2019

IOT Forensics Curriculum: Is It a Myth or Reality?

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Kemal Aydin
Franklin University, kemal.aydin@franklin.edu

Andy Igonor
Franklin University, andy.igonor@franklin.edu

May 16th, 10:00 AM

IOT Forensics Curriculum: Is It a Myth or Reality?

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Kemal Aydin
Franklin University, kemal.aydin@franklin.edu

Andy Igonor
Franklin University, andy.igonor@franklin.edu

IOT FORENSICS CURRICULUM: IS IT A MYTH OR REALITY?

Bilge Karabacak
Lead Faculty
Franklin University
Columbus, OH 43215
bilge.karabacak@franklin.edu

Kemal Aydin
Lead Faculty
Franklin University
Columbus, OH 43215
kemal.aydin@franklin.edu

Andy Igonor
Dean, Ross School of Business
Co-Executive Director, Center for Public Safety & Cybersecurity Education
Franklin University
Columbus, OH 43215
andy.igonor@franklin.edu

ABSTRACT

In this research paper, two questions are answered. The first question is "Should universities invest in the preparation of an IoT forensics curriculum?". The second question is "If the IoT forensics curriculum is worth investing in, what are the basic building steps in the development of an IoT forensics curriculum?". To answer those questions, the authors conducted a comprehensive literature review spanning academia, the private sector, and non-profit organizations. The authors also performed semi-structured interviews with two experts from academia and the private sector. The results showed that because of the proliferation of IoT technology and the increasing number of attacks against IoT devices, developing IoT forensics curriculum should be considered by the universities. It is worth mentioning that IoT forensics can be one of the main driving factors for securing IoT devices. However, because of the peculiarity and novelty of the domain, and the challenges of IoT forensics, it is difficult to prepare a course-centric curriculum at the very first step. Rather than doing this, universities can collaborate with various stakeholders from the private sector and government agencies to spot and study in real-world cases and let these cases build and evolve an IoT forensics curriculum.

Keywords: Internet of Things, cyber forensics, digital investigation, curriculum, semi-structured interview

1. INTRODUCTION

Internet of Things (IoT) is no longer an emerging technology today. It has quickly become mainstream with billions of IoT devices with IP addresses actively processing. According to a 2017 report by Gartner, there will be 20 billion IoT devices by 2020 (Hung, 2017).

For a long time, there were lots of devices with embedded circuits in almost every part of our lives. Today, IoT technology brings networking capabilities and Internet connectivity to traditional embedded devices (Watson, Labs, & Dehghantanha, 2016). Essentially, IoT can make almost every object in our lives smart through internet-connected devices so that they can interact with each other and exchange data. They can also be controlled and monitored remotely over the Internet or local networks.

There are lots of different IoT devices from different vendors in the market (S.Harichandran, Breitinger, Baggili, & Marrington, 2016). An IoT device is not a single element, but a group of devices working harmoniously to produce value for the humankind otherwise called an IoT network. An IoT network comes with lots of hardware and software components belonging to an IoT device itself and supporting equipment. These components may include but not limited to sensors, actuators, embedded circuits, mobile applications, communication channels, and cloud infrastructures (Voas & Laplante, 2017).

IoT devices have been used in almost every sector and every part of our lives. There are lots of IoT solutions to everyday problems. As a consumer, one can have smart door locks, trackers, bike locks & trackers, smart kitchen appliances, smart sprinkler systems, smart thermostats, and smart vents. Enterprise manufacturing, cutting-edge medical equipment, the latest agricultural innovations all use IoT devices to bring efficiency to their solutions.

The complexity and variety of IoT technology also bring with it lots of cyber vulnerabilities. According to a survey made by Gartner, nearly 20 percent of organizations observed at least one IoT-based attack in the past three years (Contu, Middleton, Alaybeyi, & Pace, 2018). Recent cyber incidents associated with IoT devices are shared here in the literature review section. IoT devices have more vulnerabilities compared to conventional information technologies (Watson & Dehghantanha, 2016) (Sha, Wei, Andrew Yang, Wang, & Shi, 2018). IoT brings many security challenges. Conventional endpoint security solutions such as antivirus software and device hardenings fail at IoT devices because of poor vendor security practices and constrained hardware (Yu, Sekar, Seshan, Agarwal, & Xu, 2015). Knowing that the proliferation of IoT hacking will increase with every passing day, it is not difficult to guess that IoT hacking will soon become commonplace. Almost every day one can see an IoT hacking incident in the media. So, it is vital to include IoT devices in digital investigations and understand the contribution of the devices to the security breaches and data leakages (Watson & Dehghantanha, 2016).

Besides, two factors can make a forensics investigator become motivated about IoT forensics. Firstly, IoT devices are directly associated with objects in our daily lives; the effects of cyber-attacks can be life-threatening (Nik Zulkipli, Alenezi, & B. Wills, 2017). Secondly, if successfully performed, IoT forensics can help to solve ordinary crimes like theft, vandalism, and as a result, it can be helpful to law enforcement (Meffert, Clark, Baggili, & Breitinger, 2017). Because compared with the traditional computer systems, more evidence from the physical world can be

extracted by investigating the IoT devices (R. C. Hegarty, Lamb, & Attwood, 2014). Therefore, forensic investigation of IoT devices is essential in solving cases and identifying cybercriminals.

However, IoT forensics is still an emerging topic. It comes with many challenges. IoT forensics tools and techniques are not mature. Even leading digital forensics software developers in the market may lack efficient IoT forensics tools. Challenges of IoT forensics emanates from the unique characteristics of IoT devices such as proprietary software and hardware, diversity of the devices and vendors, lack of standardization in the sector, insufficient storage spaces, storage of data in various location including cloud infrastructures, custom data formats (Conti, Dehghantanha, Franke, & Watson, 2018; Hossain, Fotouhi, & Hasan, 2015). IoT forensics is the missing piece of the evolution of connecting every device in the world (Watson & Dehghantanha, 2016). The challenges are detailed in the third section.

Despite the systemic challenges of IoT forensics, it is an essential topic, and its importance will increase with every passing day. So, organizations including universities should prepare for this challenge without delay.

In this paper, the authors make a comprehensive literature review on IoT forensics and share the results with the reader. Literature review covers up-to-date cyber incident statistics and recent remarkable IoT attacks, IoT forensics tools in the market and private sector's opinions, the efforts of the top universities in the United States, academic research on IoT forensics, and finally curriculum development efforts of the universities and academics. Literature review shows that the efforts on IoT forensics are still in its infancy. In addition to the literature review, the authors performed semi-structured interviews with two experts to discuss the need and essential steps of IoT forensics curriculum. Finally, the authors created the necessary building steps of the IoT forensics curriculum by using the results of the literature review and semi-structured interviews.

Paper organization is as follows. After the introduction, the literature review is done in the second section. There are six subsections of the literature review including discussion. After the literature review, the authors share the details of semi-structured interviews and the necessary steps towards building an IoT forensics curriculum in section three. Section four is the discussion and future work, and section five is the conclusion.

2. LITERATURE REVIEW

IoT forensics is a new topic compared to the other areas of digital forensics. Nevertheless, there are considerable amount of academic papers on this topic. Software companies are competing to release new tools or to add IoT device compatibility to their existing software. Literature review section has seven subsections. In the first subsection, recent IoT incident statistics and cyber attacks on IoT devices are shared. The implications of the incidents and the need for IoT forensics are discussed. The second subsection gives information about the tools in the market that makes IoT forensics. The second section also shares the opinions of the leading forensics companies on IoT forensics. The third subsection shares the results of the research on the curricula and other activities of the universities in the United States. The fourth subsection summarizes the specific research efforts on IoT forensics. The fifth subsection summarizes the textbooks that give place to IoT forensics. The sixth subsection summarizes IoT forensics/digital forensics curriculum development efforts by academia. The seventh

subsection is the discussion of the literature review.

2.1 INCIDENT STATISTICS AND IOT ATTACKS

2018 report from Trustwave company provides results on how companies and individuals using IoT devices are vulnerable to cyber-attacks. Survey results shared that 64 percent of surveyed organizations have deployed IoT devices. However, more than 30 percent of the organizations think that their IoT security strategy is not so important, or not important at all. Unfortunately, 61 percent of the surveyed companies have already experienced an IoT security incident (Josh Fruhlinger, 2018).

In October 2016, Mirai malware exploited vulnerable IoT devices like digital cameras and DVR players that have default usernames and passwords. The infected devices caused a very disruptive DDoS attack causing a number of websites going down including Twitter, the Guardian, Netflix, Reddit, and CNN (Nicky Woolf, 2016).

Again in 2016, the Food and Drug Administration confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to administer the device so that it can show incorrect pacing or shocks. The devices are used to monitor and even control the patients' heart functions and prevent heart attacks. This vulnerability potentially may result in the death of humans (Selena Larson, 2017).

Another vulnerability is seen in TRENDnet's cameras, which has been used in various cases like home security and baby monitoring. According to the TechNewsWorld, cameras had a vulnerability that let unauthorized people knowing the IP address of the device to see and sometimes listen to what camera captures (Richard Adhikari, 2013).

Fourth and last example is from the automotive sector. In 2015, two researchers exploited a vulnerability in Jeep, controlled the car by using a built-in cellular network feature. The researcher had the capability of speeding up, slowing down and steering it (Andy Greenberg, 2015).

The statistics and the recent incidents show how IoT devices are vulnerable, what may the effects of these vulnerabilities and how crucial it is to make efficient IoT forensics investigations.

2.2 IOT FORENSICS TOOLS IN THE MARKET AND PRIVATE SECTOR'S OPINIONS

Authors reviewed the products and services of leading digital forensics companies, which are FireEye, CYFOR, Guidance Software, AccessData, and Cellebrite. These companies are also the ones that had been selected by ABI research firm to analyze current digital forensics solutions that not only help organizations in detecting cybercrime but also predict and prevent such attacks from occurring (Sen & Menting, 2015). In addition to these companies, the authors also reviewed the products of Oxygen Forensics, Paraben Corporation, MSAB, and Magnet Forensics.

FireEye is the leading company that provides hardware, software, and services to fight with cyber-attacks, protect against malware. FireEye continually researches exploiting specific IoT devices including smart home systems, industrial control systems, and shares the results in the company blog page. In 2014, FireEye acquired Mandiant, which is the prominent cyber forensics company. Mandiant prepared very influential APT (Advanced Persistent Threat) reports that uncovered the state-sponsored cyber attacks against United States companies and networks. After this acquisition, FireEye started providing digital

forensics investigation and incident response as a service. They have a lot of experience and knowledge on cyber forensics, and they have been performing IoT forensics by using in-house developed tools and scripts. However, they do not sell or distribute any tools on cyber forensics including IoT forensics.

CYFOR is a service company based in the United Kingdom. Among their services, mobile forensics is noticeable as it resembles IoT forensics. However, there is no specific service on IoT forensics.

Guidance Software is the leading companies that develop software on digital forensics. According to a blog post by the company, Guidance software's EnCase Mobile Investigator works with the latest IoT and mobile devices (Udeshi, 2017). According to the blog post, EnCase Mobile Investigator supports Amazon Alexa cloud data, as well as data from drones, Fitbit smartwatches, Google Wear devices, and many more. EnCase Mobile Investigator product has the capability of investigating GPS devices, drones, smart watches, tablets, and smartphones.

AccessData is another leading company that develops popular FTK forensics software. The company has not developed any specific IoT forensics tool or software so far. Nevertheless, the company's whitepaper presents interesting and illuminating results on IoT forensics (Accessdata, 2017). The white paper reflects the results of the survey conducted by the participation of the nearly 200 representatives from the public sector. According to the survey, 75% of the surveyed officials experienced various technical problems with IoT device, including gathering evidence, preserving evidence, and presenting findings. Cloud acquisition is a crucial part of IoT forensics. 87% of the respondents stated the need for new tools to span multiple cloud solutions to capture and analyze data from the cloud.

Cellebrite develops devices that perform data extraction, transfer, and analysis for cellular phones and mobile devices. Their analytics solutions capture and analyze data from multiple IoT devices including drones, mobile devices, computer, telco, and cloud-based sources.

Oxygen Forensics Detective can make digital investigations on Amazon Alexa and Google Home. The product can also extract GPS locations from drones.

Paraben Corporation provides a 16-hour online IoT forensics training. The course covers nine different IoT environments. Paraben Corporation's E3 DS software product can be used to make forensic analysis on smartphones, GPS, tablet and IoT. The company does not provide the details of the IoT devices on that E3 DS product makes the analysis.

MSAB's XRY Drone product extracts, decodes and views data from leading drone models. The company also has products for data recovery from mobile devices, mobile forensics, and cloud forensics.

Magnet Forensics Axiom product has the capability of analyzing smartphones, cloud services, and IoT services.

Besides these companies, the efforts of a non-profit organization, the Digital Forensic Research Workshop (DFRWS) is worth mentioning. The mission of DFRWS is to cultivate cooperation among digital forensics professionals to address the emerging challenges of the field. The organization has created an IoT Forensic Challenge with the support of two researchers from the School of Criminal Sciences at the University of Lausanne and the private company Seculabs (DFRWS, 2019).

In conclusion, the private sector is aware of the importance of the IoT forensics, although the number of companies that have IoT

forensics products is minimal, and the maturity of the existent products is low. In general, companies are at the beginning phase of developing comprehensive IoT forensics products.

2.3 THE EFFORTS OF THE UNIVERSITIES

Authors reviewed the curricula and also dedicated research labs of the first 25 best engineering schools in order to mine the courses, programs, and research activities on digital forensics. U.S.News & World Report's best engineering school list is used while analyzing the top universities (U.S.News, 2018a). U.S. News is a trustworthy source for university rankings because they have a formal methodology and a variety of trusted data sources to validate their rankings (U.S. News, 2018b) (Wikipedia, 2018).

The review of the curricula of the top 25 US best engineering schools showed that only eight schools offer courses, programs or facilities like research labs on digital forensics. Among those, some of the universities are advanced in the area while some are at the beginning stages.

One of the universities that offer a comprehensive program in digital forensics is Carnegie Mellon University (CMU). CMU has a Cyber Forensics and Incident Response (CyFIR) Track, which has four courses. These courses are Applied Information Assurance, Host-Based Forensics, Network Forensics, and Cyber Forensics and Incident Response Capstone courses. The courses of the CyFIR track are hands-on and taught through the well-known CERT division of the university.

Purdue University is also doing comprehensive studies in the field of digital forensics. Purdue has a lab called Cybersecurity & Forensics Lab covering both applied and basic research. The other functions of the lab are providing training and consultancy to law enforcement bodies around the world. Purdue University has a rich curriculum that covers BS, M.S., and Ph.D. programs. The master level courses are Cyberforensics for the Apple Ecosystem, Cyberforensics of the Cloud and Virtual Environments, Cyberforensics of File Systems, Cyberforensics of Malware, and Network Forensics. Ph.D. level courses include Advanced Research Topics in Cyber Forensics and a workshop session that cover File Systems Forensics and Mobile / Embedded Device Forensics topics.

Georgia Institute of Technology has a Master of Science program in cybersecurity. It provides an elective network forensics course among other courses in cybersecurity domain. University also provides a standalone course named Digital Forensics for Incident Response once a year. It is designed as an introduction to digital forensics and incident response field.

University of Illinois--Urbana-Champaign provides two undergraduate courses in digital forensics area. What makes this university unique is that it provides these courses under the Digital Forensics Education Initiative. The initiative emphasizes the interdisciplinary nature of the digital forensics and includes the law, criminal psychology, sociology, and business domains in the courses. Two courses also have advanced technical topics such as mobile forensics, reverse engineering, and malware. University shares all course and lab materials with other institutions free of charge.

University of Southern California Viterbi School of Engineering provides Computer and Digital Forensics program, which is designed as a minor program for USC students. The minor program includes Digital Forensics, Advanced Digital Forensics, Digital Law and Privacy, Mac, OSX and iOS Forensics, Mobile Device Forensics, Cyber Breach Investigation, and two other cybersecurity related courses.

John Hopkins University's Whiting School of Engineering provides a Cybersecurity Master of Science program. Computer Forensics and Digital Forensics Technologies and Techniques courses are within the curriculum of the MS program

Northwestern University McCormick School of Engineering provides undergraduate-level Digital Forensics and Incident Response course within the Electrical Engineering & Computer Science Department.

University of Maryland Cybersecurity Center provides graduate-level Digital Forensics & Incidence Response course which emphasizes proper forensic handling of evidence, and legal aspects of national and international law regarding forensics.

Due to the space constraints, only the first 25 schools are analyzed, and the results are shared with the readers. American Higher Education System has more than 5,000 colleges and universities (Selingo, 2015). There might be universities that could have studied on IoT forensics with a much superior effort. As a future work, a more comprehensive literature review will be made to explore the efforts of other US-based universities.

Table-1 summarizes the current offerings of the universities. Carnegie Mellon University, Purdue University, University of Illinois--Urbana-Champaign, and the University of Southern California have comprehensive programs, initiatives, or lab on digital forensics. The other four universities provide an only limited number of courses. None of the universities has any course dedicated to IoT forensics. Cybersecurity & Forensics Lab within Purdue University is a noticeable effort because of the training, research, and consultancy it provides. These efforts provide necessary inspiration and foundational resources about how to build an IoT forensics curriculum. The multidisciplinary nature of the courses prepared by the University of Illinois--Urbana-Champaign should be taken as a good practice. The hands-on structure of lectures at Carnegie Mellon University is also another prime example of an effective digital forensics curriculum. Finally, the courses from the University of Southern California is an excellent example of diversity, decomposition, and granularity of the topics covered in digital forensics.

Table 1
Universities Offering Digital Forensics Courses or Programs

2018 U.S. News Ranking	**University**	**Summary of Courses & Major Efforts**
6	Carnegie Mellon University[1]	Four hands-on courses provided within Cyber Forensics and Incident Response (CyFIR) Track
7	Purdue University[2]	Cybersecurity & Forensics Lab (For research, training, and consultancy) Advanced and rich courses that cover BS, M.S., and Ph.D. students

[1] https://www.cmu.edu/ini/academics/cyfir.html
[2] https://polytechnic.purdue.edu/facilities/cybersecurity-forensics-lab

2018 U.S. News Ranking	**University**	**Summary of Courses & Major Efforts**
8	Georgia Institute of Technology[3]	One elective network forensics course at master level One standalone course opened once in a year (open to the public)
9	University of Illinois--Urbana-Champaign[4]	Two interdisciplinary and hands-on courses prepared by Digital Forensics Education Initiative (University shares all course and lab materials with other institutions free of charge)
10	University of Southern California[5]	Computer and Digital Forensics minor program that has 8 courses
18	John Hopkins University[6]	Two courses provided within the Cybersecurity Master of Science program
20	Northwestern University[7]	One undergraduate-level course within the Electrical Engineering & Computer Science Department
22	University of Maryland[8]	One graduate-level course provided by Cybersecurity Center

[3] http://catalog.gatech.edu/programs/cybersecurity-ms / https://pe.gatech.edu/courses/digital-forensics-for-incident-response
[4] http://publish.illinois.edu/digital-forensics/curriculum
[5] https://itp.usc.edu/academics/computer-digital-forensics/
[6] https://ep. jhu.edu/programs-and-courses/programs/cybersecurity
[7] https://www.mccormick.northwestern.edu/eecs/courses/
[8] http://www.cyber.umd.edu/education/grad-classes

2.4 ACADEMIC RESEARCH ON IOT FORENSICS

There is remarkable academic research on IoT forensics. These research activities not only propose solutions on specific challenges of IoT forensics but also shed light into possible additions to an IoT forensics curriculum.

Karabiyik and Akkaya provide a comprehensive overview and classification of IoT forensics research and applications in the device, network, and cloud levels (Karabiyik & Akkaya, 2018). Authors also share the challenges of the domain and areas for future research.

Meffert et al. summarizes the challenges of digital investigations associated with IoT devices and proposes FSAIoT, a centralized Forensic State Acquisition Controller implemented by an open source IoT device controller named OpenHAB (Meffert et al., 2017). FSAIoT can collect "controller to IoT device", "controller to cloud", and "controller to controller" states of IoT devices to determine the sequence of events occurred. Researchers performed a proof of concept implementation of FSAIoT framework to share the results with other researchers. In their proof of concept, they have used various IoT devices including IP camera, door sensor, motion sensor and IP camera controller to secure a server room. They used the log files stored in the IoT device controller's file system. Log files are used to store the device states and timestamps of the states. They extracted the timeline of the events from beginning to the end of the events such as door open, door closed, motion detected, camera captures suspect, and again door open and finally door close. Researchers' argument was leveraging the acquisition of the state of IoT devices helps painting a clear picture of events. They show the correctness of this argument by implementing a proof of concept. FSAIoT framework is a proof of concept study. Researchers should improve FSAIoT's features so that it would gather historical data, acquire data from many devices, and be compatible with different network connection types. Without improvements like these, the framework is far from being a practical tool to be used in real-world investigations.

Zulkipli et al. also stresses the difficulties of IoT forensics investigations and brings two approaches to ensure that evidence is collected and preserved throughout the investigation (Nik Zulkipli et al., 2017). These approaches cover the pre-investigation phase and investigation phase, which is implemented by the proposed real-time investigation. Pre-investigation phase is the readiness of the organization and forensics investigators before cyber incidents occur. There are two classes of pre-investigation readiness. These are management readiness and technical readiness. Management readiness includes obtaining management support, having training, preparing documents like investigation strategy, policies, and procedures among other things. Technical readiness includes the process of scoping meaning that the investigator should be able to narrow down potential pieces of evidence and devices to make faster and efficient investigations. The real-time investigation consists of monitoring the IoT devices for abnormalities, and once an abnormal behavior is detected, it consists of identifying, collecting and preserving the data concurrently and automatically. A real-time investigation has three components. These are time synchronization, sufficient memory and storage, and stable communication among components. The article does not share any pilot application for the proposed result. Also, the technical details of the real-time investigation are limited in the paper.

Hegarty et al. discusses the fundamental, overarching challenges of IoT forensics, and

identifies the key areas that solutions should target (R. C. Hegarty et al., 2014). Authors summarize the IoT forensics challenges in four distinct phases of a forensics investigation. These phases are identification, preservation, analysis, and presentation. For the identification phase, the primary challenge is the uncertainty of where the data is stored, and also the data came from. Authors propose using the National Building Information Model Standard to integrate IoT data into the standard[9]. For the preservation phase, the authors state the complexity of data volatility in IoT environments. Authors recommend further research to determine the technical and legal implications under various circumstances. They also emphasize that the scope of the warrants should be extended to cover both individuals and service providers because IoT data is stored in the cloud. For the analysis phase, the authors state the interaction between IoT devices and cloud environments and emphasize the technical and legal difficulties of analyzing the data in the cloud. Authors recommend distributed data analysis techniques to analyze the data in the cloud, which is also an academic study (R. Hegarty, Merabti, Shi, & Askwith, 2012). For the presentation phase, the authors state the conflicting grammar of the data among different IoT devices. Because of the limited memory, battery, bandwidth resources of IoT devices, they use lossy compression techniques and so granularity of data may reduce. There are some works on standardization of metadata and using Ontological descriptors; however, the adoption of these standards is limited.

Oriwoh et al. propose a 1-2-3 Zones approach and Next-Best-Thing Triage (NBT) Model for IoT forensics investigations (Oriwoh, Jazani, Epiphaniou, & Sant, 2013). 1-2-3 Zones approach answers the question of "where to look?" for digital forensics investigators. The zones are an internal network, gateway/boundary services, and cloud services respectively. The NBT model is used to determine which devices were connected, which pieces of evidence were left behind after its removal from the network. Authors say that evidence can be acquired from devices that are either directly connected or somehow linked to the IoT devices that are not available.

As a result, the academic works on IoT forensics emphasize the challenges specific IoT forensics and propose solutions. However, academia is at the beginning of devising comprehensive and established solutions to the challenges. Recommended solutions can be classified into two main domains. The first domain consists of procedural, processual, legal, organizational improvements of the preparation, data acquisition, analysis, and presentation steps. Second domain consists of some technical contributions. However, most of the technical improvements are dedicated to specific cases and needed to be studied more to make these methods more efficient and universal.

2.5 BOOK CHAPTERS ON IOT FORENSICS

Authors reviewed three textbooks that have dedicated chapters on IoT forensics.

Lakhani and Muniz's book on digital forensics gives a section to IoT forensics under chapter-7: Endpoint Forensics (Lakhani & Muniz, 2018). The section gives an overview of the IoT forensics by sharing general characteristics of IoT devices and listing IoT data collection points.

Reiber's book on mobile forensics investigations has two chapters on IoT (Reiber, 2018). Chapter-3 gives information about IoT devices. Chapter-16 focuses on the forensic analysis of IoT, wearables, and drones. Chapter-16 shares the details of the device and

[9] https://www.nationalbimstandard.org

cloud-based forensics investigation for Amazon Alexa, Google Home, Apple Watch, Fitbit, and Drone of DJI.

Van Duren and Russell's book on IoT security spare a chapter on IoT forensics (Van Duren & Russell, 2018). The title of the chapter is the IoT Incident Response and Forensic Analysis. Book gives general guidelines for incident response and forensic analysis of incidents involving IoT devices. Dedicated chapter on IoT forensics also shares many external resources for forensic investigation and analysis of the IoT devices.

2.6 CURRICULUM DEVELOPMENT EFFORTS

IoT forensics is a new and emerging area. It has many technical challenges because of the nature and diversity of the devices. Currently, there is no study by universities to develop a focused and dedicated IoT forensics curriculum. Nevertheless, there are some efforts by academics and universities. This subsection is dedicated to these efforts.

University of Illinois--Urbana-Champaign hosted four workshops between 2013 and 2016. The workshop is named "Digital Forensics Curriculum Standards Workshop" and funded by the National Science Foundation. The 2016 workshop gave place to IoT forensics under the dedicated session titled "New Topics for Digital Forensics Curriculum". The other two topics in the session were "Mobile Device Forensics" and "Cloud Forensics".

Voas and Laplante share their ideas about IoT Curriculum (Voas & Laplante, 2017). The focus of their paper is not about IoT forensics. They propose curricular topic recommendations by organizing the topics according to the Computer Science Curricula 2013, which is a joint publication of the IEEE Computer Society and ACM. There are numerous academic papers about the preparation of digital forensics curriculum. (Bashir, Applequist, Campbell, DeStefano, & Garcia, 2014; Cruz & Duffany, 2012; Tu, Xu, Wira, Balan, & Cronin, 2012). Bashir et al. propose a multidisciplinary undergraduate curriculum. Cruz and Duffany propose a graduate certificate program. Tu et al. offer a digital forensics program both for undergraduate and graduate levels. Neither of these studies mentions IoT forensics topic.

One of the most attention-grabbing academic studies on IoT is the Internet of Things Bachelor of Science degree prepared by Florida International University Department of Electrical and Computer Engineering[10]. The degree has online course offerings as well[11]. BS degree has a vibrant and diverse curriculum. Among courses offered, there is an elective course titled IoT Forensics. The prerequisite of the course is Embedded Programming for IoT. There is no further information found online about the course. The other forensics courses are Introduction to Digital Forensics Engineering and Introduction to Malware Reverse Engineering; both are electives. Florida International University is the 145th university in the list of U.S. News & World Report's best engineering school list. To the best knowledge of the authors, it is the only university in the United States that provides a specific curriculum on IoT.

2.7 SUMMARY AND DISCUSSION

To summarize, IoT attacks will soar up because of the inherent vulnerabilities of IoT devices. As a worst-case scenario, the attacks have the potential of threatening human life directly. Most forensics companies are unprepared for what is coming. The limited

[10] https://internetofthings.fiu.edu

[11] https://fiuonline.fiu.edu/programs/online-undergraduate-degrees/bachelor-of-science-in-internet-of-things.php

number of universities have research activities and dedicated curriculum in digital forensics. Worse than that, IoT forensics is not even on the agenda of the universities. Academic research efforts on IoT forensics is very isolated and far from producing practical and efficient solutions. Currently, there are no curriculum development efforts on IoT forensics. There are only a few promising efforts by universities like Florida International University and Purdue University among some others. The number of universities doing IoT forensics research is in dire need of an increase. IoT forensics research should help to create and to build IoT forensics programs with cutting-edge curricula.

3. RESEARCH

The authors of the current study performed semi-structured interviews with two forensics experts to determine the primary constructs of an IoT curriculum, which are presented in this section. Research made for the effort of discovering IoT forensics curriculum was purely qualitative. Therefore, the interview results were qualitative, and they were evaluated qualitatively by the authors. The subsections in section-3 are built by consolidating the answers of the domain experts.

All of the questions of semi-structured interviews were open-ended questions about the IoT forensics and IoT forensics curriculum. Interview questions did not have multiple-choice answers. The respondents were allowed to answer the questions freely without any pressure from the authors. The requested information was qualitative rather than quantitative.

During the research, semi-structured interviews were used as the initiator of the long-lasting and evolving interviews among each expert and author.

Selection of the experts was made purposefully by the authors according to (Coyne, Dipn, & Rgn, 1997). Experts have much experience in their fields. Authors consider that those experts would provide valuable information for the research. The first expert has more than five years of theoretical and hands-on experience in the digital forensics field. He was also the manager of a governmental forensic laboratory. He made many forensics investigations throughout his career. The second expert also has much past practical experience in digital forensics area as a forensics investigator. He has a Ph.D. degree in cybersecurity and is currently working as a full-time faculty at a research university.

Semi-structured interviews are made by each expert individually to prevent any bias. The authors managed the interviews, asked further questions, and requested clarifications on the matters. Semi-structured interviews were conducted exhaustively until saturation; namely until the authors had nothing else to contribute.

The initial questions were:

1. What are the specific technical challenges of IoT forensics?
2. What are the specific legal challenges of IoT forensics?
3. Is the IoT forensics worth preparing a specific curriculum/program for a university? Why?
4. What specific action should take a university to address the challenges specific to IoT forensics domain? Please feel free to speak every aspect including courses, research activities, cooperation, and collaborations.
5. Which kind of stakeholders should a university be in contact with? If the university is planning to have an IoT forensics curriculum?
6. Which courses should an IoT forensics curriculum have?

7. What do you think about the interdisciplinary nature of IoT forensics? What kind of topics resides in the intersection of technical IoT forensics curriculum with other technical/non-technical fields? Do these fields have to be addressed in the curriculum? To what extent?
8. There are thousands of different IoT devices has been using in many different sectors? How should a university handle this complexity?

The following subsections are composed by analyzing, organizing and consolidating the ideas of the experts and the literature as well. There are three subsections. In the first subsection, the IoT forensics ecosystem is introduced. The second subsection shares the main activities of a research lab pursuant to IoT forensics challenges. The third subsection gives the list of the possible courses in an IoT forensics curriculum.

3.1 IOT FORENSICS ECOSYSTEM

Preparation of an IoT forensics curriculum is not an easy-going effort. It is not only to specify, prepare and lecture the courses but also always to keep in contact with communities and to support the curriculum with a laboratory.

A university should not be perfectionist while preparing an IoT curriculum. Instead, it should start doing supporting activities as soon as possible and let the curriculum be mature in the progress of time.

There should be two essential supporting processes for the IoT forensics curriculum because IoT forensics is a very specialized and unique topic. Firstly, a research lab must support the curriculum. Secondly, the university should maintain close contacts with relevant stakeholders including vendors and the government.

IoT forensics is a developing topic. It may not be feasible to prepare a course-focused curriculum at first because of the immaturity of the tools and techniques in this domain. At this phase, research on IoT forensics is an essential means in order to explore the topic, to become familiar with the challenges, and to find solutions that also support the curriculum.

The flowchart in Figure-1 shows the main activities of the university that is planning to start an IoT forensics curriculum. The flowchart is prepared by taking the main points of the interviews and literature into account. It also shows the interrelations of the activities. It does not show every detail. Note that a university can adopt a completely different approach, so the flowchart should be taken as a suggestion.

Because of the novelty of the topic, the IoT forensics research laboratory should be in the center of all activities. The focus of the laboratory would be to make both basic and applied research. It would be a feasible option to get government funding to set up an IoT forensics lab. The possibility of receiving government funding is high because of the current situation and the dynamics IoT forensics topic. Digital forensic capabilities of IoT forensics are not on pace with digital forensics of traditional computer technologies (Watson & Dehghantanha, 2016). So, the authors recommend that researchers should seek related government funds in this area. The first critical step that a forensics lab should take is to communicate with the government bodies, especially Law Enforcement Agencies (LEAs), in order to learn current requirements. Note that requirements would help to prioritize the research studies because there are lots of IoT devices, vendors. LEAs would provide proper answers to the questions like "Which

areas/devices are the most challenging for agents? In which areas are they stuck technically? Which devices are mostly associated with cyber crime investigation?" IoT forensics lab should procure the IoT devices and software by taking the requirements into account. IoT lab should gather the requirements not only by contacting external governmental bodies but also by making research on current trends, emerging devices, significant attacks incessantly and consistently. Finally, the IoT forensics lab should convert the requirements of LEAs into the new tools and techniques. The lab should present and share these tools with the related government agencies.

The other introductory step that an IoT forensics lab should take is to get in contact with the forensics tools vendors and to obtain tools to be used in the research laboratory. Vendors may not be willing to give their tools. At this point, the number and profiles of the students in digital forensics courses and relations of the university with the government agencies may make the vendors more eager to give their tools. As an example, if the university is providing certificate programs and online courses for the working professionals from the private sector and government agencies, and if these professionals are forensics investigators in particular; the vendors would be happy to provide their tools for the sake of promotion and presentation of their tools. Undergraduate students may not impress the vendors; however graduate students, who are seeking ways to improve their skillset would impress. If the laboratory has good relationships with the LEAs, again the vendors would be more willing to give their tools to the university. There are lots of research areas that a forensics lab can pursue. The research should focus on the areas of the IoT specific challenges. These challenges are shared in section 3.2.

A mature IoT curriculum is a long journey. It should start on the first day the funding has been received, and the research lab has begun to operate. At first, the curriculum will have traditional courses on forensics like operating system forensics, network forensics and fewer courses on IoT specific forensics. As IoT forensics lab conducts research on the challenges and makes collaboration with stakeholders, the curriculum will evolve, and more IoT specific courses will be added. The curriculum should already have the foundational courses that help understand the structure of IoT devices like embedded systems and also the courses about legal issues. While IoT forensics lab provides new tools, techniques, and materials like labs, not only the content but also the scope of the curriculum will evolve. It may start with a certificate program, then transform into a minor program and evolve into a graduate-level program. The details of the courses of the proposed curriculum are shared in section 3.3.

IoT forensics lab should also get in contact with the standard bodies like ISO, NIST. One of the forensics challenges associated with IoT devices is the lack of standards in hardware, software, data formats, and log standards. IoT forensics lab may provide its opinions and implications on standardization of specific technologies to the standards bodies. These ideas can be discussed in groups and committees, and finally, IoT vendors may be required to follow certain standards. It is worth reminding that legal authorities may request data from their IoT products in the near future (Watson & Dehghantanha, 2016). The collaboration with the standards bodies will increase the capability of the devices so that forensics investigators may gather evidence efficiently and without losing time. The details of the relations like industry partnerships, public and private partnerships, are out of the scope of this paper.

Finally, the IoT forensics laboratory should have a public face. It is worth mentioning at this point that IoT forensics can be one of the main driving factors for securing IoT devices. One of the focus points of the IoT forensics lab should be the security of IoT devices. By using the results of the pilot studies and cases, the laboratory will come with the ideas to secure the IoT devices and environments to stop the cyber attackers. Therefore, IoT forensics laboratory should present hardening guides, procedures, checklists, tutorials in a public portal.

To conclude, the primary goal of the forensics laboratory should be creating an IoT forensics ecosystem. There are a lot of stakeholders, interrelationships, inputs, and outputs in this ecosystem as seen at Figure-1. The most course-centric part of this ecosystem is shown in rectangle without round edges on the left. This rectangle is the part where most curriculum-related activities are done. Because of the peculiarity of the topic, there are several prerequisite studies in order to create a comprehensive curriculum that meets the needs. IoT curriculum is one of the essential outputs of an IoT forensics ecosystem as it can be seen in the Figure-1.

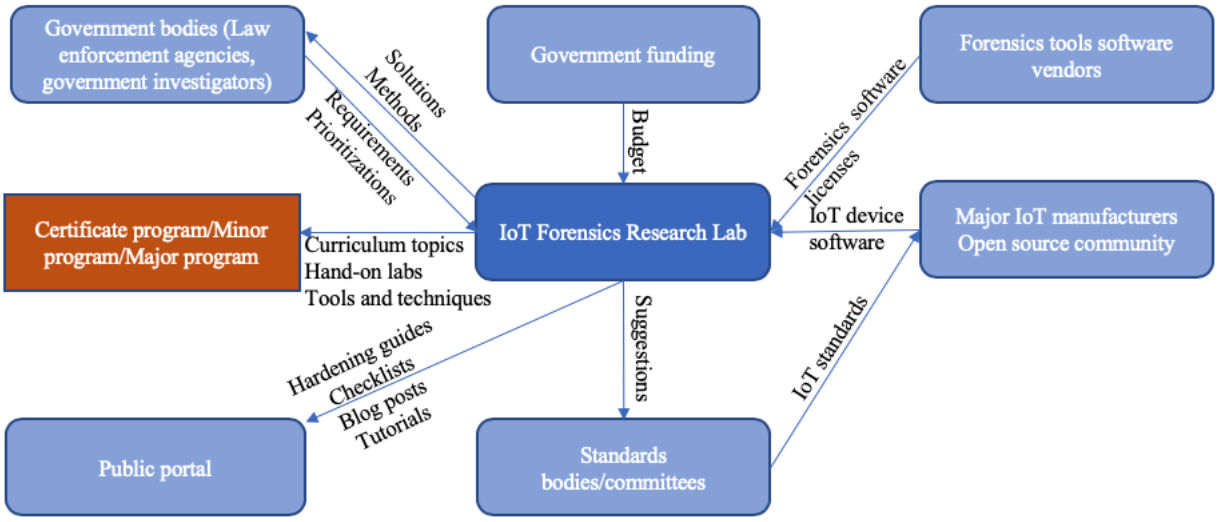

Figure 1. IoT Forensics Ecosystem

3.2 IOT FORENSICS CHALLENGES AND ACTIVITIES OF THE RESEARCH LAB

There are many challenges associated with IoT forensics. Challenges of IoT forensics emanate from the unique characteristics of IoT devices. Challenges can be consolidated into two groups, and these are technical challenges and legal challenges. IoT forensics laboratory should be the primary driving source of the solutions to the challenges of the IoT forensics domain. The curriculum should also address these challenges by taking appropriate actions and precautions in course materials, labs. However, the research activities in the research lab should precede the course and lab content. Research activities should be shaped by not only the requirements from government agencies but also from the challenges written in this subsection.

Diversity in the IoT domain is a salient challenge all by itself. There are lots of different usage areas of IoT from hearth batteries to garage doors. The diversity of usage areas results in the extreme variety of vendors. Hence, there is a vast diversity in technical features, operating systems, interfaces, communication protocols of IoT devices. (Nik Zulkipli et al., 2017) (Meffert et al., 2017). The research lab should procure the most commonly used tools first. The courses in the curriculum should give place to commonly used devices and operating systems and should have hands-on labs for commonly used devices.

The technology of IoT devices is mostly proprietary. Therefore, traditional digital forensics tools and techniques are mostly insufficient in dealing with IoT devices (Meffert et al., 2017). Because of the proprietary nature of IoT devices, forensic investigators should have experience in reverse engineering techniques; therefore, one of the activities of the lab should be to research reverse engineering specific to IoT devices. The curriculum itself should include reverse engineering topics.

Most IoT devices store very limited or no data and logs. Their local storage capabilities are very limited as well. They mostly store volatile data. Data volatility is the result of using real-time operating systems in IoT devices. (Meffert et al., 2017). In order to overcome data volatility and limited log data, investigators should deal with not only the IoT itself but also with the controller, network infrastructure, and mobile applications. To address these problems, the research lab should setup realistic IoT networks.

The data associated with the IoT device can be scattered not only to the various locations inside the network but also to the outside of the network (Attwood, Merabti, Fergus, & Abuelmaatti, 2011). It is quite common for IoT devices that the data is stored in the cloud and the device communicate with the server in the cloud. Forensics investigators who are dealing with IoT devices should try to extract data not only from an IoT device and supporting devices but also from the cloud servers. Hence the lab should do specific research on acquiring data from cloud infrastructures. The curriculum should include cloud-based forensics techniques as well.

The last two challenges are associated with the legal implications of the IoT forensics. The research laboratory should also deal with legal challenges. Because data associated with the IoT device may be stored in the cloud and scattered in different jurisdictions, digital forensics investigators may face legal challenges in accessing the data (Meffert et al., 2017). Investigators should also be educated on dealing with different jurisdictions as a result of the cloud-based infrastructures in action.

Privacy can also be a concern for the IoT forensics investigators. Many IoT devices are used personally, and they may reveal private data about individuals. To overcome privacy conflicts and prevent the problems associated with privacy, forensics investigator should know of the principles of privacy and enacted privacy laws in their jurisdictions.

3.3 PROPOSED COURSES

Independent from the IoT devices, digital forensics is naturally an inter/multi-disciplinary domain of study. University of Illinois--Urbana-Champaign has an excellent multidisciplinary curriculum that has two courses. The curriculum covers the domains of law, legal system, and psychology.

There should be two distinct domains that IoT forensics curriculum should cover. The first domain is technical, which focuses on IoT technology and the technical aspects of IoT forensics; and the second part is regulatory, which focuses on the laws and regulations associated with IoT devices. In this regard, the

proposed IoT curriculum is multidisciplinary. There is also an intersection of these two domains in which laws and regulations specific to the IoT technology emerge as shown in the Figure-2. The intersection of technology and regulation domains is the interdisciplinary part of the proposed curriculum.

When investigated from the perspective of IoT technology, one can come up with the ideas that should be covered in the courses. First of all, mobile device forensics is strongly relevant to IoT forensics. (Meffert et al., 2017) Many IoT devices are controlled and monitored by mobile applications. Also, some IoT devices may use a modified mobile operating system (Watson & Dehghantanha, 2016).

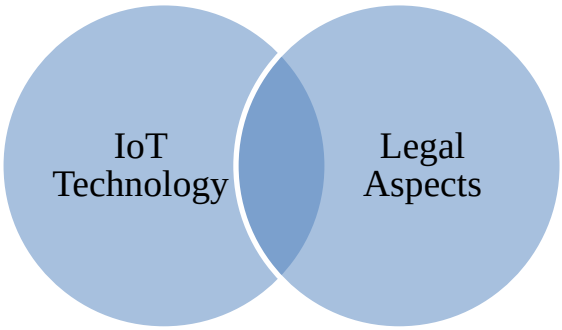

Figure 2. Disciplines of the Proposed Curriculum

Some typical operating systems are used in IoT devices[12]. RIOT OS, Windows 10 for IoT, Google Brillo, WindRiver VxWorks are among those operating systems. Therefore, IoT forensics curriculum should cover operating systems course that not only gives the basic concepts of operating systems but also focuses on IoT specific operating systems. The theory and also the practical aspects of cloud infrastructures should be lectured in the courses. The course should include commonly used cloud infrastructures such as Amazon AWS, Microsoft Azure, and Google Cloud. IoT devices are associated with the non-IP (Internet Protocol) based communication technologies like sensor and RFID technologies (Oriwoh et al., 2013). One of the courses in the curriculum should handle these topics.

The curriculum should cover the topics of embedded device technology, reverse engineering techniques of embedded devices, and decompiling of embedded software. These topics are fundamental to understand what the application is doing and where the data is being saved (Watson & Dehghantanha, 2016).

IoT forensics can be studied in three distinct but intersecting zones, which are the cloud, network, and device (Zawoad & Hasan, 2015; Karabiyik & Akkaya, 2018). Analysis of the network traffic can provide clues about what the device is doing and where the data are stored (Watson & Dehghantanha, 2016). Therefore, network forensics should also be covered by the IoT forensics curriculum.

The curriculum should include standardization studies in the United States and around the world. As an example, NIST Computer Security Resource Center's SP 800-183 Networks of 'Things' should be covered in the curriculum. Wikipedia is a valuable resource to see the standards and standards

[12] https://www.informationweek.com/iot/8-iot-operating-systems-powering-the-future/d/d-id/1324464

organizations associated with the IoT domain[13].

Legal aspects of the IoT forensics should be covered within the curriculum. The course should cover both general topics around the legal aspects of forensic investigation and specifics to IoT forensics. The curriculum should answer the question of how to deal with the data in the cloud? In today's interconnected world, data may cross the boundaries and reach a different jurisdiction (Oriwoh et al., 2013). So, it may be needed to contact with different countries to collect evidence (Nik Zulkipli et al., 2017). International organizations such as OECD has been working for decades on the different aspects of the trans-border flow of data. The curriculum may include these studies as well.

Another question related to the legal challenges is how to seize personal devices under privacy laws? Therefore, the curriculum should include current privacy laws and the main steps in a digital investigation in order to avoid the violation of the law.

It is not feasible to include all the topics in the curriculum at once because of the technical, time and budgetary limits. There are lots of advanced topics associated with the IoT forensics. These topics include but not limited to big data analytics, visualization, fixed computing, distributed computing, and artificial intelligence (Oriwoh et al., 2013; Voas & Laplante, 2017). The sky is the limit when it comes to IoT forensics. Hardware forensics techniques like JTAG, chip-off, and ISP would help in forensics investigations of IoT devices (Watson & Dehghantanha, 2016). However, these are unique and advanced topics. Decryption and decoding of the unreadable data are other advanced topics that can be covered by IoT curriculum. These topics can be included in the curriculum in the upcoming terms and years, in harmony with the evolution of the curriculum and lab activities.

A general curriculum on IoT would help to create and to mature the IoT forensics curriculum. At the end of the day when we look at the evolution of an IoT forensics curriculum, most probably we would see the IoT-specific courses at first. In this regard, the efforts of Florida International University (FIU) on IoT degree curriculum are quite robust. Notably, the IoT core courses in the curriculum of FIU are supportive of building capacity for the IoT forensics courses in the upcoming phases.

One of the most critical efforts in preparing courses from the outputs of the research activities is to give weight to the theoretical approaches and make it vendor-independent as much as possible. IoT forensics curriculum should not be vendor-specific or biased to any specific technology. Although the hands-on material and practices can be technology-depended as one expects, the general approach of the courses should be more inclusive and vendor-agnostic.

To conclude, the recommended courses or course topics included under this subsection are summarized in Table 2. Institutions that are planning to start an IoT forensics curriculum may also consider the courses offered in the IoT degree program of the Florida International University.

[13] https://en.wikipedia.org/wiki/Internet_of_things

Table 2
Proposed Curriculum

No	Course / Course topics	Response's domain (See Figure-2)
1	Mobile device forensics	IoT Technology
2	Operating system with a focus on IoT	IoT Technology
3	Cloud computing and cloud infrastructures	IoT Technology
4	Telecommunication technologies (sensors, RFID etc.)	IoT Technology
5	Embedded devices and reverse engineering with a focus in IoT	IoT Technology
6	Network forensics with a focus on IoT	IoT Technology
7	IoT standards	IoT Technology / Legal Aspects
8	Legal aspects of digital forensics with a focus on privacy and cross-border data flow	Legal Aspects / Intersection of the Technical and Legal Domains

4. DISCUSSION AND FUTURE WORK

Before preparing this paper, the authors conducted research to answer research questions. These questions were:

1. Should universities invest in the preparation of an IoT forensics curriculum?"
2. If the IoT forensics curriculum is worth investing in, what are the basic building steps in the development of an IoT forensics curriculum?

To answer these questions, the authors did semi-structured interviews with two experts and also performed a comprehensive literature review spanning universities, private organizations, and non-profit organizations.

Authors hope that the research revealed valuable results for the institutions in higher education. Authors consider this study as the very first step of the effort to answer these questions. After conducting research, the authors came up with clear answers and provided those answers in this article. However, the IoT technology and forensics topics are comprehensive. Therefore, authors think that further research might help to provide more clear and focused answers to these research questions. Literature review focused on mainly academic works, private sectors and slightly on the non-profit organizations. Contacting government agencies including LEAs, extending research on the studies of non-profit organizations, primarily focusing on standardization organization will help to reach interesting and helpful results on IoT forensics roadmap. With the same purpose, making focus group interviews with more experts in cybersecurity and digital forensics domains will help to obtain results useful for the institutions in higher education.

With these ideas in their minds, authors are planning to research the gaps in current IoT standards in the perspective of forensics so

that it is aimed to determine any need for a new standard and improvements in the current standards.

As another future work, authors are planning to set up a meeting with the scholars in the Florida International University to discuss the topics around IoT forensics, as the FIU has made much progress in the subject of IoT technology.

Finally, Franklin University offers a rich cybersecurity curriculum to its students. Franklin University provides online courses for working professionals all around the United States. Franklin University also manages the Center for Public Safety & Cybersecurity Education, which makes collaboration with local communities, LEAs, and the private sector. Therefore, Franklin University is a suitable institution to start a pilot application and then apply for a government fund. As the very first step, scholars in the Franklin University are planning to get the primary challenges they face during investigations from the local LEAs.

5. CONCLUSION

Our goal with this article is to provide a set of necessary steps for the institutions in higher education to use when creating a curriculum on IoT forensics. Although a limited number of academic curriculum efforts on IoT forensics can be seen today, it will not be the case for tomorrow. Because of the proliferation of IoT technology and the increasing number of attacks against IoT devices, the creation of IoT forensics curriculum will be inevitable by the universities. Because of the peculiarity and novelty of the domain, and the challenges of IoT forensics, universities should be in the center of the efforts of creating an IoT forensics ecosystem. This ecosystem should have various stakeholders from the private sector, government agencies, and non-profit organizations.

REFERENCES

Accessdata. (2017). The Future of Data Is Here, and There's No Going Back: The Public Sector's New Paradigm.

Andy Greenberg. (2015). Hackers Remotely Kill a Jeep on the Highway—With Me in It | WIRED. Retrieved January 5, 2019, from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/?mbid=social_twitter

Attwood, A., Merabti, M., Fergus, P., & Abuelmaatti, O. (2011). SCCIR: Smart Cities Critical Infrastructure Response Framework. In A. Hussein, H. Tawfik, D. Al-Jumeily, A. K. Nagar, & O. Abuelmaatti (Eds.), 2011 Developments in E-systems Engineering (pp. 460–464). Dubai: IEEE Computer Society.

Bashir, M., Applequist, J. A., Campbell, R. H., DeStefano, L., & Garcia, G. L. (2014). Development and dissemination of a new multidisciplinary undergraduate curriculum. ADFSL Conference on Digital Forensics, Security and Law, (c), 161–170.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546. https://doi.org/10.1016/J.FUTURE.2017.07.060

Contu, R., Middleton, P., Alaybeyi, S., & Pace, B. (2018). Forecast: IoT Security, Worldwide, 2018.

Coyne, I. T., Dipn, H., & Rgn, R. (1997). Sampling in qualitative research. Purposeful and theoretical sampling; merging or clear boundaries? Journal of Advanced Nursing, 26(3), 623–630.

Cruz, A., & Duffany, J. (2012). Development of a Graduate Certificate Program in Computer Forensics. In Tenth LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2012). Panama City. Retrieved from http://laccei.org/LACCEI2012-Panama/RefereedPapers/RP014.pdf

DFRWS. (2019). Forensic Challenge. Retrieved January 5, 2019, from https://www.dfrws.org/dfrws-forensic-challenge

Hegarty, R. C., Lamb, D. J., & Attwood, A. (2014). Digital Evidence Challenges in the Internet of Things. In Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis.

Hegarty, R., Merabti, M., Shi, Q., & Askwith, R. (2012). Scalable Distributed Signature Detection. In Proceedings of the 7th International\ Workshop on Digital Forensics & Incident Analysis (pp. 27–37). Heraklion, Greece.

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In 2015 IEEE World Congress on Services (pp. 21–28). IEEE. https://doi.org/10.1109/SERVICES.2015.12

Hung, M. (2017). Leading the IoT: Gartner Insights on How to Lead in a Connected World. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Josh Fruhlinger. (2018). Top cybersecurity facts, figures and statistics for 2018 | CSO

Online. Retrieved January 5, 2019, from https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html

Karabiyik, U., & Akkaya, K. (2018). Digital Forensics for IoT and WSNs. ArXiv:1811.09239 [Cs]. Retrieved from http://arxiv.org/abs/1811.09239

Lakhani, A., & Muniz, J. (2018). Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer (First Edition). Cisco Press.

Meffert, C., Clark, D., Baggili, I., & Breitinger, F. (2017). Forensic State Acquisition from Internet of Things (FSAIoT). Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17, 2017, 1–11. https://doi.org/10.1145/3098954.3104053

Nicky Woolf. (2016). DDoS attack that disrupted internet was largest of its kind in history, experts say | Technology | The Guardian. Retrieved January 5, 2019, from https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Nik Zulkipli, N. H., Alenezi, A., & B. Wills, G. (2017). IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things. Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, (May), 315–324. https://doi.org/10.5220/0006308703150324

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of Things Forensics: Challenges and Approaches. Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 608–615. https://doi.org/10.4108/icst.collaboratecom.2013.254159

Reiber, L. (2018). Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation (Second Edition). McGraw-Hill.

Richard Adhikari. (2013). Webcam Maker Takes FTC's Heat for Internet-of-Things Security Failure | Privacy | TechNewsWorld. Retrieved January 5, 2019, from https://www.technewsworld.com/story/78891.html

S. Harichandran, V., Breitinger, F., Baggili, I., & Marrington, A. (2016). A cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. Computers & Security, 57(March), 1–13.

Selena Larson. (2017). FDA confirms that St. Jude's cardiac devices can be hacked. Retrieved January 5, 2019, from https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/

Selingo, J. J. (2015, July 20). How many colleges and universities do we really need? Washington Post.

Sen, M., & Menting, M. (2015). Digital Forensics (ABI Research).

Sha, K., Wei, W., Andrew Yang, T., Wang, Z., & Shi, W. (2018). On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 83, 326–337. https://doi.org/10.1016/j.future.2018.01.059

Tu, M., Xu, D., Wira, S., Balan, C., & Cronin, K. (2012). On the Development of a Digital Forensics Curriculum. Journal of Digital Forensics, Security and Law, 7(3). https://doi.org/10.15394/jdfsl.2012.1126

U.S. News. (2018a). Best Engineering Schools. Retrieved December 30, 2018, from https://www.usnews.com/best-graduate-

schools/top-engineering-schools/eng-rankings

U.S. News. (2018b). Methodology: 2019 Best Engineering Schools Rankings. Retrieved December 30, 2018, from https://www.usnews.com/education/best-graduate-schools/articles/engineering-schools-methodology

Udeshi, R. (2017). Why you need forensic in an IoT world. Retrieved from https://www.guidancesoftware.com/blog/digital-forensics/2017/10/03/why-you-need-forensics-in-an-iot-world

Van Duren, D., & Russell, B. (2018). Practical Internet of Things Security (Second Edition). Packt Publishing.

Voas, J., & Laplante, P. (2017). Curriculum considerations for the internet of things. Computer (Published by the IEEE Society), 50(1), 72–75. https://doi.org/10.1109/MC.2017.27

Watson, S., & Dehghantanha, A. (2016). Digital forensics: the missing piece of the Internet of Things promise. Computer Fraud & Security, 2016(6), 5–8. https://doi.org/10.1016/S1361-3723(15)30045-2

Wikipedia. (2018). U.S. News & World Report Best Colleges Ranking. Retrieved December 30, 2018, from https://en.wikipedia.org/wiki/U.S._News_%26_World_Report_Best_Colleges_Ranking

Yu, T., Sekar, V., Seshan, S., Agarwal, Y., & Xu, C. (2015). Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things (p. HotNets-XIV Proceedings of the 14th ACM Workshop o). Philadelphia: ACM.

Zawoad, S., & Hasan, R. (2015). FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. In 2015 IEEE International Conference on Services Computing (pp. 279–284). IEEE. https://doi.org/10.1109/SCC.2015.46

