8-2019

# IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions

Tina Wu
*University of Oxford*

Frank Breitinger
*University Liechtenstein*

Ibrahim Baggili
*University of New Haven*, ibaggili@newhaven.edu

## Publisher Citation

Wu, T., Breitinger, F., & Baggili, I. (2019, August). IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions. In Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES '19 (Article no. 46). ACM.

## Comments

Dr. Baggili was appointed to the University of New Haven's Elder Family Endowed Chair in 2015.
This is the authors' version of the paper published in ARES '19 Proceedings of the 14th International Conference on Availability, Reliability and Security by ACM. ISBN: 978-1-4503-7164-3. The paper of record can be found at http://dx.doi.org/10.1145/3339252.3340504

# IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions

Tina Wu
Tina.wu@cs.ox.ac.uk
University of Oxford
Oxford, UK

Frank Breitinger
Ibrahim Baggili
FBreitinger@newhaven.edu
IBaggili@newhaven.edu
University of New Haven
West Haven, Connecticut

## ABSTRACT

Interactions with IoT devices generates vast amounts of personal data that can be used as a source of evidence in digital investigations. Currently, there are many challenges in IoT forensics such as the difficulty in acquiring and analysing IoT data/devices and the lack IoT forensic tools. Besides technical challenges, there are many concepts in IoT forensics that have yet to be explored such as definitions, experience and capability in the analysis of IoT data/devices and current/future challenges. A deeper understanding of these various concepts will help progress the field. To achieve this goal, we conducted a survey which received 70 responses and provided the following results: (1) IoT forensics is a sub-domain of digital forensics, but it is undecided what domains are included; (2) practitioners are already having to examine IoT devices even though they felt undertrained; (3) requirements for technical training, software and education are non-existent; (4) high priority on research should be to develop IoT forensic tools, how to preserve volatile data and methods to identify and acquire data from the cloud; (5) improvements to forensic tools should be aimed at data acquisition (imaging) and device disassembly / forensic process; (6) practitioners' perspectives on research direction differ slightly to non-practitioners in that the focus should be on breaking encryption on IoT devices rather than focus on cloud data forensics; (7) future research should focus on developing initiatives and strategies to overcome data encryption and trail obfuscation in the cloud and ongoing development of IoT forensic tools. The responses to the survey question on the definition of IoT forensics helped us formulate a working definition. This has provided a clearer understanding of the subject, which will help further advance the research area.

## KEYWORDS

Internet of Things, IoT Devices, IoT Forensics, IoT Challenges, Cloud, Definition, Survey

**ACM Reference Format:**
Tina Wu, Frank Breitinger, and Ibrahim Baggili. 2019. IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3339252.3340504

## 1 INTRODUCTION

The Internet of Things (IoT) has enabled the creation of everyday objects into smart devices e.g. smart fridges, locks or home assistants, that connect to online services and platforms. The amount of human interactions with these systems creates a new paradigm of evidential data. However, the tools and technologies in digital forensics that are meant for conventional computing are not fully capable of supporting the IoT infrastructure [39]. Forensic practitioners now face challenges such as the lack of tools and methodologies for analyzing IoT devices, exponential increase in data volume, variety of non-standardized IoT devices [16, 23] and datasets for training [13]. Additionally, a comprehensive survey effort has not been conducted to understand the reality of these challenges.

While there are many technical challenges in IoT and IoT forensics, there are also non-technical ones. For instance, it has yet to be determined which devices are considered IoT devices, what information an investigator can get (hope to get) from these devices, or how to acquire forensically relevant data [36]. On the other hand, there are many unexplored areas in IoT forensics such as the type of resources required in education, training or the specialized skills forensic investigators need to analyze IoT devices, or the type of forensic tools or methods to extract data from these devices. Lastly, there is no clear understanding of the term IoT forensics.

In this paper we present the feedback of 70 respondents to our 20 question online survey with the intention to gain a better understanding of the key issues in IoT and IoT forensics. We aim to understand concepts such as its definition as well as current and future research directions. In detail, this paper provides the following contributions:

- It outlines the community's interpretation and views on concepts such as: IoT in general, IoT devices, and IoT forensics including types of evidence obtainable from devices.

*ARES '19, August 26–29, 2019, Canterbury, United Kingdom*
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-7164-3/19/08...$15.00
https://doi.org/10.1145/3339252.3340504

- It exemplifies the investigative experiences and capabilities of practitioners and that many feel unprepared in IoT forensics.
- It discusses the participants' view on digital evidence found on IoT devices.
- It identifies and prioritizes current and future research challenges so that efforts can be concentrated on these issues.
- Based on our survey results and previous work, we present a working definition of IoT forensics in Section 6.1.

The structure of this paper is as follows: first, we present the related work where we focus on IoT forensics frameworks and IoT forensics challenges in Section 2. Next, we outline the survey methodology in Section 3 followed by the analysis of the results in Section 4. The limitations are outlined in Section 5. The last two sections provide a discussion (Section 6), conclusion (Section 7) and future research.

## 2 PREVIOUS WORK

For analyzing the previous work, we utilized several repositories and regular search engines. However, the amount of literature found was rather limited. For instance, searching on Google for "definition of IoT Forensics" (in quotes) revealed only 9 results where some pointed to the same article on different platforms (e.g., [39] can be found on ieeexplore, dl.acm.org and researchgate).

Therefore, the following subsections start by summarizing the few existing definitions in Section 2.1, followed by research on theoretical IoT forensic frameworks in Section 2.2 and a limited number of practical approaches (see Section 2.3). The challenges for IoT forensics are discussed in Section 2.4.

### 2.1 Digital forensics and IoT Forensics Definitions

At the Digital Forensic Research Workshop (DFRWS) [26] defined digital forensics as follows:

> *"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and preservation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."*

Consequently, current attempts to coin IoT forensics are similar. For instance, [39] defined IoT forensics as a separate branch of digital forensics and identify it as three different fields: cloud, network and device level forensics. The authors defined IoT forensics as:

> *"The identification, collection, organisation and presentation processes deal with IoT infrastructures to establish facts about incidents."*

Similarly, [24] broke down IoT forensics into domains such as cloud services, visualization, mobile devices, fixed computing, sensor and RFID technologies and artificial intelligence. While, [1] separated IoT forensics as a combination of different technology zones: IoT, network and cloud zones. Although these preliminary definitions exist, IoT forensics is still in the early stages of research and thus there is currently no universally accepted definition.

### 2.2 IoT Forensic Frameworks

Given the limited literature on the definition of IoT forensics, this section focuses on IoT forensic frameworks and the limited number of practical approaches which will provide a better understanding of the different areas that need to be covered in the definition.

In early research, several theoretical frameworks were developed to conduct investigations on IoT devices. For instance, [24] developed a model to systematically identify sources (i.e. where to look for evidence) using 3 zones. Zone 1 focuses on the internal network (hardware, software and networks (e.g. Bluetooth, Wi-Fi). Zone 2 targets the periphery devices (between internal and external network e.g. IDS/IPS, Gateway or Firewall). Lastly, Zone 3 "covers all hardware and software that is outside of the network in question" such as cloud or Internet Service Providers.

[25] presented the Forensics Edge Management System (FEMS) to provide an autonomous forensic service. A layering approach is used, with the network layer used to collect data from the sensors, this is then managed by the perception layer and the application layer is used to interface with the end users. FEMS collects and stores the data only if it goes over a predefined threshold.

Besides providing a definition (see Section 2.1), [39] also proposed a Forensic Aware IoT (FAIoT) model. They implemented a secure, centralized repository so evidence can easily be collected and analysed. Their approach is to constantly monitor registered IoT devices and access to the evidence is provided to law enforcement using an API service. A top-down investigative approach is proposed by [27], based on the triage model and [24] 1-2-3 zoning model, and uses the internal, middle and external networks to investigate intrusions.

A generic framework called Digital Forensic Investigation Framework for IoT (DFIF-IoT) has been proposed by [18]. They describe the proactive process which occurs before an incident and the reactive process that occurs after. Recent work by [40] proposed that an Application Specific Digital Forensic Investigative Model is beneficial in that the collection of evidence is specific to the type of IoT application. Although the forensic process will be similar depending on the IoT application e.g. smart home,smart city etc. the extraction methods may differ.

### 2.3 Practical Approaches

As research progressed, efforts have been focused on recovering forensic artifacts from consumer IoT devices, from the device itself, cloud or mobile device.

[22] presented the Forensic State Acquisition from Internet of Things (FSAIoT). This is a general framework and practical approach in gathering state changes on IoT devices e.g. device on and off. In their solution they acquire state changes from the logs in real time using the Forensic State Acquisition Controller (FSAC).

[5] presented an acquisition framework on a smart home hub. In their work they extracted and analyzed data from the smart hub's flash memory and were able to obtain a list of user interactions with the smart devices and detailed history of data uploaded to the cloud.

[7] proposed a method to extract cloud native artifacts from the Amazon ecosystem using unofficial APIs. Based on this concept they proposed a tool called Cloud-Based IoT Forensic Toolkit (CIFT) that provides identification, acquisition and analysis of native cloud artifacts.

[10] examined forensic artifacts stored on an iPhone backup file which were produced by the Nest mobile application. They developed a tool called the Forensic Evidence Acquisition and Analysis System (FEAAS) which generates a report listing user events either created by the Google Assistant through voice commands or through the user on the iPhone mobile application.

## 2.4 IoT Forensic Challenges

The advances in digital systems together with the beginning of the IoT era has brought us to a crucial period in digital forensics. [11] identified that many tools and techniques that once worked with traditional forensics will become obsolete due to the progress of technology. A recent paper by [20] laid out digital forensics research for the next five years and found there was a lack of funding towards research, training and forensic tools in IoT and these should be one of the most important research opportunities in the future.

The diverse number of IoT devices has made it difficult for forensic investigators to acquire and analyze data using traditional digital forensic methods. Many IoT systems have varying functions, customized operating systems/file structures and a number of wireless transmission protocols. This makes it difficult to identify and acquire data from IoT devices when no tools or methods have been developed [8, 16].

Data is often separated and either stored locally or remotely in the cloud which is out of the users control. Therefore identifying the location of the data can be a challenge for investigators. Data may also be stored in a different country, with different regulations and limitations on investigators having physical accessibility [39].

[11] has identified that many IoT devices use proprietary file systems and will often require reverse engineering. Many of these devices create large amounts of data making it time consuming for an investigator to identify the crucial pieces of evidence related to the crime. [1] noted that there is limited storage on IoT devices, which means the data has a short lifespan and will quickly be overwritten.

# 3 SURVEY METHODOLOGY AND DESIGN

## 3.1 Survey creation and design

The following methodology was used to create and disseminate the survey:

(1) A literature review was conducted (summarized in Section 2).
(2) The survey was designed to gather demographic information about the cyber forensic respondents, opinions on the definitions of IoT forensics, experience in the analysis of IoT devices and data, current and future research priorities. The questions were developed from reviewing existing literature but also reflect discussions/feedback from forensic practitioners.
(3) We obtained permission through the university's ethics committee. This restricted us from collecting any identifiable information and disclaiming that it posed any risk or harm to subjects.
(4) The survey was created using the Baseline system and distributed via various digital forensic mailing lists, groups on LinkedIn, forensic groups/forums online and private contacts.
(5) All data was exported in XLSX / CSV and downloaded for offline processing.
(6) The data was analyzed and the descriptive statistics as well as some cross-comparisons are summarized in the results section.

Before releasing the survey, it was shared with a small group to receive initial feedback on the questionnaire. Overall, the final survey consisted of 20 questions:

- 10 Multiple choice
- 5 Likert scale
- 3 Free response
- 1 Multiple selection (check box)
- 1 Ranking

## 3.2 Survey overview

*3.2.1 Sample considerations.* The survey was available online for eight months before the data was exported. The main target group were individuals with a cyber forensics background, from academia and industry with diverse range of experiences and training. It was also of interest to examine if the perspectives of practitioners and non-practitioners were different in relation to the priorities of current and future research challenges. Practitioner motivations may differ in that they have undertaken investigation, so it was important to ascertain whether their experience had an impact on their views regarding current research focus and future challenges.

*3.2.2 Survey analysis.* While some of the basic analysis was carried out on the survey platform, the majority of the analysis was accomplished in Microsoft Excel and R. To analyze free response questions, we read all responses, then identified and coded categories based on frequently used terms, and lastly we grouped them.

*3.2.3 Survey data.* Participants were provided with answer options either nominal or ordinal. When possible, the survey responses were logically arranged in a meaningful order to increase the quality of the results. The arrangement of ordinal data allowed the application of tests designed to identify trends in the responses.

*3.2.4 Survey reliability.* In total, $n = 70$ participants submitted responses. The calculated required sample size was $n = 60$ indicating that the number was large enough to make inferences from and that statistical tests were unlikely to exhibit type II errors (two-sided t-test, alpha = 0.05, using a medium effect size of 0.5 and power of 0.99). It should be noted that we aspired to obtain a higher response rate, but taking into consideration that IoT forensics is a relatively new area, we deemed the sample size acceptable.

## 4 RESULTS

The results of survey was divided into six sections: demographics, definitions, IoT forensic investigations, evidence, current and future challenges in IoT forensics which are reflected in the upcoming subsections.

### 4.1 Demographics

The results of the demographics questions are presented in Table 1. The majority of our ($n = 70$) participants were either American or European (80%) and 33-64 years old (83%). Most of the respondents worked in education or a training facility. 53% of the respondents had 10 years or more of experience.

The respondents from the education/training facility, were a mix of researchers, students, professors and industry instructor, however, 52% were professors. Practitioners accounted for 39%, working in the private sector organizations or state/local law enforcement. Thus, we had a mix of experience, academic researchers and practitioners that provided input.

| **Country** | **Percentage** |
|---|---|
| Africa | 4 |
| America | 41 |
| Asia | 3 |
| Europe | 39 |
| Middle East | 3 |
| North America | 6 |
| Oceania | 4 |
| **Age** | |
| 18-24 | 4 |
| 25-34 | 13 |
| 35-44 | 33 |
| 45-54 | 26 |
| 55-64 | 24 |
| 65+ | 4 |
| **Gender** | |
| Female | 13 |
| Males | 87 |
| **Years of Experience in Cyber Forensics** | |
| Less than 1 | 10 |
| 1-3 years | 16 |
| 4-6 years | 13 |
| 7-9 years | 8 |
| 10+ years | 53 |
| **Occupation Category** | |
| Education/training facility | 39 |
| Federal law enforcement | 3 |
| Legal system | 1 |
| Private sector organization | 23 |
| State/local law enforcement | 12 |
| Other | 4 |
| **Primary occupation** | |
| Industry instructor | 4 |
| Law enforcement practitioner | 16 |
| Non-law enforcement practitioner | 23 |
| Professor | 23 |
| Researcher | 20 |
| Student | 7 |
| Other | 7 |

**Table 1: These percentages account for 70 of the participants**

### 4.2 Definitions

This section discusses participants' definitions of IoT, IoT devices and IoT forensics. Definitions are important as they enable us to form an accepted and common understanding of a word or subject. Thus, they allow for a mutual understanding of a topic under discussion.

*4.2.1 Definition of IoT.* IoT is still evolving, therefore, many interpretations exist and the definition remains fuzzy. A sound definition can provide a better understanding of the subject, lead to further research and advance the understanding of this emerging concept. Therefore, the beginning of the survey asked participants to report their agreement of the definition of IoT. Four definitions from *Wikipedia, NIST, Gartner* and *IoT Analytics* were shown and participants had to choose between strongly agree to strongly disagree on each of them. The definitions are as follows:

Wikipedia definition [37]:

> *"The Internet of things is the inter-networking of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data."*

NIST definition [35] :

> *"Jeffrey Voas from NIST defines IoT using a model he calls the Network of things that relies on 4 key components to function, sensings, computing, communication and actuation. The network of things model relies on sensors, a communication channel, an aggregator, and the cloud in order to function. Network of Things Model."*

Gartner definition [12]:

> *"The Internet of Things is sensors and actuators embedded in physical objects that are linked through wired and wireless networks."*

Analystics definition [3] :

> *"The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."*

All 70 participants answered this question and the results are shown in Figure 1. Most participants agreed / strongly agreed with the definition found on Wikipedia (84%) followed by the definition given by Jeffrey Voas from NIST (71%). However, there is no clear favorite and participants found all definitions (though different) valid.

*4.2.2 IoT Devices.* The next set of questions focused on IoT devices where participants were asked what they considered to be an IoT device. From the options offered *Smart Home Appliances* received the highest responses (97% agreed) closely followed by

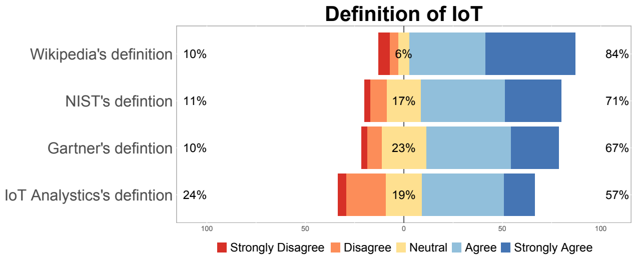

**Figure 1: This Likert scale uses a 5 point scale ("strongly agree" to "strongly disagree"), participants were asked to rank which definitions of IoT they agree and disagree with the most.**

*Hub based internet devices* (89%), *Home Assistant* (89%) and *Internet connected sensors* (86%). Detailed results are summarized in Table 2.

Next, we asked participants whether an IoT device has to be constantly connected to the Internet. Out of the 69 answers, the majority (84%) responded with 'no'. However, this shows that there is still uncertainty / disagreement as to what exactly constitutes as an IoT device.

| Type of IoT Device | Percentage |
|---|---|
| Self Driving Cars | 70 |
| Smart Phones | 43 |
| Drones | 61 |
| Hub based Internet devices (ex. Internet connected light bulbs) | 89 |
| Internet connected sensors (ex. sensors monitoring power plants and factory machines.) | 86 |
| Bluetooth peripherals | 44 |
| Wearables (ex. Smart Watches) | 74 |
| Home Assistants (Google Home, Amazon Alexa, etc) | 89 |
| Smart Home Appliances | 97 |

**Table 2: This multiple selection checkbox question allowed participants to select as many choices they considered applied, participants were asked to select options that they considered to be an IoT device**

*4.2.3 Definition of IoT Forensics.* We first asked participants if they consider IoT forensics a sub-domain of digital forensics where 90% answered with 'yes'. This shows that it is widely accepted as a sub-domain and similar to other sub-domains such as mobile forensics, network forensics etc. where the name of the domain defines the focus area. However, the ubiquitous nature of IoT devices makes it difficult to draw a definite conclusion to what domains are included. The 10% that said 'no' to this question were primarily from private sector.

Next, in a free response question, we asked participants about their interpretation of IoT forensics. 64 participants responded and we received a variety of answers. However, we excluded 23 of the responses as they were either too short (e.g., *"digital forensic in the context of IoT"*), were not specific to IoT forensics or were unclear (e.g., *"internet connected devices, either through Bluetooth or sensors or TCP/IP"*)

We organized the remaining 41 responses (which often included similar terms), then extracted keywords and clustered them under one general term as shown below:

- Collection, preservation, analysis and presentation of IoT devices and data (17)[1]
- Embedded devices (7)
- Non-traditional computers (6)
- IoT network traffic (4)
- Cloud (3)
- Others (4)

While the above points mostly focus on network and devices, one respondent addressed necessary skills that *"IoT forensics is largely reverse engineering and is more like forensic analysis of unknown devices"*. One individual wrote that *"IoT forensics is no different from other IT and remains parts of digital forensics"*. While another commented that *"IoT forensics is largely a buzzword for internet connected devices"*.

In addition to the above points, one individual referred to how the evidence can be used: *"Dealing with evidence that relates to the IoT devices themselves (e.g. using them for illegal purposes, evidence of hacking attacks, etc.) and also evidence that has been gathered by IoT devices but relates to crimes that are otherwise unrelated (e.g. home security system knowing that a person was home at a particular time, cameras capturing events, GPS information from wearables, etc.)."*

Interestingly, the responses focus more on IoT devices rather than the process, outcome of an investigation or a combination of traditional forensic steps. A detailed list of the results is shown in A.

## 4.3 IoT Forensic Investigations

The two subsections focus on investigative experiences and capabilities.

*4.3.1 Investigative Experience.* To gain a better understanding of participants' experience with IoT devices, we asked *Have you ever been involved in an investigation where they have had to analyze IoT data?*. From the 70 responses, 62% (43) answered no, 11% (8) answered not myself but I know a colleague and 27% (19) marked yes.

In further analysis, we split the data into practitioners and non-practitioners as shown in Table 5. The results show that practitioners are already investigation IoT devices. On the other hand, a high number of non-practitioners have not been involved in IoT investigations.

| Occupation | Investigating IoT data / devices | | |
|---|---|---|---|
| | Yes (%) | No (%) | Total (%) |
| Practitioner | 16 | 23 | 38 |
| Non-practitioner | 7 | 47 | 54 |
| Other | 4 | 3 | 7 |
| **Total (%)** | 27 | 73 | 100 |

**Table 3: Cross correlating participants occupation vs whether they have been involved in an IoT investigation**

[1] The parenthetical numbers indicate the number of times a general idea was mentioned.

The respondents that stated they had either been involved in an investigation with IoT data or knew a colleague who had, were asked to include brief case details. Three respondents did not put any case details as it was either confidential or sub judice. The following responses were received along with their count:

(a) Home virtual assistant: Amazon Alexa (4), Google home
(b) Smart wearable devices e.g Fitbit (3)
(c) Mobile device that was exposed to IoT devices (2)
(d) CCTV and DVRs (2)
(e) Raspberry Pi for research purposes
(f) Industrial IoT device
(g) IP camera that was found to have been installed without authorization
(h) Home automation system whereby the contractors have been accused by the home owner of illegally accessing the home system
(i) Smart refrigerator
(j) Implanted health device
(k) Smart TV: to recover data to show there was interaction at a particular time
(l) Infotainment systems from vehicles to show GPS information

From these provided case details, it is interesting to see that there is an association with the answers provided in Section 4.2.2 on 'IoT Devices' where *Smart Home Appliances* are ranked highest. Besides our participants, there have been several public cases that involved some of the points listed beforehand. For instance, in 2015 a man was charged in a murder investigation based on data extracted from an Amazon Echo [21]. In another case, data was taken from a Fitbit device and used in a murder investigation to challenge a suspect's version of the events [34].

*4.3.2 Investigative Capability.* Subsequently, we asked participants whether they felt they were in a position to analyze IoT devices, this included communication channels and network traffic. This was a free response question with 62 answers which can be summarized as follows:

- 47% (29) said they were in a position,
- 31% (19) stated they were not and
- 22% (14) were unsure

As this was a free response question the 31% (19) stated that they had *"insufficient training"*, or felt they were *"not fully qualified to do so"*. Others also stated they were *"close, but encryption would obfuscate it"*. The participants that stated they were unsure mentioned that it *"depended on the type of IoT device e.g. physical interface, OS, protocols"*. Some participants thought they were *"not quite ready but working towards it"*.

For the 47% (29) who said yes they felt capable of analyzing IoT devices, we correlated them with the question *whether they have been involved in an investigation analyzing IoT devices*. This showed that 11 had been involved in an investigation. Of these 11, half (6) were practitioners and the majority (10) had ten or more years of experience. As expected, respondents with 10+ years of experience were more confident in their capabilities (See Table 4).

This high number of trained employees could be a result of the [29–31] (RCFL) which "is a one stop, full service forensics laboratory and training center devoted entirely to the examination of digital evidence in support of criminal investigations"[2].

| **Years of experience** | **Position to analyze IoT devices** | | | |
|---|---|---|---|---|
| | **Yes (%)** | **No (%)** | **No answer (%)** | **Total (%)** |
| Less than a year | 1 | 7 | 1 | 10 |
| 1-3 years | 1 | 11 | 3 | 16 |
| 4-6 years | 6 | 4 | 3 | 13 |
| 7-9 years | 3 | 6 | 0 | 9 |
| 10+ years | 30 | 19 | 4 | 53 |
| **Total (%)** | 41 | 47 | 11 | 100 |

**Table 4: Cross correlating participants experience vs whether they consider themselves in a position to analyze an IoT device**

## 4.4 Evidence on IoT Devices

Again we used a free response question about evidence which had two parts. First, we asked participants what type of evidence they thought could be obtained from IoT devices. Second, we asked why they think this evidence is important. As with other free response questions, we summarized / clustered the results. The first part of the question received the following responses, with the general themes shown below:

(1) User behaviour (6)
(2) GPS data (6)
(3) Sensor data (5)
(4) Connection history e.g IP addresses (5)
(5) Logs (5)
(6) Data on IoT device states (3)
(7) Data stored on the cloud (2)
(8) Telemetry data (2)
(9) Data from Intrusion Detection Systems (IDS)
(10) Configuration data
(11) Photos, videos, audio
(12) Records of conversations
(13) Network related information
(14) Heart rate data
(15) Modified firmware
(16) Events records by the IoT device

The second part of the question was to *explore the importance of the evidence* which received 21 responses. From those, we first extracted the comments that were related to why the evidence was important. The responses were then grouped based on the most frequently used terms, this also included individual direct quotations:

- Trace behavioural patterns of users, then use the data to recreate criminal activity or draw meaningful conclusions about a suspect's modus operandi (11)
- Timeline of events to trace incidence in question (2)
- To correlate data
- Determine unexpected behaviour in IoT networks
- Metadata gives clues to what happened

[2] https://www.rcfl.gov/about (last accessed 2019-01-17).

- Trace unauthorized interactions and data sharing
- It can tell us something that no human may have observed
- What the state of an environment is at the time an incident occurs
- That a person has been in a place at a certain time or that a person has done a certain action
- Aid investigations such as intelligence, criminal, accident, wrongful death, injury, corporate cases for manufacturing equipment failure/damage, and larger scope such as electronic voting

## 4.5 Current Challenges

This section identifies the important challenges currently faced by investigators in the IoT environment with regards to legislation, cloud, training, software and acquisition.

### 4.5.1 *Current Issues.*

To learn about the current issues, we asked participants to rank nine topics with 1 being the most important and 10 being the least. Topics and results are shown in Figure 2. The results indicated that the important issues are technical training (82%), software (80%) and education (78%) whereas funding, legal issues and cloud data storage currently have less relevance.

Technical training holds the highest priority and this reinforces why over half of the participants felt they were unable to undertake and analyze an IoT device.

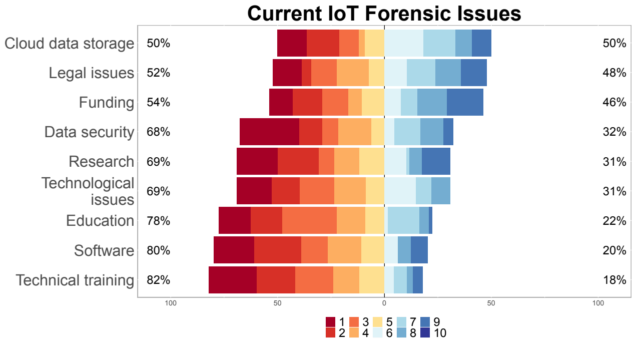

**Figure 2: On a scale of 1 to 10 (1 being the most and 10 being the least important) participants had to rank the various challenges listed on the left.**

A subsequent question asked their view on various statements regarding legislation, data encryption, cloud and the security of IoT devices. The exact statements and the results are presented in Figure 3, which shows that 83% of the respondents thought IoT devices currently have weak security.

Similar to our findings, a study by [17] points out several other security challenges in the IoT landscape. These included constraints on memory and energy on IoT devices which make it hard to port computationally expensive cryptographic algorithms. With the growing number of IoT devices, current security schemes lack scalability meaning these schemes would not be suitable for IoT devices. These challenges could be contributing factors as to why IoT devices have weak security.

IoT devices having weak security is not unexpected as there have been many documented security flaws found on consumer IoT devices such as baby monitors, home security cameras or smart thermostats [33]. However, legislation is being introduced to combat weak security on IoT devices, for example, in California a law is being introduced to ban default passwords [38]. In a similar effort, the UK government has released a "Code of Practise for Consumer IoT Security" document which sets out guidelines to ensure the secure design of IoT consumer products [9].

The majority of respondents strongly disagreed with the statement that *Legislation regarding IoT forensics is currently up to date.* This is not surprising as legislation has always been behind technology and is one of the main challenges in digital forensics [2]. Current legislation that governs the way data is gathered, studied, analyzed and stored are aimed at traditional computing technology [4, 14]. Therefore, in order to standardize processes, training programs and tools, legislation will need to be reviewed to include IoT devices.

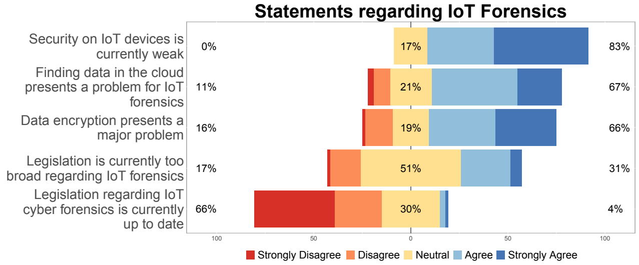

**Figure 3: This Likert scale used a 5 point scale and asked participants if they agree or disagree with each of the statements listed on the left.**

### 4.5.2 *Research Directions.*

The participants were asked *where should research be focused on in order to combat current issues.* The majority of participants thought that research should focus on the IoT forensic tools (57%), preserving volatile data (41%) and cloud data forensics (40%).

| Research directions | Occupation | | |
|---|---|---|---|
| | Practitioners (%) | Non-practitioners(%) | Total (%) |
| Legislation updates | 3 | 9 | 11 |
| Jurisdictional issues | 1 | 7 | 9 |
| Cloud data forensics | 10 | 30 | 40 |
| Preserving volatile data | 14 | 27 | 41 |
| IoT forensic tools | 27 | 30 | 57 |
| Breaking data encryption on IoT devices | 13 | 7 | 20 |
| Memory retrieval | 7 | 11 | 19 |
| No answer | 1 | 2 | 3 |
| **Total (%)** | 77 | 123 | 200 |

**Table 5: Cross correlating whether participants have been involved in an investigation vs where research should be focused**

We then cross-correlated these results with the practitioners and non practitioners. This showed that both groups thought IoT forensic tools and preserving volatile data were the most important areas. However, practitioners thought breaking encryption on IoT devices is a more important area to focus on than non-practitioners, who ranked cloud data forensics higher as shown in Table 5.

*4.5.3 Improvements to Tools.* Focusing on tools, we asked participants what areas of improvements are required in forensic and software tools used on IoT devices. The results are shown in Table 6 and show the respondents thought data acquisition / imaging (73%) and device disassembly forensic process (63%) are the most in need of improvement.

We continued to study whether the results would differ from the perspectives of practitioners and non-practitioners and found no difference. We also cross-correlated this against whether they had been involved in an investigation and again found no difference.

| Areas in need of improvement to forensic and software tools | Percentage |
|---|---|
| Data preservation | 33 |
| Data acquisition [Imaging] | 73 |
| Data encryption | 30 |
| Memory acquisition | 43 |
| Device disassembly and forensic process | 63 |
| Other | 6 |

**Table 6: The multiple selection checkbox question allowed participants to select as many areas in forensic and software tools which need improvements.**

*4.5.4 Challenges in Acquisition.* To gain a better understanding of acquisition challenges, we asked participants what they considered to be the most challenging area. Out of the 68 responses, 38% considered cloud storage as the most challenging area followed by on-device memory (28%), on-device storage (19%) and network (15%). When looking at this together with the question *areas of research to focus on to combat current issues*, one of the main areas highlighted was cloud data forensics; this was also highlighted as being the most challenging area to find (Section 4.5.1) and acquire data from. This is a clear indication that finding easier ways to identify and acquire data from the cloud should be a priority research area in cloud data forensics.

We investigated whether there was any difference of opinions between practitioners and non-practitioners which is summarized in Table 7. We found practitioners thought on-device storage and on-device memory as the most challenging area to acquire evidence. Whereas, non-practitioners thought cloud storage and on-device memory is most challenging.

## 4.6 The Future Challenges

The last question was a Likert scale question and focused on future challenges. In particular, we asked participants to *rate how much they agree or disagree that the following present a challenge to the future of IoT forensics.* The results are shown in Figure 4 and indicate that data encryption, lack of forensic tools and trail obfuscation (particularly as it pertains to cloud forensics) are the most challenging issues that need to be focused in the future of IoT forensics.

| Challenges in acquisition | Occupation | | |
|---|---|---|---|
| | Practitioners (%) | Non-practitioners (%) | Total (%) |
| Cloud storage | 7 | 30 | 37 |
| On-device memory | 11 | 16 | 27 |
| On-device storage | 13 | 6 | 19 |
| Network | 4 | 10 | 14 |
| No answer | 3 | 0 | 3 |
| **Total (%)** | 39 | 61 | 100 |

**Table 7: Cross correlating what participants considered challenging in acquisition vs their primary occupation**

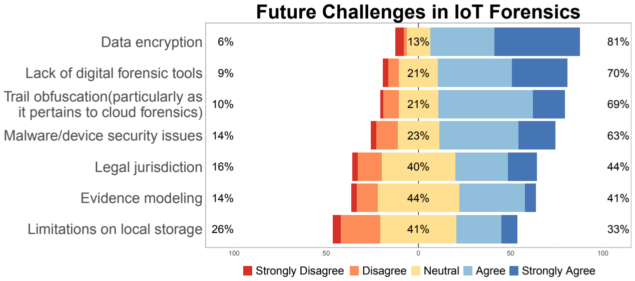

**Figure 4: This Likert scale uses a 5 point scale (“strongly agree" to “strongly disagree"), participants were asked to rank which of the statements would be challenging for the future of IoT forensics by agree and disagree with the most.**

# 5 LIMITATIONS

There are several limitations in this survey. First, this survey only had 70 participants which is a small number and answers may vary with a larger group participating. Secondly, the demographical distribution is not even, as the majority came from America or Europe, were primarily males, had 10+ years of experience and were occupied in the education/training facility sector. Thirdly, although being very careful, there is the possibility for human error while analyzing the results especially the free-response questions which cannot be automated.

# 6 DISCUSSION

The results from this survey have identified a number of key issues in IoT forensics.

## 6.1 Towards a definition for IoT Forensics

Based on the definitions summarized in Section 2.1 and the responses from our survey, we propose the following working definition for IoT forensics:

> *"Internet of Things (IoT) forensics is a sub-domain of digital forensics and involves the collection, preservation, analysis and presentation of data obtained from IoT devices for the purpose of collating historical data of interactions from IoT device(s) to reconstruct criminal / exonerating events or obtaining remnants of data that indicates a malicious act or exploitation of an IoT device. It consists of various domains / skills including networking, embedded device, cloud, mobile, host based forensics and reverse engineering."*

Note, that there was some disagreement on what constitutes an IoT device (discussed in Section 4.2.2) e.g. disagreement on an IoT device needing a constant Internet connection. As IoT forensics develops, participant views may change and a universal definition may be accepted.

As a follow-up to the survey, we posted our working definition of IoT forensics to various mailing lists and forums and received the following feedback: one respondent felt they *"Did not think that IoT as being just solely a criminal events or data that would indicate malicious acts or exploitation"*, while another respondent wrote that embedded devices should be changed to *"embedded systems"* as this would then cover traditional embedded devices. Another respondent felt that the collection of data was not only from the IoT device but also any system(s) connected to the IoT device. Based on these recommendations we updated the definition and concluded the following:

> *"Internet of Things (IoT) forensics is a sub-domain of digital forensics and involves the collection, preservation, analysis and presentation of data obtained from or connected to the IoT device(s). The purpose of this is to collate historical data of interactions from or connected to the IoT device(s) to reconstruct the events involving a malicious act or exploitation of an IoT device to be used for civil or criminal proceedings. It consists of various domains / skills including network, embedded systems, cloud, mobile, host based forensics and reverse engineering."*

## 6.2 Readiness for IoT

In terms of capability of analyzing IoT devices, 53% of the participants felt they were either not or unsure they were in the position to analyze IoT devices. The participants that said they were not or unsure stated that this was due to *"insufficient training"* or felt they were *"not fully qualified"*. On the other hand, this was an objective question and therefore we do not know what skills the 47% (answering yes) have. In order to counteract short term, we may need more training and education facilities for IoT forensics to prepare law enforcement. There has to be expert discussion of the skills needed by investigators in the area of IoT forensics. Maybe it is insufficient to only operate tools; maybe we need highly technical people (e.g., reverse engineering experts). This is further supported by the responses when the participants were asked to rank issues IoT forensics is facing today, with the most important issues being technical training, software and education.

Issues regarding the lack of training have previously been highlighted in research in the field of cyber forensics. [15] found that the cyber forensic field required more Education, Training and Certification (ETC) facilities, newer programs, revision of the current curriculum and more funding in training materials should be one of the highest priorities.

## 6.3 Lack of IoT Forensic Tools

The findings from this survey found the majority of participants thought that research should specifically focus on developing tools in IoT forensics to identify and acquire data from the cloud. This coincides with a study published by [20] who found that there is a lack of forensics tools in general which included IoT forensic tools.

Currently only a few IoT forensics tools have been developed. This includes cloud acquisition tool that acquires cloud-native artifacts [7] , however this tool has only been developed and tested on the Alexa ecosystem. [5] found from their previous experience of using unofficial APIs that they can change without notice, making this an unreliable method of extraction.

[10] developed a tool that automatically acquires artifacts from iOS devices. Their tool presents a readable report that provides a timeline of user events and whether the mobile application or voice command through the Google Assistant triggered an event.

[5] extracted data from a smart hub, however they have only presented a method that works specially with the Almond smart hub and no tool was developed to automatically extract or analyze the data. Therefore further research should be focused on developing IoT forensic tools that would work reliably across a range of devices.

Many of these tools have been developed for specific tasks such as the analysis of data from iOS or acquisition and analysis of cloud native artifacts. There has been no effort to provide any interoperability with each other. This makes it difficult and time-consuming for a investigator as they are unable to establish a correlation between multiple sources of evidence. Hence, a tool needs to be developed so historical patterns of activity can be established from various data sources.

## 6.4 Challenges

The majority of participants thought the cloud as one of the key areas of current research, more specifically identifying and acquiring data in the cloud. There are several possible reasons why the cloud is one of the challenges; the cloud infrastructure is normally under the control of the IoT provider, the actual physical location of the data could be hidden or potentially cross different boundaries of jurisdictions, and distributed across cloud computing platforms [28]. Another reason could be that access to data within the cloud can only be provided with user credentials. Although there is a potential to obtain these during the investigation, the lack of certainty can prevent the progress of an investigation [25].

The findings have also highlighted that data encryption and trail obfuscation (cloud) are key areas that need to be focused on in future research. Both data encryption and trail obfuscation are anti-forensic techniques already known as obstacles in digital forensics. Future research should work on initiatives and strategies to address these growing problems. Data encryption presents a major challenge and has already been highlighted in previous literature as a continuous problem [6]. The results show that participants are also worried about data encryption in the IoT domain. Maybe we have to focus on more non-traditional approaches, for example, [32] identified the potential of electromagnetic side channel as a method to analyse encrypted devices.

Trail obfuscation in the cloud has been highlighted as one of the future challenges in IoT forensics. It could be a problem for the future when data is deleted from the cloud making it difficult to gain remote access. Data may be recoverable however it is challenging to recover and identify ownership [19].

Jurisdiction and legislation was regarded as a relatively low priority for current research and future challenges. However, as there was only one representative from the legal profession in the demographic, we think a follow-up survey targeting the judiciary viewpoint would be beneficial. This would help identify any legal issues such as privacy.

## 7 CONCLUSION AND FUTURE RESEARCH

In this work, we presented and discussed the 70 responses of our 20-question online survey. Our results show while participants agree on some aspects of IoT forensics (e.g. that IoT forensics is a sub-domain of digital forensics), there is also disagreement on IoT, IoT devices and IoT forensics (e.g. which devices are considered IoT devices, and whether IoT devices are constantly connected).

Participants agreed that IoT forensics includes a wide range of domains which makes it difficult to draw a definite conclusion as to what is included (e.g. cloud, network and reverse engineering). When asked to define IoT forensics, respondents were mostly focused on the different types of IoT devices instead of an actual definition. Thus, to come up with the definition for IoT forensics, we primarily focused on the definition for digital forensics (quoted in Section 2.1) and expanded it by adding the sub-domain specific properties. Although this definition is a good starting point, it will require further refinement and validation as the field develops.

Additionally, our results show that participants (~ 30%) have had experience in examining IoT devices / data although over 50% did not feel prepared. As a consequence, we need to think about increasing education programs / technical training to prepare the workforce to deal the exponential increase in the usage of IoT devices.

Results following this survey indicated that there are many IoT forensic challenges ahead, as technology develops these challenges will increase. We summarize the key findings as follows:

- Besides education, participants see major challenges in encryption and cloud storage which overlaps with other existing literature
- The most important research areas identified are developing IoT forensic tools, how to preserve volatile data and cloud data forensics
- With limited IoT forensic tool the focus on development of tools should be on identifying and acquiring data from the cloud

IoT forensics is a relatively new topic and we received responses from 70 participants. We expect the field to progress and grow in the future, a follow up survey could then be conducted with a larger sample size. Also, the working definition of IoT forensics would need to be further refined and validated.

## REFERENCES

[1] Saad Alabdulsalam, Kevin Schaefer, M. Tahar Kechadi, and Nhien-An Le-Khac. 2018. Internet of Things Forensics - Challenges and a Case Study. In *IFIP Int. Conf. Digital Forensics.*

[2] James Ami-Narh and Patricia Williams. 2008. Digital Forensics and the Legal System: A Dilemma of our Times. *ECU Publications* (Dec. 2008).

[3] IoT Analystics. 2018. What is Internet of Things Analytics (IoT Analytics)? - Definition from Techopedia. https://www.techopedia.com/definition/31460/internet-of-things-analytics-iot-analytics

[4] Association of Chief Police Officers. 2012. *ACPO Good Practice Guide for Digital Evidence.* Technical Report. Association of Chief Police Officers.

[5] Akshay Awasthi, Huw O.L. Read, Konstantinos Xynos, and Iain Sutherland. 2018. Welcome pwn: Almond smart home hub forensics. *Digital Investigation* 26 (jul 2018), S38–S46. https://doi.org/10.1016/j.diin.2018.04.014

[6] Eoghan Casey, Geoff Fellows, Matthew Geiger, and Gerasimos Stellatos. 2011. The growing impact of full disk encryption on digital forensics. *Digital Investigation* 8, 2 (nov 2011), 129–134. https://doi.org/10.1016/J.DIIN.2011.09.005

[7] Hyunji Chung, Jungheum Park, and Sangjin Lee. 2017. Digital forensic approaches for Amazon Alexa ecosystem. *Digital Investigation* 22 (2017), S15–S25. https://doi.org/10.1016/j.diin.2017.06.010

[8] Mauro Conti, Ali Dehghantanha, Katrin Franke, and Steve Watson. 2018. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems* 78 (jan 2018), 544–546. https://doi.org/10.1016/j.future.2017.07.060

[9] Department for Digital, Culture Media & Sport. 2017. *Secure by Design: Improving the cyber security of consumer Internet of Things Report.* Technical Report. Department for Digital, Culture Media & Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment$_d$ata/file/686089/Secure$_b$y$_D$esign$_R$eport$_.$pdf

[10] Gokila Dorai and Ibrahim Baggili. 2018. I Know What You Did Last Summer : Your Smart Home Internet of Things and Your iPhone Forensically Ratting You Out. In *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018.* 1–10. https://doi.org/10.1145/3230833.3232814

[11] Simson L Garfinkel. 2010. Digital forensics research: The next 10 years. *Digital Investigation* 7 (aug 2010), S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

[12] Gartner. 2017. Internet of Things Defined - Tech Definitions by Gartner. https://www.gartner.com/it-glossary/internet-of-things/

[13] Cinthya Grajeda, Frank Breitinger, and Ibrahim Baggili. 2017. Availability of Datasets for Digital Forensics And What is Missing. *Digit. Investig.* 22, S (Aug. 2017), S94–S105. https://doi.org/10.1016/j.diin.2017.06.004

[14] Timothy Grance, Suzanne Chevalier, Kent Karen, and Hung Dang. 2006. Guide to Integrating Forensic Techniques into Incident Response | NIST. *Special Publication (NIST SP) - 800-86* (sep 2006). https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response

[15] Vikram S. Harichandran, Frank Breitinger, Ibrahim Baggili, and Andrew Marrington. 2016. A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security* 57 (2016), 1 – 13. https://doi.org/10.1016/j.cose.2015.10.007

[16] Robert Hegarty, David J. Lamb, and Andrew Attwood. 2014. Digital Evidence Challenges in the Internet of Things. In *INC.*

[17] Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan. 2015. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In *2015 IEEE World Congress on Services.* IEEE, 21–28. https://doi.org/10.1109/SERVICES.2015.12

[18] Victor R. Kebande and Indrakshi Ray. 2016. A Generic Digital Forensic Investigation Framework for Internet of Things (IoT). *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)* (2016), 356–362. https://doi.org/10.1109/FiCloud.2016.57

[19] Keyun, R., Carthy, J., Kechadi, T. 2011. Cloud Forensics An Overview. *7th IFIP Conference on Digital Forensics* January (2011), 35–46.

[20] Laoise Luciano, Ibrahim Baggili, Mateusz Topor, Peter Casey, and Frank Breitinger. 2018. Digital Forensics in the Next Five Years. In *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018.* ACM Press, New York, New York, USA, 1–14. https://doi.org/10.1145/3230833.3232813

[21] Jimmy McCloskey. 2018. CSI Alexa: The smart home has become the new crime scene witness. https://www.the-ambient.com/features/smart-home-crime-scene-264

[22] Christopher Meffert, Devon Clark, Ibrahim Baggili, and Frank Breitinger. 2017. Forensic State Acquisition from Internet of Things (FSAIoT). In *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17.* 1–11. https://doi.org/10.1145/3098954.3104053

[23] Ana Nieto, Ruben Rios, and Javier Lopez. 2018. IoT-Forensics Meets Privacy: Towards Cooperative Digital Investigations. *Sensors* 18, 2 (feb 2018), 492. https://doi.org/10.3390/s18020492

[24] Edewede Oriwoh, David Jazani, Gregory Epiphaniou, and Paul Sant. 2013. Internet of Things Forensics: Challenges and approaches. *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing* (2013),

608–615.

[25] Edewede Oriwoh and Paul Sant. 2013. The forensics edge management system: A concept and design. In *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*. 544–550. https://doi.org/10.1109/UIC-ATC.2013.71

[26] Gary Palmer and Mitre Corporation. 2001. *A Road Map for Digital Forensic Research*. Technical Report. DFRWS. http://isis.poly.edu/kulesh/forensics/docs/DFRWS$_{\mathrm{R}}$M$_{\mathrm{F}}$inal.pdf

[27] Sundresan Perumal, Norita Md Norwawi, and Valliappan Raman. 2015. 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)*. IEEE, 19–23. https://doi.org/10.1109/ICDIPC.2015.7323000

[28] Ameer Pichan, Mihai Lazarescu, and Sie Teng Soh. 2015. Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation* 13 (2015), 38 – 57. https://doi.org/10.1016/j.diin.2015.03.002

[29] Regional Computer Forensics Laboratory. 2014. *Regional Computer Forensics Laboratory Annual Report for Fiscal Year 2014*. Technical Report. U.S. Department of Justice.

[30] Regional Computer Forensics Laboratory. 2015. *Regional Computer Forensics Laboratory Annual Report for Fiscal Year 2015*. Technical Report. U.S. Department of Justice.

[31] Regional Computer Forensics Laboratory. 2016. *Regional Computer Forensics Laboratory Annual Report for Fiscal Year 2016*. Technical Report. U.S. Department of Justice.

[32] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. 2018. Electromagnetic Side-Channel Attacks: Potential for Progressing Hindered Digital Forensic Analysis. In *Proceedings of the International Workshop on Speculative Side Channel Analysis (WoSSCA 2018)*. ACM, Amsterdam, Netherlands. https://doi.org/10.1145/3236454.3236512

[33] Omer Shwartz, Yael Mathov, Michael Bohadana, Yuval Elovici, and Yossi Oren. 2018. Opening Pandora’s Box: Effective Techniques for Reverse Engineering IoT Devices. In *Smart Card Research and Advanced Applications*, Thomas Eisenbarth and Yannick Teglia (Eds.). Springer International Publishing, Cham, 1–21.

[34] Michelle Taylor. 2017. Murdered WomanâĂŹs Fitbit Log Used to Charge Husband. Website. https://www.forensicmag.com/news/2017/04/murdered-womans-fitbit-log-used-charge-husband

[35] Jeffrey Voas. 2016. Demystifying the Internet of Things. *Computer* 49, 6 (June 2016), 80–83. https://doi.org/10.1109/MC.2016.162

[36] Steve Watson and Ali Dehghantanha. 2016. Digital forensics: the missing piece of the Internet of Things promise. *Computer Fraud & Security* 2016, 6 (jun 2016), 5–8. https://doi.org/10.1016/S1361-3723(15)30045-2

[37] Wikipedia. 2018. Internet of things - Wikipedia. https://en.wikipedia.org/wiki/Internet$_{\mathrm{o}}$f$_{\mathrm{t}}$hings

[38] Zack, Whittaker. 2018. California passes law that bans default passwords in connected devices. Website.

[39] Shams Zawoad and Ragib Hasan. 2015. FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015* (2015), 279–284. https://doi.org/10.1109/SCC.2015.46

[40] Tanveer Zia, Peng Liu, and Weili Han. 2017. Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT). In *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES ’17*. 1–7. https://doi.org/10.1145/3098954.3104052

# A RESPONSES FROM PARTICIPANTS' INTERPRETATION OF IOT FORENSICS

The tables shown below represents 41 responses from participants' interpretation on IoT forensics. For a discussion of these see Section 4.2.3.

| Category | Response |
|---|---|
| Collection, preservation, analysis and presentation of IoT devices and data | Investigation/analysis of real-time and prior crimes committed using IoT; the collection of evidence/data artefacts (footprints) from the IoT sensors/actuators/nodes/devices that would aid law enforcement in resolving cases. |
| | IoT forensics is the application of the digital forensics process to handling potential evidence that might be contained in an IoT device. |
| | The identification, preservation, collection, analysis and presentation of data from any 'smart' device. |
| | IoT forensics the smart forensic methodology for investigate IoT based crimes into more deeper level . |
| | The necessity of analysing data from objects we wouldn't in the past have expected to contain personal information, for example refrigerators and light bulbs. |
| | IoT forensics is the practice of collecting, analysing, and reporting on digital data acquired from physical devices that have the ability to connect, communicate and exchange data over wired or wireless networks. |
| | IoT forensics is a forensic sciences branch which deals with the development of scientifically proven methods to acquire evidence from IoT devices and to analyse this evidence. |
| | The use of forensically methods and tools to investigate IoT Devices (e.g. Smart Meters) to get digital evidences which are proof for a court of law. |
| | The analysis of data created by IoT devices in order to get insights for a forensic case |
| | Examination of IoT devices and IoT data with the goal to find evidence for actions taken or omitted. |
| | Gathering evidence and presenting the analysis of the evidence in a legally admissible way. |
| | Investigation process of an incident that involves internet enabled device, which includes the identification of the source of instantiation of connection. |
| | Digital forensic examination and analysis of IoT devices and data |
| | The recovery and interpretation of data from IoT systems in order to create understanding of the events which led to the data being deposited. |
| | The location, collection and analysis of cyber forensic data from components of the IoT, whether purely local or at aggregation and transmission points. It also include analysis of the analyses of IoT data. |
| | Analysis of sensors and controls with communications. Std Who what when where and how |
| | IoT forensics is the systematic processing of an IoT devices that is mostly likely a portion of an investigation. |
| Embedded Devices | Recovery and analysis of data relevant to investigation from any specialized (not general purpose computing) internet connected device |
| | The retrieval and analysis of artefacts retained on and sent by embedded devices to local or remote instances including the cloud and social media |
| | The acquisition and processing of data collected from embedded devices that have an internet component that is part of its function. |
| | The process of extracting (collecting) relevant data from networked physical devices and embedded electronic items for analysis purposes. |
| | Forensics in IoT devices Like embedded devices which have (in)direct connection over the internet to a central resource for example for Management purposes or control of the devices states. |
| | Embedded device in electronic log and data investigations |
| | I would consider IoT forensics, the analysis of data generated by special purpose embedded systems. Smart watches are becoming general purpose, as tablets and phones already are, and there are forensic tools for them. There are relatively few such tools for things like nest thermostat, ring doorbell, video surveillance, industrial control, vehicle control, healthcare diagnostics, electronic voting. The tools tend to be platform specific, and because embedded software platforms may be shared between these, it may be helpful to consider how that affects the practice. Also consider that, from a forensics perspective, we are likely primarily interested in the data from the devices, which means either devices that retain data, or cloud forensics of data uploaded. Do we draw a line between cloud acquisition, and acquisition from devices themselves? Probably not. Look at cell phone forensics, where the tools for imaging phones are taking on features to use credentials from the phone to download data from associated cloud services. |
| Non-Traditional Computing | Examination of IP connected devices which are not regular computers, PCs, smart phones, tablets etc |
| | Forensics on small-resource network nodes |
| | Analysis of non-PC electronics |
| | IoT forensics is the act of recovering evidence from network enabled devices that are not traditional computers. |
| | Forensic of the equipment which have internet connection data and which is not classified as computer or mobile forensic |
| | IoT forensics is the analysis of 'host' and network based artifacts of non-traditional devices that have little computers and the ability to communicate over the internet or within an intra-net. |

| Category | Response |
|---|---|
| IoT Network Traffic | Studying the underlying hidden data/communications being sent or stored by IoT type devices. This could include traditional networking appliances as well. |
| | IoT forensics consists of systems and methods to investigate potential incidents in IoT networks for creating, collecting, analysing and evaluating data as evidence. Compared to computer forensics IoT forensics can be seen as a specialization taking care of highly distributed, loosely coupled, unreliable networks and resource constrained devices. |
| | Acquisition and analysis of evidence from IoT devices. This can be evidence stored on device itself, or communicated elsewhere, and may include more abstract sources such as network patterns, etc. |
| | Imaging (capturing) and analysing volatile and non-volatile storage and network traffic related to an IoT device |
| Cloud | IoT is a branch of digital forensics which deals with IoT related crimes and includes investigation of the connected devices, the sensors as well as the cloud of data. |
| | Getting information from IoT devices which presented in court can be held as evidence. This can be in the cloud, in the network, in the device (chip-off) etc. |
| | IoT forensics is the acquisition and analysis of at-rest device and cloud-resident data from a sensor or single-function device. It is also the reverse-engineering and analysis of data in-transit between the IoT device and its ultimate destination. |
| Others | I think IoT is largely a buzzword for Internet connected devices that are "specific purpose computing" as opposed to "general purpose computing". Forensics is the usual definition of processes/tools to collect/analyse digital evidence. |
| | Dealing with evidence that relates to the IoT devices themselves (e.g. using them for illegal purposes, evidence of hacking attacks, etc.) and also evidence that has been gathered by IoT devices but relates to crimes that are otherwise unrelated (e.g. home security system knowing that a person was home at a particular time, cameras capturing events, GPS information from wearables, etc.). |
| | Why IoT forensics! It is all Forensic Research, some components are connected through any kind of protocol is that IoT? Of course IoT differs from other IT, but it remains part of Digital Forensics. |
| | The biggest difference between IoT forensics and other digital forensics is that IoT forensics is largely reverse engineering. IoT devices are so diverse that one can never be an 'IoT expert' and it is really more about the forensic analysis of unknown digital devices. |

## B COMPLETE SURVEY QUESTIONS

In the following is the complete survey questions:
Questions 1: What is your country of residence?

- Drop down list provided

Questions 2: Which age group do you belong to?

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+

Questions 3: What is your gender?

- Male
- Female
- Other

Questions 4: How many years have you worked in cyber forensics?

- Less than 1
- 1-3 years
- 4-6 years
- 7-9 years
- 10+ years

Questions 5: What is your primary occupation in cyber forensics?

- Law enforcement practitioner
- Non-law enforcement practitioner
- Industry instructor
- Professor
- Student
- Researcher
- Other

Questions 6: Which category does your occupation most fit into?

- Federal law enforcement
- State/local law enforcement
- Military
- Legal system
- Education/training facility
- Private sector organization
- Other

Questions 7: Do you consider IoT forensics as a sub-domain of cyber forensics?

- Yes
- No

Questions 8: Please rate how much you agree/disagree with the following definitions of what IoT is:

- The Internet of things is the internetworking of physical devices,vehicles,buildings and other items embedded with electronics, software,sensors, actuators,and network connectivity which enable these objects to collect and exchange data.
- Jeffrey Voas from NIST defines IoT using a model he calls the Network of things that relies on 4 key components to function, sensings, computing, communication and actuation. The network of things model relies on sensors, a communication channel, an aggregator, and the cloud in order to function
- The Internet of Things(IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.
- The Internet of Things is sensors and actuators embedded in physical objects that are linked through wired and wireless networks

Questions 9: What do you consider to be an IoT device? (Check all that apply)

- Smart Home Appliances
- Self Driving Cars
- Smart Phones
- Drones
- Hub based Internet devices (ex. Internet connected light bulbs)
- Internet connected sensors (ex. sensors monitoring power plants and factory machines.)
- Bluetooth peripherals
- Wearables (ex. Smart Watches)
- Home Assistants (Google Home, Amazon Alexa, etc)

Questions 10: Does an IoT device need to be constantly connected to the Internet?

- Yes
- No

Questions 11: Have you ever been involved with an investigation where you have to analyze IoT data?

- Yes
- No
- Not myself but I know of a colleague who has.

Questions 12: In your own words, what is IoT forensics?

- Text submission accepted

Questions 13: Would you consider yourself in a position to analyze an IoT device including its communications channels and network traffic?

- Text submission accepted

Questions 14: How would you rank the following issues IoT forensics is facing today (1 being the highest)?

- Software tools
- Funding
- Education
- Technical Training
- Legal Issues
- Technological Issues
- Data Security
- Cloud Data Storage
- Research

Questions 15: What evidence do you think we can acquire from IoT devices? Why is this evidence important?

- Text submission accepted

Questions 16: What are the areas that are most in need of improvements to forensic and software tools used on IoT devices?

- Data preservation
- Data Acquisition[Imaging]
- Cloud forensics

- Data Encryption
- Memory acquisition
- Device disassembly and forensic process
- Other

Questions 17: Which is the most challenging area to acquire IoT evidence from?

- Cloud storage
- On-device memory
- On-device storage
- Network

Questions 18: Please rate how much you agree or disagree with the following statements:

- Legislation regarding IoT cyber forensics is currently up to date
- Legislation is currently too broad regarding IoT forensics
- Data encryption presents a major problem
- Security on IoT devices is currently weak
- Finding data in the cloud presents a problem for IoT forensics

Questions 19:Where should research be focused in order to combat current issues? (select up to 2)

- Legislation updates
- Jurisdictional issues
- Cloud data forensics
- Preserving volatile data
- IoT Forensic Tools
- Breaking Data Encryption on IoT Devices
- Memory Retrieval

Questions 20:Please rate how much you agree or disagree that the following present a challenge to the future of IoT forensics:

- Data encryption
- Trail obfuscation(particularly as it
- Pertains to cloud forensics)
- Evidence modeling
- Limitations on local storage
- Legal jurisdiction
- Malware/device security issues
- Lack of digital forensic tools