Educating the Examiner: Digital Forensics in an IoT and Embedded Environment

Iain Sutherland[1], Huw Read[1, 2] and Konstantinos Xynos[1, 3]
[1]Noroff University College, Agder, Norway
[2]Norwich University, Northfield, USA
[3]MycenX Consultancy Services, Stuttgart, Germany
iain.sutherland@noroff.no
hread@norwich.edu
kxynos@mycenx.com
DOI: 10.34190/EWS.21.041

Abstract: The Internet of Things (IoT) is an interconnected world of semi-autonomous systems capable of automation, communication and monitoring. It encompasses all manner of systems and embedded devices, communicating using various protocols and standards. Sometimes these devices are purpose built for commercial or industrial environments and at other times generic builds provide domestic solutions. These systems have the potential to hold a significant amount of information on user preferences and activities as well as on the surrounding environment. Some data will usually reside on the device itself, or as seen in many cases, within a manufacturer supported cloud solution. Mobile and web applications will then provide a way to interface with the data or the device. The question arises as to the readiness of the Digital Forensic Examiner. There is a requirement to correctly identify the value of IoT and embedded systems at the crime scene. Once identified, the examiner needs the skill and knowledge to access, interpret and present the information that may be contained in this ever-expanding wide variety of devices found in home and work environments. The skills required by the Digital Forensic Examiner has progressed further from the analysis of hard drives and file systems. It must address the growing demand and requirement to be able to understand how embedded firmware operates. In some cases, this includes interpreting embedded code, memory structures and proprietary file formats. This paper discusses the increasing complexity of the changing environment. It reviews the types of skills and training needs and the subject areas for consideration when training forensics examiners over the next five to ten years.

Keywords: digital forensics, IoT, investigative strategy, training, skill sets

1. Introduction

The increase in the use of smart technology or smart devices (composed of an embedded processor, memory and a communication channel) is expanding the interaction between users and the variety of digital devices. There has been a migration away from user data and user activities being held just in laptop and desktop systems. A user may now interact with a range of devices with capabilities that may vary from simple environmental monitoring to more complex information gathering and processing. These environments have the potential to capture a user's activities in increasing detail, potentially providing information on timing, location and preferences. This information will be of interest to an examiner in determining a user's actions or whereabouts. These devices are frequently designed to carry out a specific, often limited activity but the user may be unaware of the amount of data gathered by the device. Examiners have an interest in access to any potential sources of information that may assist them in their casework. In terms of abilities, an investigative team would need to know many different systems/environments and have prior access in order to know what devices to examine and which sources will provide the greatest opportunity for intelligent, actionable information.

2. The environment

Evidence to date (Sarris et al, 2020) regarding the development of complex software systems suggests that integrating numerous smaller components creates concern with regard to updates and ongoing maintenance. The complexity of software leads to bugs and security flaws, while the interaction between software can lead to unintended functionality; for example MITRE's CWE (Mitre, 2020) list focuses on identifying weaknesses that lead to vulnerabilities that may be exploited by cyber criminals. The ever-present complexity of software is an indication of the potential problems to come with more complex Internet of Things (IoT) environments. Security flaws in these devices can also be exploited by malware such as Mirai (Zhang et al, 2020) and Reaper (TrendMicro, 2017) spreading specifically through IoT systems.

Examples of these emerging environments are the continuously evolving smart homes which are causing concern on privacy (Bronshteyn, 2020), in particular with examples like the always on and listening Amazon Alexa (Shackleton, 2019). The need to analyse the behaviour of such systems is becoming increasingly apparent. As noted in the Interpol Review of Digital Evidence 2016-2019 (Reedy, 2020), criminals are early adopters of technology, an example being Smart TV's (Sutherland et al, 2014) and the subject of a search warrant in 2015 (Brewster, 2017, Bronshteyn, 2020). Cyber criminals may also be unwittingly capturing information on illegal / illicit activity, allowing examiners to take advantage of the systems, as noted by Bronshteyn (2020) and Shackleton (2019).

3. The challenges and needs of the digital forensic examiner

The digital forensic examiner is no longer solely concerned with laptop and desktop systems and the 'traditional' Windows, MacOS and Linux operating systems and associated file systems commonly used on these devices. The popularity of mobile phones introduced mobile-oriented OS, such as iOS and Android, as other important operating systems and possible sources of information. IoT devices typically include some form of control device, often a smartphone used to communicate with the device or a central hub. Although smartphones can provide some information either stored locally and presented in the control application, or from data stored in a cloud storage system, it has been shown that these different views of data (on-device, cloud, app) can result in varying quality of evidence (Awasthi, 2018). The challenge is that relying on the application may not provide access to all of the useful data on the device. While many IoT devices, like other embedded systems, often run versions of the Linux and more recently Windows 10 IoT operating systems, the actual IoT devices tend to have very limited connectivity and may also run proprietary code with no permanent file system. Accessing and interpreting the data will require a very specific approach (Watson, 2016) for which traditional guidance (e.g. ACPO see Horsman, 2020) is unsuitable.

There are obvious risks to limiting analysis to just the control application on the smartphone and the point and click options of the digital forensic tool set. Investigating this type of environment increasingly requires an in-depth understanding of devices and potentially components at a hardware level.

4. Towards defining a skill set

4.1 Guidelines, standards and skill sets

Discussions addressing digital investigation challenges tend to have a government and industry focus, with a limited emphasis on the role of academia. Indeed, in recent work by Casey et al, (2019) which determine 4 goals for mitigating such challenges, academia is not mentioned. In the United States of America, the NICE (NICCS, 2020) workforce framework has been publicly available since 2017, with its most recent revision in NIST (2020). It is moving towards describing the broad spectrum of cybersecurity work; one of the goals is to allow educational establishments and employers to describe the roles in a common language. "Work roles" are made of "tasks" which require "knowledge" ("a retrievable set of concepts within memory") and "skills" ("the capacity to perform an observable action"). An employee's ability to do the job, or a student's ability to demonstrate proficiency, can be assessed via "competencies" which test the person's "knowledge" and "skills'', thereby their ability to perform "tasks" for the "work role". Of particular interest are the predefined "work roles" relating to digital forensics (Fig. 1, NICCS, undated).

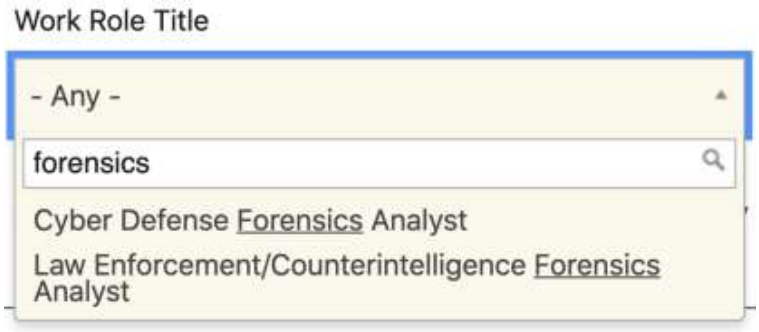


Figure 1: NICE workforce framework work roles for digital forensics

For both of these digital forensic focused work roles (Fig. 1.), a number of skills and knowledge items are presented, along with a number of capability indicators for entry, intermediate and advanced levels. Whilst there is no mention of embedded or IoT systems specifically, and it is unclear how often these work roles are updated to reflect changes in technology (no timestamps on the webpage), the framework does have the flexibility to incorporate additional tasks as identified by an employer or an educator. However, it should be highlighted that whilst the NICE framework does not specifically provide guidance for digital forensic academic programmes, it is possible to infer what may be expected of one by examining the work tasks.

In the UK a programme was developed for certifying masters degrees in digital forensics. GCHQ defined in 2015 an outline set of criteria that a digital forensics degree needed to meet in order to achieve their certification. This programme is now maintained by the NSCC (2019) as an Integrated Masters with a specific Digital Forensics Pathway. This document has a series of appendices that refers to the specific subject areas of both the core computer science sections and the specific subject pathways (including digital forensics). The indicative topics are described at a very high level. The core computer science programme requires coverage of embedded systems; debugging including JTAG and UART and side channel analysis. It also requires low level techniques and tools for malware analysis and reverse engineering. There is a mention of mobile devices in the forensics element of the degree programme. This document is dated in early 2019 and highlights the increasing importance of embedded systems although there is no specific mention of IoT devices.

The international standard on ISO/IEC 27037:2012 "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence", defines some key skills for the Digital Evidence first responder. In terms of recognition this is focussed on networking concepts, while the acquisition of evidence is broader and mentions "*RAID, database, appliances and miniaturized devices*;" (ISO/IEC 27037:2012). A related standard, ISO/IEC 27042:2015 "Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence", takes a different approach in defining how competencies and proficiencies can be described. The international standards date back to 2012 and 2015 and as standards, as to be expected, are focussed on the practice and procedure rather than defining the skills required to complete the investigative tasks.

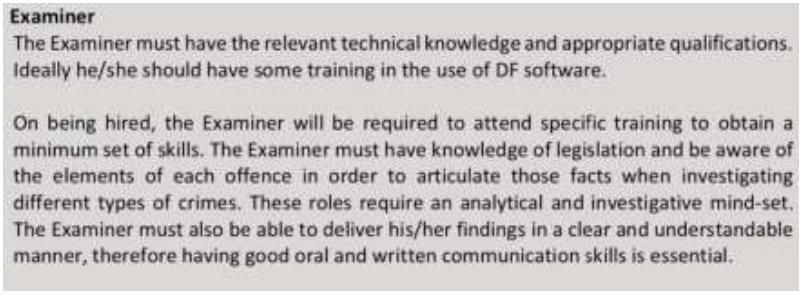
4.2 Digital forensic laboratories and skill requirements

One further area to explore is the documentation and standards for creating digital forensics laboratories which, in addition to outlining laboratory requirements, also comment on the basic skill sets or roles for digital forensic examiners. There are a number of documents looking at forensic best practice (ACPO 2012a), laboratory operations and staffing of digital forensic laboratories including ACPO (2012b). These could provide some basis for determining the required skill set from the perspective of operating a laboratory. The ACPO lab managers guide ACPO (2012b) defines the following roles and responsibilities within a computer crime unit:

- 1. Administration / Reception Officer
- 2. Triage Officer
- 3. Physical examiner/imager
- 4. Previewing Examiner
- 5. Advanced Examiner
- 6. Quality Assurance Officer
- 7. Training Officer

ACPO roles of interest are: Triage Officer (filtering cases), the Physical examiner/imager (identification imaging), the Previewing Examiner (automated processes and bespoke) and the Advanced Examiner (Specialist examination). These would all require specific knowledge in their areas. The best practice guidelines have the same issue as the international standards in that they date back to 2012. Considering the pace of change in the forensics environment, both of the ACPO guides (2012a, 2012b) in forensics terms are somewhat dated, and there have been suggestions that the principles and practices at least need revision (Horsman, 2020). Reedy (2020) also notes that *" ...best practice guidelines were established over a decade ago and do not meet the challenges of smart technology, and some do not address memory forensics, database forensics, or network forensics...".* A more recent guide defining the development of a forensics laboratory (INTERPOL, 2019) outlines the requirements for an examiner as shown in Figure 2, highlighting the laboratory specific nature of an

examiner. An examiner would inevitably develop the skill set for the tasks commonly covered in the laboratory in which they are employed.



Examiner

The Examiner must have the relevant technical knowledge and appropriate qualifications. Ideally he/she should have some training in the use of DF software.

On being hired, the Examiner will be required to attend specific training to obtain a minimum set of skills. The Examiner must have knowledge of legislation and be aware of the elements of each offence in order to articulate those facts when investigating different types of crimes. These roles require an analytical and investigative mind-set. The Examiner must also be able to deliver his/her findings in a clear and understandable manner, therefore having good oral and written communication skills is essential.

Figure 2: INTERPOL (2019) description of an examiner role

The document (INTERPOL, 2019) also outlines a skill set list for the Digital Forensics Examiner; data recovery, computer forensics, mobile phone forensics, audio video and image forensics and emerging technologies. Considering the DFL skill set Checklist (Appendix A of INTERPOL, 2019), a number of skills are identified, the closest related to IoT being the *emerging technology* category. However, such embedded systems are not a standalone category, as the knowledge and skills required for embedded systems would also be needed to extract evidence from devices in some of the other categories listed in the framework. The list of emerging technologies includes vehicle, shipborne, drone and other 'new' technologies. The skill set required is the need to access, extract and interpret data from a range of embedded computing devices, clearly a need to cover more than traditional computing technologies. The document also defines aspects of the proposed roles including a technical understanding of data storage, microchip operation and basic electronics in addition to practical skills and possibly most critical logical thinking and analytical skills (INTERPOL, 2019). JTAG, Chip-off, rooting and Jailbreaking are all skills now required by the digital forensic examiner (INTERPOL 2019). Therefore, an increasing broad skill set, and a greater depth of knowledge is needed by the forensic examiner, unless there is a degree of specialization separating digital forensics into specific knowledge, skills and abilities to deal with IoT, triage in the crime scene and other niche requirements (i.e. cloud-based acquisition etc).

5. Training the digital forensics examiner

Digital forensic examiners in post are recommended to undergo training and, or certification in the tools they are using (INTERPOL, 2019). There are a number of university undergraduate programmes in place to educate new digital forensic examiners. These programmes face a number of challenges. Reedy (2020) notes that *"digital forensics is becoming inaccessible due to the increasing expense and complexity…"*. Cost is clearly also a factor for universities when considering new study programmes. A number of papers exploring curriculum development including Tu et al (2012) and notably Lang et al (2014), outline several key areas for concern in developing a forensics curriculum. The following sections highlight a selection of the challenges and concerns raised in Lang et al (2014) and reflect on IoT and embedded challenges.

5.1 Digital forensics curriculum challenges

One of the most significant issues and possibly greatest opportunities can be argued to be the lack of a specified digital forensics curriculum design. There are a number of perspectives of what should be included in a digital forensics curriculum. NIST have proposed a framework for the development of cyber security materials via NICE (NIST, 2020). In addition to Tu et al (2012) and notably Lang et al (2014), there has been other work in the area including Srinivasan (2013) exploring integrating digital forensics into a security curriculum. The general consensus is the applied nature of the program, but also the need to learn both theory and skills in a number of topics, as well as having test devices at hand to practice the processes and procedures.

The addition of an IoT skill set poses a challenge (Yaqoob et al, 2019) in further extending what may already be a full curriculum. For example, the need to understand how to extract contents directly from solid state storage on a PCB and interpret the contents is highly-specialised, and requires several electrical engineering, computing and digital forensic-specific prerequisites in order to understand the implications of such low-level analysis. Fig. 3 provides a focussed insight into the overlaps that occur between the three domains of forensics, electrical engineering and computing. Therefore, as a simplification the problem can be split into two realms, hardware and software.

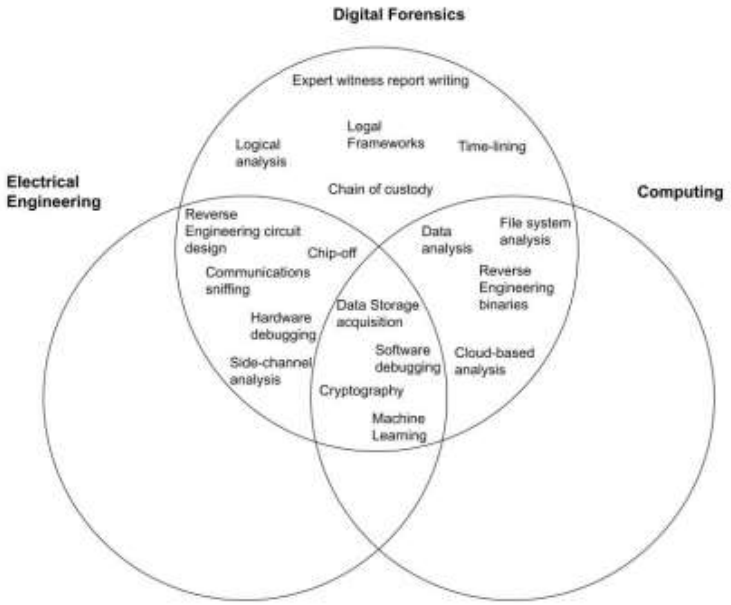


Figure 3: Relationship of selected key skills (focusing on digital forensics)

When dealing with the hardware there is a need for some knowledge in electrical engineering. This would cover some basic concepts required when dealing with hardware related challenges of a case. This requirement is not limited to IoT devices, since it is seen already in mobile device forensics (e.g., chip-off) and CCTV systems. The main advantage of having physical access and interrogating IoT devices, and other such related devices, in such a way is that it provides more opportunities for interacting with the device and the OS. Interactions could involve debugging interfaces (e.g. kernel boot argument manipulation, JTAG, UART, terminal/SSH), sniffing of communication channels (e.g. SPI, CAN, RFID, Wifi, BLE, Zigbee etc), networking capabilities (e.g. Wifi, BLE, Zigbee etc) and even accessing storage mediums (e.g. memory cards, storage chips (SPI flash, NAND, eMMC), EEPROM etc.). Reverse engineering circuit design is just as important in identifying device capabilities and data sources.

Once the hardware issues have been addressed and the device's software and data has been dumped, the focus shifts to the software. The analyst will need to know how to overcome the formats of the extracted data (e.g., related or specific to the hardware device and medium involved) in order to proceed. From then on the problem is one very familiar to the digital forensic analyst. In most cases the device's file system will be extracted along with configuration details, and where present, saved data. An understanding of the type of OS used by embedded systems (e.g. Linux, Android, QNX etc.), processor architectures (e.g. MIPS, ARM), possible cloud-based APIs, mobile control devices and some binary reverse engineering would also be needed. This knowledge enables the investigator to understand sources of data and possible changes that would occur on the system being investigated. This would create specialists in IoT digital forensics that are able to understand and approach the system depending on the individual requirements of an investigation.

Combining hardware and software knowledge can be seen as follows: If an analyst wanted to boot a system as root and bypass the login prompt they could implement the following; they could dump the system using a hardware device (e.g. SPI), make a modification to the kernel boot arguments that force the system to boot as root and write the flash back to the system. This would involve knowledge of hardware and software capabilities of a device. The forensic value of this type of approach is open to debate since the device would have to be shut down, modified and started again, therefore losing any volatile data. With root access to the system, it would then be possible to extract forensic images of the live system as and when needed, including volatile artifacts.

5.2 Teaching and delivery resources

There are a variety of textbooks available for teaching digital forensics. However, the process of creating textbooks can take a number of months and could lag behind as the subject rapidly evolves. Most educational institutions would combine core textbooks with research papers to provide the latest and most up to date material. Textbooks are also written for the largest markets, typically the USA and to a lesser extent Europe. This is a challenge as digital forensics is a combination of computing and law, so textbooks with legal system information are often inappropriate due to jurisdictional differences. Staff training and continued development in the aforementioned areas is important, although not without difficulty. This is especially true when a computing graduate would have to be aware of some electrical engineering topics. Recruiting staff with this specialised knowledge and experience would be even more of a challenge.

Given the disparate nature of devices considered to be part of the digital forensics discipline, existing corpora such as Digital Corpora (2021), cannot be expected to provide samples of all devices. Teaching images are time consuming to develop, and so need to be reused due to the degree of effort involved in creating the material. However, studies have shown (Carthy et al, 2018 and Woods et al, 2011) it is possible to integrate the development of such material into the pedagogical outcomes of digital forensic courses, but these have focused on familiar technology/media rather than exploring possibilities with new devices. Focused challenges help with the direction of digital forensic research (e.g. DFRWS, 2018) but less so with the educational aspects of the discipline.

While data recovery may be addressed in some forensics degrees, the inclusion of data extraction and IoT / embedded systems introduces another dimension in the generation of appropriate case studies and practical sessions.

5.3 Jurisdictional issues

There are several challenges when considering legal aspects and how they relate to digital forensics. Local laws and customs relative to where a student is studying, geographic location of crime, location of digital evidence and location of organisation holding data (e.g., CLOUD Act, 2018) all make it challenging to provide an appropriate in-depth review of legal issues.

5.3.1 Laboratory resources

Core digital forensics concepts can be taught with standard computing facilities and open-source software tools. However, to cover all of the stages of an investigation and to provide the required practical skills and experience, some considerable investment is required. The initial investment cost may be prohibitive to most academic institutions when factoring in the specialist hardware, software licenses, staff training and continuing professional education, not to mention the required student computers. The laboratory may share some similarities with a cyber security laboratory, the benefit of a closed network with local storage for shared resources. If the laboratory is running commercial software locally, these computers are likely to be more expensive than those in a standard university laboratory.

If a laboratory is expected to examine IoT devices and other embedded systems, then there are additional expenses. Hot air rework stations, air handling systems, dismantling benches and associated tools are not uncommon. Specialist analysis hardware such as Saleae Logic Analyzer, Hardsploit, JTAGulator, BusPirate and Hydrabus and associated consumables (cables, clips) in addition to staff training and the development of safety policies and procedures would all be required.

5.4 Changing environment for the delivery of courses

The COVID-19 pandemic in 2020 and 2021 has seen many higher education institutions move to online delivery. This poses a challenge for any degree programme where practical elements are included, but especially with applied courses. Simulating a network and associated security problems in a series of virtual machines is possible. Gaining practical experience in extracting the contents of an SPI chip or mobile device using specialist hardware is not possible. The shift online increases the likelihood of enrolling international students, further exacerbating the challenges relating to legal frameworks and different jurisdictions.

5.5 Discussion and conclusions

The increasing connection between cyberspace and the physical world resulting from IoT and embedded devices presents an increasingly complex, evolving environment for Digital Examiners. The volume of data that could potentially be useful is expanding, but so is the distribution of that data across increasingly varied devices and systems. The Examiner, in addition to 'traditional' multiple operating and file systems, also has to process embedded code and devices with more esoteric file systems. The increasing importance of network forensics and the need to deal with multiple devices communicating over a variety of different protocols means the Digital Examiner will need to conduct triage on-site, as well as be aware of the device's capabilities. While Hitchcock et al (2016) argued that triage could be undertaken on site by a non-specialist, there was also an acknowledgement that training would be required for the more advanced tasks such as memory capture. The interconnected nature of the systems and the volatility of data means that evidence dynamics will also be an increasing feature of the environment.

It is possible to derive a number of conclusions. The emerging technologies referred to in appendix 1 in INTERPOL, (2019) which in addition to social media, database, cryptocurrency and biometric technologies highlighted shipborne, vehicle and drone systems. The latter are likely to include embedded systems, but so will other INTERPOL categories, in particular audio and video systems (Martin et al, 2021). In exploring the current environment and the challenges facing the digital forensic examiner, and having reviewed some of the issues with creating a suitable digital forensics curriculum, it is clear that digital forensics training will now need to address a number of areas:

- 1. An understanding of the technologies in an embedded system, in particular the communication standards and protocols used which could be JTAG, SWD, UART, USB, I2C, SPI, etc that enable extraction of data directly from the physical device. These require an additional knowledge base, to extract information from the device.
- 2. An ability to use appropriate tools to examine bus communications and data stored in SPI flash, NAND and other PCB mounted components. In addition to write-blockers, other tools would be required, but not limited to; Saleae Logic Analyzer, Hardsploit, JTAGulator, BusPirate and Hydrabus. These will become part of the digital forensics toolkit as will the necessary skills to use these tools to extract intelligible data from IoT devices and embedded systems. The investigator, during initial evidence seizure and triage, must be competent with such tools and methods to be prepared to capture volatile data on-site (Zulkipli, 2021).
- 3. An ability to interpret the findings from disparate devices and place them in comparative context within the environment. To have the competency to interpret the evidence dynamics of the system and the relative importance of the findings. In the longer term, incorporating advanced Machine Learning systems (i.e., Huybrechts et al, 2018) that help identify custom binaries and protocols, and support the new processes and procedures of working with IoT and embedded devices.
- 4. The continuing evolution of technology focussed on securing information in the device using features such as Physical Unclonable Functions (PUFs) (Gao, 2020) will only make accessing data more challenging. In addition, the increasing adoption of device encryption means Digital Forensics Examiners will also ideally need to collaborate closely with IoT and embedded device manufacturers, who in turn will have to implement forensic readiness methods as part of the physical device's life cycle.

The low-level understanding required to analyse firmware and to access systems via a variety of methods is essential. As technology moves to fully adopt cryptographic elements and enhanced device security (ENISA, 2017), it is highly possible that security specialists, such as cryptographers and a cryptoanalysis team, would also be part of the future team of Digital Forensics Examiners. When considering the broad range of skills needed for the Digital Forensics Examiner, it is clear that there are significant challenges when, for example, creating a university degree. A series of specialist forensics topics, building on a computer science degree may no longer be sufficient. The range of required skills has broadened to cover aspects of computing, electronics and law.

Acknowledgements

Special thanks to Septimiu Mare and Andrew Blyth for some insightful conversations.

References

ACPO, (2012a) Good Practice Guide for Digital Evidence, Police Central E Crime Unit, March 2012 https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

ACPO, (2012b) Good Practice and Advice Guide for Managers of e-Crime Investigation, Official Release Version V0.1.4 http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf Now available at - https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_and_Advice_for_Manager_of_e-Crime-Investigation.pdf

Awasthi, A., Read, H.O., Xynos, K. & Sutherland, I., (2018) Welcome pwn: Almond smart home hub forensics. Digital Investigation. 2018, 26, 38–46.

Brewster T., (2017) That Time Cops Searched A Samsung Smart TV For Evidence Of Child Abuse. Available online at: https://www.forbes.com/sites/thomasbrewster/2017/02/07/samsung-smart-tv-fed-search-child-pornography/?sh=5a25469417d7 Last Accessed 22 Feb 2021.

Bronshteyn G., (2020) Searching the Smart Home. Stanford Law Review, February 2020, Volume 72, Available online at: https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf

Carthy L., Little R., Øvensen E., Sutherland I. & Read H.O.L., (2018) Committing the perfect crime: A teaching perspective. 17th European Conference on Cyber Warfare and Security 28 - 29 June 2018, Oslo, Norway.

Casey, E., Geradts, Z. & Nikkel B., (2019) Editorial: Transdisciplinary strategies for digital investigation challenges, Digit. Invest. 25 (2019) 104.

CLOUD Act., (2018) Clarifying the Lawful Use of Overseas Data Act of 2018, Pub. L. No. 115–141, 132 Stat. 348 (codified as amended in separate sections of 18 U.S.C.); available online at https://cli.re/BwPk5Q

DFRWS, (2018) DFRWS 2018 challenge. Available online at: https://github.com/dfrws/dfrws2018-challenge

Digital Corpora., (2021) Producing the digital body. Available online at: https://digitalcorpora.org/

ENISA, (2017) Baseline Security Recommendations for IoT, Available online at: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

Gao, Y., Al-Sarawi, S.F. & Abbott, D., (2020) Physical unclonable functions. Nat Electron 3, 81–91 https://doi.org/10.1038/s41928-020-0372-5

Hitchcock B., Le-Khac N-A. & Scanlon M., (2016) Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. DFRWS 2016 Europed Proceedings of the Third Annual DFRWS Europe, Digital Investigation Volume 16, Supplement, 29 March 2016, Pages S75-S85

Horsman, G., (2020). ACPO principles for digital evidence: Time for an update? *Forensic Science International: Reports*, *2*, December 2020, [100076]. https://doi.org/10.1016/j.fsir.2020.100076

Huybrechts T., Vanommeslaeghe Y., Blontrock D., Van Barel G. & Hellinckx P., (2018) Automatic Reverse Engineering of CAN Bus Data Using Machine Learning Techniques. In: Xhafa F., Caballé S., Barolli L. (eds) Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2017. Lecture Notes on Data Engineering and Communications Technologies, vol 13. Springer, Cham. https://doi.org/10.1007/978-3-319-69835-9_71

INTERPOL, (2019) Global Guidelines for Digital Forensics Laboratories. INTERPOL Global Complex for Innovation Available online at: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf

ISO/IEC 27037:2012, (2012) Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO/IEC 27042:2015, (2015) Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence.

Lang A., Masooda B., Campbell R. & DeStefano L., (2014) Developing a new digital forensics curriculum. Digital Investigation 11, (2014) S76-S84

Martin E D., Sutherland I. & Kargaard K., (2021) *IoT Security and Forensics: A Case Study*. ECCWS 2021, 20th European Conference on Cyber Warfare and Security, held at the University of Chester, UK

MITRE, (2020), Common Weakness Enumeration: A Community-Developed List of Software & Hardware Weakness Types. Available online at: https://cwe.mitre.org

NICCS, (undated) National Initiative for Cybersecurity careers and studies, NICE Cybersecurity Workforce Framework Work Roles https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles

NIST, (2020) Special Publication 800-181 Revision 1 Workforce Framework for Cybersecurity (NICE Framework) this publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-181r1 Also: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

NSCC, (2019) National Cyber Security Centre (a part of GCHQ) Certified Master's in Cyber Security. Certification Of Integrated master's Degrees (Computer Science and Digital Forensics (Pathway C) https://www.ncsc.gov.uk/files/Certification-IntMasters-Issue-4_0-Feb-2019.pdf

Reedy P., (2020), Interpol review of digital evidence 2016 - 2019, Forensic Science International: Synergy, Volume 2, 2020, Pages 489-520, ISSN 2589-871X, Available online at: https://doi.org/10.1016/j.fsisyn.2020.01.015.

Srinivasan S., (2013) Digital Forensics Curriculum in Security Education, Journal of Information Technology Education: Innovations In Practice, Volume 12, 2013 http://www.jite.informingscience.org/documents/Vol12/JITEv12IIPp147-157Srinivasan1232.pdf

Sarris, D., Xynos, K., Read, H. & Sutherland, I., (2020) "Toward a methodology for the classification of IoT devices", European Conference on Cyber Warfare and Security 2020 (ECCWS), Chester, UK

Shackleton, J., R., (2019). Alexa, Amazon Assistant or Government Informant?, 27U. Miami Bus. L. Rev.301, Available at: https://repository.law.miami.edu/umblr/vol27/iss2/6

Sutherland, I., Read, H., Xynos, K., (2014). Forensic analysis of smart TV: A current issue and call to arms. Digital Investigation. 11. Issue 3 Sept. 2014 10.1016/j.diin.2014.05.019.

TrendMicro, (2017) Millions of Networks Compromised by New Reaper Botnet. Available online at: https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/millions-of-networks-compromised-by-new-reaper-botnet Last Accessed 22 Feb 2021.

Tu, M. Xu D. & Cronin K., (2012) "On the Development of Digital Forensics Curriculum." Journal of Digital Forensics Security and Law 7 (2012): 13-32. DOI:10.15394/jdfsl.2012.1126 Corpus ID: 9263719

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

Woods, K., Lee, C., Garfinkel, S., Dittrich, D., Russell, A. & Kearton, K., (2011) Creating Realistic Corpora for Forensic and Security Education, (2011) ADFSL Conference on Digital Forensics, Security and Law, 2011.

Yaqoob, I., Hashem, I.A., Ahmed, A., Kazmi, S.M., & Hong, C., (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems, 92, 265-275. Available online at: https://doi.org/10.1016/j.future.2018.09.058

Zhang, X., Upton, O., Beebe, N.L., & Choo, K.K.R., (2020) IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers, Forensic Science International: Digital Investigation, Volume 32, Supplement, 2020, 300926, ISSN 2666-2817, Available online at: https://doi.org/10.1016/j.fsidi.2020.300926.

Zulkipli N., H., N., Willis G.B. (2021) An Exploratory Study on Readiness Framework in IoT Forensics, Procedia Computer Science, Volume 179, 2021, Pages 966-973