Evidence Gathering in IoT Criminal Investigation

François Bouchaud[1(✉)], Thomas Vantroys[2], and Gilles Grimaud[2]

[1] IRCGN - Forensic Science Laboratory Gendarmerie Nationale, Cergy, France
francois.bouchaud@gendarmerie.interieur.gouv.fr
[2] Univ. Lille, CNRS, Centrale Lille, UMR 9189 - CRIStAL, 59000 Lille, France
{thomas.vantroys,gilles.grimaud}@univ-lille.fr

Abstract. The Internet of Things (IoT) is a new paradigm. It enables communication between physical "things" through a common and distributed architecture. It is based on objects deeply rooted in the intimate lives of users. The devices are constantly scanning and interacting with this physical world. They bear witness to past events and are therefore a rich source of information for criminal investigations. The collection of evidence from the connected infrastructure is a decisive phase of the success of the police investigation. It is about removing objects from their initial environment and placing them in a controlled and secured area. This action allows the evidence to be preserved for later examination. It is crucial, but nevertheless difficult. It can alter or destroy valuable data during manipulation. Moreover, the difficulty lies in the heterogeneous nature of the devices and their strong dependence on the environment. This paper focuses on the collection of IoT devices at the local level, linked to an investigative strategy. It presents several tools and methods to retrieve the objects and proposes to evaluate its relevance in a use case.

Keywords: Internet of Things · IoT Investigations · Collection and sealing

1 Introduction

In the Internet of Things (IoT) markets, new devices and services are being created to make our lives easier and more connected. Manufacturers and service providers are offering their customers a wide range of offers and options. This IoT infrastructure organizes communication between physical "things" through a common and distributed network [9]. It opens up to the Internet. Technically, these connected objects are exploited by several operating systems and connect to various network technologies at the same time. To communicate, some solutions require specific gateways. These characteristics of heterogeneity, interactivity and dynamism make the architecture more complex than a conventional sensor network. However, it creates value in the services and exchanged data.

S. Goel et al. (Eds.): ICDF2C 2020, LNICST 351, pp. 44–61, 2021.
https://doi.org/10.1007/978-3-030-68734-2_3

From a forensic point of view, this development affects the investigation procedure and these technical acts. Digital forensics (DF) has become an important science for tracking malicious or undesirable activities and finding perpetrators. It is the discipline of identifying, acquiring, analyzing and searching for evidence from a digital source [18]. It aims to introduce cohesion and consistency into the vast field of extracting and examining traces from a crime scene. The search for truth is conducted in such a way that the original incriminating traces are not compromised. Dedicated tools, hardware or software, are available to assist the investigator. However, due to the many dependencies between objects and data management policies, the collection and the analysis of this ecosystem challenges the investigator. Collecting evidence from a connected infrastructure is a decisive phase in the success of a police investigation. It involves removing objects from their original environment and placing them in a controlled and secured area. This action is crucial and difficult. It can alter or destroy valuable data.

This article proposes a collection framework to take into account a criminal scene with IoT devices. Contrary to the study of computers and telephones, connected objects refer to a notion of iteration of selection. Moreover, heterogeneous devices make up the crime scene, having strong dependencies on the environment.

Section 2 of this article highlights the need to collect a connected object and data from its communication infrastructure; Sect. 3 covers previous work in the field of digital forensic collection; Sect. 4 describes the collection framework for the IoT environment; Sect. 5 tests them in a use case; Sect. 6 presents the operational impact factor; Sect. 7 presents the conclusion of the article and the next step of this research.

2 The Need for a Forensic Data Collection Framework

This section defines the collection requirements of a connected object and associated data in the context of the criminal investigation. In addition, it presents encountered difficulties.

2.1 Connected Objects as Evidence Receptacles

The Internet of Things is a complex whole. Its visible and physical part is a local ecosystem defined by the objects, gateways and mobile terminals of connected users. Thus, the concept of "local" is linked to the location and environment of the people involved in the incident. Connected object are "small" object integrating sensors or actuators, with processing logic by a microcontroller. It is generally self-sufficient in energy, powered by a battery. It can include several physical interfaces such as connectors, sockets and buttons, but also wireless communication modules. It collects local data and transmits it to a cloud computing service over the network. Similarly, it receives commands from a management server and returns operational reports. Gateways and user terminals are more conventional in their operation and architecture, acting as an interface between

systems or externally. Their operating systems offer a significant abstraction between the software and the hardware on which it runs.

From a forensic perspective, each module of the infrastructure contains usable data. In Oriwoh et al. [20], the authors list potential sources of evidence on the architecture of the Internet of Things. The search for traces is triggered by criminal activity or by the normal operation of devices. It represents a phenomenon or event in a given context. On the basis of this information, the justice system seeks to determine the causes and circumstances of the incident. Digital forensic procedures recommended by the National Institute of Standards and Technology (NIST) are internationally accepted [15]. It is an "application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data". These four successive steps are applicable in the IoT environment. Traces must therefore be collected with care and rigor. This technical operation is carried out by taking into account the needs of the investigation in the search for the truth.

This technical operation is a critical phase, especially in the context of a connected environment. Indeed, the collection is constrained by the technical characteristics of this heterogeneous and distributed environment.

2.2 Problem

Evidence gathering is a challenge for the community of digital forensics. Several scientific works list the difficulties inherent in this subject. In Zareen et al. [27], the authors describe them according to three characteristics: architecture, technology and applications. In particular, this article highlights the difficulty of acquiring data due to the heterogeneity of objects. For example, smart devices have a variety of different operating systems [13]. This element has an impact on collection, particularly in the development of a universal approach. According to Miorandi et al. [17], the evidence extraction process may also be more complicated than traditional computing. This is due to the data formats, protocols and involved physical interfaces. Many dependencies between objects complicate the collection. A change in the environment can lead to the writing of logs or the loss of information [23].

Digital evidence is inherently fragile. It can be altered, damaged or destroyed by improper handling or examination [22]. In addition, it is not easily copied and stored in its original state [4]. There is a risk of a remote shutdown of devices or overwriting of evidence. Care must therefore be taken to document and adapt the collection method to the encountered constraints. These operations must be carried out according to the physical characteristics of the object to be studied and the sought data. Faced with this observation, a question arises. What protection measures must be taken to guarantee the non-alteration and optimal conservation of the stored data ? The challenge is to transfer a connected object from its natural environment to a new controlled containment zone without damaging the container and contents.

The scientific community proposes various solutions to take into account the environment and exploit the data.

3 Previous Work

In this section, we present a state of the art of forensic collection of connected objects. We explore the operational limitations of these approaches.

3.1 Literature Review

The process of collecting objects is irreversible because they are removed from the environment. It requires the establishment of controlled sampling protocols [10,11]. Analytical quality assurance from the crime scene to the laboratory must be implemented [8]. It is no longer based solely on legal considerations. For example, work must be done on sealing, traceability of operations and continuity of evidence.

Several strategies have been developed by the scientific community to collect data in a connected environment. Some work proposes interfacing with existing infrastructure. In Zawoad et al. [28], the authors describe the Forensics Aware IoT (FAIoT) model. It is a kind of central repository of reliable evidence. From a specific Programmable Logic Controller (PLC), investigators access data on IoT platforms. This approach requires collaboration between private companies and the police to implement this access. There is an inherent bias in data processing. Only locally synchronized data is accessible. In Copos et al. [7], the authors collect traffic data from the intelligent home network. This solution requires a good knowledge of the network and its accessibility.

In Oriwoh et al. [19] and Perumal et al. [21], the authors present an approach to take the whole environment into account. It is divided into three study areas: the local environment composed of objects and gateways, the Internet with IoT platforms and the service interface for customers (Fig. 1). This approach is relevant in the forensic context. It structures the analysis process on the basis of existing solutions.

Indeed, data collection in the cloud consists of requisitions from operators. The client interface includes the application environment and web portals. It is processed using digital forensic tools. However, device located in zone 3 (gateway) can also play a role in local environment (zone 1), such as mobile phones. It acts as a gateway across a shared network. It also serves as an interface for service consumers. The local area network is often seen as a black box of heterogeneous devices. It is unique in its configuration, topology and the objects that make it up.

3.2 Specific Constraints

Often, devices cannot be turned off to preserve hours of modified, created and accessible data, as suggested in [19]. There are two working hypotheses. The first

is to acquire the data directly. This is called live forensic acquisition [1,14,25,26]. This approach applies only to known devices. It requires privileged access to the target system. In the second case, it is not possible to retrieve the information without tampering with the system. It is necessary to maintain the device in the found state for further processing. This problem is dealt with before the device is sealed. However, the device can be turned off when the lost data is of no interest or affects the rest of the investigation.

Sometimes data is scattered across several devices on the same network. It is also stored on external services [2]. This note refers to dependencies between devices. Thus, it is necessary for the investigator to master the topology of the network and its sub-networks. An analysis phase should include the study of the path taken by the data. This work allows understanding their coherence with the system. The collection phase is developed in one reading per branch to maintain the dependencies.

Another challenge is the legal limits of the investigation. Some of the most legal aspects are listed by Ruan et al. [24] and Oriwoh et al. [19]. Data travels between multiple devices or services in the cloud. It is often difficult to find the data when it is on servers in a third country. This is made impossible in the absence of agreement between countries.

In response to these constraints, we propose a framework to facilitate the retrieval and storage of data from a crime scene.

4 Collection Framework and Tools

In this section, we present the framework for data collection. This phase can be broken down into several actions. First, we take charge of the crime scene by isolating different networks. We study the roles and dependencies between objects. Then we collect and extract them, according to network topologies. Finally, we package them. This approach is defined according to the operational constraints and the implementation strategy.

4.1 Crime Scene Data Collection

In this subsection, we study the process of handling connected objects at a crime scene. It is defined according to the dependencies between objects and their technical characteristics. Beforehand, we assume that the IoT environment is divided into three study areas: local (1), online (2) and service interface (3) (Fig. 1). Thus, in the collection phase, we focus on zones 1 and 3. Only data from these zones are directly accessible to investigators. Access to the data on the online platform (2) therefore requires the intervention of a third party by requisition.

Global Approach. This methodology focuses on the examination of the crime scene as a whole. It consists of three successive steps. The first is the identification of local equipment in order to obtain a mapping of the connected environment.

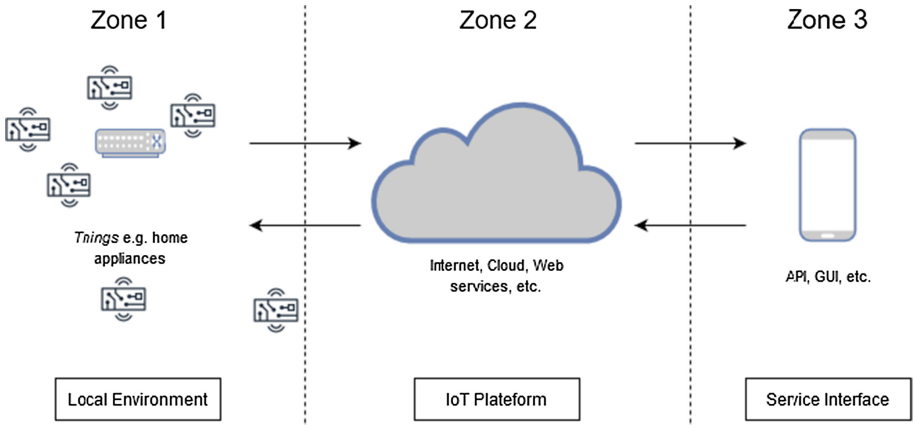

Fig. 1. Zones of Digital Forensics derived from Oriwoh et al. [19]

The second is to determine the technical characteristics of the equipment and its normal operation. The third step is to isolate the networks in order to limit interactions, data leaks and to facilitate data extraction (Fig. 2).

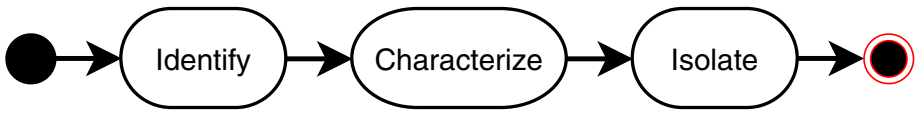

Fig. 2. Crime scene examination methodology

First, we are looking for different equipments. Then we determine their role in the infrastructure: connected objects or gateways. There are two categories of connected objects. The first one includes devices that communicate directly with the outside world. The second contains objects that depend on a third party to communicate. In addition, there are several types of gateways. This distribution is defined according to the provided services. The first group provides access to the Internet or to external networks in zone 2. The second provides the link between IoT-specific protocols and other classical protocols. They constitute network nodes of zone 1. Hybrid solutions are also present. This articulation is deduced from the study of communications, protocols and families of devices. Objects based on short-range networks (Bluetooth, ZigBee, Wi-Fi, etc.) communicate with the external network using a local gateway. Objects based on long-range networks (SigFox, LoRa, etc.) use an external public gateway managed by private operators. On the basis of this information, we draw up a map of the various networks. We obtain the local environment tree with its different branches. The branches symbolize communications. The base of the trunk is the main gateway to the Internet. The specific gateways for the different protocols

are the nodes. The leaves are the connected objects. This tree structure is used to determine the dependencies between the devices.

Second, we identify and classify local equipment according to technical characteristics related to the type of memory (volatile or static) and network dependencies. We want to understand how data is synchronized over the network and the normal operation of the objects. Synchronization can be automatic, semi-automatic or manual. The type of exchanged data, the data management policy and their position in the infrastructure are also important elements in understanding the environment. The identification of objects and their synchronization modes are based on a reference database. It is informed on the basis of feedback from surveys and knowledge of the devices.

Third, we seek to disaggregate and isolate parts of the local environment. This approach is developed from the general to the specific. Local infrastructure must be isolated from the outside world. We break the links between the different areas (1, 2 and 3). The mapping of the infrastructure gives the points of interaction with zone 2. Concretely, the investigator physically disconnects the wired Ethernet communication. He removes the SIM cards or scrambles communications. Interference is a time-limited measure. It is only applied when there is no other way to interrupt the communication. Then we take care of the different networks of the local environment identified during the mapping. The network standards used in IoT today can be classified into three basic network topologies: point-to-point, mesh and star (Fig. 3). The Mesh network can be hierarchical or not. These characteristics have an impact on the collection of equipment and its data.

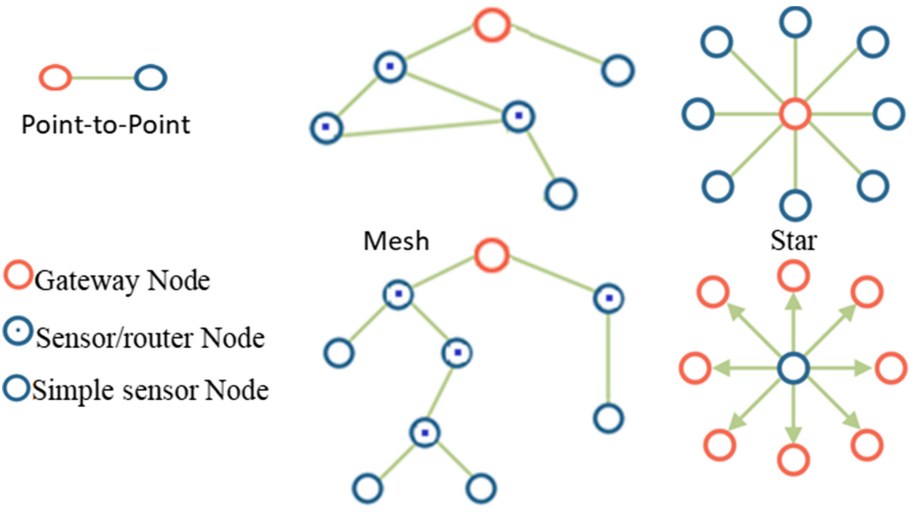

Fig. 3. Network technologies appropriate for the Internet of Things

The point-to-point network establishes a direct connection between the connected object and its gateway. The object accesses the Internet or another network via the gateway. An example of this type of network is a Bluetooth connection between a mobile phone and a connected watch. By breaking the radio link, the gateway and the object are isolated from the network.

The star network consists of a central node to which all other nodes in the network are connected. This hub serves as a common connection point for all other nodes. All the peripheral nodes can therefore communicate with each other via the hub only. An example of this topology is a Wi-Fi network in a house. The hub is the link to the outside world. This architecture makes it easy to add or remove nodes without impacting the network. All the intelligence of the network is concentrated on a single node. This concentric approach facilitates network management. Thus, peripheral nodes can be removed and isolated of the networks one by one. By directly removing the central node, the objects lose connectivity. The network is cut off from the world. However, it can still exchange and store data internally. This network topology is notably developed with the SigFox and LoRa protocols. The object interacts with several gateways. In this case, the recommended solution is to isolate the object from the network.

A mesh network consists of a gateway and connected objects, some of which have routing capabilities. Thus, one object is connected to one or more other objects, acting as nodes in the same network. The gateway allows data to reach the outside world. Thanks to this mesh, the data is potentially relayed by several nodes before reaching its destination. This concept is called a route. Over time, the nodes establish new routes based on their operating states and the physical characteristics of the medium. In some cases, this architecture is hierarchical. The parent node is the master of the network, called the "cluster tree". This structuring is used in home automation according to a relay construction. It compensates for distance issues or noise and obstacles. For example, the Enedis intelligent link network is built on this model [6]. For a hierarchical mesh network, by disconnecting the routers, the connected objects are isolated from the network. However, this operation must start from the ends of the branches to the core of the network. For a classic mesh network, we look for different closed and open loops that make up the network. We isolate the two types of loops. This gives us sub-networks. The open loops are treated according to a hierarchical approach. Closed loops are considered as a connected whole.

The study of the network topology gives a first reading of the collection methodology. Depending on the protocols in place, different containment measures are established. They must take into account dependencies.

Special Case of Targeted Research. Targeted research is a special case of the comprehensive crime scene approach. It is carried out during the examination of a specific object. The aim is to promote efficiency. Thus, this approach includes all the steps described above. However, it focuses on the direct environment of the target object and its dependencies.

A mapping of the network is carried out. It gives an overall view of the environment and the connected present objects. Based on this information, the investigator has the dependency tree between the devices. Instead of studying all the branches, he targets the network he is interested in. He studies the characteristics of the target object and the attached devices. He extracts all these devices from the same branch, with regard to interactions and dependencies. It ignores other devices that interact with the target object.

After reviewing the process of supporting the connected objects in the local infrastructure, we are interested in extracting them from the environment and packaging them. We discuss the sealing of IoT devices and the preservation of the stored data.

4.2 The Sealing

In this section, we develop the concept of sealing and the preparatory acts for proper packaging. The seizure and imposition of legal seals are an act of judicial police. It consists of placing an object or a document at the disposal of justice to be used in the manifestation of the truth. Seizures are carried out following the spontaneous surrender of an object or following a judicial search. Like physical objects, digital data stored in memory media are subject to seizure. The investigator seals either the physical medium containing the data or a copy of the data. Prior to collection, steps are taken at the time of collection to preserve biological traces such as DNA or fingerprints.

The seal must guarantee the integrity of the data present in the device. It protects the content from any physical or digital interaction with the outside. For digital evidence, it protects the content from exposure to electromagnetic fields. Thus, it must be made according to the characteristics and the condition of the object. If the medium cannot be deactivated or must remain activated, the object is packaged in a Faraday cage. As soon as possible, it is permanently powered by an external battery. This action increases the life of the object. The operating time must be estimated according to the capacity of the power supply. This information must be prominently displayed on the seal. If the holder can be deactivated, the object is conditioned in such a way that it cannot be reactivated. The seal must comply with the provisions set out in the Treatises on Digital Forensics [5,12,16].

4.3 Process to Follow

The crime scene consists of connected objects and gateways with more or less dependencies. Figure 4 resumes the different operations. After checking their operating status (on or off), the switched-off device is placed directly under seal. In addition, the device switched on without dependencies is disconnected and isolated from the network.

If it has no internal memory, it is placed in a seal in the switched-off state. Indeed, in a second step, the object identifiers can be used in requisitions from operators. If it has a memory, it is processed in the field or in the laboratory. The

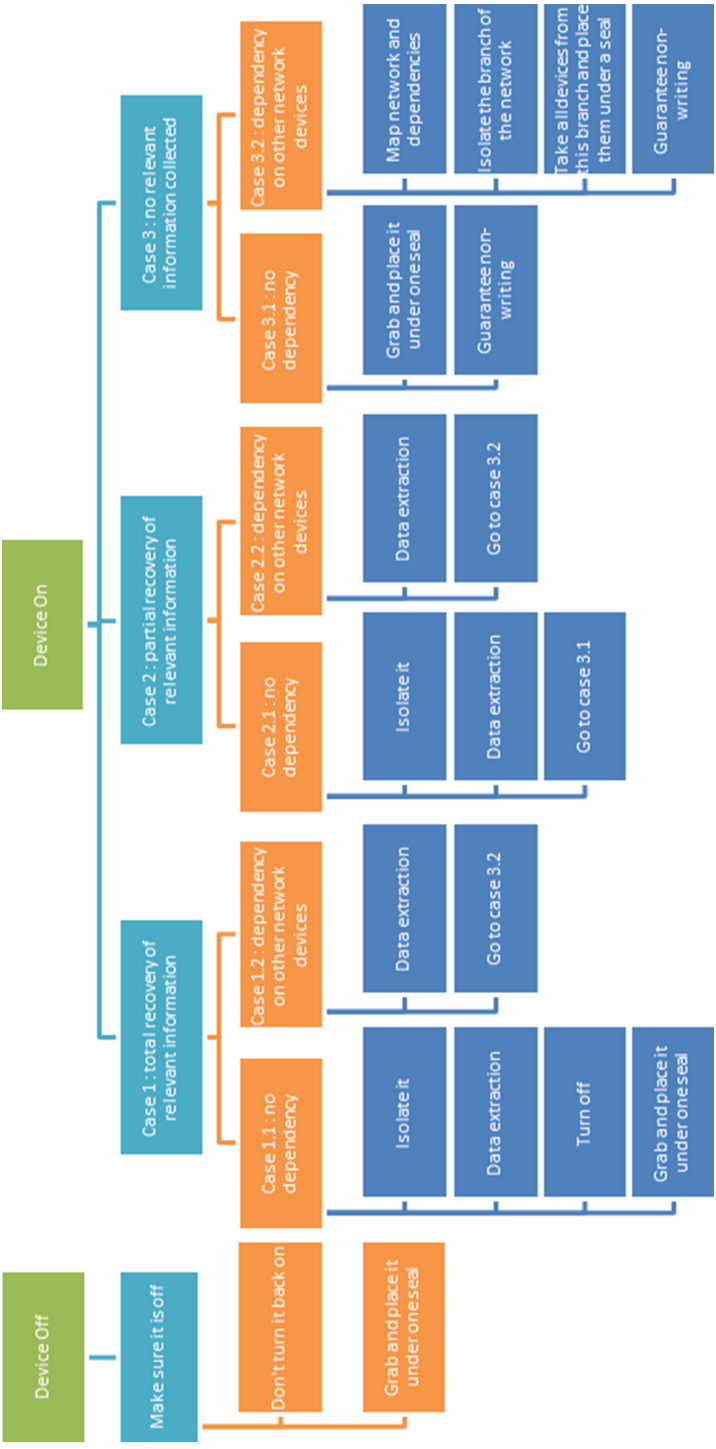

Fig. 4. Collection framework for IoT devices

data retrieval is carried out according to the available tools. For example, many gateways have open communication ports. The extraction is performed according to the availability of services such as with Telnet or a programmable logic controller (PLC). It is therefore performed locally or on the network depending on the scenario or the required data. Nevertheless, local acquisition is always preferred. In addition, some connected objects contain external storage media. A study of the connected watch market highlights the presence of storage and SIM cards in one third of the products. Conventional forensic acquisition methods are applicable to this type of electronic medium. Verification of the extracted data is necessary to establish their integrity for legal purposes. A comparison of the hashes of the original data source and the acquired data is performed. However, this verification is not performed in the case of direct acquisition [3,15]. This action changes the source. Depending on the collected data, the device is turned off or left on.

When it is not possible to extract all the data relevant to the investigation, it is placed in a state as close as possible to its input state. Each device shall be placed in a unique seal. Objects containing dependencies shall be considered as a whole. The treatment is different when the investigator puts them under seal. To limit entry, they should be placed in a common seal. However, an impact study must be carried out beforehand.

Thus, the dependencies between objects and the accessibility of the data with forensic tools motivate the choice of a field acquisition method.

5 Evaluation of Forensic Tools in an Investigative Exercise

This section assesses the collection methodology presented in the previous session on a survey exercise. We conduct an operational impact study.

5.1 Presentation of the Scenario

On April 10, 2018 at 8 a.m., the police is alerted by a neighbor of a burglary in an apartment. The police intervened quickly at the scene of the crime. A patrol arrives at 8:15 am. It discovers that the front door of the apartment is forced. The place also shows many traces of struggle and violence. Objects are broken on the floor. A dead person is found lying on a bed in room 2. The investigators therefore implement the first protective measures by freezing the crime scene. A forensic team, including a digital specialist, takes charge of the crime scene at 9:00 am.

5.2 Presentation of the Environment

The apartment is $45\,\mathrm{m}^2$ ($5\,\mathrm{m} \times 9\,\mathrm{m}$). It consists of three separate rooms: an entrance (room 1), a bedroom (room 2) and a living room (room 3). It contains many connected objects (Fig. 5). It is equipped with a home automation

system from an Orvibo kit. It contains two opening sensors (1 and 2) and a motion sensor (3) coupled with a Wi-Fi camera (4). This kit is located in room 1 and controls two external openings. It communicates with the ZigBee protocol via a dedicated hub (5). It is located in room 3. The home automation system also consists of a Philips light bulb (6 and 7) connected to its hub (8). They are located in rooms 2 and 3 of the apartment. Otherwise, four Sen.se Cookies are hidden in different rooms. They turn household objects into connected objects. In our case, the Cookies monitor the water supply level of the coffee machine (9), the room temperature (10), the position of the bicycle (11) and the physical activity of the victim (12). All these objects are connected with a proprietary protocol to the Sen.se Mother (13). It is located in room 3. These different gateways, the Amazon Echo (14), the RaspberryPi0 (15) and the M136W IP camera (16) are connected to the Internet via WinkHub 2 (17).

The victim is on the bed in room 2. She has an Apple Watch 3 (18) on her right arm and an iPhone SE (19) in her pocket. Hidden in the bed is a sleep sensor called the Terraillon Dot (20). Other items in the apartment include a Sens'it (21), a Heroz bracelet (22) and a Nokia scale (23).

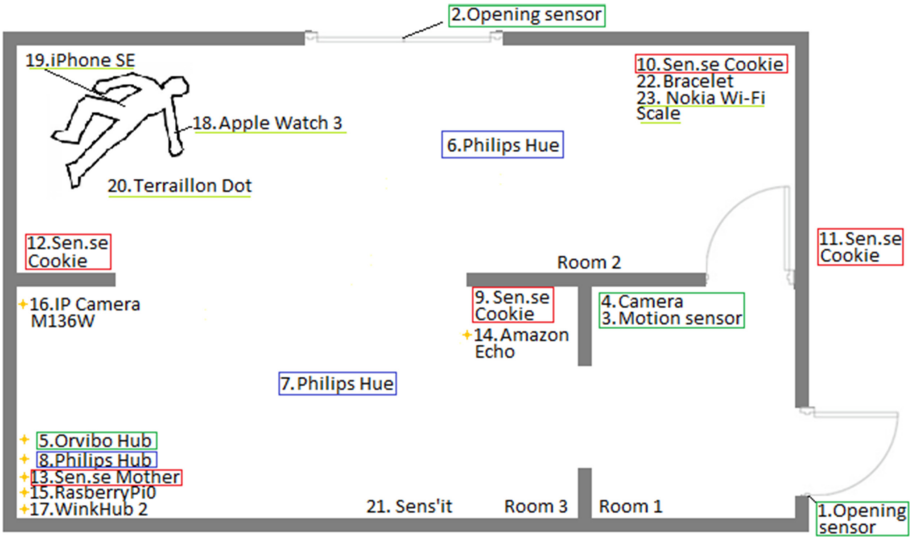

Fig. 5. Home layout with the IoT devices

5.3 Application of the Collection Methodology

Analysis of Local Network. The local infrastructure consists of four networks connected to the Internet (Fig. 6). Each network is treated independently.

The first network contains three connected objects: an Apple Watch 3, a Terraillon Dot and a Nokia scale. The smartwatch and the sleep analyzer are

connected to the phone via Bluetooth. The scale uses Wi-Fi or Bluetooth protocol to communicate. The iPhone SE acts as a gateway. It provides Internet access to the connected objects.

By disconnecting the Global System for Mobile (GSM) communications, 4G and Wi-Fi networks from the smartphone, the device group is isolated from the outside environment. Thus, the SIM card is removed as a precautionary measure. The phone is placed in airplane mode.

The second network contains three connected objects: a M136W IP camera, an Amazon Echo and a Rasberry Pi0. It integrates three independent environments: Orvibo, Sen.se and Philips. The WinkHub 2 gateway provides Internet access to different connected objects and environments. It can be seen that a link between the first and second network is broken when the Wi-Fi connection of the iPhone is cut. By disconnecting the Ethernet cable from the WinkHub 2, the second network is isolated from the outside world.

The third and fourth networks are only made up of independent and connected local objects: Heroz and Sens'it. Heroz communicates via Bluetooth. However, in our case it is not connected to any gateway. Sens'it uses the SigFox protocol to communicate. It exchanges directly with the outside world through external gateways.

This first manipulation gives us four independent networks disconnected from the Internet. By breaking the links, we limit a migration of information to external platforms. We also avoid possible interactions between these networks.

Device Characterization. Studying the normal functioning of objects and their gateways helps us to determine the environments containing useful data and their locations. We rely on a technical database of the equipment, which is filled by the investigators. We also study the dependencies between objects.

Some connected objects use automatic synchronization of their data with the network. Thus, they store locally little useful information related to the survey. This is the case of the objects making up the Philips and Sen.se networks. However, the relevant data are contained in the gateways. They are linked to network activity and system configurations. Some objects are more versatile in their operation. This is the case with the objects of the first network and the Orvibo infrastructure. Thus, each object must be treated individually. In the first network, the data from the Apple Watch 3 and the Nokia scale are automatically synchronized with the iPhone SE. For the Terraillon Dot, a manual synchronization action must be performed by the user application. Note that the local data are also present in their internal memory.

Therefore, these different objects must be processed individually. The smartphone concentrates a lot of relevant information by acting as a gateway (zone 1) and a user interface via applications (zone 3). For the Orvibo network, all objects synchronize automatically. However, they do not have the same data management policy. The motion and opening sensors do not contain any useful data in memory. The Orvibo camera contains external storage in the form of an

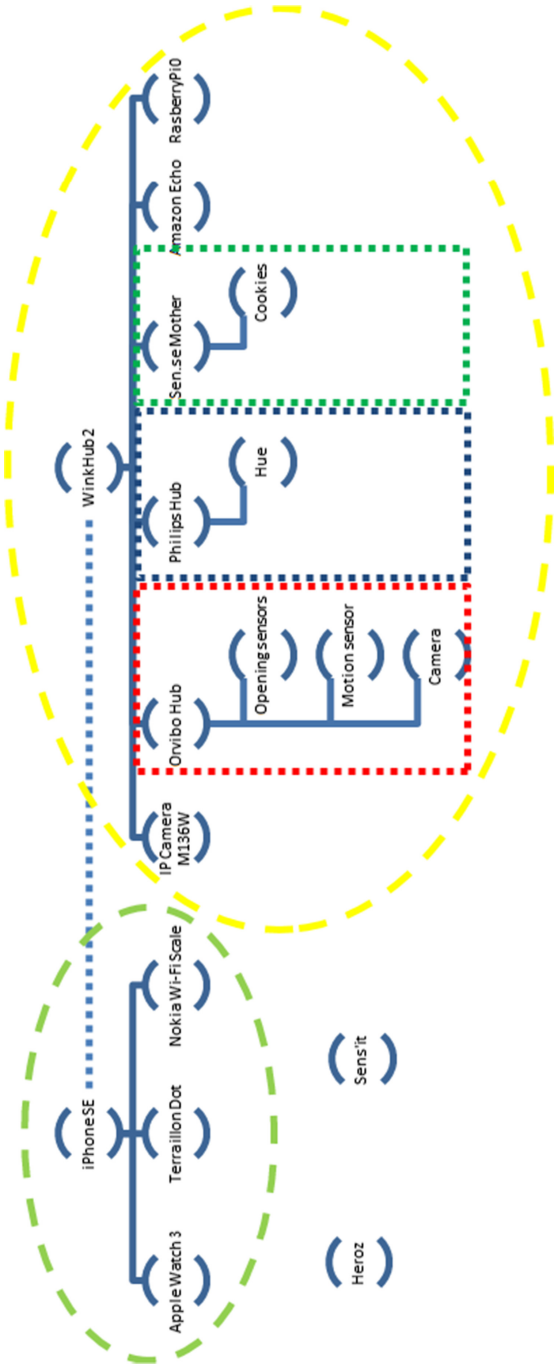

Fig. 6. Global mapping of the IoT environment

SD card. It acts as a buffer in case the network is lost. The gateways contain data about network activity and system configurations.

The other six devices in networks 2, 3 and 4 are processed independently. Heroz, Sens'it and the M136W IP camera synchronize automatically with the network. They do not contain any relevant data in our case. Amazon Echo, RasberryPi0 and WinkHub 2 synchronize some data with the network. They keep the relevant information locally. They must therefore be processed individually.

Analysis of Network Topology, Grab and Seal. Network 1 is structured in a point-to-point relationship. Each object is independent. Thus, connected objects can be isolated individually by disabling the Wi-Fi and Bluetooth connection on the smartphone. We are not able to perform data extraction from the Nokia scale and Terraillon Dot outside the laboratory. In fact, we need specific extraction equipment. The scale and the sleep analyzers are switched off by removing their internal batteries. We perform data extraction from the AppleWatch 3 and iPhone SE with our standard forensic tools. These devices are turned off. All objects in Network 1 are independently sealed for laboratory analysis.

Network 2 consists of a main network and peripheral networks. The main network is a hierarchical mesh network. The three independent edge networks are star networks: Orvibo, Philips and Sen.se. Thus, we start at the end of the branches and move towards the trunk of the network. The Orvibo and Philips objects communicate via ZigBee with their gateways. Sen.se is based on a proprietary protocol. The gateways play a hybrid role as an interface between networks and protocols. In a first step, we cut the link between the main gateway and each environment. Then all objects are disconnected from its gateway. This is also done with the M136W IP camera, the Amazon Echo and the RasberryPi0. We are not able to extract data from connected Philips, Orvibo and Sens'it objects and the Amazon Echo outside the laboratory. In fact, we need specific equipment for a chip off and reading storage memories. We perform data extraction from the Philips, Orvibo and Sens'it hubs. Indeed, the extraction of the Philips hub is done from the PLC and for Orvibo from Telnet. The M136W IP camera does not have any data relevant to the investigation. The SD cards of the Orvibo camera and the RasberryPi0 are also recovered. These devices are turned off by removing their internal batteries or power supply. All objects in network 2 are independently sealed for laboratory analysis.

Network 3 is already isolated from any grid. It can be managed as an offline object. Network 4 is structured according to a star topology. It communicates with external gateways. It must be isolated from the network by being placed in a Faraday cage.

Some devices are not collected in accordance with the investigation strategy. However, it is necessary to know their roles and identifiers, such as the Federal Communications Commission Identification (FCCID) number. This information may be used for analysis or for requests from IoT platform operators.

6 Operational Impact Factor

Several operations are carried out successively to collect devices and data: breaking network links to isolate the local infrastructure from the Internet, removing external cards, extracting data, changing the status of the devices and sealing them. Each action generates or deletes data. This section looks at the impact of these different operations.

Connected objects depend on a local infrastructure. They form a connected whole. Thus, a change in the infrastructure can cause logs to be written to the systems. By breaking the physical or radio links, the impact on writing is limited. It results from a loss of the network. However, we limit the leakage of stored information from the secondary network to the primary network. The study of the Sen'se gateways, Philips and Orvibo, did not reveal any writing in the logs once disconnected. However, an event is created when we disconnect the Amazon Echo in the directory: */system/dropbox/*. These manipulations must therefore be traced in the legal proceedings.

Data extraction can generate traces and loss of information. Direct acquisition leaves a write in the RAM. It modifies a potential source of information. Moreover, the result of a live forensic acquisition is neither repeatable nor reproducible. The only method of acquiring memory without alternation is Crash Dump. Unfortunately, it cannot be activated manually. The acquisition of internal memory during runtime also leads to a more or less significant alteration of the medium. Some methods cause the system to boot or to change to raise privileges or to exploit a security flaw. In order to control the impact of these solutions, operations can be performed in controlled laboratory environments.

A clean shutdown of the operating system necessarily generates a rewriting in the system. It is linked to the recording of application data in the RAM. Conversely, a hard shutdown consists of cutting off the power supply. It protects the memory of new entries. Implementing a system shutdown can result in: writing to event logs, deleting temporary files, purging caches, and system corruption. It may be accompanied by the execution of a script or application leading to the erasure or encryption of data. If the machine has a human-machine interface, we must record the date and time of the machine, the network to which it is connected and the applications running in the background. This operation must be carried out before switching off and sealing the object.

In some cases, the object cannot be deactivated or stopped. Thus, it continues to live and to write data into memory. The risk is that the data may be rewritten on important elements of the investigation after it has been sealed. This is especially the case with an active GPS watch, such as the Apple Watch 3, so it is more interesting to limit its operation. Thus, the investigator may have to stop the applications to freeze the state of the object. This technical act is comparable to putting a mobile phone in airplane mode. These technical operations must be retraced in its procedure. However, keeping objects connected with the seal alive also pose power supply problems. The device must be powered continuously to maintain the volatility of the data in memory.

Thus, any manipulation must be the subject of a note mentioning the act performed and its timestamp.

7 Conclusion

Introducing the Internet of Things (IoT) into the society provides more opportunities for forensic investigations. Connected objects are the actors and direct witnesses of events. However, the objects are heterogeneous and interconnected to the network. Their manipulation generates or alters the contained data. Faced with these results, the investigators must define a methodology to apprehend them. In this article, we present a collection framework. We study the alteration and the impact of the various actions carried out.

The next step in this research is to extract and analyze them. The challenge is to understand the interaction between connected objects and contextualized data in order to respond to a court.

References

1. Adelstein, F.: Live forensics: diagnosing your system without killing it first. Commun. ACM **49**(2), 63–66 (2006)
2. Attwood, A., Merabti, M., Fergus, P., Abuelmaatti, O.: SCCIR: smart cities critical infrastructure response framework. In: 2011 Developments in E-systems Engineering, pp. 460–464. IEEE (2011)
3. Brezinski, D., Killalea, T.: Guidelines for evidence collection and archiving. Network Working Group (1), February 2002. http://www.ietf.org/rfc/rfc3227.txt
4. Carrier, B., Spafford, E.: Getting physical with the digital investigation process. Int. J. Digit. Evid. **2**(2), 1–20 (2003)
5. Casey, E.: Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic press, Cambridge (2011)
6. Chauvenet, C., Etheve, G., Sedjai, M., Sharma, M.: G3-PLC based IoT sensor networks for SmartGrid. In: 2017 IEEE International Symposium on Power Line Communications and its Applications (ISPLC), pp. 1–6. IEEE (2017)
7. Copos, B., Levitt, K., Bishop, M., Rowe, J.: Is anybody home? inferring activity from smart home network traffic. In: 2016 IEEE Security and Privacy Workshops (SPW), pp. 245–251, May 2016. https://doi.org/10.1109/SPW.2016.48
8. Crispino, F.: Computerized forensic assistance software (FAS 1.0) for training and standardized investigation in distributed and disconnected services. Forensic Sci. Int. **132**(2), 125–129 (2003)
9. Dorsemaine, B., Gaulier, J., Wary, J., Kheir, N., Urien, P.: Internet of Things: a definition & taxonomy. In: Al-Begain, K., AlBeiruti, N. (eds.) 9th International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST 2015, Cambridge, United Kingdom, 9–11 September 2015, pp. 72–77. IEEE (2015). https://doi.org/10.1109/NGMAST.2015.71
10. Dovaston, D.: The police perspective. Sci. Justice **40**(2)(1), 150–151 (2000)
11. Gallop, A.: Private practice public duty. Sci. Justice **40**(2)(1), 104–108 (2000)
12. Granja, F.M., Rafael, G.D.R.: The preservation of digital evidence and its admissibility in the court. Int. J. Electron. Secur. Digit. Forensics **9**(1), 1–18 (2017)

13. Hahm, O., Baccelli, E., Petersen, H., Tsiftes, N.: Operating systems for low-end devices in the internet of things: a survey. IEEE Internet Things J. **3**(5), 720–734 (2016)
14. Inoue, H., Adelstein, F., Joyce, R.: Visualization in testing a volatile memory forensic tool. Digital Invest. **8**, S42–S51 (2011)
15. Kent, K., Chevalier, S., Grance, T., Dang, H.: Guide to integrating forensic techniques into incident response. NIST Spec. Publ. **10**(14), 800–86 (2006)
16. Kornblum, J.: Preservation of fragile digital evidence by first responders. In: Digital Forensics Research Workshop (DFRWS), pp. 1–11 (2002)
17. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of Things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
18. Nelson, B., Phillips, A., Steuart, C.: Guide to Computer Forensics and Investigations. Cengage Learning, Boston (2014)
19. Oriwoh, E., Jazani, D., Epiphaniou, G., Sant, P.: Internet of Things forensics: challenges and approaches. In: 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 608–615, October 2013. https://doi.org/10.4108/icst.collaboratecom.2013.254159
20. Oriwoh, E., Sant, P.: The forensics edge management system: a concept and design. In: 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, pp. 544–550. IEEE (2013)
21. Perumal, S., Norwawi, N., Raman, V.: Internet of Things (IoT) digital forensic investigation model: top-down forensic approach methodology. In: 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), pp. 19–23, October 2015. https://doi.org/10.1109/ICDIPC.2015.7323000
22. Pichan, A., Lazarescu, M., Soh, S.: Cloud forensics: technical challenges, solutions and comparative analysis. Digital Invest. **13**, 38–57 (2015)
23. Qin, Y., Sheng, Q., Falkner, N., Dustdar, S., Wang, H., Vasilakos, A.: When things matter: a survey on data-centric internet of things. J. Netw. Comput. Appl. **64**, 137–153 (2016). https://doi.org/10.1016/j.jnca.2015.12.016, http://www.sciencedirect.com/science/article/pii/S1084804516000606
24. Ruan, K., Carthy, J., Kechadi, T., Crosbie, M.: Cloud forensics. In: Peterson, G., Shenoi, S. (eds.) DigitalForensics 2011. IAICT, vol. 361, pp. 35–46. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24212-0_3
25. Thing, V.L., Ng, K.Y., Chang, E.C.: Live memory forensics of mobile phones. Digital Invest. **7**, S74–S82 (2010)
26. Vömel, S., Freiling, F.: A survey of main memory acquisition and analysis techniques for the windows operating system. Digital Invest. **8**(1), 3–22 (2011)
27. Zareen, M., Waqar, A., Aslam, B.: Digital forensics: latest challenges and response. In: 2013 2nd National Conference on Information Assurance (NCIA), pp. 21–29. IEEE (2013)
28. Zawoad, S., Hasan, R.: FAIot: towards building a forensics aware eco system for the Internet of Things. In: 2015 IEEE International Conference on Services Computing, pp. 279–284, June 2015. https://doi.org/10.1109/SCC.2015.46