A Concept Forensic Methodology for the Investigation of IoT Cyberincidents

Juan Manuel Castelo Gómez[1], Javier Carrillo-Mondéjar[2], José Roldán-Gómez[3] and José Luis Martínez Martínez[1]

[1] *Universidad de Castilla-La Mancha. Albacete Research Institute of Informatics. Investigación 2, Albacete 02071 (Spain)*
[2] *Department of Computer Science and Systems Engineering, University of Zaragoza. María de Luna 1, Zaragoza 50018, (Spain)*
[3] *Department of Computer Science. University of Oviedo. Federico García Lorca 18, Oviedo 33007 (Spain)*
Email: juanmanuel.castelo@uclm.es, jcarrillo@unizar.es, roldangjose@uniovi.es, joseluis.martinez@uclm.es

The number of Internet of Things (IoT) forensic investigations has increased considerably over recent years due to the weak nature of the security measures of its devices. In order to ensure the effectiveness and completeness of their examinations, investigators rely on forensic models, frameworks, and methodologies. However, given the novelty of the environment, the existing ones are not refined enough, and the conventional counterparts do not satisfy the requirements of the IoT. Consequently, further improvements are needed in order for a more suitable IoT methodology to be designed. After reviewing the proposals from the research community for the development of procedures for performing IoT investigations, this article presents a practical concept methodology for conducting IoT forensic investigations that details step-by-step the whole examination process from its opening to its closing. In order to test its effectiveness and feasibility, it is submitted to a theoretical, a practical, and a hybrid evaluation. Firstly, by comparing its level of detail, practicality, and content with the related work. Secondly, by assessing its performance in two practical scenarios that depict real-life forensic investigations and the challenges that they present. And, finally, by studying how the existing models from the research community would have behaved in these cases. After performing these three different evaluations, it can be concluded that the results achieved by the proposed methodology were satisfactory, confirmed the feasibility of the proposal, and showed clear benefits compared to the related work in terms of practicality and level of detail.

Keywords: Cybersecurity; Digital Forensics; IoT Forensics; Internet of Things; Forensic Methodology

1. INTRODUCTION

Forensic sciences and standardization are two sides of the same coin. For investigators, having a formalized and structured process to follow which assures that investigations are performed with all the necessary guarantees means that, regardless of the conclusions drawn, the integrity, authenticity, and reliability of the evidence presented cannot be questioned. It is of such vital importance that, over the years, several forensic process models have been proposed by the community. In addition, even standards organizations, in an effort to make sure that these models were adopted, have developed their own proposals. Some examples are the Request for Comments (RFC) 3227 [1], which has been widely used as a reference for establishing the order of volatility of the evidence, or the multiple standards published by the International Organization for Standardization (ISO), such as ISO/IEC 27037:2012 [2], ISO/IEC 27042:2015 [3] or ISO/IEC 27050:2016 [4].

Over the years, these models have been constantly improving and adapting to the necessities of digital forensics to such extent that they have set the standards allowed in court when a forensic investigation is part of a legal process. As a result, the development of forensic

methodologies has become crucial in the field. Failing to properly design them results not only in inefficient and incomplete examinations, but also in unusable proof in a court of law.

In view of this, whenever a new digital scenario appears, investigators need to evaluate its requirements and quickly create solutions to assure that examinations are handled correctly. Given the huge increase in the number of IoT malware samples detected, something that ultimately leads to the materialization of cyberincidents, the IoT environment stands out as being of critical interest. By taking advantage of the weak security measures implemented on IoT devices and systems, and with a prediction of more than 15 billion units connected in 2023 [5], cybercriminals find it very appealing to attack them. More than 57 million malware attacks on smart devices were detected in the first half of 2022 [6], 77% more than the previous year. But also worrying are the statistics regarding how these attacks are produced, with 73.89% of them targeting the Telnet service, which is well-known to be deprecated due to its insecurity [7].

The research community, being aware of this, has already expressed its concerns. Proposals, such as [8], [9] or, more recently, [10] and [11], highlight the fact that the novel features of the scenario, such as its heterogeneity and complexity, mean that there is a serious need to design general and specialized IoT models, and that a traditional approach will not be functional enough for the requirements of the environment.

Consequently, with the appearance of the IoT, forensic investigators find themselves facing an easily exploitable and high-sensitivity-data-handling environment in which the solutions used until now in investigations are not the most appropriate ones. As happened when other new environments appeared, such as the cloud or the smartphone, an adaptation of methodologies, procedures and tools, as well as the creation of new ones, is mandatory so that the IoT investigations are carried out in a complete, efficient and proper way.

In this article, a step-by-step practical forensic methodology for the investigation of IoT cyberincidents is introduced that provides guidelines on how to approach an IoT examination from its opening to its closing. By combining a conventional model with an early IoT concept methodology, and addressing the challenges encountered when performing analysis in this environment, a six-phased proposal is presented that addresses the whole IoT environment, regardless of the context in which the investigation is taking place.

1.1. Research Questions Formulated

With the goal of this research set, the following questions arise when evaluating its feasibility:

- **(RQ1)** Is it reasonable to approach the development of IoT forensic procedures from a generic perspective, or the heterogeneity of the environment is too great to allow that?
- **(RQ2)** Can conventional forensic procedures be adapted, to a certain extent, to the requirements of the IoT?
- **(RQ3)** Has the forensic community enough knowledge about the IoT to cover in detail the whole investigative process of an IoT investigation?
- **(RQ4)** Is it possible to address these issues, and the main challenges encountered by the research community, and present an IoT forensic procedure that complies with the requirements of IoT investigations and meets the standards of the forensic community?
- **(RQ5)** If so, how does this proposal compare with the related work? Can it be used in practical real-life IoT forensic scenarios, or its application is limited to a theoretical environment?

1.2. Contributions

The contributions of this study are as follows:

- We study the current state of IoT forensics, detailing the challenges and requirements of this new environment compared with those of traditional forensics.
- We present a review of the proposals from the research community for the design of methodologies, models, and frameworks for performing IoT investigations.
- We propose a detailed step-by-step guideline that covers all the aspects of an IoT forensic methodology from the opening to the closing of an investigation. It combines a conventional model with an early IoT concept forensic methodology with the aim of meeting both the standards set by the scientific community, and the forensic requirements of the IoT.
- We submit our proposal to a theoretical evaluation, comparing it with the existing models, showing that it stands out in terms of detail, practicality, and that covers aspects of the investigation that the related work does not.
- We test the proposal in two practical case studies that depict scenarios that are common on IoT investigations, and that show some of the challenges that investigators face when examining IoT devices. In both experiments, the results achieved by the proposed methodology are satisfactory and confirmed the feasibility of the proposal.
- Finally, we carry out a hybrid evaluation in which we determine how the proposals from the research community would have behaved in these two case studies, showing that only one of them would have been able to cover all the aspects of the investigation in the two scenarios presented, but doing so with a lower degree of detail and specificity

than the authors' methodology.

The rest of the paper is organized as follows. Section 2 describes the motivation behind this research. Section 3 discusses the proposals from the community regarding the design of IoT forensic methodologies, models, and frameworks. A concept practical methodology for performing investigations in the IoT environment is presented in Section 4. The proposal is submitted to a theoretical, practical, and hybrid evaluation in Section 5 to assess its effectiveness, and feasibility, as well as whether it improves the related work. Using the knowledge extracted from the experiment, Section 6 answers the research questions. Finally, we present our conclusions in Section 7.

2. RESEARCH MOTIVATION

In this section, the two main reasons which motivate this proposal are described. Firstly, we argue why it is necessary to develop new solutions for IoT investigations by explaining the main difference with traditional ones, and, secondly, we present the forensic challenges that come up on investigations due to the new characteristics that IoT devices bring to the digital world.

2.1. Unsuitability of Traditional Solutions for IoT Investigations

As described above, due to the characteristics of the IoT environment, traditional forensics solutions in their current state are not suitable to be used on IoT investigations. Some of the key features which motivate this are:

- Heterogeneity of the environment: the application of the IoT has created a high number of new scenarios in which technology is present. Contexts such as eHealth, critical environments, smart homes, smart industries or smart cities have been developed and are constantly growing. In each one of them, the tasks that are performed are unique and very diverse, as well as are the data that are handled. This means having devices and systems specifically designed to operate in a context, thus having almost no resemblance with traditional ones, both in terms of software and hardware, and also making traditional forensic tools incompatible with IoT systems.
- Number of devices in a network: an IoT environment is usually comprised of multiple units. For example, the simplest smart home kit has around five or six devices. In a traditional scenario, having to study multiple devices only occurred in very specific incidents, such as a malware infection that has spread through the network. This aspect increases the complexity of IoT investigations, since now it is necessary to determine how many devices are in a network and how each one of them should be studied.
- Interoperability: added to the quantity of devices present in an IoT network, they are designed for interchanging data, rather than performing complex operations. Therefore, the evidence becomes more dynamic, while in traditional forensic investigations it has a more static nature. These aspects make it much more difficult to retrieve a piece of evidence, having to consider approaches that can allow the collection of on-the-fly data.
- Technical specifications of the devices: the amount of storage of IoT devices is very limited, as is also their dedicated memory. Given these circumstances, the pieces of evidence that can be located on them are fewer in number than on traditional devices, which can store greater amounts of information. This means that the data stored on a device may have a limited lifetime, and the discovery of a piece of evidence is more crucial, since they are present in smaller numbers. In addition, it impedes the carving of data, as it is easier to randomly overwrite a memory address. Another influential aspect is that their computational power is very low, so no demanding tasks can be carried out by them, which affects the plausibility of executing a remote analysis. A third significant feature is that it is not unusual to find an IoT device that is powered by a battery, which leads to the possibility of a device completely running out of battery without saving its state. Therefore, if a remote/live acquisition needs to be carried out, it may be impossible to do so if the investigator does not have physical access to the device, and even if they do, the restart process will alter the data stored on it, compromising its integrity. This also occurs in smartphone forensics, but this problem can be overcome with the use of hardware acquisition devices, which, at the time of designing this proposal, do not exist for the IoT.
- Use of the cloud: the cloud can be the base of an IoT network, or it can be used as support to compensate for the limited computational capacities of the devices. Operations such as data storage or the execution of applications are some examples, but it can also be the place where the whole architecture is built. Therefore, it must be considered as another potential source of evidence when examining an IoT environment. Traditional forensics addresses the investigation of the cloud individually, but not as a part of a network, and it has proven to be one of the most difficult scenarios to analyze due to the bureaucracy involved in requesting the data from the provider and the impossibility of having physical access to the device.
- Accessibility: not only are there several devices

in an IoT network, but they can also be located in different places. Furthermore, they can be embedded in objects, which hinders the task of physically accessing them. Consequently, an investigator has no option but to remotely interact with them, which is not desirable in conventional forensics, in which an offline approach is the preferred one.

2.2. Forensic Challenges in IoT Investigations

The characteristics described above, consequently, have an impact on how IoT investigations should be performed in order to assure their effectiveness and completeness. The most relevant aspect which derive from them are the following:

- Range of investigations: due to the high number of devices, the number of sources of evidence becomes greater, thus making the range of the investigation larger and having to identify, acquire and analyze a greater number of sources of evidence. In addition, it also means having to determine how many devices are part of the IoT network so that no one is overlooked. Consequently, it is necessary to establish a way to study the data which provides information on how the network is structured, which may vary depending on the protocol/s being used to establish communication.
- The IoT as an entity: given the interoperability of the environment, an action performed by an IoT device has a high chance of affecting the rest of units in the network. This works the same way when an incident arises. The importance of a single device reduces gets replaced in favour of the whole IoT network, acting as an entity. Therefore, an IoT methodology should be modelled so that conclusions extracted from the analysis phase can be drawn from the perspective of the environment, not from the point of view of the device.
- Lifetime of the evidence: since most of the date is exchanged on-the-fly and the amount of storage of IoT devices is quite low, the lifetime of the evidence is, consequently, very short, with some proposals such as [12] measuring the time of life of IoT data. This requires the investigation phase to prioritize the study of the devices depending on the value of the data that they handle in order not to lose pieces of evidence. In order to do this, a procedure must be design to establish a study order. This may require performing an analysis of a device, as well as thoroughly studying its features, so that the investigator can gather more information about it.
- Difficulty of performing the acquisition: since normally the type of storage is a flash memory chip soldered to the IoT device's board, the offline acquisition methods available are the Joint Test Action Group (JTAG), In-System Programming (ISP) and chip-off. However, carrying out these techniques is not only feasible, as it requires the investigator to be able to perform them, which may not be the case, obviously, for the device to be compatible with the technique and, finally, having physical access to the unit. Unfortunately, the alternative method is performing a remote/live acquisition, which requires a compatible tool, either in the form of an external software or a native command, which is not guaranteed to be available in an IoT system. In addition, it is crucial to adapt this acquisition technique so that the evidence can be retrieved assuring its integrity and authenticity.
- The importance of network data: given the difficulty of accessing the data stored in the volatile and non-volatile memory, added to the fact that most of the data generated by IoT devices is in the form of network packets, the traffic becomes a crucial source of information in investigations. Two main issues arise when handling this type of data: its lifetime is very short, and the amount of IoT protocols being currently used in quite high, so it is necessary to determine how each one of them operates. This means developing solutions to study the encrypted network traffic as well, so that the highest amount of information can be extracted, with proposals such as [13], focusing on this. Consequently, methodologies should give the corresponding importance to network traffic and provide guidelines on how to acquire and analyze it.
- Lack of tools and computational power to perform remote/live analysis: apart from the limitations in terms of forensic soundness that these techniques have, the constrained-power IoT devices are not able to execute demanding tasks, so the usefulness of this method is reduced compared to traditional scenarios. Therefore, the tools used in this environment must, firstly, be compatible with the multiple operating systems that coexist in the IoT, and, secondly, comply with the lack of computational power of IoT units. The other existing source of information is the native commands included in the system, but there is no assurance on the level of usefulness of the data that they present, since there are usually very few ones available. Under these circumstances, new proposals must address these issues in order to compensate for the difficulty of following an offline analysis, and make the remote technique a feasible one for IoT investigations.
- Development of a generic IoT model: as mentioned above, the need to develop procedures for performing forensic investigations in the multiple contexts of the IoT is crucial but, in order to do so, a general model should be designed first so that it can serve as a reference, and then be adapted to a specific scenario, thus ensuring that

all the subsequent methodologies will satisfy the basic requirements of a forensic analysis, and that investigations will be performed in an effective and complete manner. Certain aspects, such as forensic soundness, which is essential in an investigation, are common to all contexts, so addressing them accordingly from a general point of view, which will ultimately become a reference, will guarantee compliance in all of them. However, this means that the way of approaching an investigation cannot be totally identical for all scenarios. For example, the criticality of the data in an eHealth context or a smart industry is far greater than in a smart home, so they should be treated accordingly. Therefore, in order to make the development of a generic model a reasonable possibility, it is necessary to find the shared similarities that would make it possible to standardize some aspects of an investigation, such as the state in which the sources of evidence are designed or the way to interact with the devices. In addition, they differ in other aspects, such as the operating system they run (if they do) or the type of devices that are present in them.

3. RELATED WORK

The first proposal of an approach to an IoT methodology can be found in [8]. It describes the uniqueness of the IoT from a forensics perspective, and compares it with traditional investigations. It highlights aspects such as the number of devices, the quantity and type of data, and the location of evidence. In order to address IoT-related investigations, it proposes a network-zone-based model that encompasses the following three zones: "internal network", "middle network" and "external network". The aim of this model is to offer guidelines on where to look for evidence. In addition, a complementary model is presented which describes the phases that need to be followed when performing an IoT investigation, but this is done briefly and from a theoretical perspective.

Based on the above proposal, [14] presents a methodology using Hadoop that is focused on covering the whole investigation process. It mentions useful aspects such as warrant obtention, triage examination and the chain of custody. However, it has a low degree of detail and no instructions are given on how to perform the tasks, thus it mostly just narrates an IoT investigation. Furthermore, the model is illustrated with a flowchart diagram in which several entities are present, but no details are given on whether they are phases to carry out, actions or a zone delimitation.

A generic IoT investigation framework that complies with ISO/IEC 27043:2015 is proposed in [15]. It is divided into three modules: proactive process, IoT forensics and reactive process. The first one addresses the activities needed for making the IoT environment forensically ready. The second one describes what infrastructures have the potential to contain evidence, dividing them into "Cloud Forensics", "Network Forensics" and "Device Level Forensics". In the final module, there is a brief mention of what actions should be performed when an incident arises. It shows a vast improvement compared with previous proposals, although there is a considerable lack of detail from a practical perspective, especially when describing the module destined to address the investigation process.

Likewise, focusing on the forensic readiness of the environment, and also adopting ISO/IEC 27043:2015, [16] describes a six-phase framework which aims to design cyber-physical systems that can facilitate forensic investigations. It does not cover any practical aspect of IoT investigations, but it is of interest with regard to taking proactive measures.

A new approach is followed in [17], in which a very detailed methodology centered on privacy aspects of investigations is proposed. It complies with the requirements of ISO/IEC 29100:2011, and divides the proposal into six phases, following the Enhanced Systematic Digital Forensic Investigation Model (ESDFIM). It covers the whole investigation process and does so with a reasonable degree of detail, complementing some of the phases with workflow diagrams. However, its practicality is questionable, since the whole concept depends on the installation of a piece of software named ProFiT, which is in charge of collecting and storing the information. In addition, not much information is provided on how an investigator should act in each of the phases.

The first proposal which approaches the design of IoT methodologies taking by into account the different contexts of the environment is [18]. In particular, it consists of three independent components: "Application-Specific Forensics", "Digital Forensics" and "Forensic Process". The first one is the one that is shaped around the characteristics of the context in which the investigation is taking place. It provides some brief guidelines on how to handle the smart home, wearable technology and smart city contexts. The second describes the information that can be present, differentiating between "Things Forensics", "Network Forensics" and "Cloud Forensics", treating the latter two from a general perspective, and the first one from a context viewpoint. The last component focuses on the process itself; it divides it into phases, but does not provide any details on how to approach them.

Interestingly, some pieces of research opt to focus on certain phases of an investigation. This is the case of [19], which presents a moderately detailed phase-division model for evidence acquisition. It basically divides the process into identification and capture. With regard to the former, it provides seven procedural steps centered on detecting possible sources of evidence, with this phase being embodied in the Last-on-Scene (LoS) algorithm. For this purpose, the IoT zone is

divided into three parts, namely the "Personal Area Network (PAN)", the "Intermediate Area Network (IAN)" and the "External Area Network (EAN)", which are inspected as listed. Regarding the capture process, another seven steps are proposed from a theoretical viewpoint, without mentioning any practical actions. The authors also suggest that it would be of interest to complement this approach with an online platform that manages and stores the cases and their data, also allowing investigators to collaborate with each other. With respect to this platform, they acknowledge that it is a proposal that has been presented in different pieces of research, but it is still at an early stage.

A change of approach can be found in [20], which is focused on studying a specific IoT context, in particular the smart vehicle. It provides some brief guidelines on how to examine autonomous automated vehicles (AAVs), and specifies how the data contained in the system should be handled in order not to alter it. Although it is theoretically explained, a short practical example is presented in which the data of a vehicle's electric control module (ECM) is acquired.

Another vehicle-related proposal is described in [21], which introduces a very detailed framework for the Internet of Vehicles (IoV). It focuses on providing guidelines for acquiring data, as well as storing it securely by using a distributed infrastructure. For this purpose, it is divided into two services: the "Forensics Gateway", which is a service embedded in the IoT device in charge of collecting the data, and the "IoV-Forensic Service", which stores the acquired data. In addition, it proposes an algorithm for verifying the integrity of the evidence collected, with is tested together with the framework in a simulated hypothetical scenario to evaluate the efficiency of the proposal.

Also following a context-centered approach, but focused on the smart home environment, we have [22], which presents a forensic investigation framework. It is divided into seven phases, covering everything from the preparation off-site to the analysis of the data, and it offers a certain degree of flexibility, since not all the phases are required in an investigation. The practical phases, namely the acquisition and analysis of data, are not detailed from a practical perspective, especially the latter, which is quite short. Regarding the acquisition, some guidelines are offered on where the data might be stored, but no instructions on how to capture it are given. Apart from that, it offers a reasonable degree of detail and presents three interesting practical case studies in which the methodology is tested.

A combination of fog computing and IoT forensics is proposed in [23], which presents an investigation framework based on the principles of the Digital Forensic Research Workshop (DFRWS) [24]. It consists of six modules that are focused on detecting possible suspicious activity and, if this occurs, collecting the pertinent evidence. For these purposes, the authors develop a fog node that is connected to an IoT device, and the former filters and analyzes the data generated by the latter. Furthermore, the fog node notifies the rest of the devices in the network when a potential threat is detected, and stores the data from the affected nodes. To test the proposal, they present two theoretical use cases involving a smart refrigerator and a smart city. The work only addresses incident detection and, regarding the forensic process, the identification and acquisition phases. However, the authors mention that it would be ideal for the framework to be implemented as a middleware architecture, and used jointly with a methodology.

A seven-phase methodology focused on addressing investigations on IoT prototyping hardware platforms is introduced in [25]. It follows the conventional forensic model and covers everything from the review phase to the presentation, but does so in quite a brief way, not detailing any of the phases. In addition, it presents a tool called RIFT that acquires the non-volatile and volatile information stored in the Raspbian [26] operating system. Regarding the former, it collects the detected sources of evidence, as well as summarizing the captured files in a .csv document, which stores their timestamps and hashes. With respect to the volatile data, it gathers the information regarding the state of the General Purpose Input/Output (GPIO) pins.

In [27], a framework for IoT systems is presented. It seems to be divided into four phases, but the last one cannot be read, since the figure which shows them is partially covered. Therefore, only three can be studied, and these are: "Identification", "Preservation" and "Analysis". Almost no details are given for each phase, only the challenges associated with each one, such as the lack of detailed logs or tools. The only relevant aspect that can be extracted from the proposal is that the methodology seems to follow a traditional approach.

An extension of the Digital Forensic Investigation Framework for the Internet of Things (DFIF-IoT) proposed in [15] is presented in [28]. It is a framework formed of nine components and complies with the ISO/IEC 27043. It covers everything from pre-incident detection to the forensic investigation. With respect to the latter, not many details are given on how to perform it. However, it mentions that the identification process is divided into "Device-level Forensics", "Network Forensics" and "Cloud Forensics", and the investigation process is comprised of the "Initialization", "Acquisitive" and "Investigative" phases.

In [29], a framework for IoT digital forensic investigations is proposed, but the work focuses on compiling a list of tools for investigators to use. It follows a three-layer architecture, these being the "Top Layer", formed of the cloud and cloud-like architectures, the "Middle Layer", focused on the network aspect of the IoT and communication between applications, and the "Bottom Layer", in which the IoT end devices are

present. No details are given on how to acquire or analyze the data, as it mostly narrates the investigation process. However, a list is provided of open-source tools that are suitable for the proposed layers, highlighting that general ones must be used since there are none that are IoT-centered.

The first proposal which adopts an eminently practical approach is [30], which introduces a methodology addressing the wearable technology context. Although it covers the initiation and processing of the investigation, there is a clear lack of detail, and it also fails to provide structured and organized guidelines. However, it mentions key practical aspects of the examination that are not discussed in previous works, such as how to acquire the memory of a wearable device or the need to check whether it is connected to the cloud. Another novel aspect is the use of an acquisition method which is used on smart phones, namely the JTAG, which clearly suits the IoT environment. In addition, the methodology is tested in two practical cases, and various tools that could be used in this type of investigations are mentioned.

A very complete and detailed model is presented in [31]. It follows a holistic approach, and is divided into three phases: "forensic readiness", "forensic initialization" and "forensic investigation". Consequently, it covers the proactive, incident and active phases of a cyberincident. With regard to the latter, it is divided into modules, like the other ones, five in this case, and covers everything from evidence acquisition to investigation closure. Although it is very structured and detailed, it lacks certain features from a practical and technical perspective. For example, there are no details given on how to identify a source of evidence. In addition, in the most practical phases, namely "evidence acquisition" and "evidence examination and analysis", theoretical tips are given, but it would be more effective to provide concrete practical techniques.

Focused on industrial control systems [32], proposes a model that combines classic Information Technology (IT) processes with the forensic knowledge for Operational Technologies (OT) that complies with the Industrial Internet Reference Architecture (IIRA). It is one of the first proposals that lists the tasks that should be performed by an investigator during the investigation, covering from the preparation to the reporting process. Although the authors do not mention any specific techniques, the model is quite detailed, and its performance is tested through a semi practical evaluation in which the model is followed in three hypothetical real-life incidents.

Addressing data acquisition [33], presents an Integrated Intelligent IoT Investigation Framework (IIIF) that uses a unified repository to collect the data generated in an IoT ecosystem. This proposal relies on a data unifier that collects the data acquired from a forensic tool, stores in a repository and structures it so that it can be analyzed. To unify these data, processes such as data cleaning, data integration and data transformation are used. However, as it is an early concept version, the detail given on how this data unifier operates is quite low, as well as, in order for it to work, it requires of a successful acquisition phase, which does not always occur on IoT investigations. In order to test its feasibility, a short theoretical comparison is made with other existing frameworks.

Another framework, but focused on harnessing radio frequency signals to identify IoT devices in a scene is [34]. It is divided into three stages that focus on modelling low-rate, short-range wireless sensing deployments and tracking the location of IoT devices by studying their radio signals. Using real-time traffic, the authors are able to predict the physical location of the device. The proposal is tested with devices with IEEE 802.15.4 radio, showing that they are capable of monitoring devices that are within up to 55 meters.

Having a similar goal [35] introduces a model to identify interconnectivity between IoT devices. This is done by proposing a framework named Service-Interconnectivity-based IoT Forensics (SIIF) that is based on existing ones, namely [28, 15, 18]. It covers from the identification to the presentation of evidence by listing eight phases, with two of them destined to offer guidelines on how to determine interconnectivity between devices. Although the starting point of the framework is quite practical, as it uses a proof-of-concept tool to study interconnectivity in six IoT scenarios, the proposal lacks specificity due to the phases not being detailed enough, and not mentioning how to proceed in any of them or which techniques to use.

Another interesting approach is the one followed by proposals such as [36], [37], [38] or [39], in which centralized solutions for performing forensic investigations are presented, with indications on how to use them. These guidelines are in some ways similar to a methodology, as they detail the examination process, but they are of limited use considering that they can only be applied when working with the solution developed and are designed upon that basis. In addition, most of them are an at an early stage of development or are just a theoretical concept. Therefore, they are not reviewed in detail in this article since their content cannot be exported to a general methodology, but they are worth mentioning as another way of designing forensic models.

Similarly, in order to comprehend how IoT devices and systems should be studied, works such as [40], [41], [42], [43] and [44] have been reviewed, and their findings have been taken into account when designing this proposal. This type of research allows investigators to know how to acquire and analyze the information contained in the studied system or device, which is extremely useful when having to examine it themselves.

TABLE 1: Summary of the proposals from the research community

Proposal	Type	Context	Evaluation	Feasibility	Level of Detail	Approach	Limitations
[8]	Method	✗	✗	Medium	Low	Network zone division	Mainly focused on evidence location
[14]	Model	✗	✗	Medium	Low	Phase division	Gives little insight into the investigation process
[15]	Framework	✗	Critical	High	High	Module division	Lacks practical perspective
[16]	Framework	Cloud systems	Theoretical	Medium	Low	Phase division	Focused on forensic by design, not on the investigation process
[17]	Methodology	✗	Theoretical	Low	High	Phase division	Focused on privacy aspects. It depends on the installation of a piece of software.
[18]	Model	✗	✗	Low	Low	Component division	Not technically detailed, provides some investigation guidelines
[19]	Model	✗	✗	Medium	Medium	Zone division	Focused on evidence identification
[20]	Model	Autonomous Automated Vehicles	Practical	Low	Low	Only phased	Provides some brief examination guidelines
[21]	Framework	Internet of Vehicles	Practical	Medium	High	Distributed service	Relies on a distributed platform and a specific service
[22]	Framework	Smart Home	Practical	Medium	Medium	Phase division	The practical phases are not technically detailed
[23]	Framework	✗	Theoretical	Medium	Low	Module division	Completely theoretical and only addresses the identification and acquisition phases
[25]	Methodology	IoT Prototyping Hardware Platform	✗	High	Low	Phase division	Very few details
[27]	Framework	✗	✗	Low	Low	Phase division	Barely any detail is provided

[28]	Framework	✗	Critical	Medium	Medium	Component division	The actual forensic process is barely detailed
[29]	Framework	✗	✗	Medium	Low	Layer division	Focused on describing what tools to use for each layer
[30]	Methodology	Wearable Devices	Practical	High	Medium	Step division	Does not cover the whole investigation process
[31]	Model	✗	✗	High	High	Module division	It lacks technical and practical details of the reactive phase
[32]	Model	Industrial Control Systems	Semi practical	Medium	High	Activity division	Requires to have set the environment properly before the incident arises
[33]	Framework	✗	Theoretical	Low	Low	Centered on data collection	It is an early concept that depends on a yet-to-be-developed process to handle data collected from IoT acquisition tools
[34]	Framework	✗	Practical	High	High	Centered on device monitoring	Dependent on the physical proximity to the IoT device
[35]	Model	✗	✗	Medium	Low	Phase division	It does not mention any technical procedures to execute during the investigation
Proposed Research	Methodology	Generic	Theoretical, Practical and Hybrid	High	High	Phase division	Dependent on conventional techniques to perform the acquisition and preservation

A summary of the proposals is presented in Table 1, which indicates the type of each proposal, whether it is context-centered, whether it has been submitted to evaluation, the feasibility of implementing it, its level of detail, the approach followed and its limitations.

After analyzing the proposals made by the community, the following main conclusions regarding the development of IoT methodologies can be drawn:

- The reluctance to perform a remote acquisition or analysis has disappeared when examining the IoT, and, for some authors, it is even preferable to an offline approach.
- The community is keen on developing centralized platforms that can facilitate the investigation process, but it seems that it is necessary to first develop a common methodology, so that the benefits of using this type of solutions can be maximized.
- The need to differentiate between contexts and how they are approached when investigating them has been confirmed. In fact, some proposals are even context-centered or present flexible phases that can be adapted to multiple scenarios, although this is performed in a theoretical way.
- The lack of tools specifically designed for the IoT is hindering the investigation process, so for the time being, investigators have to rely on conventional ones to perform their analysis.
- Multiple proposals address the identification phase by dividing the IoT network into zones, modules or components, depending on their behaviour. Most of them suggest a similar division, which is: IoT devices, IoT network and cloud.

4. PROPOSED METHODOLOGY FOR FORENSIC INVESTIGATIONS IN THE IOT ENVIRONMENT

The approach followed in this proposal consists in adapting a well-known and reliable traditional forensic model to the above-mentioned characteristics and requirements of the devices and systems that are present in the IoT. In this section, a review of the model used as reference is presented, and we explain why it is suitable to be adapted to the IoT environment, and then we describe the proposed IoT forensic methodology.

4.1. Reference Model

The reference model used is the one proposed in [45], in which the authors review all the forensic models proposed since 1984, extracting the processes common to all of them, and grouping them together into the phases described below to generate a generic one. Since it analyzes proposals from the community that have been widely used, it has been approved by the community, and as no international standard has been adopted by investigators, the authors believe that it is an appropriate model to be used as a reference.

- Pre-Process: relates to the work that is performed before the actual investigation, such as the tool set up or the obtention of authorizations and warrants.
- Acquisition & Preservation: addresses the tasks of identifying, acquiring, collecting, transporting, storing and preserving the data.
- Analysis: involves the study of the collected evidence in order to find relevant information to draw conclusions.
- Presentation: describes the documentation process of the findings from the analysis phase.
- Post-Process: details the tasks that need to be carried out in closing the investigation, such as the return of evidence.

At the same time, this proposal extends a very brief introductory model presented in [46], which delimits the phases in which a generic IoT forensic methodology should be divided into, and describes the general purpose of each one of them. Through the publication of this work, the scientific community supports the claim of the necessity of having a structured forensic procedure for IoT investigations, and confirms that the approach of adapting a generic methodology to the IoT is a viable and interesting one.

4.2. Description of Methodology

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. As will be seen in the following sections, 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 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 that vary only slightly between investigations, such as those concerning the law or documentation, as they mainly have a static nature, and are performed once the practical tasks have been carried out. Thus, the phases that make up the proposed methodology are the following:

- Pre-Process: involves the preparation work that is done before visiting the location where the incident took place.
- Identification: the aim of this phase is to determine which of the devices that might have been involved in the incident can contain relevant evidence and, consequently, must be analyzed.
- Acquisition & Preservation: involves the process

of collecting and storing the data contained in the selected devices.
- Analysis: the process of extracting information from the devices through finding pieces of evidence, and drawing conclusions about what happened from them.
- Evaluation: involves gathering the information extracted from all the devices analyzed and how it fits into the whole environment, adopting a holistic perspective.
- Presentation & Post-Process: covers the documentation of the conclusions drawn and the closing of the investigation.

4.2.1. Pre-Process

This phase describes the actions that the investigator must carry out so that they can prepare in advance and design the action plan. It can be summarized in the following actions: 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.

With respect to the first action, depending on the type of cyberincident that has occurred, it may be necessary to perform some precautionary actions. For example, if there is the suspicion that a piece of malware might be involved, it may be advisable to isolate or power off the devices in the network so that the infection does not spread through it and in order to avoid losing valuable data. Since, acquiring and analyzing the volatile memory of IoT devices is a highly unlikely task due to the lack of proper tools to do so, powering off the devices would not have such a significant impact in terms of loss of information. However, isolating the suspected to be infected devices would allow the analysis of the network traffic, which can be extremely useful, especially given the lack of other sources of pieces of evidence.

In addition, having information regarding the type of IoT network that is going to be examined, as well as knowing the number of devices affected, their location and accessibility, their technical specifications or whether they use an operating system or firmware, 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.

Another important matter that to be determined is whether it is necessary to maintain the forensic soundness of the investigation. 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. It is advisable to gather information on whether the examination might require studying a cloud system, so that the corresponding authorization can be formalized as soon as possible, knowing that this is a long bureaucratic process.

4.2.2. Identification

As mentioned above, the range of the investigation is far greater than in conventional forensics, a fact which hinders the identification process. The delimitation of a scene used to be physical, meaning that the devices belonging to the same network were either connected via cable or through a local wireless connection. Therefore, the range would go as far as the length of the cables or the range of the access point. However, in the IoT there are devices that are capable of using cellular communications, such as 4G or 5G, and still be part of the same network, even if they are separated by miles (i.e., the traffic lights in a smart city). In addition, other communication protocols via radio, such as Z-Wave or Zigbee, are also extensively used.

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. This means that they must be analyzed, either remotely/live or offline, in order to establish this. Depending on the need to maintain the integrity of the evidence, whether the memory of the device is acquirable and the preferences of the investigator, they will opt for one or the other.

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.
- Whether it has an acquirable memory and, if so, how difficult it would be to acquire it.

For example, in a typical central node network, the device that should be studied first is the central node, since it will store the largest amount of data, and through it will flow most of the network traffic, including the most relevant data. The same occurs in a smart home, in which a home gateway or central unit performs an interconnecting function [47] [22].

In Figure 1, the steps that need to be carried out to complete the identification phase are represented in the form of a flowchart diagram.

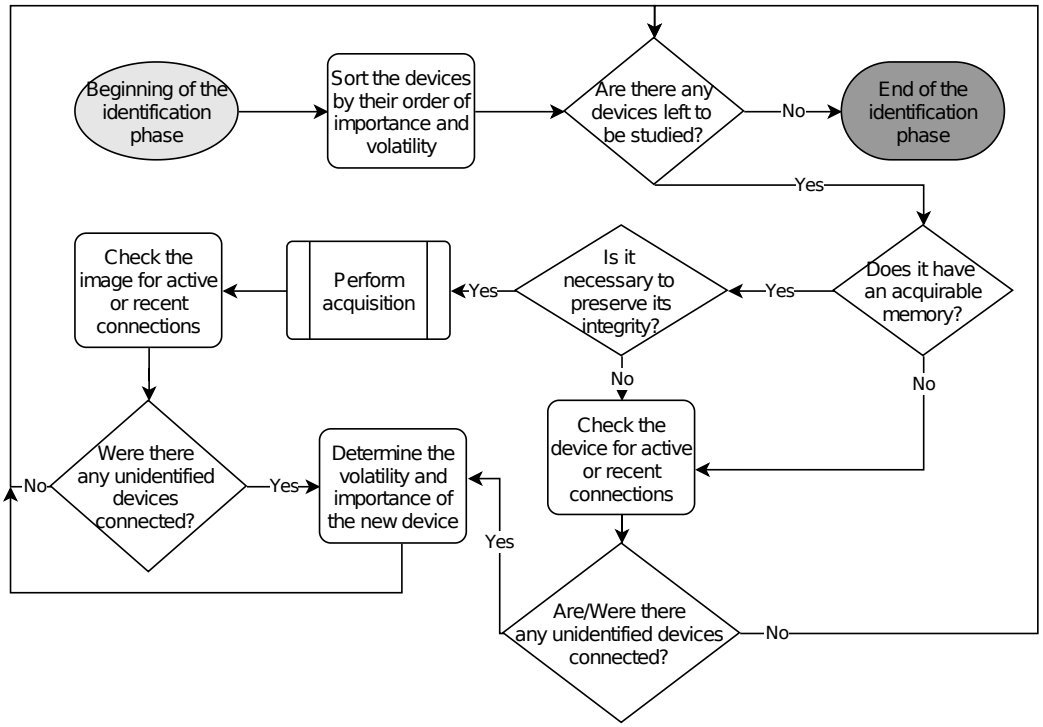

FIGURE 1. Flowchart diagram of the proposed identification phase

4.2.3. 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. In this section, a study of the main types of data that can be acquired from IoT devices, as well as the methods and tools needed to do so, is carried out. In addition, guidelines are offered on how to preserve the collected data.

Non-volatile memory. This is the largest source of evidence in this type of devices, even though their storage capacity is quite small compared with other digital systems. The main difference with respect to conventional devices is that the storage is not always removable, on the contrary, 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 JTAG, ISP, chip-off or remote/live acquisition, which have already been confirmed as successful in [48], [49], [50] and [51], should be considered when carrying out this phase of the investigation. It is a similar situation to that for smart phone forensics, but, in this case, physical access to the IoT device is not guaranteed, and there are no hardware tools that can perform the acquisition.

Therefore, the resulting non-volatile acquisition process, which is shown in Figure 2 in the form of a flowchart diagram, relies on the following techniques, which are sorted by their forensic soundness compliance:

- Extraction and acquisition: only feasible if the storage is removable. This is the most common and simple method of acquisition. The storage device, usually a microSD card, is extracted from the system, placed in a write blocker to preserve its integrity, and then either cloned or imaged.
- JTAG: a method that involves connecting to the Test Access Ports (TAPs) of the memory using a JTAG connector in order to be able to read its data and image it. It is normally 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: this involves connecting to an embedded Multi Media Card (eMMC) or an embedded Multi Chip Package (eMCP) flash memory chip to access its content. It is quite similar to the JTAG method, also requiring a connector, and the method is usually non-destructive as well, although ISP is faster.
- Chip-off: the memory is desoldered from the board and placed into a flash reader, and then its image file is created. It requires specific soldering knowledge and equipment. Furthermore, the chances of compromising the functioning of the device are quite high.
- Remote/live acquisition: this consists in executing the acquisition software directly on the device. Its main disadvantage is that the interaction with the

system will alter the data stored on it, and there are no guarantees that the collection tool will be compatible with it. 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. The information regarding the active connections of the device or its running processes can be of great value in an investigation. In order to obtain these data, the best approach is to perform a remote/live acquisition, since the cooling methods require specific equipment and are quite delicate [52]. However, this method, which is usual in conventional forensics, will alter the data stored in the system as an interaction is required [53]. 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, whose analysis will be extremely tedious and challenging.

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 remote/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.

Tools. There is no guarantee that a generic tool will be compatible with an IoT system, so an investigator must test it beforehand. As mentioned in Section 3, this is the reason why studying specific devices or systems is so useful for determining how to proceed with the examination. A list of well-known conventional forensic tools, which can also be used in IoT examinations, is presented below.

- Non-volatile memory: dd [54] is the acquisition tool par excellence, and is natively included in many Linux systems. Other recommendations are FTK Imager [55] and Guymager [56]. All of them can be used in both remote and offline methods.
- Volatile memory: Linux Memory Extractor (LiME) [57] or Linux Memory Grabber (lmg) [58] are the most flexible options, allowing the creation of the memory profile and its acquisition.
- Network: tcpdump [59] is the most reliable choice due to its compatibility options. Wireshark [60] and NetworkMiner [61] are interesting alternatives which are based on the same library as tcpdump, namely libpcap [62].

Preservation. Normally, the acquisition of a device will result in the creation of an image file together with its hash value, which will be stored on an external storage device. This unit must be secured so that only authorized people can have access to it. In addition, backup copies of the image or clone must be made and stored in different protected locations, guaranteeing that, if the original is lost or damaged, the investigation can continue [63]. If the selected acquisition method was either remote/live collection or extraction and acquisition, it is not necessary to seize the device. At most, if performing the latter, it would only be necessary to take the storage. However, if any other method is going to be performed, it may be preferable to seize the device and carry out the acquisition in the forensics lab, as it will require a specific set of equipment and environment. To ensure the integrity of the evidence, it is advisable to maintain the chain of custody. If it is not necessary to maintain the forensic soundness of the investigation, the investigator can take a more flexible approach, although they would still benefit from some of its aspects. As this process does differ from traditional investigations, only its most relevant features are mentioned in this proposal. These features are the following:

- Document how the acquisition was performed.
- If the original device is seized, place it in an antistatic sealed bag. The same is applicable if a clone of the device is made.
- Calculate the hash value of the clone or image collected.
- Take photographs of the device that has been acquired, as well as the result of the acquisition.
- Register the date and time of the acquired evidence, its identification number, its description, its format, the identity of the investigator and where it is going to be stored.

4.2.4. 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. Therefore, in this proposal, general guidelines are offered on whether to opt for a remote or offline approach, and we introduce some general tools that can be used for any system or device if the latter method is chosen.

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:

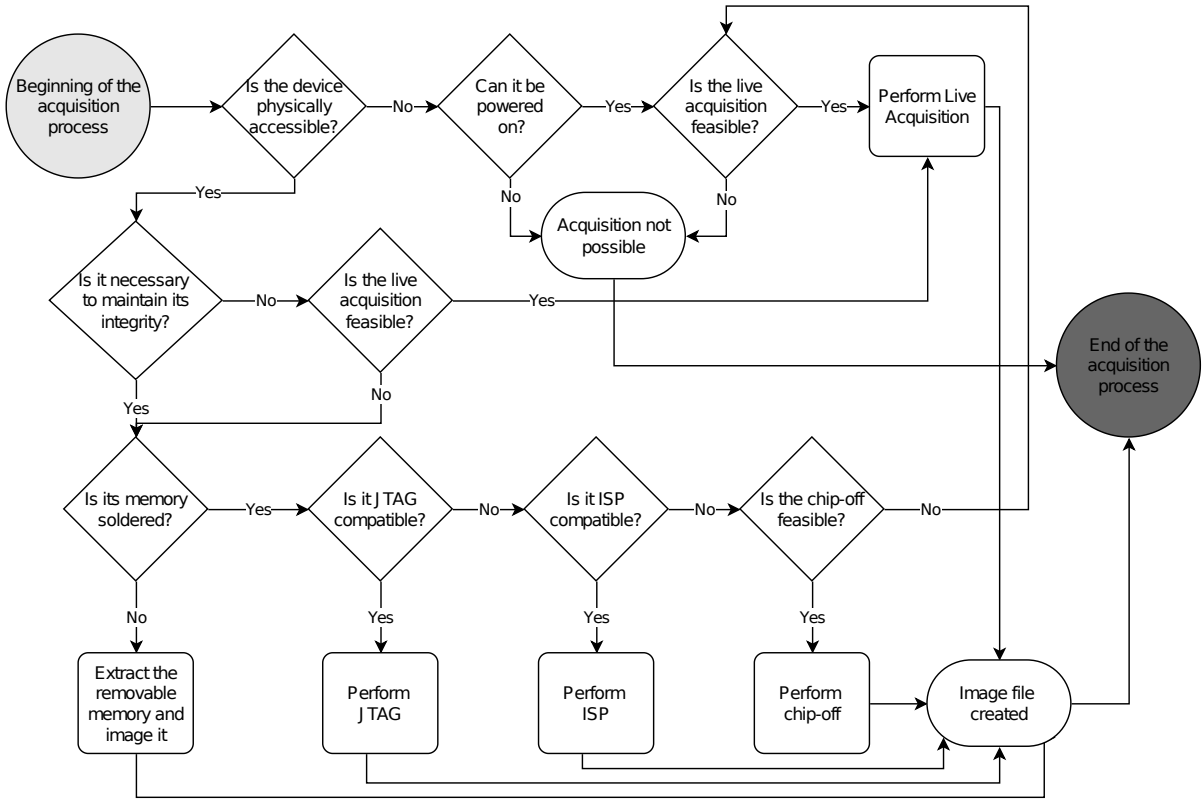

FIGURE 2. Flowchart diagram of the proposed acquisition process for collecting the non-volatile memory

- 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 remote/live analysis.
- The requirements regarding the integrity of the evidence: if it is not necessary to maintain it, the remote 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 crucial in forensic investigations, especially in the ones that are part of a legal process. Since the integrity standards are set by the forensic community, and are based on conventional scenarios, the techniques that associated with the preservation of the pieces of evidence consist on performing integrity checks using the hash codes generated after carrying out an acquisition. Therefore, until new methods are accepted as valid, IoT forensic procedures must use these techniques if they are to be used in legal processes, otherwise the conclusions extracted when following them will be unusable in a court of law.

However, the form in which the non-volatile memory of IoT devices is present, added to the fact that physical access cannot be taken for granted, and that remote/live acquisition is not always feasible, makes a remote/live analysis a more common approach than in conventional forensics. As is well known, performing a remote/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' opinion, certain flexibility should be allowed in these situations.

In addition, there are other limitations when performing a remote 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 remote/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. With this method, multiple general forensic tools, such as those presented in Table 2, can be used in the examination to extract a greater amount of information.

Anti-forensics techniques in the IoT. The anti-forensic techniques that would have a higher impact on IoT investigations would be encryption and device

TABLE 2. Tools that can be used for the offline analysis phase and their operating system compatibility

Tool \ OS	Windows	Linux-based
Browsing Tools		
FTK Imager [55]	✓	✗
Autopsy [64]	✓	✓
Volatile Memory Analysis		
Volatility [65]	✓	✓
Rekall [66]	✓	✓
Carving Tools		
QPhotorec [67]	✓	✓
Foremost [68]	✗	✓
Network Tools		
WireShark [60]	✓	✓
Network Miner [61]	✓	✓
Xplico [69]	✗	✓
Zeek [70]	✓	✓
Other Tools		
KAPE [71]	✓	✗
Log2Timeline [72]	✓	✓
ExifTool [73]	✗	✓

hardening. Fortunately, with respect to the former, IoT devices are yet-to-use an encrypted storage, as it would highly affect their computational performance, so it is not currently a concern for forensic investigators. However, it is true that there are some IoT protocols that use encryption, such as Z-Wave or Zigbee, but these protocols can be decrypted and therefore analyzed as shown in [74, 75, 76, 77]. Therefore, at the time of making this proposal, encryption is not a concern for IoT investigations. On the other hand, device hardening is more likely to have a greater impact if the security measures of IoT devices keep evolving. Disabling remote services such as SSH or Telnet has a strong impact when the analyst needs to perform a remote acquisition or analysis, as this would not allow it, but recent security reports show that there are still a high number of IoT devices that have these services enabled by default [7]. Taking this into account, the proposed methodology shows how to deal with this issue by suggesting the study of alternatives sources of evidence and listing other possible techniques that could lead to successfully acquiring the non-volatile memory of an IoT device.

4.2.5. Evaluation

Given the number of devices that are normally present in an IoT network, the analysis phase will require the examination of multiple devices. In addition, the interconnection between devices makes it 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. Through these actions, the aim is to be able to accurately establish, supported by evidence, what happened in the incident.

The process, which is presented step by step in the form of a flowchart diagram in Figure 3, starts by sorting all the pieces of evidence discovered in the analysis phase by their order of relevance. An alternative approach, which is shown in Figure 4, does the same, but arranges them according to the relevance of the device, then evaluating all the pieces of evidence detected on it, and then continues with the rest of the devices. Either way, 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 changing the viewpoint compared with the analysis phase, which was device-centered, and giving the investigation a degree of completeness. Once all the pieces of evidence have been evaluated, the investigator should be able to chronologically retrace the actions that occurred in the incident, supporting them with concrete proof, and to determine how the devices in the network were affected by it.

4.2.6. Presentation & Post-Process

This phase involves the actions needed for the closing of the investigation. It 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.

Regarding the first process, it depends on the laws in the country in which the investigation took place, but, generally, the investigator must return the original sources of evidence, if any were taken. In some cases, the investigator might even be required to destroy them [78].

The report must present the actions performed during the investigation in a clear way. In addition, the language used must be adapted to the level of expertise of the recipient, so that it can be easily comprehended. It is advisable to include the following content:

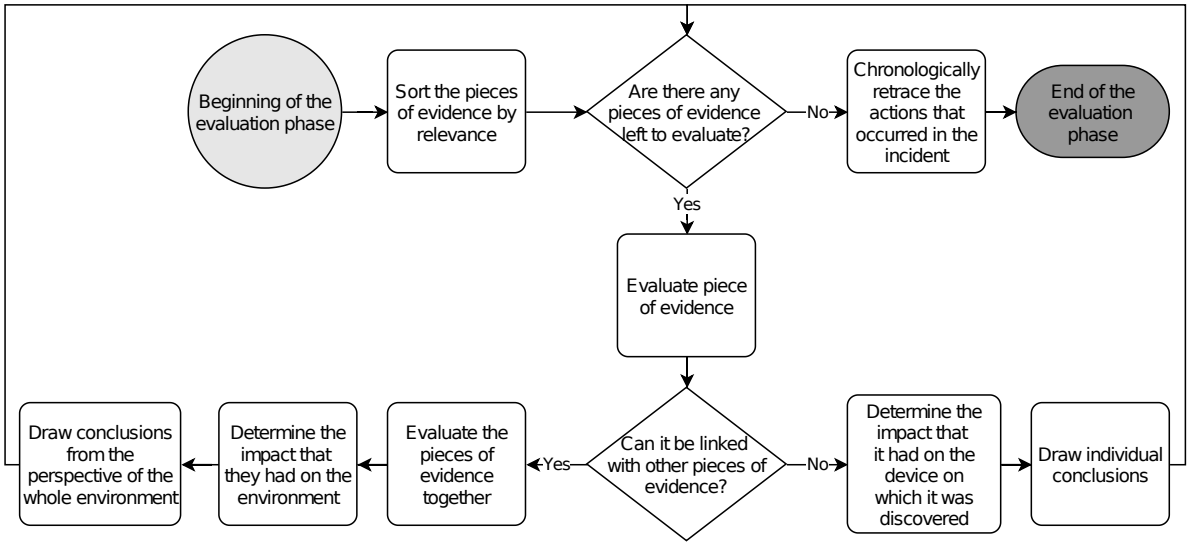

FIGURE 3. Flowchart diagram of the proposed evaluation phase

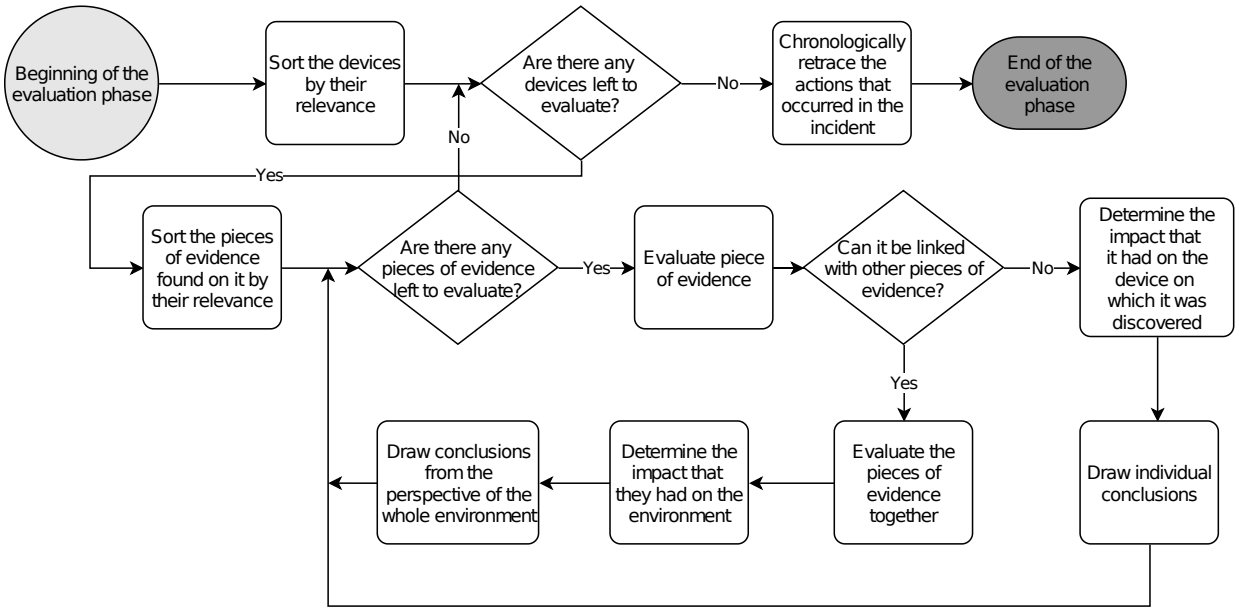

FIGURE 4. Flowchart diagram of the proposed alternative evaluation phase

- Objective and scope of the investigation.
- Events that led to the opening of the investigation.
- Preliminary considerations and methodology followed.
- Glossary of technical terms and abbreviations.
- Regulations and documents of reference used.
- Detailed description of the actions performed.
- Conclusions presenting the findings.

Finally, if it was a private investigation, the requester might ask the investigator to bring back the IoT network to a functioning state. This usually happens when malware was the cause of the incident or if any of the systems were compromised. In order to achieve this, the following actions need to be carried out:

- Clean the environment: first, it must be determined whether the malware or vulnerability is still present in the network by running scanning tools. Depending on the answer, and on the level of damage suffered by the devices, it may be sufficient to simply remove it. If not, restoring the devices might be in order.
- Restore the systems: this consists in using backup copies of the devices, returning them to their previous functioning state. 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, and also whether the vulnerability or malware is still present. If it still is, a more thorough cleaning procedure must be executed.

5. EVALUATION

In this section, the proposal is submitted to three different types of evaluation in order to determine whether it improves the related work, and whether it is feasible, practical and effective enough to be used in real-life forensic investigations.

5.1. Theoretical Evaluation

In this first evaluation, the proposed methodology is compared with the works presented by the research community, which have already been reviewed in Section 3, from a theoretical standpoint. This comparison is shown in Tables 3 and 4, evaluating the following aspects:

- Reference: whether they use any other model, methodology, framework, or standard as a reference from which to build the proposal.
- Technically detailed: whether the proposal details the technical procedures that the investigator has at their disposal to carry out the investigation.
- Practical perspective: whether the proposal is approached focusing on the application of the processes that the investigator must or has the option to execute during the investigation.
- Evaluation: whether the authors perform any kind of evaluation to test the effectiveness of their proposal and, if they do, which type is it, the three possibilities being the following:
  - Critical: the limitations of the methodology, model, or framework are described without making any comparison with the existing proposals.
  - Theoretical: the proposal is compared with the related work by studying the processes presented in them and how they differ between them.
  - Practical: the proposal is tested in a practical scenario in which it is used as a guideline to solve a forensic investigation.

In summary, the improvements of the authors' methodology with respect to the related work are stated below.

- Our proposal uses a widely-adopted traditional forensic model as a reference, which allows it to take advantage of key elements that assure the effectiveness and completeness of the methodology and, consequently, of the investigation.
- It relies on the proposals from the community regarding IoT forensic examinations of different systems and devices from the main IoT contexts, their requirements and previously proposed methodologies and frameworks.
- It studies and recognizes the characteristics common to all the contexts, and they are extracted and addressed in the form of a general methodology that can be used as a reference for IoT investigations.
- It is divided into delimited phases, providing detailed step-by-step guidelines on how to perform each stage of the forensic investigation. In addition, it addresses all of them from a practical viewpoint, so that investigators know how to approach them.
- It fully covers all the relevant phases of an investigation, namely identification, acquisition and analysis, as well as additional pre-and post-investigation ones.
- It provides a number of general tools that can be used in the process, describing their characteristics.
- It is submitted to a theoretical, a practical evaluation, and a hybrid one. Firstly, the processes described in it are compared with the ones introduces in the related work Secondly, it is also tested in two practical scenarios that could arise in real life by using it as guideline to investigate them. And, finally, it is studied how the proposals from the research community would behave in these practical scenarios and compare it with the results obtained by our methodology.

Regarding the details of the phases into which the methodology has been divided, these are the main differences with respect to previous models:

- Identification: it addresses the issue of the large number of devices by studying the logical connections established by the systems, not only by analyzing the physical ones, thereby also taking into account the fact that a device belonging to the IoT network under investigation might be in a different location to another in the same network. In addition, the devices are studied according to their importance, not on the basis of the zone they belong to.
- Acquisition: it recognizes that the investigator might not have physical access to the devices and, consequently, provides guidelines on how to perform a remote/live acquisition. Furthermore, it suggests multiple acquisition methods depending on the need to conserve the integrity of the evidence, and also considering that the physical memory might not be removable. Additionally, it covers the extraction of the main types of data that can be retrieved from IoT devices.
- Analysis: it considers the two possible approaches for the analysis, namely offline and remote/live,

TABLE 3. Theoretical comparison of the proposed research with the related work

Proposal	Reference	Technically Detailed	Practical Perspective	Evaluation
[8]	Not specified	✗	✗	✗
[14]	Standard operating procedure	✗	✗	✗
[15]	ISO/IEC 27043:2015	✗	✗	Critical
[16]	Not specified	✗	✗	Theoretical
[17]	ISO/IEC 29100:2011	✗	✗	Theoretical
[18]	Best practices in digital forensics	✗	✗	✗
[19]	Available network forensic methods and tools	✗	✗	✗
[20]	Not specified	✗	✗	Practical
[21]	Not specified	✓	✗	Practical
[22]	Not specified	✗	✗	Practical
[23]	Principles of DFRWS [24]	✗	✗	Theoretical
[25]	Common methodology	✗	✗	✗
[27]	Not specified	✗	✗	✗
[28]	DFIF-IoT [15]	✗	✗	Critical
[29]	Layered architecture	✗	✓	✗
[30]	Literature survey	✓	✓	Practical
[31]	ISO/IEC 27043	✗	✓	✗
[32]	Classic IT forensic processes and OT forensic research	✗	✓	Semi-practical
[33]	Not specified	✗	✗	Theoretical
[34]	Not specified	✓	✓	Practical
[35]	Existing frameworks [28, 15, 18]	✗	✗	✗
Proposed Research	Traditional forensic model [79]	✓	✓	Theoretical, Practical and Hybrid

also taking into account the tools available for each one. In addition, it offers flexibility regarding the forensic soundness of the investigation, so that cases that do not end in a legal process can take advantage of that.

- Evaluation: the main idea of this phase is very similar to the one that already exists in the conventional forensic process model, but it has been modified to take into account the concept of environment, which is key in the IoT. By doing so, this phase acquires a higher level of importance in the investigation.
- Regarding the rest of the phases, they are quite similar to the approach followed in conventional investigations, but they have been adapted to the characteristics of the IoT.

5.2. Practical Evaluation

In this section, the methodology is tested in two practical scenarios, which have been designed to represent real-life situations that are common on IoT investigations. In addition, we also compare how the proposals from the community that can be applied in each case would behave in these situations. It should be noted that some aspects of the case studies were performed theoretically, but the authors made sure that the actions described, as well as the practical techniques mentioned, were feasible.

5.2.1. Smart Home Investigation

The owner of a smart home system requests an investigation after their devices started to behave erratically on three different nights, with random changes in the state of some of the sensors installed, and the owner suspects that someone might have attacked their IoT system.

Pre-Process. When speaking to the owner, they mentioned that their IoT network was composed of multiple Samsung SmartThings devices. After receiving this information, the investigator studied the technical specifications of the devices to determine how to approach the investigation. Furthermore, the owner mentioned that they were not sure whether they were

TABLE 4. Phase-by-phase comparison of the proposed research with the related work

Proposal	Identification	Acquisition	Analysis
[8]	Based on network zones: internal, middle and external	Traditional approach. Not very detailed	Traditional approach. Not very detailed
[14]	Device to device communication	Live extraction	Traditional approach
[15]	Divided into cloud, network, and device level	Not detailed	Not detailed
[16]	Not addressed	Not addressed	Not addressed
[17]	Needed beforehand	Through a piece of software	Not detailed
[18]	Not detailed, although it mentions examples of data that can be found in each context	Not detailed, although it mentions that it would be like any other type of forensics	Same as the acquisition
[19]	Based on zones	Described from a theoretical viewpoint	Not addressed
[20]	Not specified	Offline	Not addressed
[21]	Not addressed	Online, by using a distributed platform	Not addressed
[22]	Traditional approach	Traditional approach	Not detailed
[23]	Through a fog node connected to the IoT device	Remote	Not addressed
[25]	Not detailed	Offline	Not detailed
[27]	Not detailed	Not detailed	Not detailed
[28]	Divided into cloud, network, and device level	Not detailed	Not detailed
[29]	Based on zones	Traditional approach	Not detailed
[30]	Physical	Offline	Offline
[31]	Not detailed	Physical and Logical	Not detailed
[32]	Based on a previous inventory	Physical and live	Offline
[33]	Not addressed	Using a data unifier that structures the data collected by a IoT tools	Not addressed
[34]	Based on radio signals	Not addressed	Not addressed
[35]	Not detailed	Not detailed	Not detailed
Proposed Research	Based on logical device communication	Flexible approach depending on the state of the source of evidence, its physical accessibility and degree of integrity. Covers offline and remote/live acquisition	Offers guidelines for offline and remote/live analysis

going to take legal action, so the integrity of the device needed to be protected in case they ended up doing so.

No warrants were needed since the IoT network was not using a cloud service, and its owner had willingly given their authorization to examine their house.

Identification. Once the investigator was present at the scene, it was confirmed that the smart router, specifically a Samsung SmartThings Wi-Fi [80], was in the house, and that it was still powered on. Knowing that the device which delimits the range of the scene is the router, it is the one that was studied first. In addition, through it flowed all the traffic of the IoT network and the rest of the devices in the home, also making it the most relevant one. However, to determine what devices were connected to it, it was faster and easier to establish this with the mobile app installed on the smart phone of the owner. In order to confirm that the information displayed by it was correct, the whole house was inspected, finding the same devices as the ones listed in the mobile app. These devices, which had already been turned off, were the following:

- A SmartThings Multipurpose Sensor V3 connected to the main door of the house [81].
- A SmartThings Motion Sensor V3 installed in the porch [82].
- A SmartThings Moisture Sensor V3 installed in a kitchen cupboard [83].
- A SmartThings Presence Sensor V2 installed in the main entrance [84].
- A SmartThings Cam installed on the porch [85].
- A SmartThings Wi-Fi Smart Plug installed in

the living room and to which the television was connected [86].
- A SmartThings Smart Bulb fitted in a lamp in the living room [87].

As these sensors were powered off, and they did not store any data regarding their state, only executing a program, it was decided that they had no relevance in the case.

Acquisition & Preservation. The only device that needed to be acquired was the SmartThings Wi-Fi router. As it was physically accessible, and the integrity needed to be preserved, an offline acquisition was performed. Knowing that, as shown in Figure 5, its storage was soldered to the board, the device was seized and transferred to the forensics laboratory. There, the investigator first tried to carry out a JTAG, but it was found to be incompatible with the device, so, since it had an eMMC memory, an ISP was performed. After that, the image file created was stored on a secure external drive, creating two additional copies, and the router was reassembled and put in a safe, which could only be accessed by the investigator.

Analysis. Since the router was imaged, an offline analysis was carried out. On browsing through the logs of the data received by the sensors, it was observed that, on three nights, the state of the smart plug and the smart bulb changed multiple times, confirming the statement of the requester. The data for the rest of the sensors was normal, nothing out of the ordinary was noticed.

When inspecting the configuration files, it was observed that the Telnet service, known to be highly insecure, was enabled on the device. Seeing that, the logs from the aforementioned service were inspected, finding that there were connections from devices that did not belong to the home network. During one of these connections, a file was downloaded from a remote server and then executed. When carrying out a carving process on the acquired memory, the file was recovered and analyzed, confirming it to be a malware sample, specifically a botnet. By studying it, it could be seen that, once it was executed on the device, it contacted the command and control (C&C) server and tried to infect other devices in the network. As it tried to do so through the Telnet and SSH services, it failed to spread since there were not any other devices with them enabled. On checking the timestamps of the remote connections, it was noticed that one of them matched the date and time when the sensors were ordered to change their state.

Evaluation. As only one device was analyzed, namely the router, all the pieces of evidence came from it, and these, in order of relevance, were: the logs showing the state of the smart bulb and the smart plug changing multiple times on three different nights, the external connections made to the router on said nights, the carved malware file downloaded in the first of these connections, and the configuration of the Telnet service. Only the first one affected other devices, specifically the smart bulb and the smart switch, but it did not cause permanent changes, since the malware failed to spread through the network.

The chronological reconstruction of events is the following: an external attacker detected that the Telnet service was enabled on the SmartThings Wi-Fi router. As it is easy to exploit, they gained access to the device, onto which they downloaded a botnet malware and executed it. Having permanent access to the router, the attacker managed to change the state of the smart bulb sensor and the smart plug multiple times on three different nights, causing the problems described by the owner.

Presentation & Post-Process. Once the evaluation phase had finished, a report was created describing the actions carried out during the investigation and its findings. In addition, the SmartThings Wi-Fi router that was seized during the acquisition phase was returned to the owner.

5.2.2. Smart Vineyard Case

A forensic investigation is solicited after the requester says that their IoT system, which is in charge of monitoring environmental parameters in a vineyard, is not working properly, and they suspect that it has been attacked.

Pre-Process. During the first conversation with the requester, they specify that the IoT system is a Libelium Smart Agriculture IoT Vertical Kit [89]. On studying its technical specifications, it was learned that it was comprised of an outlet-powered gateway [90] using a Linux kernel, with a 16 Gb Solid-State Drive (SSD), 2 Gb of Random Access Memory (RAM) and multiple connectivity modules. Additionally, there were two Waspmote boards [91] to which the multiple sensor probes were connected, with each of them having an internal Secure Digital (SD) card of 16 Gb and being powered by a rechargeable battery with a solar panel.

Regarding the forensic soundness of the investigation, no legal measures were going to be taken, so it was not necessary to preserve the integrity of the evidence. In addition, the requester mentioned that the data captured was also sent to an instance of Amazon Web Services IoT [92] to be analyzed and visualized. Since they were happy to provide access to their account, and the communication between the IoT network and the cloud was unidirectional, no warrant obtention was needed.

Identification. From the information provided by the requester, it was determined that the most relevant device in the IoT kit was the gateway, since it was the one which managed the network. In addition, studying it would allow the investigator to detect whether there were any other devices in it, apart from the ones that comprised the kit.

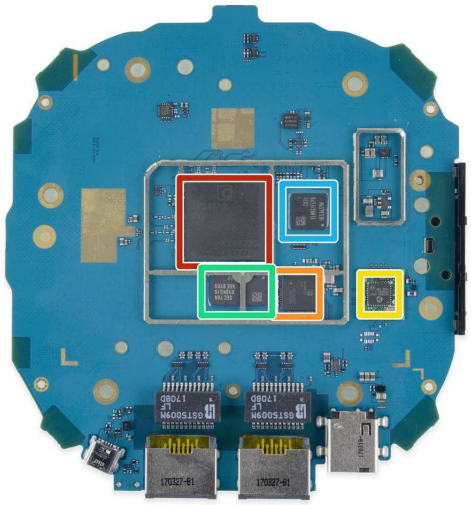

FIGURE 5. Samsung SmartThings Wi-Fi board. The non-volatile memory is highlighted in blue [88]

Therefore, the first device that was studied was the gateway, which consisted of a Meshlium 4G 868/900 access point [90] using a 4G connection. Since the requester did not want the device to be damaged, added to the fact that there was no need to preserve the integrity of the data, and that the investigator was not sure whether the storage was removable, the device was not acquired. In order to study it, once connected to the Wi-Fi network created by the gateway, the manager system was accessed through the web browser to determine which devices were connected to it, and the following were detected:

- Two Waspmote Plug & Sense! SA-PRO 868/900-PRO 5dBi [91] units with a 4G connection and the following components attached:
  - A temperature, humidity, and pressure sensor probe.
  - A PT-1000 soil/water temperature sensor probe.
  - A solar radiation sensor probe.
  - A soil moisture sensor probe.
  - A leaf wetness sensor probe [93].
- A WS-3000 anemometer, wind vane and pluviometer probe.

This result meant that no other IoT device was connected to the gateway. Regarding the Waspmote boards, since it was not possible to access them in a similarly easy way to that for the access point, and as all their sensor sockets were in use, so no more devices could be detected when studying them, and the data collected by the sensors could be studied using the logs stored in the former, it was decided to delay their acquisition until the gateway was analyzed. The same approach was taken for the sensors, since they did not store any information, only collecting the data.

Acquisition & Preservation. Since the access point was going to be analyzed following a remote/live approach, and neither the Waspmote boards nor the sensors were going to be acquired, no actions were necessary in this phase. However, it should be mentioned that, if it had been necessary, the methodology would have recommended extracting the removable memory of the Waspmote boards and imaging it. The same approach might have been valid for the access point based on its technical specifications, but this cannot be confirmed for sure, as it was not certain whether the SSD was removable.

Analysis. On inspecting the logs shown in the manager system of the access point, it was observed that the sensors were working properly and sending the data, as can be seen in Figure 6. However, when examining the data stored in the cloud, the latest measurements were not among them. When checking the cloud connector, it was detected that its configuration had been erased. Since the requester claimed that they did not do it, an extensive analysis was performed, checking the logs produced by the system. To do so, a connection was established with its File Transfer Protocol (FTP) server. When inspecting the network data, it was seen that there were two different Media Access Control (MAC) addresses, meaning that two distinct devices had connected to the Wi-Fi network. One of them matched the address of the laptop computer that the requester used to connect to the access point, but the other one was not recognized. By retrieving the logs generated after the unidentified device connected, it was observed that the cloud connection configuration was altered minutes afterwards. By checking the timestamps, it was discovered that, when that alteration was made, the unidentified device was the only one that was connected to the Wi-Fi network, and that this time was the only occasion on which the device established connection with the access point. On seeing this, the security state of the network was inspected, observing that its

settings were still the default ones, thus not providing any protection.

To confirm that there were no other issues in the network, the investigator connected a laptop to the Wi-Fi access point and launched a network tool to examine the packets that were flowing through it, not noticing anything abnormal. Since the sensors and the Waspmote boards were working properly, and the cause of the incident had been determined, it was decided not to acquire or analyze them.

Evaluation. Only the pieces of evidence discovered on the access point needed to be evaluated, and these, in order of importance, were: the log showing the cloud connection being disabled, the two different MAC addresses in the network log, the unidentified device only being connected once, and the security state of the wireless network. None of them had an impact on any other device in the IoT. However, the first piece of evidence affected the cloud instance, which did not receive the corresponding data.

The chronological reconstruction of events is the following: an external device connected to the Wi-Fi network associated with the access point, which did not have any security measures, as its settings were the default ones. After connecting, the attacker disabled the connection between the IoT gateway and the Amazon Web Services IoT cloud, the instance therefore neither displaying nor storing the data collected, which were only stored locally.

Presentation & Post-Process. Since the requester did not find it necessary to write a report, and there were no sources of evidence to return, the only action that was taken in this phase was the reset and configuration of the access point, making sure that all its services were properly secured and working correctly. This was also done using the manager system.

5.2.3. Relevance of the Case Studies Presented

After carrying out the practical evaluation of the proposal, and concluding that it can be successfully followed in the two scenarios presented, it is necessary to argue why these case studies are an interesting way of testing the authors' methodology and reflect the forensic challenges that investigators face in IoT examinations. In particular, the reasons are the following:

- Smart Home Investigation: this scenario is of relevance because, firstly, it is performed in the context in which the highest number of IoT devices can be found [94, 95]. Secondly, the IoT kit to be examined is known to be a highly bought one. And, finally, it simulates an attack targeting an IoT device, which is quite common [7]. In terms of forensic challenges, it presents the following:
  - The integrity of the sources of evidence needs to be protected, thus having to face the difficulty of preserving data in a scenario in which a standard procedure does not exist.
  - The investigation is performed in a scenario with several IoT devices in it, and a conventional one, namely a smartphone. This means that the methodology to be followed must be able to address the high number of devices that can be found in an IoT network, and take into account the possibility of having to examine conventional devices that interact with the IoT ones. The former demands having a clear procedure on which devices need to be analyzed, when, and how to determine that, and the latter involves evaluating other sources of evidence to complement the information extracted from the IoT network.
  - When facing the acquisition process, the main source of evidence needs to be collected using the ISP technique, which is a physical one that is adapted from smartphone forensics. This shows that the procedure followed considers this technique as an interesting approach to collect data from IoT devices.
  - Finally, it proves that the proposal is flexible enough to adapt to scenarios in which the number of acquirable sources of evidence is very low and that it is able to reach valid conclusions on what occurred in the case study. In addition, it also is capable of dealing with the challenge of accessing the data stored by IoT devices, seeing that only one technique was capable of retrieving the data stored in the main source of evidence.
- Smart Vineyard Investigation: it is performed in a new context introduced by the IoT, namely smart agriculture. With this scenario, the aim is to challenge the proposal with an environment that has no resemblance with conventional ones. With respect to the forensic challenges that it presents, the main ones are the following:
  - The case study is carried out in a vineyard with several hectares of surface, meaning that the devices to be studied are not physically close, so there is no guarantee on whether the investigator must be able to physically access them. Consequently, alternatives techniques to physical one must be considered to carry out the examination, and thus the methodology must be able to contemplate them and inform the investigator on how to use them, when, and what benefits and limitations they have.
  - The integrity of the data does not have to be preserved, so the procedure to be followed must provide the investigator with techniques on how to take advantage of that fact to perform a faster examination than if it were

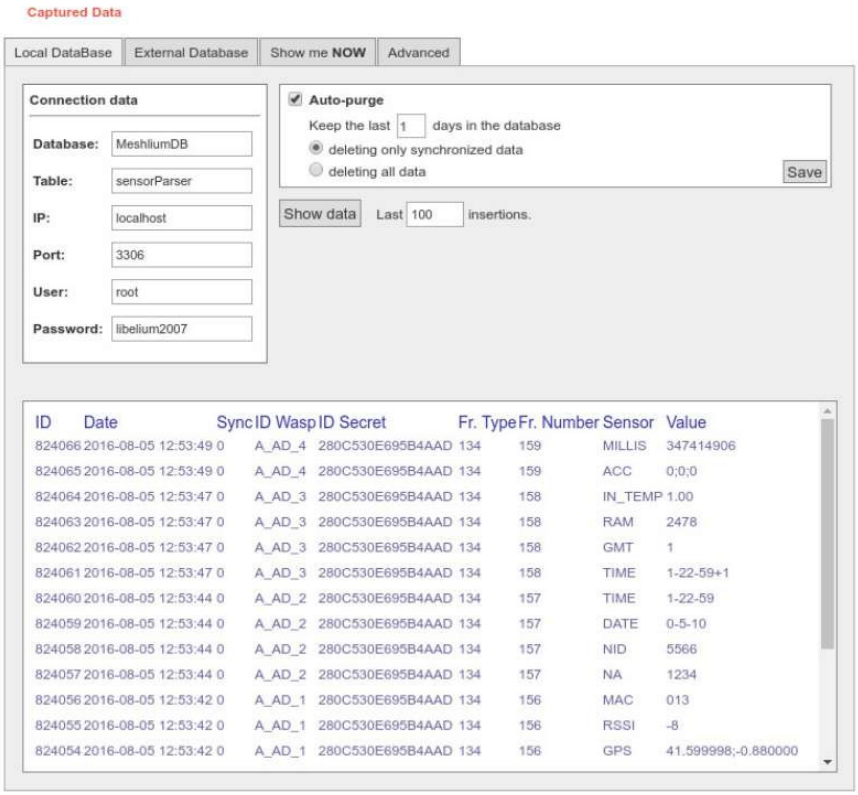

FIGURE 6. Logs from the access point showing the data collected by the sensors [90]

necessary to preserve it.

– In this case, the IoT kit interacts with the cloud, another conventional forensic scenario. Therefore, guidelines must be provided on how to evaluate whether these data have value, how to access them and when to do so.
– The accessibility of the main source of evidence, its importance, and its features suggest that the best approach to be followed when examining it is to perform a remote analysis, which is not that common in conventional forensics. As a result, the methodology must be able to clearly explain how this process works and how to perform it.

5.3. Hybrid Evaluation

Finally, a simulation is carried out to study how the models proposed by the community would have behaved if followed in the case studies described above, and their performance is compared with the methodology introduced in this article. Before presenting the results, there were some proposals that were discarded as they could not be evaluated for the following reasons:

- They rely on a not-yet-developed piece of software, device, or platform to perform the investigation: [17, 21, 23, 33].
- They depend on the implementation of the whole model beforehand, as they also cover the proactive and reactive process, in order to properly carry out the forensic investigation: [31].
- They are focused on the design of forensic-ready systems, not on the investigation process: [16].
- They model a specific context of the IoT: [20, 25, 30, 32].
- They only focus on one aspect of the investigation process: [34]
- In their practical phases, even if they lack detail, they do not mention the approach that they follow: [15, 27, 35].

5.3.1. Smart Home Investigation

The most characteristic aspects of this case study are the identification of the devices and the acquisition of the Samsung SmartThings Wi-Fi router, which are performed with techniques that are not so common in conventional forensics. The behaviour of the previous models in each practical phase is the following:

Identification. The most similar output would be obtained with [22], which would also opt for the use of the mobile app to detect which devices are present in the network, although it does not establish an order to study them. Regarding the proposals that divide the components of the network into layers or zones ([8], [19], [28] and [29]), they would end up obtaining the

same result, since the devices in the case study can be physically detected, but they would have done so in a less efficient way, as they would have studied the sensors before the router. This is not the case for [8], which establishes an order of relevance in each zone. The approach followed by [14] would have succeeded too, since it relies on logical communications to perform the identification.

Acquisition & Preservation. In none of the proposals are the JTAG, ISP or chip-off named. However, since [8], [18], [19], [22] and [28] mention that they follow a traditional or usual approach, and these methods are used in smart phone forensics, it could be interpreted that they are included and, therefore, would have succeeded.

Analysis. [8] and [18] mention that they follow a traditional or typical approach. An offline analysis, as well as carving, are techniques used in conventional forensics, so although these proposals provide fewer details on how to address this phase, there is no reason to believe that they would not have succeeded. In addition, [29] would have provided useful tools to perform the analysis, even though it fails to offer guidelines on how to use them.

5.3.2. Smart Vineyard Case

In this scenario, the models must face a remote/live analysis and the study of the cloud as a possible source of evidence, which they do, as described below.

Identification. None of the proposals that rely on a zone or layer division, namely [8], [19], [28] and [29], would have obtained an efficient result, since they do not consider the remote/live study of a device to determine whether there could be any more systems connected. Therefore, the investigator would have needed to physically study the vineyard until they had detected the devices. However, [14] might have, since it focuses on studying the logical connections, but does not mention whether they contemplate the possibility of doing that by performing a remote/live study. Regarding the identification of the cloud as a source of evidence, all of them would have succeeded in detecting it, but could only have done so by relying on the statement of the owner, since they do not examine the device to see whether the connection with the cloud exists until the analysis phase.

Acquisition & Preservation. In this case, no acquisition is performed. As was mentioned in Section 5.2.2, if it had been necessary, [8], [18], [19] and [28] would have to be assumed as successful since they mention that they follow a traditional approach. In addition, [29] lists multiple tools that would have succeeded in the process.

Analysis. The ones that could have been followed in this phase are [8] and [18]. None of them mention the possibility of performing a remote/live analysis, or give any guidelines on how to perform the process. However, since all of them opt to follow a traditional approach, we assume that they consider this method. Consequently, there are no arguments to believe that they would not have succeeded if applied during this phase.

Once all the models have been evaluated, the following conclusions can be drawn:

- There is a clear lack of detail in the previous models, which makes them difficult to follow when performing an investigation. This does not mean that they are not suitable for being used, but not being structured, detailed and clear implies that the investigator must rely on their instinct and improvise, which increases the chances of making a mistake and hinders the completeness of the process.
- Only [8] is able to cover all the practical phases of the investigation in both of the case studies presented, but it does so in a less efficient way and thanks to its lack of specificity, which allows it to cover a wide range of techniques without mentioning any of them. Therefore, as observed above, it depends on the ability of the investigator to know and identify which the appropriate ones to use are.
- Similarly, other models might also have been able to reach the same outcome as our proposal did in certain phases, but this must be assumed as well, since they do not detail whether some of the techniques used in the case studies are actually considered in their proposals.

6. DISCUSSION

After completing the experiment, and gathering a significant amount of knowledge in the design of IoT procedures, the research questions formulated in the beginning of this research can be answered.

- **(RQ1)** Is it reasonable to approach the development of IoT forensic procedures from a generic perspective, or the heterogeneity of the environment is too great to allow that?

- The study of the characteristics of IoT devices and how they affect forensic investigations shows that there are some crucial aspects of the process that are common to all IoT contexts. In particular, the way in which the non-volatile memory is present in the device, and the protocols used in the IoT, are shared among many environments. This affects the acquisition and analysis of the sources of evidence and allows the procedure to have a generic tone. However, it is true that the identification phase is greatly affected by the context in which the investigation is taking place, as the number of devices will vary, as well as the hierarchy of importance of them. Similarly, the remote/live analysis technique depends on the operating system or firmware used by the IoT device, which

normally is particular to a context.

- **(RQ2)** Can conventional forensic procedures be adapted, to a certain extent, to the requirements of the IoT?

- The proposal presented in this article shows that conventional procedures can be adapted to the IoT, as it has been one of the references from which the methodology has been built. In fact, it is very convenient to do so to ensure the soundness of the methodology, and that it complies with the standards set by the forensic community. In addition, due to the limited number of IoT-centered forensic tools and techniques, conventional ones must be used to carry out investigations in the IoT, and therefore some of the processes detailed in traditional forensics must be imported into IoT models.

- **(RQ3)** Has the forensic community enough knowledge about the IoT to cover in detail the whole investigative process of an IoT investigation?

- The study of the proposals from the research community presented in Section 3 demonstrates that there are several pieces of research that have studied some of the crucial processes of IoT investigations, specifically the identification and acquisition of sources of evidence. However, it can be concluded that the approach followed in many of them either does not meet the requirements of the IoT, or their feasibility is too low to be used in real-life examinations. Basing the identification on zones or network level, or requiring a piece of software or hardware to carry out the acquisition are some examples.

  Unfortunately, the rest of the processes of a forensic investigation are not normally addressed in the related work.

- **(RQ4)** Is it possible to address these issues, and the main challenges encountered by the research community, and present an IoT forensic procedure that complies with the requirements of IoT investigations and meets the standards of the forensic community?

- The methodology presented in Section 4 proves that it is possible to combine the knowledge that can be extracted from conventional forensic procedures with IoT ones to create a hybrid proposal that targets the whole IoT environment. Regarding the main IoT forensic challenges, which are described in Section 2, they are solved in the following way:

  - The high number of devices is solved by changing the approach followed in the "Identification" phase to a logical one.
  - The interoperability of the IoT is addressed by creating a new phase named "Evaluation" that extracts conclusions from a holistic perspective.
  - The short lifetime of the evidence is dealt with by prioritizing devices depending on the lifetime, quantity, and relevance of their data, their significance in the environment, and the difficulty that it would present to acquire them.
  - The difficulty of performing a physical acquisition is solved by considering the remote/live option as a very interesting one under certain circumstances, and justifying the importance that a remote/live analysis can have when there are difficulties in the acquisition process.
  - The importance of network data is addressed by considering it a crucial source of evidence and offering guidelines on how to acquire and analyze it.
  - Finally, the lack of IoT-centered tools is compensated with by using generic ones that are able to handle IoT data.

- **(RQ5)** If so, how does this proposal compare with the related work? Can it be used in practical real-life IoT forensic scenarios, or its application is limited to a theoretical environment?

- When compared with the related work, it can be seen that the authors' methodology makes an improvement in terms of level of detail and practicality. In addition, it is able to offer guidelines on the whole investigative process. With respect to its applicability in practical IoT forensic scenarios, the results show that the processes described in the proposal are complete enough to lead to the gathering and/or analysis of sources of evidence from which to draw conclusions that allow to determine what has occurred in an incident.

7. CONCLUSIONS

This proposal addresses the development of procedures to be followed on IoT forensic investigations. Due to the different characteristics of conventional scenarios and the IoT, the solutions used until now cannot guarantee that IoT examinations are carried out in a complete and efficient manner, thus demanding new ones to be developed.

While the research community is already trying to address this issue, the existing proposals lack practicality and detail, as they are in a very early stage of development. In addition, most of them fail to present an evaluation that can justify their feasibility and effectiveness, which hinders the possibility of using them in real investigations.

With these challenges in mind, this article presents a concept practical forensic methodology for IoT investigations that uses a conventional widely-accepted forensic model, and a short concept version of an IoT methodology as reference, and adapts them to the requirements of the IoT and its different contexts. It

is divided into delimited step-by-step phases, providing a detailed practical approach. Furthermore, it has been evaluated theoretically, practically, and in a hybrid manner, comparing it to related work and testing it in real-life scenarios, and confirming its effectiveness and usefulness, as well as its potential to be a good starting point in the development of a general IoT forensic model.

7.1. Future Work

This work is an introduction to the development of practical methodologies for IoT forensics, so there is a wide spectrum of research to cover in order to properly address this issue. Some projects involving this topic could include:

- The modelling of methodologies to conduct forensic investigations in certain contexts of the IoT, since it is impossible to address all the requirements of each one with a general one.
- Development of tools to automatize some of the phases described in this methodology and address the lack of IoT-centered forensic ones.
- The broadening of the forensic analysis of systems and devices, especially the most commonly used, with the aim of understanding how to perform the retrieval of evidence and its examination when investigating them.
- Further studies based on comprehending the interaction between IoT devices in an environment, and how to incorporate that knowledge in the design of methodologies so that the most distinctive and important feature of the IoT, namely connectivity, is taken into account.

DATA AVAILABILITY

There are no data associated with this article.

ACKNOWLEDGEMENTS

This research was supported by the University of Castilla-La Mancha under the contract 2021-POST-20518 and the project 2021-GRIN-31042, by the Spanish Ministry of Economic Affairs and Digital Transformation under the projects RTI2018-098156-B-C52 and PID2021-123627OB-C52, and by the Regional Government of Castilla-La Mancha under the projects SBPLY/17/180501/000353 and SBPLY/21/180501/000195.

REFERENCES

[1] Brezinski, D. and Killalea, T. (2002). RFC 3227: Guidelines for Evidence Collection and Archiving. `https://www.ietf.org/rfc/rfc3227.txt`.

[2] International Organization for Standardization (2012). ISO - ISO/IEC 27037:2012 - Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. `https://www.iso.org/standard/44381.html?browse=tc`.

[3] International Organization for Standardization (2015). ISO - ISO/IEC 27042:2015 - Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. `https://www.iso.org/standard/44406.html?browse=tc`.

[4] International Organization for Standardization (2016). ISO - ISO/IEC 27050-1:2016 - Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts. `https://www.iso.org/standard/63081.html`.

[5] Lionel Sujay Vailshery. Statista. IoT connected devices worldwide 2019-2030 - Statista. `https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/`.

[6] Sonicwall (2022). Mid-Year Update: 2022 SonicWall Cyber Threat Report. `https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf`.

[7] Kaspersky (2022). Kaspersky Security Bulletin 2022. Statistics. `https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2022_en_final.pdf`.

[8] Oriwoh, E., Jazani, D., Epiphaniou, G., and Sant, P. (2013) Internet of things forensics: Challenges and approaches. *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Austin, TX, USA, 20-23 October, pp. 608–615. IEEE.

[9] Lillis, D., Becker, B., O'Sullivan, T., and Scanlon, M. (2016) Current challenges and future research areas for digital forensic investigation. *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, Daytona Beach, Florida, USA, 24-26 May. arXiv.

[10] Hou, J., Li, Y., Yu, J., and Shi, W. (2020) A survey on digital forensics in internet of things. *IEEE Internet of Things Journal*, **7**, 1–15.

[11] Atlam, H. F., Hemdan, E. E.-D., Alenezi, A., Alassafi, M. O., and Wills, G. B. (2020) Internet of Things Forensics: A Review. *Internet of Things*, **11**, 100220.

[12] Sandvik, J.-P., Franke, K., Abie, H., and Årnes, A. (2022) Quantifying data volatility for iot forensics with examples from contiki os. *Forensic Science International: Digital Investigation*, **40**, 301343.

[13] Alyami, M., Alharbi, I., Zou, C., Solihin, Y., and Ackerman, K. (2022) Wifi-based iot devices profiling attack based on eavesdropping of encrypted wifi traffic. *IEEE 19th Annual Consumer Communications Networking Conference (CCNC)*, Las Vegas, NV, USA, 08-11 January, pp. 385–392. IEEE.

[14] Perumal, S., Norwawi, N. M., and Raman, V. (2015) Internet of things (iot) digital forensic investigation model: Top-down forensic approach methodology. *Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, Sierre, Switzerland, 07-09 October, pp. 19–23. IEEE.

[15] Kebande, V. R. and Ray, I. (2016) A generic digital forensic investigation framework for internet of things (iot). *IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Vienna, Austria, 22-24 August, pp. 356–362. IEEE.

[16] Ab Rahman, N. H., Glisson, W. B., Yang, Y., and Choo, K. R. (2016) Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Computing*, **3**, 50–59.

[17] Nieto, A., Rios, R., and Lopez, J. (2017) A methodology for privacy-aware iot-forensics. *IEEE Trustcom/BigDataSE/ICESS*, Sydney, NSW, Australia, 01-04 August, pp. 626–633. IEEE.

[18] Zia, T., Liu, P., and Han, W. (2017) Application-specific digital forensics investigative model in internet of things (iot). *Proceedings of the 12th International Conference on Availability, Reliability and Security*, Reggio Calabria, Italy, 29 August - 1 September. Association for Computing Machinery.

[19] Harbawi, M. and Varol, A. (2017) An improved digital evidence acquisition model for the internet of things forensic: A theoretical framework. *5th International Symposium on Digital Forensic and Security (ISDFS)*, Tirgu Mures, Romania, 26-28 April, pp. 1–6. IEEE.

[20] Feng, X., Dawam, E. S., and Amin, S. (2017) A new digital forensics model of smart city automated vehicles. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Exeter, UK, 21-23 June, pp. 274–279. IEEE.

[21] Hossain, M., Hasan, R., and Zawoad, S. (2017) Trust-iov: A trustworthy forensic investigation framework for the internet of vehicles (iov). *IEEE International Congress on Internet of Things (ICIOT)*, Honolulu, HI, USA, 25-30 Jun, pp. 25–32. IEEE.

[22] Goudbeek, A., Choo, K.-K. R., and Le-Khac, N.-A. (2018) A forensic investigation framework for smart home environment. *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 01-03 August, pp. 1446–1451. IEEE.

[23] Al-Masri, E., Bai, Y., and Li, J. (2018) A fog-based digital forensics investigation framework for iot systems. *IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, USA, 21-23 September, pp. 196–201. IEEE.

[24] Collective work of all DFRWS attendees (2001) A Road Map for Digital Forensic Research. *The Digital Forensic Research Conference (DFRWS)*, Utica, NY, 7-8 August. DFRWS.

[25] Bharadwaj, N. K. and Singh, U. (2018) Acquisition and analysis of forensic artifacts from raspberry pi an internet of things prototype platform. *International Conference on Advanced Computing, Networking and Informatics (ICACNI)*, Singapore, 1-3 June, pp. 311–322. Springer Singapore.

[26] Foundation, R. P. (2020). Raspberry Pi OS for Raspberry Pi. `https://www.raspberrypi.org/downloads/raspberry-pi-os/`.

[27] Sathwara, S., Dutta, N., and Pricop, E. (2018) Iot forensic a digital investigation framework for iot systems. *10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, Romania, 28-30 June, pp. 1–4. IEEE.

[28] Kebande, V. R., Karie, N. M., Michael, A., Malapane, S., Kigwana, I., Venter, H. S., and Wario, R. D. (2018) Towards an integrated digital forensic investigation framework for an iot-based ecosystem. *IEEE International Conference on Smart Internet of Things (SmartIoT)*, Xi'an, China, 17-19 August, pp. 93–98. IEEE.

[29] Al-Sadi, M. B., Chen, L., and Haddad, R. J. (2018) Internet of things digital forensic investigation using open source gears. *SoutheastCon 2018*, St. Petersburg, FL, USA, 19-22 Apri, pp. 1–5. IEEE.

[30] Kasukurti, D. H. and Patil, S. (2018) Wearable device forensic: Probable case studies and proposed methodology. *6th SSCC: International Symposium on Security in Computing and Communication*, Bangalore, India, 19-22 September, pp. 290–300. Springer Singapore.

[31] Sadineni, L., Pilli, E., and Battula, R. B. (2019) A holistic forensic model for the internet of things. *15th IFIP WG 11.9 International Conference*, Orlando, FL, USA, 28-29 January, pp. 3–18. Springer International Publishing.

[32] Karagiozidis, A. and Gergeleit, M. (2022) An OT Forensic Model Based on Established IT Forensics Using IIRA. *IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, Stuttgart, Germany, 06-09 September, pp. 1–8. IEEE.

[33] Surange, G. and Khatri, P. (2022) Integrated intelligent IOT forensic framework for data acquisition through open-source tools. *International Journal of Information Technology*, **14**, 3011–3018.

[34] Jacob, R. and Nisbet, A. (2022) A forensic investigation framework for internet of things monitoring. *Forensic Science International: Digital Investigation*, **42-43**, 301482.

[35] Kim, J., Park, J., and Lee, S. (2023) An improved IoT forensic model to identify interconnectivity between things. *Forensic Science International: Digital Investigation*, **44**, 301499.

[36] Meffert, C., Clark, D., Baggili, I., and Breitinger, F. (2017) Forensic state acquisition from internet of things (fsaiot): A general framework and practical approach for iot forensics through iot device state acquisition. *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES)*, Reggio Calabria, Italy, 29 August - 1 September. Association for Computing Machinery.

[37] Zawoad, S. and Hasan, R. (2015) Faiot: Towards building a forensics aware eco system for the internet of things. *IEEE International Conference on Services Computing*, New York, NY, USA, 27 June - 2 July, pp. 279–284. IEEE.

[38] Hossain, M., Karim, Y., and Hasan, R. (2018) Fif-iot: A forensic investigation framework for iot using a public digital ledger. *IEEE International Congress on Internet of Things (ICIOT)*, San Francisco, CA, USA, 02-07 July, pp. 33–40. IEEE.

[39] Oriwoh, E. and Sant, P. (2013) The forensics edge management system: A concept and design. *IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*,

Vietri sul Mare, Italy, 18-21 December, pp. 544–550. IEEE.

[40] Chung, H., Park, J., and Lee, S. (2017) Digital forensic approaches for amazon alexa ecosystem. *Digital Investigation*, **22**, S15 – S25.

[41] Clark, D. R., Meffert, C., Baggili, I., and Breitinger, F. (2017) Drop (drone open source parser) your drone: Forensic analysis of the dji phantom iii. *Digital Investigation*, **22**, S3 – S14.

[42] Jo, W., Shin, Y., Kim, H., Yoo, D., Kim, D., Kang, C., Jin, J., Oh, J., Na, B., and Shon, T. (2019) Digital forensic practices and methodologies for ai speaker ecosystems. *Digital Investigation*, **29**, S80 – S93.

[43] Gregorio, J., Alarcos, B., and Gardel, A. (2019) Forensic analysis of nucleus rtos on mtk smartwatches. *Digital Investigation*, **29**, 55 – 66.

[44] Hadgkiss, M., Morris, S., and Paget, S. (2019) Sifting through the ashes: Amazon fire tv stick acquisition and analysis. *Digital Investigation*, **28**, 112 – 118.

[45] Yusoff, Y., Ismail, R., and Hassan, Z. (2011) Common phases of computer forensics investigation models. *International Journal of Computer Science & Information Technology (IJCSIT)*, **3**, 17–31.

[46] Castelo Gómez, J. M., Carrillo Mondéjar, J., Roldán Gómez, J., and Martínez Martínez, J. (2021) Developing an iot forensic methodology. a concept proposal. *Forensic Science International: Digital Investigation*, **36**, 301114.

[47] Han, J., Jeon, Y., and Kim, J. (2015) Security considerations for secure and trustworthy smart home system in the iot environment. *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South), 28-30 October, pp. 1116–1118. IEEE.

[48] Le-Khac, N.-A., Jacobs, D., Nijhoff, J., Bertens, K., and Choo, K.-K. R. (2020) Smart vehicle forensics: Challenges and case study. *Future Generation Computer Systems*, **109**, 500–510.

[49] Badenhop, C. W., Ramsey, B. W., Mullins, B. E., and Mailloux, L. O. (2016) Extraction and analysis of non-volatile memory of the zw0301 module, a z-wave transceiver. *Digital Investigation*, **17**, 14 – 27.

[50] Wurm, J., Hoang, K., Arias, O., Sadeghi, A., and Jin, Y. (2016) Security analysis on consumer and industrial iot devices. *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, Macao, China, 25-28 January, pp. 519–524. IEEE.

[51] Elstner, J. and Roeloffs, M. (2016) Forensic analysis of newer tomtom devices. *Digital Investigation*, **16**, 29 – 37.

[52] Gupta, K. P. and Nisbet, A. (2016) Memory forensic data recovery utilising ram cooling methods. *14th Australian Digital Forensics Conference*, Perth, Australia, 5-6 December, pp. 11–16. Research Online.

[53] VöMel, S. and Freiling, F. C. (2011) A survey of main memory acquisition and analysis techniques for the windows operating system. *Digit. Investig.*, **8**, 3–22.

[54] Computer Hope. Computerhope.com (2020). Linux and Unix dd Command. `http://www.computerhope.com/unix/dd.htm`.

[55] AccessData Corp. Forensic Toolkit (FTK) (2020). Using Command Line Imager. `https://accessdata.com/product-download`.

[56] Guy Voncken. Guymager.net (2020). Guymager Free Forensic Imager. `http://guymager.sourceforge.net/`.

[57] 504ENSICS Labs (2020). 504ensicsLabs/LiME. `https://github.com/504ensicsLabs/LiME`.

[58] Pomeranz, H. (2020). halpomeranz/lmg. `https://github.com/halpomeranz/lmg`.

[59] tcpdump (2020). Tcpdump/Libpcap public repository. `https://www.tcpdump.org`.

[60] Wireshark Foundation. Wireshark.org (2020). Wireshark - Network Protocol Analyzer. `https://www.wireshark.org/`.

[61] Netresec (2020). NetworkMiner - The NSM and Network Forensics Analysis Tool. `https://www.netresec.com/?page=Networkminer`.

[62] The Tcpdump Group (2020). the-tcpdump-group/libpcap. `https://github.com/the-tcpdump-group/libpcap`.

[63] Al-Khateeb, H. and Cobley, P. (2015) (2015) How you can preserve digital evidence and why it is important. *A Practical Guide To Coping With Cyberstalking*, April, pp. 50–62. Andrews UK Limited, Luton, UK.

[64] Brian Carrier. Sleuthkit.org (2020). Autopsy - The Sleuth Kit. `http://www.sleuthkit.org/autopsy/`.

[65] volatilityfoundation (2020). The Volatility Foundation - Open Source Memory Forensics. `https://www.volatilityfoundation.org`.

[66] Forensics, R. (2020). Rekall Forensics. `http://www.rekall-forensic.com/`.

[67] CGSecurity. CGSecurity.org (2020). PhotoRec ES - CGSecurity. `http://www.cgsecurity.org/wiki/PhotoRec_ES`.

[68] United States Air Force Office of Special Investigations. Foremost.org (2020). Foremost - Recovery Tool. `http://foremost.sourceforge.net/`.

[69] Gianluca Costa & Andrea De Franceschi. Xplico.org (2020). Xplico - Open Source Network Forensic Analysis Tool (NFAT). `http://www.xplico.org/`.

[70] Zeek (2020). The Zeek Network Security Monitor. `https://zeek.org/`.

[71] Eric Zimmerman (2020). Kroll Artifact Parser and Extractor - KAPE. `https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape`.

[72] Joachim Metz. Github.com (2020). Log2timeline Supertimeline Tool. `https://github.com/log2timeline/plaso`.

[73] Phil Harvey (2020). ExifTool by Phil Harvey. Read, Write and Edit Meta Information. `https://www.sno.phy.queensu.ca/~phil/exiftool/`.

[74] Yassein, M. B., Mardini, W., and Almasri, T. (2018) Evaluation of Security Regarding Z-Wave Wireless Protocol. *4th International Conference on Engineering & MIS (ICEMIS 2018)*, Istanbul, Turkey, June 19 - 20. Association for Computing Machinery.

[75] Badenhop, C. W., Graham, S. R., Ramsey, B. W., Mullins, B. E., and Mailloux, L. O. (2017) The Z-Wave routing protocol and its security implications. *Computers & Security*, **68**, 112–129.

[76] Fouladi, B. and Ghanoun, S. (2013) Security Evaluation of the Z-Wave Wireless Protocol. *Blackhat USA*, Las Vegas, NV, USA, 27 July - 1 August. Neominds.

[77] Fan, X., Susan, F., Long, W, and Li, S. MIT Computer Science and Artificial Intelligence Laboratory. Security Analysis of Zigbee. (2017). https://courses.csail.mit.edu/6.857/2017/project/17.pdf.

[78] NCSCL Quality Manager. (2017) (2017) *Procedure for Evidence Management*. North Carolina State Crime Laboratory. North Carolina, USA.

[79] Du, X., Le-Khac, N., and Scanlon, M. (2017) Evaluation of digital forensic process models with respect to digital forensics as a service. *arXiv*, **1708**, 01730.

[80] Samsung Electronics America (2018). Samsung SmartThings Wifi ET-WV525 User Manual. http://www.libelium.com/downloads/documentation/meshlium_technical_guide.pdf.

[81] Samsung Electronics America (2020). Samsung SmartThings Multipurpose Sensor | Owner Information Support | Samsung US. https://www.samsung.com/us/support/owners/product/multipurpose-sensor-version-3/.

[82] Samsung Electronics America (2020). Samsung SmartThings Motion Sensor | Owner Information Support | Samsung US. https://www.samsung.com/us/support/owners/product/motion-sensor-version-3/.

[83] Samsung Electronics America (2020). Samsung SmartThings Moisture Sensor | Owner Information Support | Samsung US. https://www.samsung.com/us/support/owners/product/moisture-sensor-version-3/.

[84] Samsung Electronics America (2020). Samsung SmartThings Presence Sensor | Owner Information Support | Samsung US. https://www.samsung.com/us/support/owners/product/presence-sensor-version-2/.

[85] Samsung Electronics America (2020). Samsung SmartThings Cam | Owner Information Support | Samsung US. https://www.samsung.com/us/support/owners/product/smartthings-cam/.

[86] Samsung Electronics America (2020). SmartThings Wifi Smart Plug SmartThings - GP-WOU019BBAWU | Samsung US. https://www.samsung.com/us/smart-home/smartthings/outlets/smartthings-wifi-smart-plug-gp-wou019bbawu/.

[87] Samsung Electronics America (2020). SmartThings Smart Bulb - GP-LBU019BBAWU | Samsung US. https://www.samsung.com/us/support/owners/product/GP-LBU019BBAWU.

[88] iFixit (2018). Samsung Connect Home Teardown. https://www.ifixit.com/Teardown/Samsung+Connect+Home+Teardown/104807.

[89] Libelium Comunicaciones Distribuidas (2020). Libelium Smart Agriculture IoT Vertical Kit Guide. http://www.libelium.com/downloads/quick-start-guides/quick_start_guide_agriculture_vertical_kit.pdf.

[90] Libelium Comunicaciones Distribuidas (2020). Meshlium Xtreme Technical Guide. http://www.libelium.com/downloads/documentation/meshlium_technical_guide.pdf.

[91] Libelium Comunicaciones Distribuidas (2020). Waspmote Plug & Sense! Technical Guide. http://www.libelium.com/downloads/documentation/waspmote_plug_and_sense_technical_guide.pdf.

[92] Amazon Web Services, I. (2020). AWS IoT - Amazon Web Services. https://aws.amazon.com/iot/.

[93] Libelium Comunicaciones Distribuidas (2020). Waspmote Plug & Sense! Sensor Guide. http://www.libelium.com/downloads/documentation/waspmote_plug_and_sense_sensors_guide.pdf.

[94] Grand View Research. Consumer iot market size, share & trends analysis report forecasts, 2023 - 2030. https://www.grandviewresearch.com/industry-analysis/consumer-iot-market-report.

[95] Josh Howarth. Exploding Topics (2022). IoT Statistics (2023-2030). https://explodingtopics.com/blog/iot-stats.