm.es (J.M. Castelo Gómez), javier.carrillo@uclm.es (J. Carrillo Mondéjar), jose.roldan@uclm.es (J. Roldán Gómez), joseluis.martinez@uclm.es (J. Martínez Martínez).

## Introduction

There are several aspects that differentiate the IoT from conventional forensic scenarios. Firstly, the number of devices present on an IoT network is usually higher than on other contexts. The devices are designed to perform simple operations and interchange data between them, rather than carrying out demanding tasks by themselves. Consequently, their computational capacity is low, also having a small amount of storage and memory. Secondly, the relationship between the IoT and the cloud is more important, which means that is not unusual to find the cloud as the base of the IoT network, or as a complement on which the demanding tasks are executed. And, thirdly, physical accessibility is not always guaranteed on the IoT; a device might be located in a different place than others on the same network, even miles away.

Another key aspect is the high number of contexts that coexist in the IoT. Since there is not a clear delimitation to what is considered IoT, multiple scenarios that greatly differ between them coexist. eHealth, smart home or smart industry are a few examples of it. This has an impact on digital forensics as the data that they handle do not have the same degree of sensitivity, thus requires to be treated accordingly. In addition, the devices and, more particularly, the operating systems and firmwares that they run, usually are specifically designed for the context that they are in. In view of this, the forensic IoT solutions also need to be adapted to the different contexts that exist in the environment.

Under these circumstances, an interesting approach for the design of IoT forensic solutions might be to use the widely-accepted conventional models and adapt them to the characteristics of the IoT. Therefore, the goal of this paper is to present a concept methodology for conducting IoT forensic investigations which uses a conventional model as a reference. Its purpose is to gather the characteristics shared by all IoT devices and systems in a concept proposal that covers the whole investigation process, so that ultimately it can serve as a general guideline and also be used for the development of procedures to address specific IoT contexts.

### Proposed concept IoT forensic methodology

The conventional model used as a reference is the one proposed in (Du et al., 2017), in which the authors review all the forensic models proposed since 1984, extracting the processes common to all of them, and grouping them together. With the intention of adapting the characteristics of the IoT to the processes described in the reference model, a reformulation of the phases is necessary. Consequently, the "Identification" process has been converted into a phase due to its greater complexity in IoT investigations. Similarly, the "Evaluation" task, which was conventionally executed during the analysis, emerges as another phase, given the

https://doi.org/10.1016/j.fsidi.2021.301114

holistic aspect of the environment, added to the fact that there are a higher number of devices from which to draw conclusions. However, the "Pre-Process", "Presentation" and "Post-Process" phases remain almost identical to the ones in conventional forensics, since they cover aspects, such as those concerning the law or documentation, which mainly have a static nature. Thus, the phases that make up the proposed methodology are the following: Pre-Process, Identification, Acquisition & Preservation, Analysis, Evaluation, and Presentation & Post-Process.

*Pre-Process*

This phase describes the actions that the investigator must carry out so that they can prepare in advance and develop the action plan, which can be summarized in the following: obtain information about the incident, learn the characteristics of the IoT network affected and the devices present in it, and establish the degree of forensic soundness required in the investigation.
The first one allows the investigator to determine what equipment it will be necessary to transport to the scene, and gives them time to study the devices and decide how they should be handled. Determining whether it is necessary to maintain the forensic soundness of the investigation means that, if the requester does not consider it necessary, the investigator can adopt a flexible approach when analyzing the sources of evidence. The obtaining of warrants, depending on the legal system of the country in which the investigation is taking place, is another element to consider in this phase.

*Identification*

As mentioned above, the range of the investigation is far greater than in conventional forensics. In the IoT there are devices that are capable of using cellular and radio communications, such as 5G, Z-Wave or Zigbee, and still be part of the same network, even if they are separated by miles. As a result, a physical examination of the scene will not be sufficient to cover the entire range. To do so, the investigator must rely on the logical connections that are active, or that recently were, on the devices.
Given the number of devices that can be present in a network and, due to their small amount of memory, the volatility of the information they contain, an order must be established to determine which one should be studied first. To do so, we propose to sort them on the basis of their importance and volatility, which can be measured in terms of the following parameters: the lifetime, quantity and relevance of the data that a device handles, the significance of the device in the IoT environment, and whether it has an acquirable memory and, if so, how difficult it would be to acquire it.

*Acquisition & Preservation*

The acquisition phase is greatly affected by the technical specifications of the devices and their physical access. As a result, although the collection techniques do not vary compared with conventional forensics, as new IoT-centered ones have not been developed at the time of making this proposal, a review of when to perform them is needed.

*Non-volatile memory*. The main difference with respect to conventional devices is that it is more common to find the non-volatile memory soldered to the board that forms part of the IoT device. As a result, certain methods, such as Joint Test Action Group (JTAG), In-System Programming (ISP), chip-off or live acquisition, which have already been confirmed as successful in (Le-Khac et al., 2018), (Badenhop et al., 2016) and (Wurm et al., 2016), should be considered when carrying out this phase of the investigation. Therefore, the resulting non-volatile acquisition process relies on the following techniques, which are sorted by their forensic soundness compliance:

- Extraction and acquisition: only feasible if the storage is removable.
- JTAG: it is a harmless option for soldered storage, and can also be used on non-soldered ones, but the compatibility of the device with the JTAG is not guaranteed.
- ISP: it is quite similar to the JTAG method, but involves connecting to an embedded Multi Media Card (eMMC) or an embedded Multi Chip Package (eMCP) flash memory chip to access its content.
- Chip-off: it requires specific soldering knowledge and equipment. Furthermore, the chances of compromising the functioning of the device are quite high.
- Live acquisition: it is the only option if the device cannot be physically accessed or if the above methods cannot be carried out. However, if the integrity does not have to be preserved, it might be preferable to performing a JTAG or chip-off, as it is faster and simpler. In addition, this method does not damage the device.

*Volatile memory*. In order to obtain these data, the best approach is to perform a live acquisition, since the cooling methods require specific equipment and are quite delicate (Gupta and Nisbet). However, live acquisition, which is usual in conventional forensics, will alter the data stored in the system as an interaction is required (VöMel and Freiling, 2011). Another crucial issue is that, in order to analyze the acquired data, it is necessary to create a profile of the memory that is being acquired. Therefore, the investigator must ensure that both tasks are feasible. If not, the usefulness of the data will be vastly reduced, only providing access to a raw memory image.

*Network traffic*. The interconnection between IoT devices makes the network traffic an extremely useful piece of data. Since the centralized solutions that capture data on-the-fly are still at early stages of development, the only way to collect this type of data is through live acquisition. Given these circumstances, the best approach might be to extract the network traffic from devices through which the greatest number of packets are sent, namely a router or the IoT gateway. In this way, only a small number of devices will need to be altered in order to perform the acquisition.

*Analysis*

This phase is the most difficult to generalize, since the detection of evidence depends on the system that is under examination, the type of incident that has occurred, and the laws regarding digital forensics of the country in which it happened. As happens with the acquisition phase, every device must be studied individually. Depending on its characteristics, it might be of interest to perform one analysis method or another, but it does not mean that such devices should be analyzed by following the same one. There are two crucial aspects that have to be considered:

- The feasibility of the acquisition process of the device: if no method succeeds in acquiring its memory, there is no other option but to perform a live analysis.
- The requirements regarding the integrity of the evidence: if it is not necessary to maintain it, the online examination is a viable approach, although it is preferable to perform an offline technique in order not to alter the data stored in the system.

*Forensic soundness*. The preservation of the integrity of a piece of evidence is mandatory in forensic investigations, especially in the ones that are part of a legal process. However, the form in which the non-volatile memory of the devices is present, added to the fact that physical access cannot be taken for granted, and that live acquisition is not always feasible, makes an online analysis a more common approach than in conventional forensics. As is well known, performing a live examination compromises forensic soundness, as the data contained in the source of evidence will be altered. However, in some cases it might be the only way to examine a device, so, in the authors's opinion, certain flexibility should be allowed in these situations.
There are other relevant limitations when performing an online analysis on an IoT device. First and foremost, there are not many IoT-centered forensic tools and, even if there were more, the probability of them being compatible with the system that is being examined is low, given the variety of existing firmwares and operating systems. Consequently, the investigator must rely on the native ones available in the system. Secondly, executing demanding tasks on devices with such a low computational power means that it will take a great amount of time for them to complete. As a result, a live analysis might be useful when you want to check a certain aspect which the investigator knows how to extract using native tools. In the remaining cases, it is preferable to opt for an offline approach.

*Evaluation*

Given the interconnection between IoT devices in a network, the analysis phase will certainly require the examination of multiple devices as it is highly likely for an incident to affect several. Under these circumstances, a new phase is needed to, firstly, gather all the evidence collected and confirm that the individual conclusions drawn are correct, secondly, now that all the devices have been analyzed, determine whether any pieces of evidence can be linked together, and, thirdly, interpret the results from the perspective of the whole environment.
The process starts by sorting all the pieces of evidence discovered in the analysis phase by their order of relevance. When a piece of evidence is being evaluated, it must be determined what impact it had on the system in which it was found and, after that, one must consider whether it could have affected other devices in the network. In order to establish this, a link between the pieces of evidence must be found. This might allow the investigator to find new pieces of evidence, or fit others together that, when studied individually, did not make sense. Then, the most important task is carried out: the linked pieces of evidence are studied together, drawing conclusions from the perspective of the whole environment, thus giving the investigation a degree of completeness.

*Presentation and Post-Process*

This phase involves the actions needed for the closing of the investigation, which can be divided into three processes: writing and presenting the forensic report, returning the original sources of evidence and, in some cases, reconstructing and restoring the systems affected. With regards to the latter, the following actions need to be carried out:

- Clean the environment: it must be determined whether the element which caused the incident is still present in the network and whether the level of damage suffered by the devices calls for them to be restored.
- Restore the systems: if there are no backups, a reconstruction of the systems must be performed, and this requires reinstalling the corresponding operating system or firmware, as well as the pertinent applications.
- Evaluate the effectiveness of the actions performed: once the systems have been restored, one must check whether they are, indeed, behaving properly.

## Conclusions

In view of the characteristics and limitations of the IoT and their differences with those of conventional forensics, a concept IoT forensic methodology has been developed that addresses them by using a widely-adopted conventional model as a reference. This work is a first step for the design of a practical IoT forensic methodology to ultimately develop a widely-accepted model.

## Acknowledgements

This research was supported by the University of Castilla-La Mancha under the contract 2018-PREDUCLM-7476 and the project 2020-GRIN-28846, by the Ministry of Science and Innovation, Spain under grants FPU 17/03105 and FPU 17/02007, by the Ministry of Economic Affairs and Digital Transformation, Spain under the project RTI2018-098156-B-C52 and by the Regional Government of Castilla-La Mancha under the project SBPLY/17/180501/000353.

## References

Badenhop, C.W., Ramsey, B.W., Mullins, B.E., Mailloux, L.O., 2016. Extraction and analysis of non-volatile memory of the zw0301 module, a z-wave transceiver. Digit. Invest. 17, 14–27.

Du, X., Le-Khac, N., Scanlon, M., 2017. Evaluation of digital forensic process models with respect to digital forensics as a service. CoRR abs/1708.01730.

K. P. Gupta, A. Nisbet, Memory Forensic Data Recovery Utilising Ram Cooling Methods.

Le-Khac, N.-A., Jacobs, D., Nijhoff, J., Bertens, K., Choo, K.-K.R., 2018. Smart vehicle forensics: challenges and case study. Future Generat. Comput. Syst. (109), 500–510.

VöMel, S., Freiling, F.C., 2011. A survey of main memory acquisition and analysis techniques for the windows operating system. Digit. Invest. 8, 3–22.

J. Wurm, K. Hoang, O. Arias, A. Sadeghi, Y. Jin, Security analysis on consumer and industrial iot devices, in: 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 519–524.