IoT and cloud forensic investigation guidelines

I. Mitchell[1], S. Hara[2], J. Ibarra Jimenez [3], H. Jahankahni[4], and R. Montasari[5]

[1,2]Middlesex University, London, UK
[s.hara, i.mitchell]@mdx.ac.uk
[3,4]University of Northumbria, Newcastle, UK
[jaime.jimenez, hamid.jahankhani]@northumbria.ac.uk
[5]Huddersfield University, Huddersfield, UK
r.montasari@hud.ac.uk

Keywords— Cyber Physical Systems, Digital Forensic Frameworks, Blockchain, Cloud, IoT

1 Introduction

The only thing that is constant is change, has often been attributed to the Greek philosopher, Heraclitus (c.500 BCE). Some 2,500 years later never has their been a more apt quote for today's society, with its constant use of technology and hence change. Currently, it is estimated that 2.5×10^{18}, or 2.5 quintillion, bytes of data are written every day. This astronomical figure is likely to increase over the next 5 years with the introduction of two major technologies: Blockchain; and, the Internet of Things (IoT). The data generated by the two technologies will be cloud based and hence, the problem for law enforcement and e-Discovery analysts is how is it possible to conceive that every piece of technology has been investigated? Paul Kirk understood in 1953 when he wrote about forensic evidence, "Only human failure to find it, study and understand it can diminish its value" [23]. Combining these pre-technological age quotes, the problem can be defined as, the human failure to find, study and understand digital evidence in an ever changing world of technology will diminish its value.

The starting point is unusual and requires structure. This has been recognised by the call to develop Digital Forensics Frameworks (DFFs) in the inaugural Digital Forensic Research Workshop [33], its response has been phenomenal with over 20,000 papers written on DFFs. This implies that there is no *silver bullet*, and it is no surprise since these frameworks are structured and need refining each time a change in technology occurs. However, guidelines are based on principles *and* procedures and there are some exceptional frameworks that were pioneering in the development of accommodating both. For example, in [5] there is a tiered approach that allows principles and practices to synergize, using Standard Operating Procedures (SOP) to *maintain* principles and opportunities to question and add to the knowledge to *improve* quality. In the UK the over-riding document is ACPOs Good Practice Guide for Digital Evidence, [40], others have accompanied this document over the years and include, but not limited to, [15, 37]. There is a need to research the need for a DFF with principles, SOP, and guidelines for technologies that include IoT and cloud. Joining

the two together and treating them as one, rather than deploying different DFFs for each, which the remainder of this chapter investigates.

Section 2 provides some of the background information, including definitions and suggestions to be considered in the IoT network. Section 3 provides a rationale for the approach and the technology used and how this may be involved in illegal activities. Section 4 proposes some guidelines and improvements of SOPs in this area. Finally, section 5 concludes and discusses the findings from the research.

2 Background

IoT devices are becoming more prevalent in society, with an expected 21.5 Billion devices connected by 2025 [24], and when an incident occurs in the vicinity of such devices then they should be considered as potential digital evidence. A network of IoT devices is often referred to as a smart environment, or more frequently as a cyber physical system [17]. Is there a need for yet another framework? It could be questioned that: i) there is no need for such frameworks since the IoT devices are not that important; or, ii) that there are adequate SOPs and frameworks already in place? The remainder of this section tries to provide answers to these questions.

2.1 A need for another framework?

To answer the first question would require some evidence of a security breach in cyber physical systems via an IoT device. There are many systems available but let us consider Body Area Networks (BAN) that include an array of medical devices, e.g., pacemakers. In [4] there is evidence of how to 'hack' a pacemaker provided by the National Health Service (NHS) in the UK. This study [4] shows that pacemakers can be hacked and the severe consequences that a security breach could result in. The study went on to show that Medical Consultants and Coroners, did not consider the security of the device when purchasing, or inspecting the device when it failed, respectively. Whilst these devices transmit on restricted frequencies, this does not deter the criminally minded with malicious intent to break these rules and commit further crimes. This is not an isolated incident, Body Area Network devices, or implantable medical devices, require more sophisticated technology to improve the quality of patients' lives, many of whom their lives depend on this technology. In [6] we can see a range of issues with these devices and there is a need for cyber-security experts to be consulted during the acquisition of implantable medical devices.

The pacemaker attack [4] was not an off-the-shelf attack and required some skill. However, there is evidence of other IoT devices having their security breached with simple attacks using off-the-shelf malware and/or exploiting IoT devices were the users leave the default settings for passwords. In Finland [9] it is reported that a DDoS attack prevented the heating of buildings in sub-zero weather conditions, and was a result of the devices having default passwords. Furthermore, studies in [38] shows that in 2017, 48% of U.S. Companies using IoT devices have suffered a security breach, these included devices from teddy bears to warehouse equipment.

In summary, the consequences of these attacks on cyber physical systems range from life-threatening [4, 6, 9] to denial of service [38]. Regardless of the consequences, an incident has occurred that requires a digital investigation and the collection, preservation, acquisition, analysis, reporting and presentation of material.

This chapter is concerned with providing a framework, under which the digital investigation is guided, and able to produce digital evidence that is acceptable and admissible in a court of law and therefore, to answer the first question, when cyber physical systems are compromised there is a need for the development of investigative techniques, which includes new frameworks.

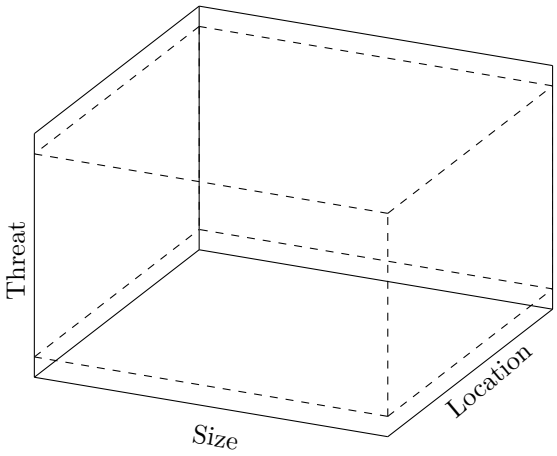

Figure 1: IoT classification continuum, derived from a combination of [31, 32, 36].

2.2 IoT Classification Continuum

To answer the second question a more detailed look at IoT devices is required. There are classifications of IoT devices [31, 32, 36], which relate to three different criterias: Memory size; Physical location; and, threat-level. Combining these three areas into a continuum can help Digital Forensic Investigators, DFIs, to make decisions about how the First Response Team proceed. Based on knowledge about the case type and the smart environment they are about to investigate, a DFI will be guided by the classification of the device and help develop a strategy for seizure (alongside existing recommendations) . For example, location can guide the search strategy, whilst memory size may guide the order of volatility and in certain situations give rise to the issue of contamination of the device due to small memory sizes and information being overwritten. This is particularly an issue if first responders do not have information that a digital incident scene is a smart environment. Finally, with many IoT devices threatening critical national infrastructures the search strategy may prioritise the discovery of a particular IoT device. The IoT classification continuum is there to help DFIs and FRTs to search, seize and gather physical IoT artefacts. The need for forensic procedures to collect information from smart environments is in demand and the classification continuum can help.

2.3 Cyber Physical System Forensic Readiness

In [21] we see a review of current techniques and their approaches, which essentially decomposes the problem into three areas: device; network; and, cloud. IoTDots [1] focuses on the data capture and analysis, and is an important tool in the capture of data from devices and the subsequent reconstruction of events.

In both these papers forensic readiness is touched on, and there is a challenge presented by the range of IoT devices to make the network forensic ready. Some attempts have been proposed [30] and a solution is the use of BlockChain Technology, BCT (for an introduction to blockchain see [41, 14]).

IOTA [13] is a permissionless BCT that allows the exchange of cryptocurrency via IoT devices on a cyber physical system. During an investigation it would be necessary to look at all devices in the cyber system. There are a combination of three things required in the investigation: device identification; spatio-temporal information of each

IoT device, which can be used for exculpatory and inculpatory evidence; and, the state information of the IoT device, which can be used for attribution and who is ultimately responsible and in control.

Like it or not Cyber physical systems are here to stay and increasingly likely to be part of our everyday lives in the future. As already shown is §2.2, it is not inconceivable that someone could instruct an IoT device to do something illegal. This is where the immutable append-only distributed ledger forged by consensus algorithms, of BCT, would allow DFIs to search the relevant part of the Blockchain representing that cyber physical system. Then it would be possible to reconstruct events by reverse engineering the extracted information from the Blockchain and accounting for every device's state and spatial-temporal information in a cyber physical system.

There would be concerns over confidentiality and privacy of data? There already is concern over this data, e.g. see [3], however, this is no defence. Our brief description of BCT is lacking, we failed to explain that the data is encrypted and IOTA's consensus algorithm, tangle [34] is resistant to quantum computations. The latter part is important and means that our information on our blockchain is resistant to spoliation or direct contamination from adversaries. More importantly, there is no data, the data recorded or generated by the IoT device is still stored on the cloud. The crucial issue is retrieving the data with e-consent. Many IoT devices store data on the cloud that the DFI will not have sufficient privileges to access. This could be for a combination of reasons, but mainly falls on the right of privacy, and incompatible jurisdictions. BCT provides a restricted access to an itinerary of IoT devices' state, ID, and spatio-temporal information related to the investigation. Data relating to these devices would have to be obtained through Special Point of Contacts, SPoCs and subject to normal procedures and processes.

Using something like IOTA [13, 35] would standardise cyber physical systems auditability of IoT devices. Furthermore, there is the use of smart contracts [10, 11] that could prevent IoT devices completing something socially unacceptable or of illegal consequence. Where systems rely on external sources of information to change state, e.g., stock exchange, weather reports, other IoT devices, etc..., then there would be an issue of centralisation and trust. To avoid centralisation and dependency on a single source of information an oracle could be introduced and is defined as, *"an interface that delivers data from an external source to smart contracts"* [2]. This would ensure the authenticity and promote trust between objects in the cyber physical system. Therefore, to make cyber physical systems forensic ready, will require a permissionless blockchain using oraclized sources of information in combination with smart contracts.

2.4 Proposed Framework/ Summary

There exists IoT DFF and our second question is do we require another one? Quality is often misunderstood, and in Digital Forensics we are not proposing a completely new DFF, but more of an improve version of current DFFs. Quality is maintaining principles and improving practices, in this chapter it is proposed that for reasons above a new improved version of DFF for IoT is proposed based on the work thus far. The authors would like to think that in a few years, this model will also be reviewed, distilled and improved.

The proposed framework is Digital Forensic Incident Process Model, DFIPM, and its main purpose is to allow DFIs to recover IoT artefacts from the three categories: device; network; and, cloud. Then based on IoT levels of relevance determine possible root cause of the cyber incident. The basis of our work considers [18, 27], which will be explained in the following section 3.

3 Method

Digital forensic frameworks provide theoretical guidance to practitioners of digital forensics but they have become too prescriptive in their approach. Their design was / is to ensure that all evidence that is acquired, handled, processed and presented from crime scene to a courtroom meets the legal jurisdictional requirements. Earlier digital forensic frameworks evolved from dealing with devices that were largely unconnected and stand-alone to more current frameworks that present investigative methodologies for cloud, networks and IoT.

This chapter proposes that SOP should be considered for digital investigations. These SOPs will draw best practice from current guidelines and digital frameworks to produce a single consultative provision with a focus on practical application for evolving technologies for both civil and criminal crimes.

4 Digital Forensic Investigation Process Model, DFIPM

The proposed framework, DFIPM, has been developed from high to low-level approach and consists of seven phases, or processes. The seven phases are at a higher abstract level with more detail provided at a low-level in sub-phases. Figure 2 presents the abstract level of the DFIPM. This abstract model work with eight concurrent processes and are known as principles and listed below:

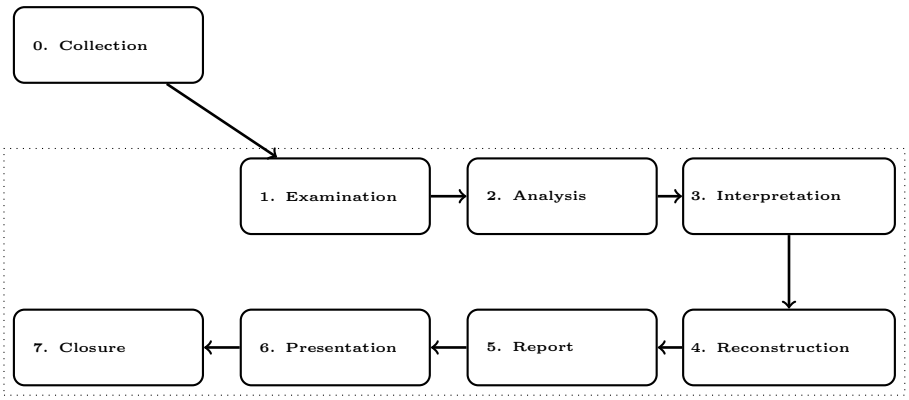

Figure 2: Activity Diagram for Digital Forensic Investigation Process Model, DFIPM, for Cyber Physical Systems

1. *Preservation* - Maximising evidential integrity must be maintained, where possible, throughout all stages of the framework. It is paramount that all possible precautions have been taken during the seizure and acquisition of the artefact.
2. *Evidence Continuity* - Using a chain of custody the custodian of the artefact must be recorded each time it is transferred. A record of these events provide an auditable record of evidence movement, see [26] for a more detailed explanation.
3. *Information Flow Management* - Permission for investigators to interact with the variety of laws, regulations and guidelines appropriately due the entire life-cycle of processing the artefact.
4. *Case Management* - manage, record and keep track of artefacts involved in the case. In [8] it is highlighted the importance of this principle as one of the main

components of scaffolding to bind all artefacts, evidence, reports, supporting documentation for the building of a strong case.

5. *Prepared Techniques and Standardised Tools* - DFIs need to use diverse tools and techniques during the investigation and this principle is covered extensively in [22]. Whilst the range of tools that are approved is adequate for traditional computer forensics, it is in much need of updating for IoT devices.
6. *Authorised consent* - All personal data must have associated permission. This data should not be compromised or disclosed. A further option of a smart contract could be used to ensure that the data permissions are not breached. Mutual Legal Assistants, MLAs, and SPoCs will provide guidance and accessibility to data.
7. *Documentation* - The documentation should record the entire life-cycle of the investigation. All changes, contemporaneous notes and preventative techniques should be included.
8. *Physical Investigation* - Interviews with bystanders or other people in the location is crucial and should be carried out by qualified personnel. However, in a digital incident scene there are more questions relating to digital devices that may require specialisms. Always include an interviewer in your FRT who has both knowledge and expertise in technology and interview techniques. All interviews need recording and added to the report.
9. *Training* - As a principle training and competence of staff is often overlooked. It is now included in the code of conduct in the FSR **??**, which Digital Forensic Laboratories have to comply with for accreditation.
10. *Search* - FRTs always require search strategies at incident scene. Often due to conditions outside the control of the investigation, e.g., weather, budgets, time management, FRTs only get one chance to complete the search and seizure of the area. Some IoT devices are going to be difficult to find, or unintentionally contaminated. Forensic readiness, combined with the classification of IoT devices will at least provide a itinerary of IoT devices to be avoided and seized, if possible, or data to be considered in the reconstruction of events.

4.1 Examination

Pareto's 80/20 rule is not just confined to business, it is also present in digital forensic investigations with 80% of the work dedicated to nearly 20% of the framework's two phases: Examination; and, Analysis. In [7] it is argued that examination and analysis should be one single phase, however, this was before IoTs were available and mass marketed. They indicated that there were slight differences when applying to traditional digital forensic analysis, e.g., HDD and simple network forensics. These slight differences have been exacerbated over the years with the introduction of new technologies and have different goals and aims and therefore they are considered as two different phases.

Examination is primarily concerned with the identification and extraction of potential digital evidence, that could be either inculpatory or exculpatory. Whereas analysis involves detailed and methodical standard operating procedures that factually support the reconstruction of the event. Figure 3 shows an activity diagram followed by a list explaining each of the sub-phases.

1.1 *Survey* – Surveying the Digital Incident Scene is the first sub-phase in the Examination phase and enables DFIs to discover pieces of evidence for a specific case type and depends on the skill level of the suspect, which can be underestimated. Predicting the suspect's skill level would lead DFIs to decide on procedures, techniques and methods in the analysis phase. The main objective

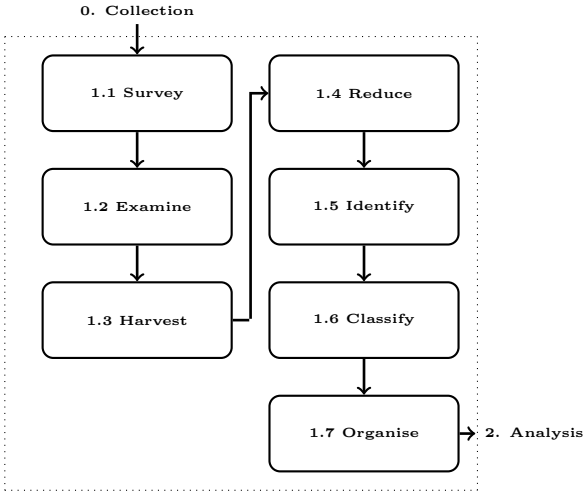

Figure 3: Activity Diagram for the Examination process showing sub-phases

of this sub-phase is to identify potential digital evidence, including in unusual locations of the system architecture [29], again use of BCT and an itinerary of IoT devices can be used here on forensic ready cyber physical systems.

1.2 *Examine* – DFIs must perform a detailed examination of the image acquired. File and folder structure is indexed using NIST approved software, e.g., Access-Data's FTK, Axiom for cloud-based data artefacts.

1.3 *Harvest* – Order the harvest and collected data. File and folder structure is indexed to provide an order of data acquired. The output of this stage is to produce a logical and catalogued data set [28]. This also includes any data gleaned of the forensic ready blockchain and used to identify IoT devices in the survey stage.

1.4 *Reduce* – 'Digital litter' is a downside in any investigation, during triage there needs to be ways of identifying relevant and irrelevant files. There are files that are relevant to the system and crucial to it operation, however, may be irrelevant to the investigation. There are many files that are not crucial to the operation of the system and irrelevant to the investigation. Then there are just the many files that have been saved or duplicated and never accessed. Most forensic tools, e.g. AccessData's FTK, will compile a list of all files enabling legal teams to categorise into used or unused data. The DFI has to have an *order of relevancy* to identify files that are important to the investigation and thus reduce and de-duplicate material being searched.

1.5 *Identify* – Once the sub-phases have been completed a clear identification of relevant potential digital artefacts should be recorded.

1.6 *Classify* – Grouping data with similar patterns, which can accelerate the process of analysis focused on the case type.

1.7 *Organise* – After these sub-phases it may be required to re-organise and provide new focus for the investigation.

4.2 Analysis

This is the most intensive phase in the framework due to the amounts of data collected combine with levels of complexity. With the examination phase complete the DFIs

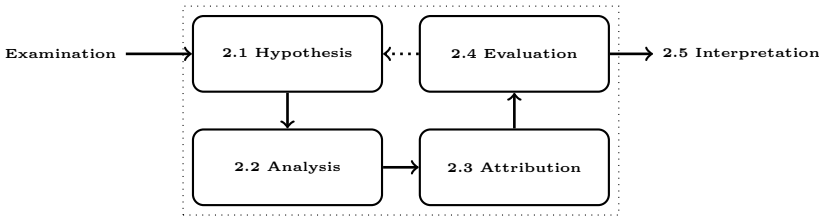

Figure 4: Activity Diagram for Analysis Phase

have the main patterns and characteristics of the incident encountered identified. This is based on the Evidence searching phase from [7] and is iterative, if the evaluation of results does not yield any attribution or cannot be validated, then a new hypothesis can be form and the analysis life-cycle can continue. The stopping criteria would be when there is definitive attribution (of at least the machine, not the person) and evaluation of the results are valid. Figure 4 shows the activity diagram of the analysis phase, the sub-phases are explained in the list below.

2.1 *Hypothesis* – using information from previous phases, the DFI can make hypotheses regarding the cyber-crime and map the root cause of the incident by remaking a sequence of events that changes the current state of the system. The hypotheses are built on the following:

- Assumptions are based on the results of the different stages form the Examination phase;
- Digital evidence organised from the Examination phase; and,
- Documentation of their findings.

2.2 *Analysis* – The DFIs have to perform a deep investigation to the organised information collected form the Examination phase on the hypothesis defined from the previous sub-phase. In addition, it must be completed by competent and train personnel using NIST approved software. The credibility of the potential evidence should consider the relevance, admissibility and weight. Not all collection of evidence can be analysed using NIST approved software, especially in the domain of IoT, any non-standard software used should be accompanied with detailed contemporaneous notes and reproducibility reports.

2.3 *Attribution* – Attribution is left to courts or tribunals, however, the digital evidence should provide facts that associate a user to the event identified in the analysis stage. For example, in some cases, DFIs can use access logs, traffic, personal device, IoT logs, to associate a user to an event. If no attribution can be found then the next sub-phase, Evaluation, cannot be valid and the DFI revisits the hypothesis.

2.4 *Evaluation* – Once the attribution has been assigned, the validity of the results are tested. On the successful validation of results the hypothesis can be accepted and the output is passed on to the next phase.

4.3 Interpretation

The Interpretation phase is for using standardised practices to explain the facts discovered across the investigation with the results obtained from the Analysis phase. After the hypothesis has been accepted and validated the interpretation phase delivers statements with legal context for later reporting and presentation phases. Figure 5 shows the activity diagram for the interpretation phase and the sub-phases are explained below.

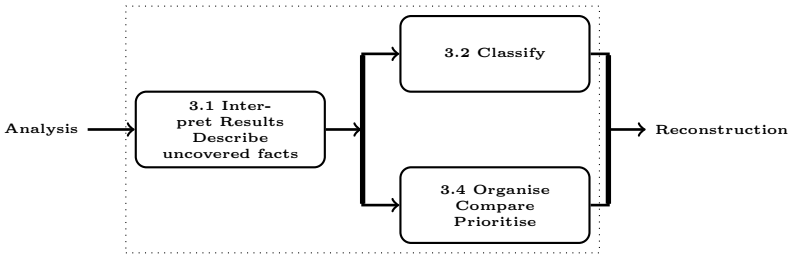

Figure 5: Activity Diagram for Interpretation Phase

3.1 *Interpret Results* – The interpretation of the results will depend on the availability of data and circumstances around the development of the case [19]. In addition DFIs may require information from individuals involved in the operation in order to carry out a more effective interpretation. This sub-phase is concerned with mapping the analysis to the goal and scope of the investigation. During this process DFIs must analyse links and use timeline tools in order to reconstruct events.

3.2 *Classify* – The classification of the event under scrutiny may support other facts; it is rare that a single event leads to a single incident, it is normally the amalgamation of a series of events that leads to the incident. These events need to be classified and put in some hierarchical order; this may also benefit timeline analysis, again the forensic readiness can provide a dynamic timeline analysis using the information gleaned from the blockchain.

3.3 *Organise* – Simultaneously, these events can be organised and given priorities.

4.4 Reconstruction

The previous three stages have parallel streams for the device; network; and, cloud data. This phase collates the data from these parallel streams to form an overall picture of the cyber physical system.

The reconstruction of events provides admissible evidence and typically for smart environments will involve a simulator. The simulation of events needs to be reproducible and can be problematic with non-deterministic systems, such as cyber physical systems [17] that rely and respond to user interaction.

There are further problems predicted in the reconstruction of smart environments. Blockchain engineering will undoubtedly be introduce to manage the security, authenticity and integrity of the communication between IoT devices, but this will only help if investigators are given sufficient read access permissions. In the proposed model this information would be governed by a permissionless blockchain, IOTA, and information regarding the identity, spatio-temporal and state would be accessible. The data would be accessed via a different parallel stream, as indicated in fig.9.

Blockchain analysis will be required to identify which components were activated and as a result completed transactions which result in the generation of blocks. There are many simulators of smart environments, however, these simulators do not allow for the simulation of blockchain components.

The consolidation of events in a smart environment, will require significant work and emphasis on the results from the interpretation phase. Figure 6 shows the activity diagram for the reconstruction phase, followed by the description of the sub-phases.

4.1 *Consolidation* – In the interpretation phase it was mentioned that there may be a number of events that lead to a culminating activity that is considered illegal. The consolidation sub-phase is responsible for putting all the events together

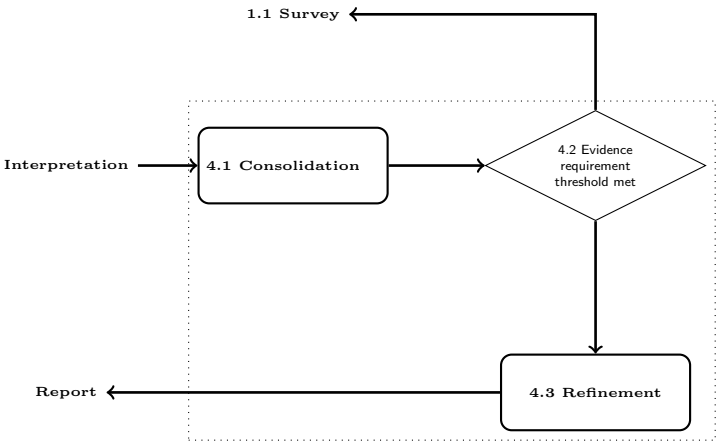

Figure 6: Activity Diagram for Reconstruction Phase

and in a simulated environment looking at how these event are accumulated into a single action. For example, in a smart home/environment with many IoT devices, it may be necessary to track a certain device and its changing states over time to exonerate or incriminate some behaviour of the accused. The consolidation phase may indicate multiple actions of an individual using many IoT devices and other digital artefacts.

4.2 *Threshold* – All evidence has to meet a threshold to stand scrutiny in a court of law. Increasingly, it is becoming difficult for the DFIs to explain to legal representatives the details about the information gathered. It is suggested that counsel is arranged between parties and reconstructions to date are demonstrated, showing the output of the consolidation process. If the threshold is reached then the next stage of reporting can begin, however, if the threshold is not met then going back to the survey sub-phase in the Examination phase would be considered or ultimately closing the case.

4.3 *Refinement* – If counsel returns positive feedback and the threshold is met, then refinement of the consolidation process can begin, ensuring reproducibility of the results. To this point the principles are continued throughout all of the sub-phases and therefore the reproducibility is not be a problem.

4.5 Report

Documentation is a principle, the report is the phase that collates all the information hitherto, into a comprehensive report with precise details of each phase. All evidence presented should uphold scrutiny [16] and the DFI is to remain impartial and rely on the known facts [5]. Unlike single device or multiple independent device investigations, where the software used can automatically generate the report, IoT investigations are different and some investment is required from the law enforcement agencies to ensure the generation of documentation is integrated, automated and consistent. The report must have conclusions that are reproducible by independent third parties and include the following [39]:

- *Seizure forms* – Authorisation, Evidence logs, transportation of evidence logs, attendance logs, photo/videos, contemporaneous notes, interview notes, and other documentation used at the incident scene.

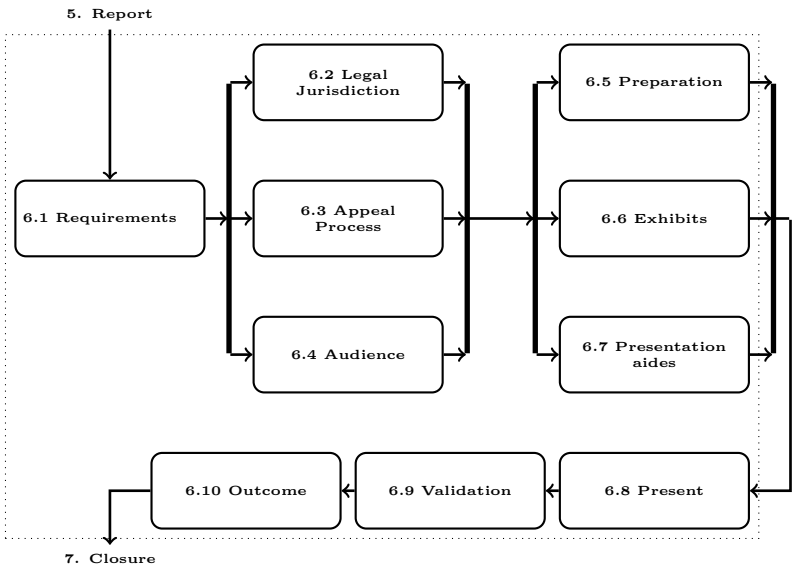

Figure 7: Activity Diagram for Presentation Phase

- *Evidential Continuity* – The chain of custody forms, showing the transfer of evidence to custodians.
- *Reconstruction & Analysis* – A brief outline of any reconstruction and analysis methods used and the revealed results.
- *Software licenses* – Provide valid licenses of any software used.
- *Personnel* – Certificates and brief biopics of personnel involved in the case.
- *Other* – and all the information from the other phases.

Due to the multimedia, videos etc.., it is advised that the report take on a different structure than traditional linear paper-based reports. The information about the case would be held on a private cloud, the report should take on a multimedia form and be non-linear based, e.g., web-based/html. This would certainly ease the burden on collating evidence and generating a single linear based report. Due to the parallel streams in the DFIPM, multiple teams can work interdependently and when ready make available via a report the information required, this can then be pointed to via an organised hyperlink.

4.6 Presentation

The presentation phase is not without peril, but good preparation to a wide range of audience, use of user-friendly and non-technical vocabulary and adhering to the facts should prevail. Figure 7 shows the activity diagram for the presentation phase and the sub-phases are discussed in the following list.

6.1 *Requirements* – Case type will determine the structure of the report. It is recommended that the report is a non-linear collection of documents stored on private cloud. The advancements of technology allows us to record video of the reconstruction of events, which can provide excellent guidelines on reproducibility and show that Standard Operating Procedures (SOP) are being followed. This has the consequence of non-linear means that the focus is on the content,

there should be a standard set-up for the identified case type and then the DFIs are left to populate and manage the content.

6.2 *Legal Jurisdiction* – Ensure that the seizure of all material was authorised by correct legal authority and appropriate forms are included in the report.

6.3 *Appeal Process* – Whilst the outcome of the case could be successful, the appeal process has to be considered. The documents and related evidence should be archived and stored for no longer than the time required to lodge an appeal.

6.4 *Audience* – Some documents in the report may require some re-writing using a simplified and non-technical vocabulary understood by a wide range of audience.

6.5 *Preparation* – The preparation of appropriate individuals to be called to give evidence. You do not want your expert on Mobile Phones presenting evidence on a WiFi enabled coffee machine that has been used to complete a DDoS attack on an organisation's network. The individual presenting should be involved in the reconstruction, be briefed and defer questions to other experts in the case when unable to provide a direct answer. IoT Forensics may require several experts to give evidence, this opens the opportunity for the defence to build upon any inconsistencies given in their testimonies. There needs to be a coherent and comprehensive narrative based on facts, and therefore it is recommended that during pre-trial briefs everyone is invited.

6.6 *Exhibits* – Ensure evidence bags, labels and accompanying forms have correct and matching information for each artefact presented.

6.7 *Presentation Aids* – Elaborate diagrams and video may be required to explain complexity of the IoT system.

6.8 *Present* – This sub-phase represents the live presentation complete in a legal setting; where possible, it is advised that this be recorded or notes taken of performance of the many individuals that may be involved. This feedback can be useful for the debriefing.

6.9 *Validation* – Did the validation of the hypothesis succeed after the presentation, was there anything omitted?

6.10 *Outcome* – The outcome of the case based on the evidence provided.

4.7 Closure

Closure is not only about closing the case. It is also concerned with the destruction or return of evidence and concerned with debriefing and improving quality of the procedures and processes used.

7.1 *Outcome* – The outcome of the case can be used to assess the strengths and weaknesses of the organisation's policies, procedures and regulatory compliance.

7.2 *Hypothesis* – The DFIPM is an iterative process and allows DFIs to visit any of the preceding phases.

7.3 *Critical Review* – Regardless of the outcome, a critical review of the case should be written and should identify good practice and make recommendations.

7.4 *Identify lessons learned* – During the critical review and debrief there should be a list of recommendations that should serve to improve the professional practices and overall quality of the digital forensic laboratory.

7.5 *Store, destroy, re-cycle or up-cycle* – Destruction should be a last resort of any material. Many organisations are striving for carbon neutral footprints and the destruction of evidence should be a last resort. Evidence can stay in the evidence store and be used for training personnel. Many of the elements of the artefacts

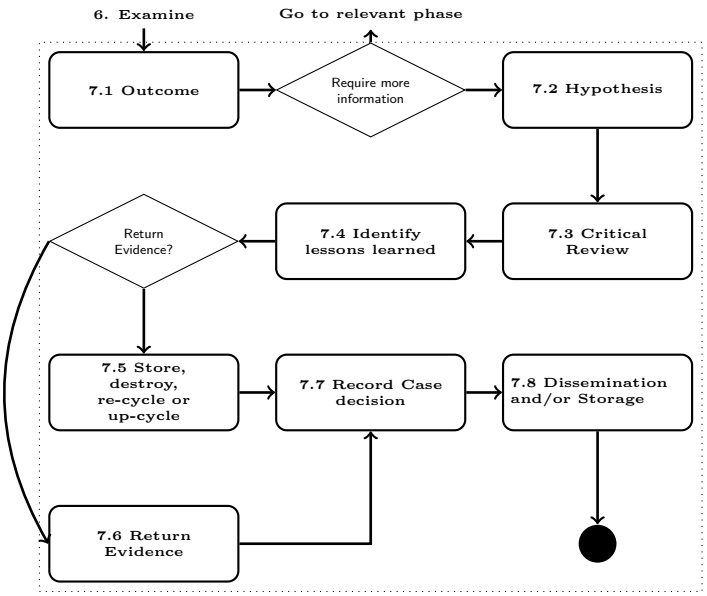

Figure 8: Activity Diagram for Closure Phase

can be re-purposed or sold, if appropriately wiped of any information. The key point here is that only at this point can the artefacts be considered for reuse or destruction, where reuse is chosen ensure that there is a strict guidance policy regarding GDPR [12], e.g. the right to be forgotten, if the suspect is cleared of all charges.

7.6 *Return evidence* – Depending on the outcome of the case and the case type, the priority should be to return the evidence. It should be noted that for some case types evidence cannot be returned.

7.7 *Record Case decision* – A record of the case decision should be included in the critical review.

7.8 *Dissemination and/or Storage* – Relevant information regarding the case must be disseminated to all authorised stakeholders. It may include notification regarding the return to previous processes, acceptance or rejection of the hypothesis, a failure to demonstrate in a believable manner the reconstruction of events or other reasons.

4.8 Summary

Figure 9 shows the overview of the proposed DFIPM merging multiple architectures that IoT interacts with, the principle that it must have, the "Privacy by Design" principle – remember any digital evidence may uncover private data irrelevant to the case – and the mandatory aspects that would lead to a reliable investigation process assuring data privacy. During the evidence collection or acquisition it is necessary to isolate the type of information gathered, separating them into device, network and cloud forensics. This is because each architecture deals with different tools, methodologies and timelines, leading them to different interpretations. Once each component reaches the interpretation phase, they will all get merged into the event reconstruction phase. Then the remaining phases are completed in a serial manner, with the option of some iteration.

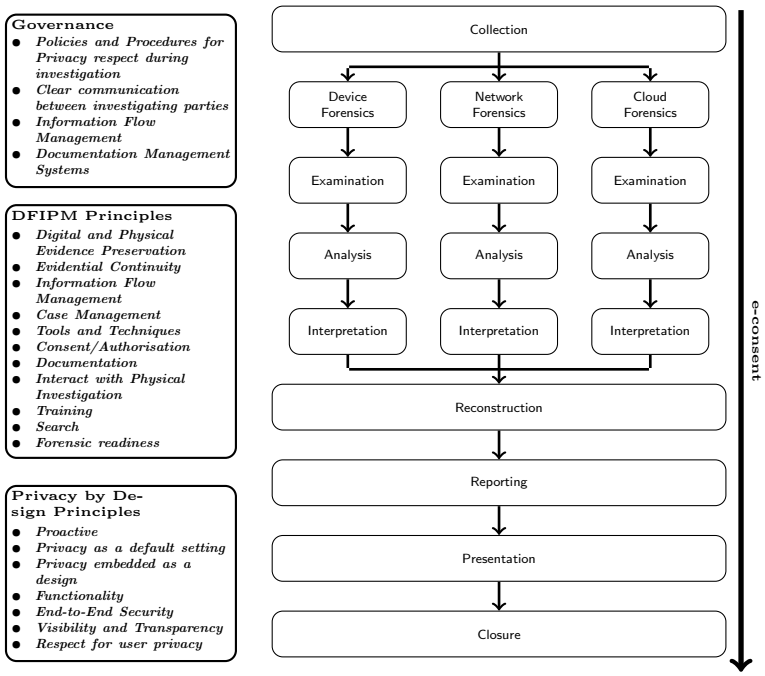

Figure 9: Overall view of DFIPM

It is this final overview in Fig. 9 that is important and shows the parallel streams working in the different domains, namely: Device Forensics; Network Forensics; and, Cloud Forensics.

5 Conclusions

The main contribution of this paper is the proposed model, DFIPM, which has three parallel streams working in each of the areas identified in cyber physical systems: device; network; and, cloud. The parallel streams produce data for the reconstruction of events phase, from where it continues through more traditional phases until it reaches the closure phase. Each phase's sub-phase is explained in detail in §4. Whilst the phases are being complete there are some over-riding principles discussed also in §4 and briefly listed as follows: Preservation; Evidential Continuity; Information Flow Management; Case Management; Tools and Techniques; Interacting with physical investigation; Training; Search strategies; and, Forensic readiness.

The use of blockchain technology, such as IOTA [35], to securely record the information about state is crucial to making cyber physical systems forensic ready. As discussed in section $2.3 blockchain technology would not provide the data that IoT devices may record, however, it can identify the device and then provide provisional access to the data. Essentially, it will allow DFIs to identify which components in the cyber physical system are to be included in the investigation. This may seem odd, but already we are seeing a wide range of devices that could amount to 100's of artefacts being seized for a single smart environment. A crucial contribution of this paper is the benefits of having access to read the records of each IoT device and then consider in subsequent phases what is relevant and whether or not to make a request to the SPoC for the associated data.

In the future this will become important, since it is quite possible that every incident will result in 100's of digital IoT artefacts being seized. By their nature cyber physical systems are constantly changing state and therefore, the challenge for digital forensics is how to capture that dynamic data and reconstruct a timeline of events. This in the past has been accomplished in many textbooks, e.g., see [20], however cyber-physical has a more interactive role with living organisms [1]. The interaction of the investigator has to be kept minimal, especially where the data from that IoT device is unlikely to be provided by the service provider and the memory (data) size of the IoT device is small. In such cases the overwriting of data due to contamination from many physical interactions between the investigators and the IoT device could lead to loss of data. Seizure and preservation have a paradoxical relationship, you cannot seize some IoT devices without contamination. However, DFIs must document every effort that seizure caused minimal changes to the IoT device, whilst maximising the possible amount of data recovered from the IoT device.

Finally we return to Heraclitus and his tenant on flux, and the quote, 'You cannot step into the same river twice'. Whilst this is often seen as a test of resilience, i.e. you will be a different person tomorrow, it also has another interpretation from the river's perspective, which is always changing. By 2025 there will be an estimated 21.5Bn IoT devices, and hence this flood of technology will make walking into the same smart environment twice an impossibility due to the state change of the IoT devices. Without necessary safeguards it will become difficult for DFIs to investigate incidents due to the number of IoTs involved and the complexity it brings. Creating cyber physical systems with non-registered or unaccountable IoT devices is likely to see a rise in challenging and socially unacceptable behaviour, as witnessed by the introduction of social media [25]. The introduction of standardised blockchain technology will make cyber physical systems not only forensic ready, but could also have the added benefit of minimising challenging or socially unacceptable behaviour, or at least finding some accountability for the incident.

Conflicting Interests:

None identified.

References

[1] Leonardo Babun, Amit Kumar Sikder, Abbas Acar, and A Selcuk Uluagac. Iotdots: A digital forensics framework for smart environments. *arXiv preprint arXiv:1809.00745*, 2018.

[2] Imran Bashir. *Mastering Blockchain.* Packt, 2 edition, 2018.

[3] BBC. Ring doorbell 'gives facebook and google user data'. `https://www.bbc.co.uk/news/technology-51281476`, 2020. [Accessed: Jan 2020].

[4] Jake L. Beavers, Michael Faulks, and Jims Marchang. Hacking nhs pacemakers: A feasability study. *Global Security, Safety and Sustainability The Security Challenges of the Connected World*, 2019.

[5] Nicole Lang Beebe and Jan Guynes Clark. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, 2(2):147–167, 2005.

[6] Carmen Camara, Pedro Peris-Lopez, and Juan E Tapiador. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of biomedical informatics*, 55:272–289, 2015.

[1] N.B. Many cyber-physical systems with wireless sensors are used with livestock

[7] B. Carrier and E. H. Spafford. An event-based digital forensic investigation framework. In *Digital forensic research workshop*, pages 11–13, 2004.

[8] Eoghan Casey, Andrew Blitz, and Christopher Steuart. Digital evidence and computer crime, 2005.

[9] Richard Chirgwin. Finns chilling as DDoS knocks out building control system. `https://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/`, 2016. [Accessed: Jan 2020].

[10] Christopher D Clack, Vikram A Bakshi, and Lee Braine. Smart contract templates: essential requirements and design options. *arXiv preprint arXiv:1612.04496*, 2016.

[11] Christopher D Clack, Vikram A Bakshi, and Lee Braine. Smart contract templates: foundations, design landscape and research directions. *arXiv preprint arXiv:1608.00771*, 2016.

[12] Council of European Union. Council regulation (EU) no 2016/679. `http://eur-lex.europa.eu/legal-content/en/LSU/?uri=CELEX%3A32016R0679`, 2018. [Accessed July 2018].

[13] M Divya and Nagaveni B Biradar. Iota-next generation block chain. *International Journal Of Engineering And Computer Science*, 7(04):23823–23826, 2018.

[14] Nabil El Ioini and Claus Pahl. A review of distributed ledger technologies. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pages 277–288. Springer, 2018.

[15] Forensic Science Regulator (FSR). Codes of Practice and Conduct for Forensic science providers and practitioners in the Criminal Justice System. Technical report, UK Govt, Birmingham, UK, 2017.

[16] Daniel B Garrie. Digital forensic evidence in the courtroom: understanding content and quality. *Nw. J. Tech. & Intell. Prop.*, 12:1-128, 2014.

[17] Edward R Griffor, Christopher Greer, David A Wollman, and Martin J Burns. Framework for cyber-physical systems: Volume 1, overview. Technical report, National Institure of Standards and Technology, 2017.

[18] Jaime Ibarra. Digital forensic investigation process model (DFIPM) to IoMT ensuring data privacy. Master's thesis, Northumbria University, Newcastle, UK, 2019.

[19] ISO17025:2017. General Requirements for the Competence of Testing and Calibrating Laboratories. Technical report, International Organisation for Standardization (ISO), Geneva, CH, 2017.

[20] Keith J Jones, Richard Bejtlich, and Curtis W Rose. *Real digital forensics: computer security and incident response.* Addison-Wesley Professional, 2005.

[21] Umit Karabiyik and Kemal Akkaya. Digital forensics for iot and wsns. In *Mission-Oriented Sensor Networks and Systems: Art and Science*, pages 171–207. Springer, 2019.

[22] Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang. Guide to integrating forensic techniques into incident response. Technical report, National Institute of Standards and Technology, 2006.

[23] Paul L Kirk. *Crime investigation; physical evidence and the police laboratory.* New York, 1953.

[24] Knud Lasse Lueth. State of the IoT 2018: Number of iot devices now at 7b - market accelerating. `https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/`. [Accessed: Jan 2020].

[25] I. Mitchell, T. Cockerton, S. Hara, and C. Evans. SMERF: Social media, ethics and risk framework. *Cyber Criminology*, 2018.

[26] I. Mitchell, S. Hara, H. Jahankhani, and D. Neilson. Blockchain of Custody, BoC. *Cyber Security Practitioner's Guide*, 2019.

[27] Reza Montasari. *The Comprehensive Digital Forensic Investigation Process Model*. PhD thesis, University of Derby, 2016.

[28] Reza Montasari. A comprehensive digital forensic investigation process model. *International Journal of Electronic Security and Digital Forensics*, 8(4):285–302, 2016.

[29] Reza Montasari and Pekka Peltola. Computer forensic analysis of private browsing modes. In *International Conference on Global Security, Safety, and Sustainability*, pages 96–109. Springer, 2015.

[30] Francois Mouton and HS Venter. A prototype for achieving digital forensic readiness on wireless sensor networks. In *IEEE Africon'11*, pages 1–6. IEEE, 2011.

[31] A. Nagasai. Classification of iot devices. `https://www.ciscoplatform.com/profiles/blogs/classification-of-iot-devices`, 2017. [Accessed: Jan 2020].

[32] Edewede Oriwoh, Paul Sant, and Gregory Epiphaniou. Guidelines for internet of things deployment approaches–the thing commandments. *Procedia Computer Science*, 21:122–131, 2013.

[33] G. L. Palmer. A roadmap for digital forensics research - report from the first digital forensics workshop (technical report dtr-t001-01-final). *Air Force Research Lab, Rome Research Site, Utica*, pages 1–48, 2002.

[34] Serguei Popov. The tangle. `http://tanglereport.com/wp-content/uploads/2018/01/IOTA_Whitepaper.pdf`, 2016. [Accessed: Jan 2020].

[35] Serguei Popov, Hans Moog, Darcy Camargo, Angelo Capossele, Vassil Dimitrov, Alon Gal, Andrew Greve, Bartosz Kusmierz, Sebastian Mueller, and Andreas Penzkofer. The coordicide. pages 1–30, 2020. [Accessed: Jan 2020].

[36] F Uribe. The classification of internet of things (iot) devices based on their impact on living things. SSRN: https://ssrn.com/abstract=3350094 or http://dx.doi.org/10.2139/ssrn.3350094, 2018. [Accessed: Jan 2020].

[37] U.S. Department of Justice . *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*. National Institute of Justice, November 2009.

[38] Altman Vilandrie. Survey: Nearly half of u.s. firms using internet of things hit by security breaches. `https://www.businesswire.com/news/home/20170601006165/en`, 2017. [Accessed: Jan 2020].

[39] D. Watson and A. J. Jones. *Digital Forensics Processing and Procedures: meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*. Elsevier, 1 edition, 2013.

[40] Janet Williams. Good practice guide for digital evidence. `http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf`, March 2012. [Accessed March 2018].

[41] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain technology overview. Technical report, National Institute of Standards and Technology, 2018.