Internet of Things Forensics: Challenges and Approaches

Conference Paper · October 2013

DOI: 10.4108/icst.collaboratecom.2013.254159

4 authors:

Edewede Oriwoh
University of Bedfordshire
16 PUBLICATIONS **35** CITATIONS
SEE PROFILE

David Jazani
University of Bedfordshire
7 PUBLICATIONS **35** CITATIONS
SEE PROFILE

Gregory Epiphaniou
University of Bedfordshire
24 PUBLICATIONS **60** CITATIONS
SEE PROFILE

Paul Sant
University of Bedfordshire
45 PUBLICATIONS **170** CITATIONS
SEE PROFILE

Internet of Things Forensics:

Challenges and Approaches

Edewede Oriwoh, David Jazani, Gregory Epiphaniou
Department of Computer Science and Technology
University of Bedfordshire
Luton, United Kingdom
{edewede.oriwoh, david.jazani,
gregory.epiphaniou}@beds.ac.uk

Paul Sant
University Campus Milton Keynes
United Kingdom
paul.sant@beds.ac.uk

***Abstract*—The scope of this paper is two-fold: firstly it proposes the application of a 1-2-3 Zones approach to Internet of Things (IoT)-related Digital Forensics (DF) investigations. Secondly, it introduces a Next-Best-Thing Triage (NBT) Model for use in conjunction with the 1-2-3 Zones approach where necessary and vice versa. These two 'approaches' are essential for the DF process from an IoT perspective: the atypical nature of IoT sources of evidence (i.e. Objects of Forensic Interest - OOFI), the pervasiveness of the IoT environment and its other unique attributes - and the combination of these attributes - dictate the necessity for a systematic DF approach to incidents. The two approaches proposed are designed to serve as a beacon to incident responders, increasing the efficiency and effectiveness of their IoT-related investigations by maximizing the use of the available time and ensuring relevant evidence identification and acquisition. The approaches can also be applied in conjunction with existing, recognised DF models, methodologies and frameworks.**

Keywords- Internet of Things; digital forensics; security; model

I. INTRODUCTION

In the Internet of Things (IoT) domain, objects such as baby monitors, cars and tablet computers are being equipped with the capability to communicate with each other, providing improved efficiencies for those who own or use them. Objects that are not of themselves smart are being embedded with smartness and communication capabilities through the use of technologies such as Radio Frequency Identification (RFID), sensors and other forms of embedded computing [1]. Communication with such objects will be done i) directly, ii) using remote methods for instance over the internet or iii) via 'learned' control or other smart devices. In the IoT, *Things* (also known as spimes or blogjects) are meant to be intelligent, autonomous and will be networked in the form of 'X' Area Networks e.g. Personal Area Networks (PAN), Home Area Networks (HAN), and Metropolitan Area Networks (MAN). These disparate technologies within the IoT are being interconnected in networks which are hybrid and evolving (i.e. changing their structure). For instance a user's X-box which is part of her HAN can become part of a neighbour's HAN when borrowed by a friend. This interconnection between smart disparate technologies and devices already offers various useful benefits and applications to end users, industry, companies and governments including in areas of transportation, healthcare, Smart Cities, etc. [2, 3]. Cisco's estimated revenue benefits that the IoT will offer is $14.4trillion between 2013 and 2022 [4].

However, various security issues, threats, and attacks in relation to the IoT have already been identified and these include surveillance, viruses, and Denial of Service (DoS) attacks [5, 6]. There has even been some discussion around the possibility of large scale disruptive botnets [7] within IoT-based networks. The need for a forensics methodology for investigating IoT-related crime is therefore pertinent. The IoT poses some challenges for forensics investigators including the widened spread of data and information, the blurring of lines between networks, and the (expectation of) privacy by users with personal networks increasingly fading into non-personal ones and private networks blurring into public ones.

Currently, the focus in the IoT domain centers on its benefits and applications as well as security and privacy issues that apply. There is little by way of a dedicated incident response methodology for Digital Forensics (DF) responders within the IoT domain. This gap is what this paper aims to fill: to propose a high-level incident response strategy for approaching IoT-based crime scenarios

The paper is structured as follows: Section II reviews previous work in the area of DF; Section III presents a hypothetical IoT crime scenario and attempts to identify sources of evidence within it; Section IV discusses the uniqueness of the IoT with respect to Digital Forensics (DF); Section V discusses forensics in the Internet of Things and introduces the 1-2-3 Zones and the requirement for a Next Best Thing (NBT) Model of digital forensics. Finally Section VI discusses future research and concludes the paper.

II. PREVIOUS WORK

Various major areas make up the IoT. These areas include Cloud, virtualisation, mobile devices, fixed computing, sensor and RFID technologies, and artificial intelligence. Forensics in the IoT will therefore encompass forensics in all these areas and more. This section presents the current situation within the DF landscape.

978-1-936968-92-3 © 2013 ICST
DOI 10.4108/icst.collaboratecom.2013.254159

A. Digital Forensics - plain and simple

Digital forensics is a field that deals with the investigation of technology-related crimes. These crimes cover those perpetrated against, using or perpetrated through technology. With the IoT, a key addition would be crimes *perpetrated by* and *originating solely from* technology.

DF investigations are carried out by trained, experienced, qualified investigators who use open source and/or proprietary tools (e.g. the Computer Aided Investigative Environment - C.A.IN.E. and Encase) to carry out tasks such as acquiring and analyzing relevant digital evidence. They employ widely accepted methodologies in order to ensure that all evidence obtained during these investigations is acceptable in a law court. Among the existing methodologies are the 4-stage Computer Forensic Investigative Process and the 13-stage Extended Model of Cybercrime Investigation (EMCI) [8]. All the methodologies have the basic underlying formula of preparation, investigation/analysis/examination, reporting/presentation/, storage (and returning evidence in some cases). In addition to these methodologies, guidelines such as the Association of Chief Police Officers (ACPO) guidelines [9] and the Standards and Principles of the Scientific Working Group on Digital Evidence (SWGDE)/International Organisation on Digital Evidence (IODE) [10] are widely recognised and appropriately applied by DF responders during investigations. These methodologies and guidelines will still prove useful in the IoT domain because, although IoT crime scenes may differ from traditional digital crimes in their increased scope, the investigations will still - to some extent - concern digital crimes and therefore will require similar (and possibly even hybrid [11]) approaches.

In typical DF scenarios the hardware devices of focus include personal computers (PC), printers and, more recently, mobile devices like cell phones, tablets and e-readers. Soft computing focal points include websites and software applications. All these will still remain points of interest and sources of evidence during IoT-related investigations. In the IoT, the evidence landscape, rather than change completely, will become broader in terms of the number and type of devices of interest, their location, the quantity of information that they will carry and their interaction with other devices. DF investigators will have to take into account the movement of people, with their IoTware, between networks (In this paper, things, devices and/or objects that make up the IoT are also referred to by the generic term 'IoTware', pronounced *yot*ware). These factors will contribute to the increased complexity of situations incident responders to IoT investigations will be faced with and they will therefore require highly efficient and effective investigative approaches which complement existing tried and tested forensic models, methodologies and frameworks. This paper recognises that for reasons highlighted in section III, the IoT introduces unique dimensions to DF and that these differences will require a unique approach to forensics in the IoT and related smart systems.

B. Cloud forensics

Cloud forensics will play a key role in the IoT forensics sphere especially since the data generated from IoTware and IoT networks are already being, or will increasingly be stored, on cloud locations. This is because cloud solutions offer various benefits including convenience, large capacity, scalability, and on-demand accessibility. However, attacks such as Structured Query Language (SQL) injection, side channel, authentication, man-in-the-middle attacks, and insecure virtual machine deletion, etc. being discovered and exploited in various cloud-related crimes have led to a need for digital forensics in the cloud environment. Cloud forensics is made difficult by the absence of agreements between parties in the cloud which can allow for investigations within and between customer cloud-based services. In addition, the (sometimes unknown) location of the sources of evidence, as well as inter-judiciary disparities can make cloud computing a challenge for DF investigators [12]. These threats and challenges to cloud environments will inevitably also apply to the IoT-based forensic investigations.

The next section introduces the hypothetical crime scenario which will provide the backdrop for the discussion on how IoT-related investigations might be approached.

III. Hypothetical Scenario

In order to answer the question posed by the title of this paper and to highlight the questions that DF investigators may have to answer in IoT-related crime situations, a hypothetical crime carried out by a Mr. X who used various IoTware to commit crimes is described.

Hypothetical Scenario

Mr. X works for 'Smart Kids' the local elementary school as an IT technician. His Personal Area Network (PAN) is made up of his mobile phone and a tablet computer. He uses free cloud storage services provided by Microsoft Sky and Amazon Cloud to store files that he has acquired illegally. His main job is corporate espionage and blackmail. He works away from home and is always on the move, accessing the Internet by piggybacking on available open networks he can find. His personal devices are not registered with any Internet or mobile service providers. He bought them second hand and paid cash for them through a decoy. He uses his phone to make and receive calls and messages only.

Mrs. Smart's Home Area Network (HAN) is made up of her laptop, her son's X-box games console, her intelligent home lighting and heating system, her car and smart medicine dispenser. Mrs. Smart is the Head teacher of 'Smart Kids'.

The local hospital, 'Healing Hands' has rolled out a system in which all electronic devices and patient related systems have been networked. This was done to improve efficiency, reduce human error and save time. The hospital's 'intelligent' medicine dispensing cabinets and patient records are also connected up to this system with different levels of access rights assigned to different services and resources at the hospital. Doctors at the hospital interact with patients remotely providing advice and recommending changes in doses without the requirement for patients to come into the hospitals.

Lastly, 'Smart Kids' has also rolled out a system in which all the computers are networked. All the entry and exit routes

(doors, gates and windows) are centrally computer controlled. In addition, the school has a central cloud system where students can store files and retrieve them and the student results are available online and can be accessed locally or remotely so students can see their results from the comfort of their own home.

Mr. X was recently laid off by 'Smart Kids' on claims that he tampered with their computer security services. He feels he was unfairly dismissed for trying out at work the skills he acquired from a security workshop. As a result, Mr. X is not happy with his former employer.

The Attack

Mr. X uses his mobile devices to access the hospital records and to carry out the following attacks:

- He starts by tampering with the medications of Mrs. Smart which she is due to pick up later that day. He gains control of her GP's hospital email account and from it, sends an email to her informing her that the renewed prescription has been reduced because her health has improved. Her smart medicine dispenser will therefore only dispense the reduced dosage. Mrs. Smart is bewildered since she has not noticed or reported any improvements in her health to her GP.
- He accesses the automatic navigation system in her car and configures it so that it selects the longest route to any destination selected.
- Using a backdoor exploit that he installed while he worked at 'Smart Kids', Mr. X accesses the school records of his son and lowers his grades. Then he makes a complaint to the local police about discrimination against his son because of his own reputation with the school.
- He fills up her son's 64Gb storage space on his Xbox with indecent images of people that neither she nor her son know.
- By escalating his privileges on her home network, he tampers with the smart lighting system in Mrs. Smart's home. The system was originally programmed to switch on her lights based on movements from room to room. Mr. X modifies the settings so that instead the lights turn off whenever Mrs. Smart and/or her son enter a room and turn on when they leave. Mrs. Smart is concerned because this means the lights stay on for the whole time that they are away from the house.

As a result of these attacks, 'Smart Kids' school requests an investigation into the problem with their computing systems. The hospital also orders an investigation to determine why certain hospital records appear to have been tampered with. Mrs. Smart is worried about her rising home electricity bills. She is also not pleased that her car has been consistently choosing the longest routes to various destinations in the last few days thus making her arrive late. She has misplaced the car manual and does not know how to override the automatic setting in her car. Mrs. Smart calls the companies that provided and installed the different services to investigate the situations. She also invites a forensics company to make sure she has not been *attacked*, a word with which she had become familiar after of the results of the digital forensic investigations into Mr. X's 'past-time' activities had been presented to the school governing body.

The next section proposes some questions that will be pertinent in the preceding scenarios.

A. Some questions that investigators who are called in to investigate these scenarios might choose to ask:

1) Questions to the hospital and school:

- Who has access to what records?
- How are these records typically accessed - locally, remotely?
- What are the permission levels and have these been breached in the past? How easy is it to breach these i.e. are there any results from penetration tests that have been carried out?
- Are there any logs kept by the hospital and school of who accessed what and when?
- Are there any security cameras around the school that might show people loitering around with laptops or other mobile devices that can be used to access the school's network?

2) Questions to the Smart lighting system designer:

- Is there any recourse from the Smart lighting system designer for the issues she has been experiencing?
- Does the designer have any system in place that might assist with forensic investigations?

3) Questions to the Smart lighting system vendor:

- Is there any recourse for the issues your customer has been experiencing?
- Do you have any incident response system in place to investigate such issues?

4) Questions to Mrs. Smart and her son:

- How is the lighting system controlled - locally or remotely? Does she have a strong password setup? Has she shared the password with anyone else or used the same password for other services?
- Do you have a firewall, intrusion detection/intrusion protection system and other such perimeter security services set up?

It is clear from the above questions that DF in the IoT will have to work closely with law enforcement and end users especially in domestic (non-commercial) cases. For instance, in the scenario presented, access will be required to Mrs. Smart's son's X-box game online records which may reveal his gaming habits etc. and this might be a cause for concern for him. Also, giving investigators access to hospital records may be a cause for concern for patients of the 'Healing Hands' hospital. Therefore a clear definition of permissions, access rights and

access methods must be agreed during the preparation stage (section V.C.1)) of any investigation.

B. *One possible approach to the problem:*

DF investigators can choose to set up monitoring and so physically and logically monitor Mrs. Smart's HAN communication network although there may be some difficulty with obtaining evidence if the devices on her network communicate using proprietary communication protocol. In that case, specialist tools may have to be designed to capture and analyse captured information.

Evidence of interest in this scenario

- Logs - hospital access logs to Mrs. Smart's records and to her physician's devices and account.
- Access logs of her son's games console
- Access logs of her car and possibly the car's black box.
- Smart lighting system logs.
- Logs of all edge devices in her home e.g. firewall, Network and Host Intrusion Detection System (NIDS and HIDS) etc.

While it is important to adequately prepare for an investigation in the IoT domain, it is important to avoid a 'Big Brother' approach to pro-active forensics. For instance, imagine a situation where DF investigators manage to track a shirt to a user based on the information being transmitted by the RFID tag on the shirt; tracking that person around a locality has to be discouraged if there is no pre-agreed legal backing for this kind of activity. Having the facility to achieve the goal should not be interpreted as the right to do so - setting these boundaries will discourage possible Wild West bounty hunter situations from developing.

In this scenario, a human was the perpetrator. In other cases, a software 'bug' can cause a smart thing to unwittingly set off a chain of events such as dispensing the wrong amount of drugs in a hospital system that uses smart medicine cabinets. This can also be set off by a poorly trained smart device. For instance a poorly trained robot nurse that should go around wards clearing up patients' dishes after they have finished their meals may adopt a poor standard and, for instance, run behind schedule as a matter of course. These examples highlight the requirement for human oversight in such systems.

IV. UNIQUENESS OF THE IOT FROM A DIGITAL FORENSICS PERSPECTIVE

There are a number of factors that should be considered when an IoT-related crime scene is approached. One such factor is the kind of hardware evidence involved. The IoT is envisaged as a system that will involve communication between a wide variety of objects from devices that already communicate (networked PCs, mobile phones, etc.) to devices that will be enabled to communicate (household appliances and human internal organs). This introduces a dimension to the DF discussion in terms of the items that are seized or cordoned off for investigation; for instance, an entire home can be cordoned off during an investigation so that the devices in them (e.g. kettles) do not get switched on/off thus ensuring the Modified Access Created Entry (MACE) values on them are not changed.

A. *Traditional vs IoT Digital Forensics*

The IoT is designed as a network of smart, decision-making, self-managing systems. The impact of this on forensics is interesting because from a point of view of number of devices, responsibility of crimes by smart things in the IoT, among others. This section presents the dimensions that IoT will introduce to DF. The IoT presents a number of dimensions which will affect the usual DF practices DF's perspective that make this discussion essential. These areas are discussed next. Forensics in the IoT might be expected to differ from traditional forensics in the following ways.

Table I highlights the areas that will be of interest in the IoT in addition to the areas under the traditional DF. A discussion about these differences is now presented.

TABLE I. IOT FORENSICS AND TRADITIONAL FORENSICS COMPARED

	IoT and Traditional forensics compared	
	Traditional forensics	***IoT forensics***
Evidence Sources	PC, Cloud, virtualization, mobile communication devices, web clients, social networks, Authentication Authorisation and Accounting (AAA) servers, gateways e.g. proxy servers.	Home appliances, cars, tags, readers, embedded systems sensor nodes, sensor networks, medical implants in humans and animals, other IoTware.
Jurisdiction	Individual, social networks, society, Company, government	Same
Number of devices	Billions of devices	50 billion by 2020 to trillions of devices
Types of evidence	Elctronic documents, standard files formats e.g. jpeg, mp3 etc.	Any and all formats possible.
Types of networks	Wired, Wi-Fi, bluetooth wireless networks, internet, mobile communications,	RFID, sensor networks, e.g. sensor to reader and vice versa.
Quantity and type of data and evidence	Up to terabytes of data	Up to exabytes of data.
Protocols	Ethernet, wireless (802.11 a,b,g,n), bluetooth, IPv4 and IPv6	RFID, Rime [14].
What to seize	Seize devices as required	Identify possible Next Best Things for source of evidence (see section V.C.3)a.)
Ownership	Individuals, groups, companies, governments, etc.	Same
Network boundaries	Relatvely clearly-definded boundaries and lines of ownership	Increasingly blurry boundary lines

1) Sources of evidence i.e. types of devices

Evidence collection in an IoT based crime scene can be expected to focus on various sources of evidence. These may include the typical computer systems i.e. desktop Personal Computers, mobile phones. With the IoT, things like household appliances may become subjects of forensics interest; dishwashers, pressing irons and baby monitors. This disparity of types of devices will introduce interesting challenges for device-level investigations.

2) The number of devices

The proliferation of interconnected and interconnection technologies is evident all around us e.g. Fleisch talks about trillions of interconnected "nerve endings" (or devices) in the IoT [13]. This is not the same scale in terms of number of devices that traditional DF has typically dealt with. With DF the focus started with a few devices, typically a desktop computer; then widened to devices on the desk and other items of interest such as USB drives, external hard drives and mobile computing devices e.g. tablets and e-book readers. This is because there might be information on the devices that may prove crucial in DF investigations.

3) The quantity and type of data

Within the IoT, we expect to see an explosion of data because of the increased number of interconnected devices that will be communicating and exchanging information across the IoT information highway. This data explosion has been discussed in [15] in which the authors anticipate a "data deluge" within the IoT domain. Gantz and Reinsel point out in their IDC (International Data Corporation) report that the expected growth of data that will be experienced from 2005 to 2020 will be 40,000 *exabytes* (where an *exabyte* is a trillion gigabytes) [16]. Within the IoT landscape, data sources in the IoT may increasingly include IoTware such as baby monitors and milk bottles all transmitting data and information and all contributing to the increase in data generated on a regular basis. This data deluge has implications for DF investigations with respect to the amount of time to be spent sifting through the increased volume of data. In addition, the *format* of the data retrieved from some IoTware may be different from what is typically encountered during traditional DF investigations and this data would have to be unraveled by investigators and placed into an understandable and usable format. There is already a push towards triage and automated forensics as methods of solving DF crimes and these two methods will almost certainly find increased use within the IoT crime domain. Automated forensics for instance is being promoted because when correctly applied it can lead to overall savings in time and money compared to the situation with traditional manual forensics methods. Triage and automation would be even more pertinent for handling DF tasks within the IoT domain.

4) The location of evidence

The storage of user data in multiple locations which may have multiple jurisdictions is already recognised issue for forensics examiners due to the locations and possible differences in laws that apply in these different locations. This issue will be mirrored in the IoT due to the use that the cloud will continue to see for the storage of IoT-generated data.

Increased juridical complexities as devices travel between networks and cross various barriers. With the IoT (in addition to the existing complexity of deciding which rules under which to prosecute cases where devices have been used between different countries) is the added dimension of devices being used between people's private, personal and public networks.

5) (Increasingly) blurring lines between networks

With traditional DF, e.g. computer and network based investigations, the boundary lines are usually clearly defined - the number of devices to be seized, the number of people involved in the communications, etc. However, with the IoT, the networks bleed into each other with Body Area Networks (BAN) moving between WANs as people travel from, for instance, their homes to their places of work. One ramification for DF will be how to handle developing efficient methods of collecting all the relevant evidence from an *Object of Forensic Interest* (OOFI) that has travelled between multiple networks, leaving multiple digital *fingerprints* in its wake. Conversely, this situation may hold some benefit for DF as it may facilitate traceability of the OOFI.

DF will be faced with issues of privacy as OOFI will be situated in areas such as hospitals where personal details such as patients' data are being collected. Therefore, obtaining the right type of permission to seize and investigate these will need to be a subject of discussion as the IoT is being developed. For instance: if the OOFI is in an internal BAN, what will be the recommended approach for DF practitioners? This is a complicated landscape that requires further exploration and the NBT approach described in this paper is a contribution to this discussion.

B. Relevant Evidence - a Scenario-based Discussion

In the IoT (or Future Internet) scenario, it will be important to discuss the meaning of relevant evidence and possibly even rank evidence by degree of relevance or importance. Responders to an incident will have to deal with questions like about what and where evidence is located in an IoT crime scene. Areas or possible attack points within a home-based IoT are numerous and it will be useful to DF as a field to highlight the areas/groups/major categories where relevant evidence may be available in an IoT home. Table II highlights possible sources of evidence in an IoT crime situation. A table like this may have to be populated by responders during every response to an incident.

TABLE II. POTENTIAL SOURCES OF EVIDENCE IN AN IOT SCENARIO

	Sources	***Example***	***Expected evidence***
Internal to network	Hardware End nodes	IoTware e.g. games consoles, fridges, mobile devices smart meters, tags, readers, embedded systems, heat controller Nest	Sensor data e.g. IP address, Rime number, sensor ID, etc.
	Network	Wired and Wireless, mobile communications e.g. GSM, sensor networks, HIDS, NIDS, HMS	Network, Logs
	Perimeter	AAA server, firewall,	Network and

	Sources	*Example*	*Expected evidence*
	devices	NAT server, IDS, NIDS, HIDS.	systems logs; authentication data, etc.
External	Cloud	Public, Private, Hybrid cloud systems.	Client Virtual Machines; logs
	Web	Web clients, web servers, social networks.	Web logs; user activity
	Hardware End nodes	Mobile devices, sensor nodes and networks,	Sensor data e.g. IP address, Rime number, sensor ID, etc.
	'X' Area Networks	Home Area Networks (HAN)	Network logs.

In the IoT domain, the cardinal questions of Digital Forensics investigations will be revised. In DF investigations, the typical cardinal questions are: *What happened? When did it happen? How did it happen?* and, *Who did it?* In the IoT Forensics, the questions investigators will ultimately be answering will be revised so that the 4th question becomes *Who and/or What did it?* (Fig. 1).

V. FORENSICS IN THE INTERNET OF THINGS

A. Points of Focus - The 1-2-3 Zones of Digital Forensics

In the IoT DF will involve knowing *where to look*. Without approaching IoT forensics this way, valuable time will be wasted looking in the wrong places for irrelevant evidence. This paper proposes a zone-based method for approaching IoT-related investigations.

Zone 1: As can be seen from Fig. 2, this is the internal zone where all hardware, software and networks (e.g. Bluetooth and Wi-Fi) that relates to a crime scene is catalogued and a decision is made about what is relevant to the case and what may hold evidence that will be useful to the case. The IoTware on these networks such as smart temperature controllers may be useful even if only for their tag identifications (tag ID) and their state i.e. asleep, awake, and active/transmitting, etc.

Figure 1. The revised Cardinal Questions of digital forensics investigations

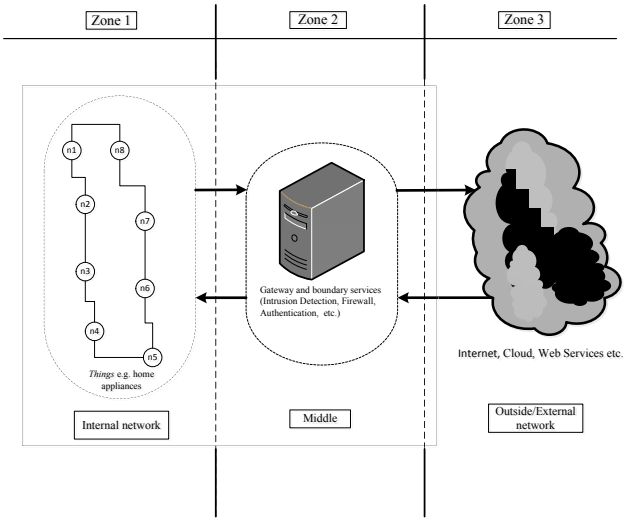

Figure 2. 1-2-3 Zones of Digital Forensics

Zone 2: In this zone resides all devices and software that are at the border of the network and that provide a communication medium between the internal and external networks. This zone all holds all public-facing devices of the networks in question. Forensics investigations will typically involve identifying these elements, cataloguing them and retrieving any available relevant evidence from them. Devices in this zone may include Intrusion Prevention and Detection systems (IPS and IDS) and network Firewalls.

Zone 3: This zone covers all hardware and software that is outside of the network in question. This zone includes evidence from all cloud, social network, Internet Service Provider (ISP) and mobile network providers' data; Internet- and web-based services, object virtual online identities, edge network, inter-network evidence (e.g. 2 neighbour's HANs), device based evidence e.g. logs from RFID tags and readers; gateway or edge devices, etc.

The application of this approach will be at the discretion of DF investigators and can be done in parallel (all Zones investigated at the same time) or a Zone of greatest priority can be identified (this can be based on the description of the reported incidence and the possibly the area of greatest impact) and a decision may be made to focus on this first.

Responding to IoT-related digital attacks using the 1-2-3 Zones described provides DF investigators with a useful method to plan and systematically approach investigations and to effectively identify possible OOFI. This approach reduces the complexity that will be encountered in IoT environments and ensures that investigators can focus on clearly identified areas and objects in preparation for investigations.

B. The Four (4) phase IoT forensics methodology

In this section, a proposed methodology for the IoT is discussed as a way of introducing the Next Best Thing Model.

In the IoT, any forensics solution that fails to take into account the nature of the IoT to continually grow, adapt and mutate may eventually become too structured to be of any use.

This is because in the IoT domain the boundaries between BAN, Personal Area Networks, Perimeter Area Networks and Premise Area Networks (PAN), Home Area Networks (HAN) and Hospital Area Networks (HAN), Local Area Networks (LAN), Neighbourhood Area Networks (NAN), Metropolitan Area Networks (MAN) and Wide Area Networks (WAN) will disappear and these networks will bleed into each other as users roam from one into another. Forensics solutions would have to recognise IoTware as they approach and join networks, and recognise when they leave. The identity and precise location of the subject of the investigation has to be established and ascertained over a period of time.

Movement of things from one network to another (Fig. 3) can have implications for forensics because of the challenge of obtaining permission at the perimeters of these disparate networks as well as within the networks.

1) Preparation

In this phase, the usual preparation steps of DF apply with additional steps. In the IoT, preparation will include all security features that are put in place eve before an incident. Such systems may include installation of security tools and software, etc. this phase involves also identifying possible areas of attacks and locations of evidence in the IoT location. This phase also involves identifying the various possible locations of evidence in the crime scene and then making a decision about what is relevant evidence. During the preparations stage phase end users, law enforcement and designers will need to agree on a set of minimal requirements that should be applicable in all IoT domains such as PANs and HANs which will enable easier investigation of IoT-related crimes.

2) Acquisition

Where typical computing devices are involved, the usual method of complete or selective imaging can be used. However, with unusual devices like baby monitors, bespoke methods may have to be developed for retrieving the data they hold especially if the interfaces available (if any at all), are not among the usual types e.g. Universal Serial Bus (USB) or Ethernet.

3) Investigation

In this phase, the investigation of the crime occurs. This phase will follow typical steps as recommended in any forensics scenario including using the industry-recognised, tried and tested tools except of course in situations where the technology before investigators is new and specialist tools are required e.g. a smart fridge with a sensor attached. In this case, the seizure and data acquisition methods might be slightly different. At this stage, and only for the sake of saving time - and storage space (imagine having to store a number of cars) - the NBT model of forensics is introduced.

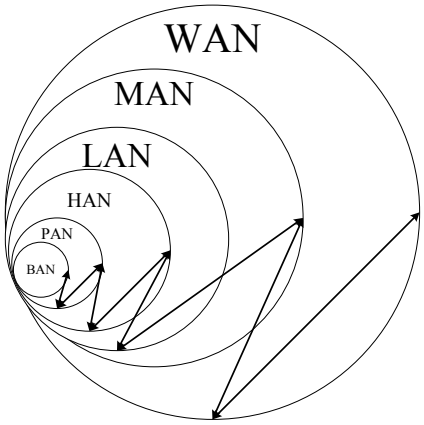

Figure 3. Movement of IoTware between inter-connected networks introduces challenges for digital forensics.

a) Next Best Thing (NBT) Triage Model

An important aspect of IoT forensics is the question of knowing *where to look*. During IoT investigations some sources of evidence might become unavailable after a crime is committed; e.g. a mobile phone might be disposed of or sensors might be removed from a HAN to a neighbour's HAN. The NBT approach can be applied to determine what devices were connected to the OOFI and what slivers of evidence, if anything, are left behind after its removal from the network. This method of forensics is proposed because within the IoT domain it might not always be possible to obtain evidence directly from sources that may be considered pertinent to an investigation. Using the NBT Model, evidentiary data can be acquired from devices that are either directly connected or somehow related to the OOFI in the event that the OOFI is not available. Consider a situation where a pacifier is the OOFI in an investigation; the best alternative evidence source would be the hospital communication link with the pacifier or a consultant's mobile or fixed monitoring device - and not the patient's pacifier. In situations where sensors deployed to capture data have been tampered with thus affecting their effectiveness, the NBT model would recommend that the evidence from the head node or a base station be captured and analysed.

4) Reporting and storage.

At this stage, any evidence collected would have been investigated and thoroughly parsed for relevant evidence. Then, a report is prepared and sent to relevant parties. The reporting can be done manually or can be an automated process using a smart forensics system. In situations where house owners register with Central Forensics Centers this report can be sent to them for further action if any is required.

C. Legal Challenges in relation to IoT Forensics

Within the IoT sphere, the current legal systems that are in place will still be largely applicable. For instance, the Computer Misuse Act (CMA) 1990 will be relevant in cases that involve the remote control of a person's home lighting system. However, from the point of view of DF, the right to access certain areas may become much more difficult to obtain. For instance, if a botnet takes over smart devices in a person's

kitchen, a legal framework will have to be in place that will allow DF incident response teams to go in and look for traditional and non-traditional computing devices as possible sources of evidence. However, if the said homeowner refuses to turn off their fridge because they do not want their food to go bad - and as long as the fridge remains turned on, it will continue transmitting malicious packets - there has to be a supporting legal structure that will allow DF investigators to turn off such devices and take them off the grid thereby bringing an end to their functions as bots at that point in time.

VI. CONCLUSION

The next stage of this research is to develop and test an IoT Digital Forensics Framework (IDFF) for use in IoT-related investigations. This framework will be tested using a Forensics Edge Management System (FEMS), a device being designed to provide automated forensics services within the IoT construct with a special focus on the IoT Home environment.

This paper proposed two approaches to digital forensics within the IoT domain considering its unique characteristics of the number and types of devices and interconnections between networks. The 1-2-3 Zones of forensics was proposed so that incident responders can map out their approach to investigations and make decisions about where exactly they should focus their attention during investigations. The Next Best Thing Triage (NBT) model of approaching IoT investigations was proposed because within the IoT domain direct access to Objects of Forensic Interest (OOFI) may not always be possible (or appropriate e.g. pacifiers). Therefore, in such situations the option of identifying and considering the *next best source of relevant evidence* may have to be taken. The design of a method of systematically deciding what this next best thing might be in different scenarios and situations can be the subject of further research.

REFERENCES

[1] J. Solomon, E. Lattimore (n.d). *Computer Forensics* [ONLINE]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.9392&rep=rep1&type=pdf.

[2] P. Jain, A. Noor and V. K. Sharma, "Internet of Things - An Introduction," *Fourth Annual Seminar of CDAC Noida Technologies (ASCNT-2011),* 2011.

[3] J. M. Hernández-Muñoz, J. B. Vercher, L. Muñoz, J. A. Galache, M. Presser, L. A. H. Gómez and J. Pettersson, "Smart cities at the forefront of the future internet," in *The Future Internet*Anonymous Springer, 2011, pp. 447-462.

[4] Bradley, J., Barbier, J., Handler, D., "Embracing the internet of everything to capture your share of $14.4 trillion: more relevant, valuable connections will improve innovation, productivity, efficiency & customer experience " 2013.

[5] H. Bos, S. Ioannidis, E. Jonsson, E. Kirda and C. Kruegel, "Future threats to future trust," in *Future of Trust in Computing*Anonymous Springer, 2009, pp. 49-54.

[6] M. Friedewald, E. Vildjiounaite, Y. Punie and D. Wright, "Privacy, identity and security in ambient intelligence: A scenario analysis," *Telematics Inf.,* vol. 24, pp. 15-29, 2, 2007.

[7] M. Dlamini, M. Eloff and J. Eloff, "Internet of things: Emerging and future scenarios from an information security perspective," in 2009, .

[8] Y. Yusoff, R. Ismail and Z. Hassan, "Common Phases of Computer Forensics Investigation Models," *International Journal of Computer Science & Information Technology,* vol. 3, 2011.

[9] Association of Chief Police Officers (ACPO), 7Safe. (). *Good Practice Guide for Computer-Based Electronic Evidence: Official Release version* [ONLINE]. Available: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

[10] The Federal Bureau of Investigation. (April 2000). *Forensic Science Communications - Digital Evidence: Standards and Principles by SWGDE and and IOCE* [ONLINE]. Available: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/.

[11] K. Vlachopoulos, E. Magkos and V. Chrissikopoulos, "A model for hybrid evidence investigation," *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security,* pp. 150, 2013.

[12] A. Induruwa, "Hidden in the clouds: The impact on data security and forensic investigation," in *Advances in ICT for Emerging Regions (ICTer), 2011 International Conference on,* 2011, pp. 77-77.

[13] E. Fleisch, "What is the Internet of Things? an economic perspective," *Economics, Management, and Financial Markets,* pp. 125-157, 2010.

[14] A. Dunkels, "Rime-a lightweight layered communication stack for sensor networks." 2007.

[15] L. Coetzee and G. Olivrin, "Inclusion Through the Internet of Things," *Assistive Technologies, Fernando Auat Cheein (Ed.), ISBN,* pp. 978-953, 2012.

[16] J. Gantz and D. Reinsel. THE DIGITAL UNIVERSE IN 2020: Big data, bigger digital shadows, and biggest growth in the far east. 2012[ONLINE]. Available: http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf.