# 4P Based Forensics Investigation Framework for Smart Connected Toys

Benjamin Yankson
byankson@albany.edu
CEHC, University at Albany
Albany, New York

Farkhund Iqbal
farkhund.iqbal@zu.ac.ae
CTI, Zayed University
Abu Dhabi, Abu Dhabi

Patrick C. K. Hung
patrick.hung@uoit.ca>
FBIT, OntarioTech University
Oshawa, Ontario

## ABSTRACT

Smart Connected Toys (SCTs) have the potential to collect terabytes of sensitive personal, contextual, and usage information which may be a subject of cybercrime or used as a conduit for cybercrime resulting in a digital forensic investigation which requires the examination of the digital artifact stored, processed or transmitted by the SCT. SCT forensics is challenging in most cases due to non-availability of specialized forensics tools and standardized evidence acquisition interface port. We explore the various privacy and security challenges plaguing the SCT industry and the possible safety risk SCT poses to children as a result of a lack of serious consideration technical controls surrounding the collection, processing, and storage of children's information and possible exposure to crime which will require digital forensic investigation. As a result of this gap in research and industry, we investigate current digital forensic solutions for SCTs and present an abstract forensics investigation framework with the focus on using non-conventional means which allow Investigators to successfully "Plan," "Preserve" "Process" and "Present" (4P) as a systematic means to conduct digital forensic analysis on an SCT in a situation where SCT is complicit in a criminal investigation or a subject of crime.

## KEYWORDS

Smart Connected Toys, Privacy, Security, Digital forensics

**ACM Reference Format:**
Benjamin Yankson, Farkhund Iqbal, and Patrick C. K. Hung. 2020. 4P Based Forensics Investigation Framework for Smart Connected Toys . In *The 15th International Conference on Availability, Reliability and Security (ARES 2020), August 25–28, 2020, Virtual Event, Ireland*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3407023.3409213

## 1 INTRODUCTION

Smart Connected Toys (SCTs) are built as part of the Internet of Things (IoT) with the potential to collect terabytes of sensitive personal, contextual, and usage information, introducing ever-increasing privacy, and serious safety concerns in cases where a hacker can compromise the device. As per the January 2019 market report published by Credence Research, Inc., the worldwide SCT market is expected to see approximately 14% growth between 2018 to 2026, which is about $69.16 billion USD [1]. The dramatic increase in the number of SCT has opened up many opportunities for consumers across the globe; yet as some SCT engages in direct communication with children, real-time tracking of children's activities and storage of personal data including name, photos, and voice recordings. Such activities present a serious issues with privacy and security of data leading to possible crime which requires digital forensic analysis; in a situation where the SCT is used as a crime instrument or a victim of a crime.

Protection from cybercrimes has become a nightmare due to the continual advancements and sophistication of hacker tools and exploit kits. Other factors include the universality of connected devices such as SCTs, increased computing power, anonymity, and an increase in the infiltration of organized crimes. One major challenge that needs to be addressed with a direct impact on SCTs, in addition to the listed factors, is the ability to conduct digital forensic analysis for small scale devices such as SCT. The task of keeping track of crimes committed using devices without a supporting tool or software to conduct forensic investigation has made cybercrime investigations more difficult. Advanced technologies greatly help cybercriminals in obscuring their online criminal activities. Hence leaving behind no digital footprints or in the case of SCTs, knowing that there are no tools or software which can easily extract evidence for the digital forensic investigation.

In the case of SCTs, or some of the other small scale IoT devices, tools, techniques, and technology abet them in pacing up the execution of online criminal activities. In this era, the cybercrime investigator should be equipped with conventional investigative skills with the right understanding of the latest methodology and tools available, especially for performing digital forensic activities, such as the recovery of deleted records in the hard drive, or memory, etc. With SCTs, inspecting digital evidence, tracking down the digital footprint of evidence, which is hard to extract, makes it more difficult. If the Investigator is unable to provide substantial evidence against the perpetrator, there is no way to prosecute suspects in a typical SCT crime case. The ability to extract evidence provides necessary facts relevant to the crime that is established to prove the guilt or innocence of an individual in the court of law. In the case of cybercrimes, electronic evidence needs to be provided before the prosecution. Electronic evidence comprises of all such material that exists electronically or in digital form. The goal of this work in SCTs digital forensic investigation is to present a conceptual framework that can be used in SCT forensic investigation and focuses on supporting or refuting a premise of a crime involving SCT. Specifically, there is a need to establish a framework for processing

*ARES 2020, August 25–28, 2020, Virtual Event, Ireland*
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-8833-7/20/08…$15.00
https://doi.org/10.1145/3407023.3409213

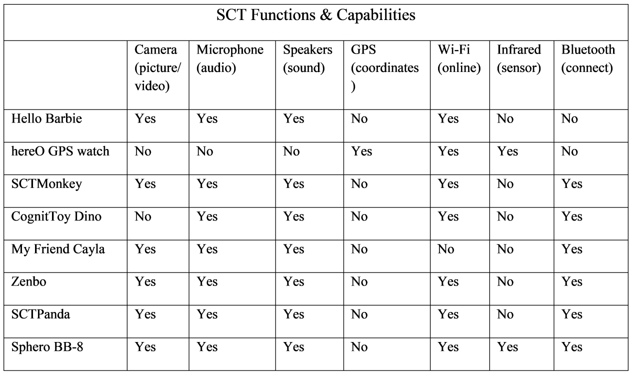
digital forensic evidence that can be garnered from the SCT, in a situation where a toy is complicit in a criminal investigation.

Digital forensics analysis constitutes the recovery and investigation of material found in digital devices through “Planning,” “Preservation,” “Processing,” and “Presentation” [2]. For the purpose of this work, the “Planning” aspect involves identifying specific Electronically Stored Information (ESI) to be collected within the SCT. “Preservation” involves using forensically sound collection principles to maintain the integrity of the ESI from the SCT. “Processing” constitutes an analysis of collected ESI to gather relevant information to the investigation. Finally, “Presentation” encapsulates the summary of factual findings and presenting those findings to the appropriate audience. The rationale for the need for the ability to conduct digital forensic analysis of SCT stems from three main premises. First, in a situation where a child has been abducted, and police have been able to locate a SCT which was used by the child prior to the abduction, we are concerned with how evidentiary information can be extracted from the SCT and forensically processed. Second, there is also a concern that SCT can be perverted, leading to the sexual exploitation of children. For example, a child predator can remotely hack into SCT and record very obscene or pornographic images of the child. Notably, child pornography is on the rise as an increasingly common type of cybercrime in the world today [3]. Third, the growth of IoT devices such as SCTs with functions which can record and store information in the cloud presents a perfect opportunity for fringe members of society to hide and take advantage of a lapse in cybersecurity solution, further engaging in activities, which contravene societal laws or can be morally incomprehensible. For these reasons, it is imperative that investigators can extract ESI from SCTs and conduct forensic analysis to support the prosecution of cybercrimes where necessary. For the purpose of this work, SCT’s ESI will constitute electronic information created, processed, transmitted, and stored by the SCT. Such evidence would be collected by an investigator in order to be analyzed during SCT digital forensic investigation. Based on the scope of this work, digital forensics will entail the application of computer science and investigative procedures for analyzing digital evidence gathered from SCTs [2]. Generally, the collection and analysis of SCT’s ESI will follow industry sound forensic principles, which include: (1) collection of the SCT’s ESI in a way which will ensure integrity (prevention of any alteration to the original data), and (2) proper preservation and documentation of evidence.

New SCTs on the market are evolving with continuous feature sets and integrating new technology, which allows the experience to become more interactive and individualized with personal preferences, making play more enjoyable. Some of the default features available on SCTs on the market include voice recognition, image recognition, speech function for jokes and storytelling, and an interactive function for learning [4, 5]. Other functions include scanning technology, location technology, and a microphone used to capture voice for further processing through an interface. Table I presents some of the current SCT on the market and data processing features.

Unfortunately, most SCTs, currently on the market listed, do not have a standard interface to connect to for data extraction. As such, there has not been any defined standard forensic framework with supporting standard operating procedure (SOP) to extract ESI [6]. Considerably, because of the tremendous amount of ESI gathered by SCT, there needs to be a thorough forensic framework to aid investigators who may find themselves with a case involving a SCT. This work presents an abstract SCT forensics investigation framework and forensic case study analysis on Mattel’s Hello Barbie SCT. In the rest of this paper, Section 2 analyzes the background and presents an overview of standardized SCT digital forensics and related information regarding the challenges of conducting forensic analysis. Section 3 discusses related work existing in this domain and what current solutions are lacking. Section 4 presents our proposed abstract 4P based forensics investigation framework. Section 5 presents a forensic case study for Hello Barbie SCT. Finally, Section 6 presents the discussions and concluding remarks.

**Table 1: Data Collection and Processing Features[22]**



| SCT Functions & Capabilities | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Camera (picture/ video) | Microphone (audio) | Speakers (sound) | GPS (coordinates ) | Wi-Fi (online) | Infrared (sensor) | Bluetooth (connect) |
| Hello Barbie | Yes | Yes | Yes | No | Yes | No | No |
| hereO GPS watch | No | No | No | Yes | Yes | Yes | No |
| SCTMonkey | Yes | Yes | Yes | No | Yes | No | Yes |
| CognitToy Dino | No | Yes | Yes | No | Yes | No | Yes |
| My Friend Cayla | Yes | Yes | Yes | No | No | No | Yes |
| Zenbo | Yes | Yes | Yes | No | Yes | No | Yes |
| SCTPanda | Yes | Yes | Yes | No | Yes | No | Yes |
| Sphero BB-8 | Yes | Yes | Yes | No | Yes | Yes | Yes |

## 2 BACKGROUND - STANDARDIZED SCT DIGITAL FORENSIC

The rise in the integration of the digital spaces and connectedness, such as the ability for SCTs to connect to WiFi networks and access the Internet, has provided ease and an avenue for modern-day criminals to conduct several illegal acts whiles maintaining anonymity [21]. Cybercriminals masquerading as others can use various web-based communication tools to conduct illegal activities. For example, a perpetrator can use the "Tor" network to conduct activities such as online harassment, identity theft, stalking, and fraud. The sophistication of small portable devices like SCT and its ability to collect tremendous amounts of sensitive information; have created an opportunity for fringe members of society to take advantage of vulnerabilities in order to steal sensitive data of SCT users. Such cybercrime poses a serious threat to the global economy and the possible safety of children [7]. SCTs used as a tool for cybercrime or the culprit of a cybercrime involve digital footprint, which a forensic investigator can collect, preserve, and process as an ESI for supporting evidence to solve SCT related cybercrime.

Currently, there is no global agreement on a definition of cybercrime because of the complexity in-depth and the width of what constitutes cybercrime [8]. There multiple definitions and interpretations of cybercrime. For example, the U.S. government does not have an official definition of cybercrime that distinguishes it from common criminal offenses [8]. There is a global collaborated attempt which has resulted in accepting an inclusive definition, which was the focus Convention on Cybercrime [9]. A per the convention treaty [9], cybercrime, such as stealing child PII, can be defined as "crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, and violations of network security" [9]. The opportunities for such crimes are becoming prevalent. For example, in 2010 and 2017 [10], the FBI issued Public Service Announcement (PSA) an alert that pedophiles could use the Barbie "Video Girl" doll-videotaping feature to make child porn [3]. In the FBI 2017 PSA, the FBI encourages consideration of security and privacy pitiful before introducing such a device into the home. The major concern was SCT can present privacy and possible contact safety concern. General cybercrimes focus on a "cyber-space offense," which is committed against a system, a network, or data. Such offenses consist of the use of infrastructure that supports cyberspace and respective services to commit crimes through a connected medium such as SCTs. Although there has been an improvement in understanding cybercrime and defining it, there is a lack of appetite to address the challenges of digital forensic investigation for nonstandard and small scale devices such as SCTs. Most small-scale devices on the market, like SCTs, do not have any external USB port, which allows easy access to the hard disk for the collection of digital evidence during a forensic investigation. Figure 1 shows Cognitoys' Dino and Mattel's Hello Barbie used in this case study at the later part of the work, demonstrating the lack of connection interface to connect a forensic workstation, which allows access to ESI on either of the devices. It is essential that investigators can collect and analyze ESI in order to help provide the required evidence to acquit or prosecute an accused. To understand the working of SCT, Figure 2. presents Google's SCT diagram demonstrating SCT integrated into a home network [11] as a schematic diagram to demonstrate the possibility of a real-world SCT use.

There are other issues relating to cybercrimes, but poignant amongst these is the understanding of the lack of a concise classification and monitoring of the offenses[6]. Cybercrime involves different and multiple acts that contravene existing privacy laws, or new laws specially designed to address technology advancement. It lacks movement on the sides of government across the globe to stipulate specifications on what is necessary to aid investigators. The juxtaposition is in the name of privacy, equipment manufacturer design controls to make it harder to extract evidence to prosecute cybercrime. Government, although inconsistent, is trying to find ways to force companies when crimes are committed that involve digital technology to have the equipment manufacturer provide access to these devices; this has been challenging. For example, in an FBI-Apple encryption dispute [12], Apple Inc. refused a court order to assist the FBI in extracting data from a locked iPhone during a digital forensic investigation [12].

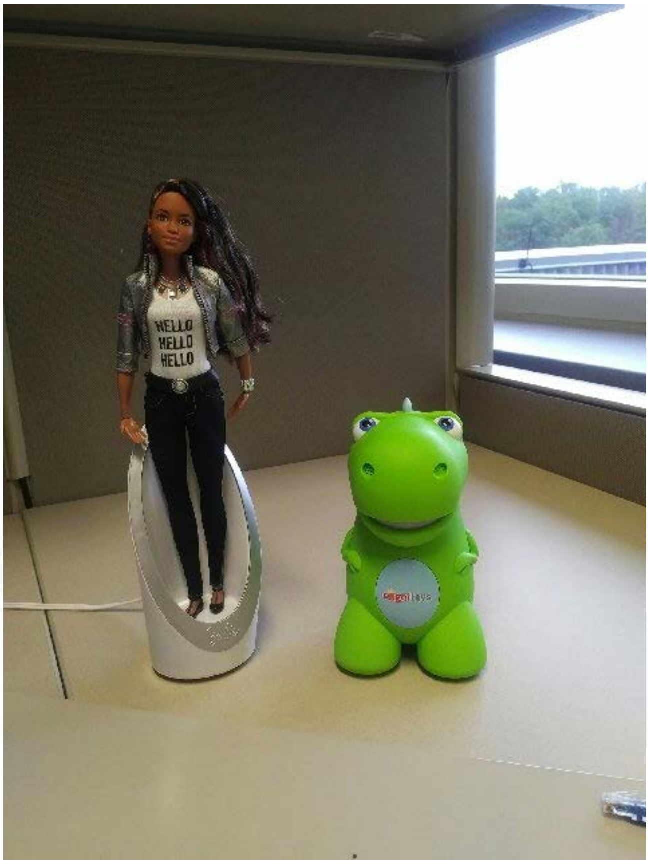


**Figure 1: Mattel's Hello Barbie and Cognitoys' Dino SCT)**

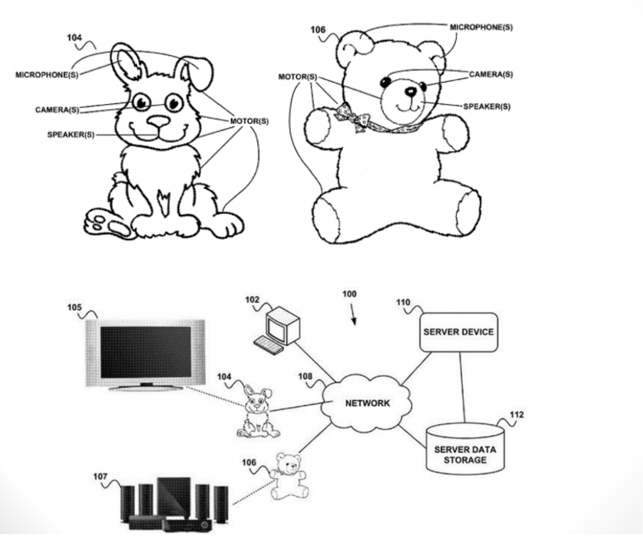


**Figure 2: Google's SCT Patent Architecture Diagram[11]**

A global study released by consulting firm PricewaterhouseCoopers [13] shows that the number of reported cyber-related security incidents around the world has gone up by 48%, which is approximately an equivalent of 117,339 attacks per day[13]. The report does not only highlight the increase in crime but also makes a point that cybersecurity incidents are becoming increasingly powerful to cause more destruction to organizations or victims, while the ability to conduct a digital forensic analysis of evidence is essential to solving crimes and putting proprietors in jail. The impact of cybercrimes on victims is wide-ranging, including but not limited to, death or self-destruction, identity theft, sexual exploitation of children, cyber-harassment, cyberbullying, intimidation, anxiety, other mental health illness, and financial loss. For example, Amanda Todd, a Canadian 15-year-old teen, committed suicide after being severely bullied after someone posted nude images of her online [14]. As such, experts, researchers, and law enforcement in the field of digital forensics must understand cybercriminal methodologies and capabilities to properly investigate and provide solid evidence to prosecute proprietors of such crimes. Considering the number of small scale devices currently on the market, Investigators must have the ability to collect and process evidence in new technologies like SCTs. Our goal of the propose abstract 4P Forensics Investigation Framework is that Investigator can leverage the framework in order to build specific and necessary Standard Operating Procedures (SOP) specific to their team and environment to detect cybercrime and design methodologies to plan, preserve, process, and present the required evidence of a crime, a breach of policy and other SCT related crimes.

Different jurisdiction legal structures are consistently under constant pressure by innovation in technology, such as SCTs, which foster opportunities for a criminal to commit crimes that are not current codified into existing laws, or in other cases where collecting required digital evidence necessary to identify these criminals and prosecuting them in the court of law is impossible. Digital crimes such as privacy breaches are on the rise due to complex factors including the ease of use of sophisticated anonymity tools to commit an offense, the widespread of use of the Internet (by users who sometimes do not clearly understand the legal framework or laws surrounding certain activities), and the low degree of sufficient evidence which ties a particular crime to a specific use of the device associated with certain real-world crimes. The issue of SCT related cybercrime and the lack therefore of forensic equipment to collect and process evidence is a multi-jurisdiction problem that is on the rise as more and more devices with capacities to store, transmit, and digitally process information floods the market[6]. It is a well-documented phenomenon that many national crime statistics and surveys by law enforcement or think tanks illustrate a steady increase in criminal activities of document cases [15]. One of the interesting points in this research is the ability to address specified crimes, which affect users of SCT, such as crimes against children, and identity theft. For the purpose of this work, the definition of what constitutes the different type of cybercrime includes [15]:

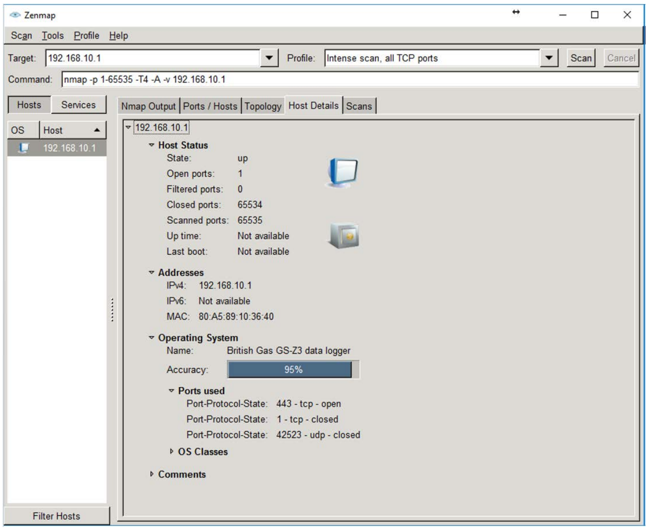
- Crimes against children: It is anything related to the exploitation of children, including child abuse resulting from the use of SCT. Most of these types of crimes involve some levels of distribution of images of children recorded with the ai SCT and forced into an act, which is contrary to what is considered acceptable. Sometimes such activities and distribution of images happen within the use of SCT and chat rooms.
- Identity Theft: Stealing of SCT related PII, such as a person's name, social insurance number (SIN), to commit fraud or other crimes.
- Corporate Data Breach: SCT related data leak/spill of user data, which is released from a secure location to an untrusted environment.
- Intellectual Property Theft: SCT related intellectual property rights/copyright and counterfeit.

## 3 RELATED WORK

There is a current limitation in this field, which allows easy access to data extraction from the SCT toy; as a result, a limited number of research works available. Base on this, we discuss:

### 3.1 SCT Digital Forensic

Some previous works, including Dhanhani et al. [16], attempted extracting and reading data from toy memory chips containing the doll unsuccessfully. The authors [16] tried other extraction methods, but due to limitations such as unavailability of forensic memory hardware and time limitation, the authors were enabled to collect any evidence from the SCT. Without and success reading data from SCT memory chip, Dhanhani et al.[16] attempted remote extraction through a WiFi unsuccessfully. The author's goal was to connect to the SCT on the same WiFi network, scan for open ports using" Znmap," and exploit possible unsecured port via telnet to access toy internal memory for volatile evidence. Figure 3 shows the authors'[16] attempt to exploit an open port for evidence collection. From the author's work[16], it was apparent that some of the challenges limiting progress made in scholarly work on forensic ESI collection for SCT result from the lack thereof of a standardized framework and related SOP needed to provide a road-map for Investigators. Although there is a growing body of works on security and privacy risk associated with the implicit and explicit dangers of using SCT[16]; there is, hardly, any serious digital forensics works as a result of lack of any serious known documented criminal cases which require evidentiary information to be extracted from the SCT itself. The author's views on the challenge also focus on current SCT and lack of supporting connection port necessary for currently available forensic hardware and software necessary to connect to SCT. As per their work [16], this requires a new and innovative



```
Target: 192.168.10.1    Profile: Intense scan, all TCP ports
Command: nmap -p 1-65535 -T4 -A -v 192.168.10.1

192.168.10.1
  Host Status
    State:          up
    Open ports:     1
    Filtered ports: 0
    Closed ports:   65534
    Scanned ports:  65535
    Up time:        Not available
    Last boot:      Not available
  Addresses
    IPv4:  192.168.10.1
    IPv6:  Not available
    MAC:   80:A5:89:10:36:40
  Operating System
    Name:      British Gas GS-Z3 data logger
    Accuracy:  95%
    Ports used
      Port-Protocol-State:  443 - tcp - open
      Port-Protocol-State:  1 - tcp - closed
      Port-Protocol-State:  42523 - udp - closed
    OS Classes
  Comments
```

**Figure 3: Result of Zmap result on a WLAN [16]**

way of extracting ESI during a digital investigation. The overall view is that current forensic tools are limited in their respective ability to collect and process ESI from SCT devices. In some cases, even if there are tools available, artifact storages vary in various models of SCT.

## 3.2 Privacy and Security Breaches

SCT security breaches and privacy violations affecting children and the respective use of the device has been well documented over the last couple of years [17]. As a result of a lack of proper security and privacy mechanism, SCT is rendered vulnerable and subject to the possibility of cybercrime against it. Basically, these vulnerabilities open up opportunities for a Hacker to hack into IoT related devices such as SCT, baby monitors exposing children sometimes at their most vulnerable period [18]. During such a period, the child can be exposed to danger if he/she is naked or where there is no parental supervision [19,29]. Some SCTs have variable sensors, for example, Bluetooth, and Global Positioning System (GPS), it can be used to track the device while children are on the move as specified in prior research work [20]. For example, the child can be monitored from point A (school) to point B (home), which can allow a child predator to abduct a child, putting his/her safety in jeopardy [21,28]. Hilts et al. [20] highlight most of the vulnerabilities of IoT devices such as SCT, which allow tracking and monitoring, putting individual users' safety and privacy at risk.

Forbrukerra [17] presents privacy and security issues concerning SCT by expanding on the existing work of Hilts et al. [30]. Forbrukerra [17] builds on Hilts et al. work by discussing actions different countries around the world are implementing concerning SCT and related security and privacy issues regarding children. Based on Forbrukerra [17] works, we can relate some of the current findings and activities, including Norway Consumer Council issued a report on specific SCT [17]. Prior to Norway's action, Germany, in 2017, labeled My Friend Cayla SCT as an espionage device, banned it, and required all households to remove it [18].

Rapid 7 [22], a security research organization, discusses notable vulnerabilities found in SCT, such as weaknesses in Fisher-Price Smart Monkey that could expose the device to an attack. As a result of Rapid7 findings [22], Fisher-Price addressed the respective weakness and avoided the possibility of a cybercrime relating to a data breach, which exposes a child's information to an attacker. Similarly to Rapid7[22] findings, Taylor and Michael [23] investigated the privacy and security vulnerability of the Hello Barbie. As per Taylor and Michael [23], the interactive nature of Hello Barbie usually leads children to divulge a significant amount of confidential information about themselves, friends, and family. The data collected by Mattel Inc., the creator of Hello Barbie, is shared with third-party companies [23]. A study by Somerset Recon Inc. [24] found that the Hello Barbie was susceptible to attack due to several vulnerabilities [24], such as "Hotspot broadcast," "Unauthorized configuring during pairing," and "Identification of open port" which lead to an attack and a cybercrime.

Denning et al. [25], investigate the security and privacy concerns of three major SCT targeted and marketed to children. The authors [25] investigated SpyKee (made by Sector/Meccano), which contains a USB webcam, microphone, and speakers amongst other functionalities, and found out that the device can be controlled by computers locally or over the Internet [25]. During the author's investigation and analysis of security controls, they found that login credentials are in plaintext, which allows the information to be subject to the man-in-the-middle attack or passive eavesdropping attack [25]. Such vulnerability implies that an attacker can sniff the login credential, use the same information to authenticate remotely, and control the robot to gather information about the family whiles the robot is in the house. Denning et al. [25] also investigated Wowees' RoboSapien V2 child robot and found that it can be manipulated to move things within the home. In this work, our goal is to build the 4P based forensics investigation framework as a baseline frame and SOP for investigating such and possible SCT related crimes.

# 4 4P BASED FORENSICS INVESTIGATION FRAMEWORK FOR SCT

Based on the challenges in conducting digital forensic analysis on SCT, we adapt an SCT conceptual model proposed by Yankson et al. [26]. The conceptual model illustrated in Figure 4 provides guidance as to the various interaction of SCT. Based on the conceptual model [26], we develop an abstract 4P based forensics investigation framework to support Investigators in conducting digital forensics analysis of a SCT. Our 4P framework focuses on "Planning," "Preservation," "Processing," and "Presentation." Our 4P based forensics investigation framework uses the conceptual model [26] to identify the overall working of SCT, including functions and related interactions with vendor Cloud storage, third-party service providers, privacy policy, and parental monitoring. Although the conceptual model (Figure 4) provides a full lifecycle use of SCT, including a depiction of the physical and social environment of the toy been use, and the core functionality of the SCT; the abstract framework we present here focuses on the challenge of successful forensic analysis of the ESI captured, process or transmitted by the SCT. Based on the current identified challenges in conducting SCT digital forensic, we present Our 4P based forensics investigation framework to conduct a digital forensic investigation for SCT, as illustrated in Figure 5.

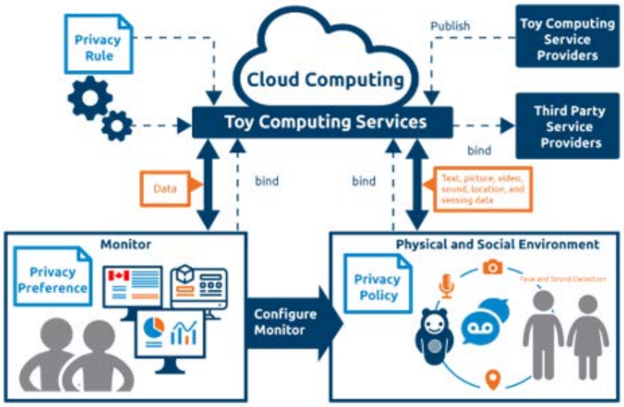


Figure 4: Smart Connected Toys Conceptual Model[26]

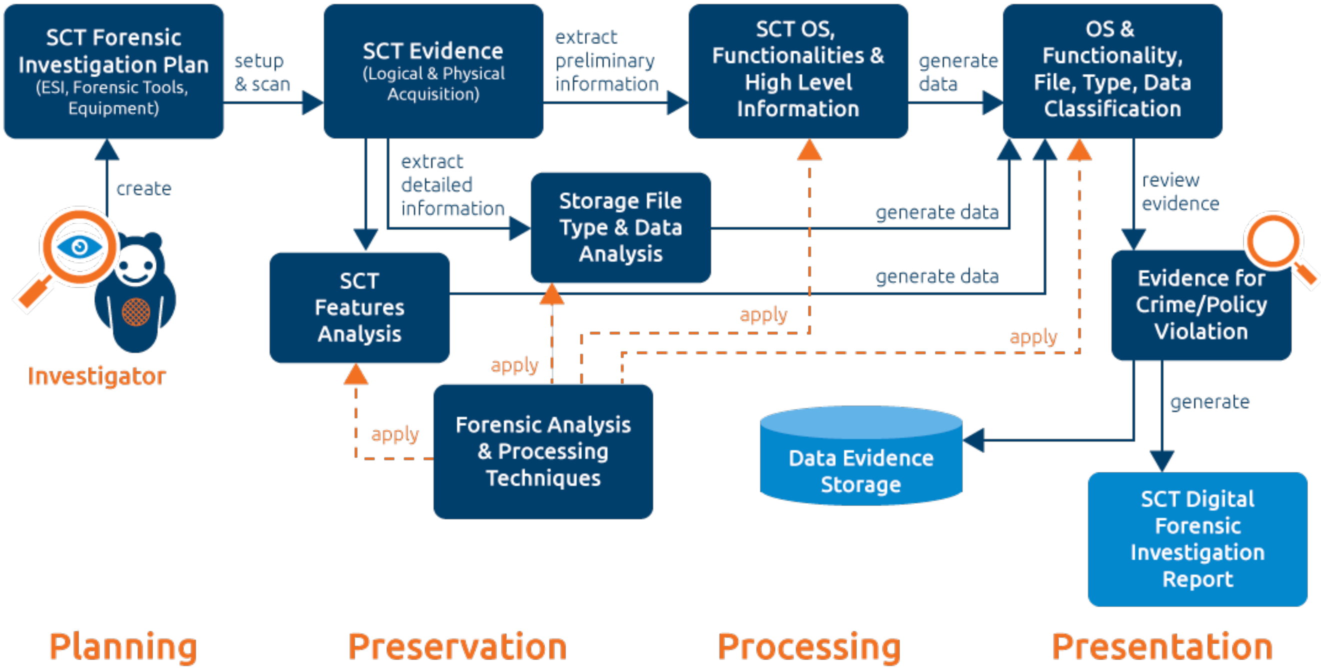

SCT Forensic Investigation Plan (ESI, Forensic Tools, Equipment)
setup & scan
SCT Evidence (Logical & Physical Acquisition)
extract preliminary information
SCT OS, Functionalities & High Level Information
generate data
OS & Functionality, File, Type, Data Classification
create
Investigator
extract detailed information
Storage File Type & Data Analysis
generate data
SCT Features Analysis
generate data
review evidence
Evidence for Crime/Policy Violation
apply
apply
apply
apply
Forensic Analysis & Processing Techniques
Data Evidence Storage
generate
SCT Digital Forensic Investigation Report
Planning
Preservation
Processing
Presentation

**Figure 5: 4P Based Forensics Investigation Framework for SCTs**

This framework begins with the "Planning Phase." We begin forensic analysis of SCT first by creating SCT forensic investigation plan of the case involving a given SCT, for example, “Hello Barbie,” as described in the case study in Section V. In this stage of the framework, the forensic Investigator determines what type of ESI is possible to collect and what equipment and digital forensic tools can be used. The Investigator spends some time to understand the workings of the SCT itself leverage on the conceptual model and various interaction of the SCT.

We proceed to the “Preservation Phase,” where we collect evidence and protect the evidence to maintain integrity. Within this phase, the Investigator prepares a setup and scan of the SCT device. The Investigator proceeds by determining the type of ESI acquisition. More specifically, the Investigator explores avenues to use accessing ESI on the SCT through logical ESI acquisition or physical acquisition. Within this “Preservation Phase,” the evidence-gathering part, the Investigator proceeds to extract the evidence and create a duplicate copy of the original evidence for storage. At this point in the investigation, the Investigator makes sure that both the original copy and duplicate copy have been hashed, and the has value is the same to maintain the integrity of the evidence. Next, at this point, the Investigator determines feature analysis by applying different forensic analysis processing and techniques on the extracted ESI. The Investigator applies forensic analysis and techniques on both the SCT features and the copy of ESI extracted and stored.

The Investigator prepares to begin the "Processing Phase” by extracting preliminary information of the SCT OS functionalities and level of information. Although this begins the "Processing Phase” of the framework, it is expected that the Investigator continues to conduct and apply forensic analysis and processing techniques to the SCT OS functionalities and the high-level information gathered. At this point, the investigation generates data from SCT OS functionalities, high-level information gathered. As illustrated in Figure 5, the Investigator also generate data from "Storage File Type & Data Analysis" step and "SCT Feature Analysis" stage and store all the information at the "OS and Functionality, File, Type, Data Classification" stage of the framework. At this stage also, the Investigator applies Forensic analysis and processing techniques on the relevant information gathered. All the evidence is reviewed to determine if a crime, statutory, or policy violation has occurred. The evidence at this point is stored in a secure evidence storage database and ready for presentation.

The Investigator proceeds to the "Presentation Phase” of the framework to generate a report of findings. Based on this proposed framework, we adapt the framework for use case conducting a forensic investigation of "Hello Barbie" SCT.

## 5 CASE STUDY – HELLO BARBIE SCT

Based on our proposed 4P Based Forensic Investigation Framework, we conduct a case study of forensic analysis on Hello Barbie SCT by Mattel Inc. Considering Barbie collect, process, and transmit significant amount interaction data from a child, it is important that we are able to gather necessary ESI in a case where it is involved in a crime, or it’s an accomplice to a crime. For this case study, we make the assumption that Barbie was involved in the illegal collection of child recordings. In such a case, the ability to conduct forensic acquisition of ESI is essential as well as gathering required facts necessary to attain conviction in the court of law, where inappropriate interaction took place. Since Barbie SCT has already developed a significant presence in North America, it is important that we address complexities of capturing forensic evidence through the understanding of SCT architecture, security framework, security complexities, which complicate ESI collection, securing and processing. The goal of this case study is to ascertain that the process of extracting digital artifacts from SCT as evidence using sound forensic principles based on the 4P Based Forensics Investigation Framework for Smart Connected Toys proposed above.

## 5.1 Digital Forensic Analysis of Mattel's Hello Barbie & Setup

Hardware and Software Requirement:

- Hello Barbie Toy – Model TN334;
- WiFi Connected Router;
- Blackberry Priv Running Android; and
- Forensic Tools including Forensics ToolKit(FTK), and OS Forensics.

Considering that this is the first time Hello Barbie(Figure 1) is set up, the SCT needed to be set up to connect to the home WiFi home network. The SCT packaged contains base station charger, 5V DC 1200mA charger, Hello Barbie doll, and instructional guide on initial setup and use. Hello Barbie requires that the owner have a smartphone capable of running the "Hello Barbie Companion" app on either Android device or iPhone. For this experiment, we use a Blackberry Priv Phone running Android to download the Hello Barbie companion app. We realize that at the time of this case study, the companion app was not available in the Canadian Google Play store, so extra measures(VPN shied) needed to be adopted to download the companion app from the United States Google Play store

The following steps below provide the basic information on forensic evidence acquisition for Hello Barbie:

- Download related app and setup SCT for first use: The initial step in setting up the SCT (Hello Barbie) is to assemble it and sit on the Charger [27].
- With an Internet-connected smartphone, visit Google play account to download the application is required at this stage (as depicted in Figure 6). Below are the instructions on how to connect the" Hello Barbie" to a home WiFi network
- Run the "Hello Barbie" app on the Smart Phone and follow default preference on the initial setup, select WiFi Network.
- Visit Toytalk.com and create an account with the registration information received from Toy talk connect Hello Barbie to a home WiFi network. It is presumed that both the toy and the companion app are connected.

At this point, both the toy and the companion app are connected to the same WiFi network. Once we have completed the setup, the SCT is ready to interact with the users. Referring to Figure 1, you must hold the center button to talk to Hello Barbie and wait for a response.

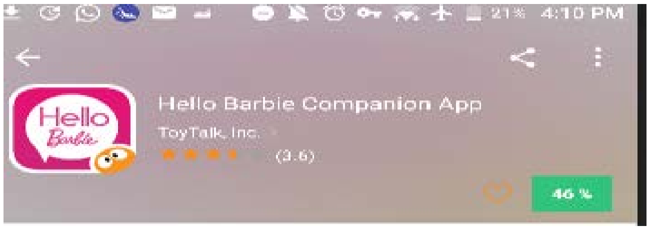


**Figure 6: Hello Barbie Companion App Download Screen**

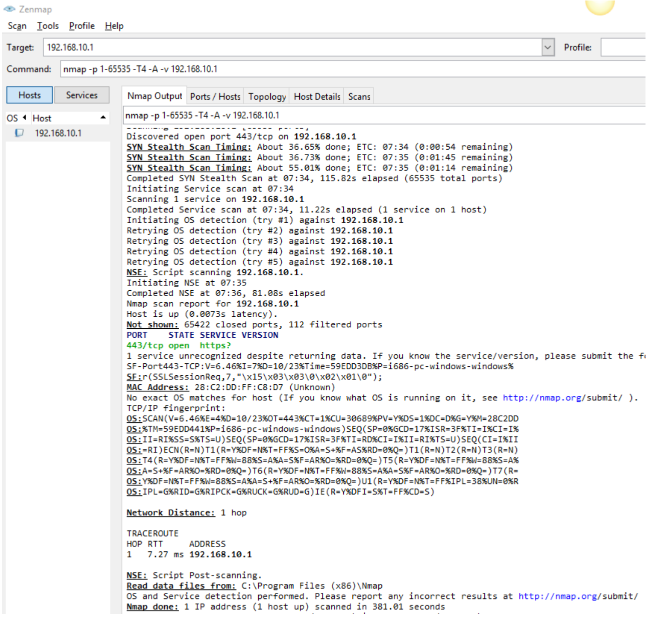
## 5.2 Barbie SCT Forensic Analysis

ESI Evidence Acquisition: Following a basic forensic framework, we begin with Planning and settle on the attempt to collect data in memory, like registers and cache contents; running processes; open ports and listening applications, and storage containers. The next logical step is considering Preservation, preserving the integrity of the data collected. We create some data and forensically analyze the data. The objective is to follow sound forensic principle such as collecting SCT ESI in a way which will prevent, where possible, any alteration to the original data that is stored in the toy; and the complete documentation of all collection, preservation, and analysis of the of data retrieved from the toy. The following effort we attempted but failed.

Nmap Analysis to Determine Target Host, Open Port, & Operating System: We use Nmap as part of evidence acquisition in order to finish the Preservation phase. Nmap is an open-source utility for network exploration, vulnerability security scanning. It comes with an extensive range of options that can make the utility more robust and add or change features to your specifications. The goal of using Nmap is to identify possible vulnerabilities on the SCT, which can lead to easy forensic data capture. Nmap can efficiently and quickly find the target, find out what ports (with what protocol) are open, discover the target OS, and cover its tracks to avoid intrusion detection. In the following tasks, we used the Nmap tool to identify open and closed ports and discover its target OS.

Finding the target host & Open Ports: Nmap can scan entire networks to look for possible targets. Finding open ports is usually accomplished through a "ping sweeping" with the –sp command. The following results in Figures 7 and 8 were produced to identify information by the SCT.

Remote Forensic Tool Acquisition: Considering that there is no interface to connect SCTs to conduct typical data acquisition, the next logical option is to seek tools with the capacity to conduct remote forensics. In the Processing phase, we use ProDiscover forensic software, which provides an avenue for performing computer and digital forensics remotely. It provides the ability to connect to the device through the network, which seems to be a good fit for the SCT forensics, considers there is no physical interface to connect to, and performs digital acquisitions. Unfortunately, most of the remote forensic tools, such as Pro Discover Forensic software, explored the required installation of a piece of software on the SCT, which at this point, we are unable to due to restriction on SCTs. Other data collection approaches include reading the toy's memory chip, which containing SCT firmware. Finally, we package and present the evidence during the Preservation Phase.



Target: 192.168.10.1

Command: nmap -p 1-65535 -T4 -A -v 192.168.10.1

```
nmap -p 1-65535 -T4 -A -v 192.168.10.1
Discovered open port 443/tcp on 192.168.10.1
SYN Stealth Scan Timing: About 36.65% done; ETC: 07:34 (0:00:54 remaining)
SYN Stealth Scan Timing: About 36.73% done; ETC: 07:35 (0:01:45 remaining)
SYN Stealth Scan Timing: About 55.01% done; ETC: 07:35 (0:01:14 remaining)
Completed SYN Stealth Scan at 07:34, 115.82s elapsed (65535 total ports)
Initiating Service scan at 07:34
Scanning 1 service on 192.168.10.1
Completed Service scan at 07:34, 11.22s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.10.1
Retrying OS detection (try #2) against 192.168.10.1
Retrying OS detection (try #3) against 192.168.10.1
Retrying OS detection (try #4) against 192.168.10.1
Retrying OS detection (try #5) against 192.168.10.1
NSE: Script scanning 192.168.10.1.
Initiating NSE at 07:35
Completed NSE at 07:36, 81.08s elapsed
Nmap scan report for 192.168.10.1
Host is up (0.0073s latency).
Not shown: 65422 closed ports, 112 filtered ports
PORT    STATE SERVICE VERSION
443/tcp open  https?
1 service unrecognized despite returning data. If you know the service/version, please submit the f
SF-Port443-TCP:V=6.46%I=7%D=10/23%Time=59EDD3DB%P=i686-pc-windows-windows%
SF:r(SSLSessionReq,7,"\x15\x03\x03\0\x02\x01\0");
MAC Address: 28:C2:DD:FF:C8:D7 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.46%E=4%D=10/23%OT=443%CT=1%CU=30689%PV=Y%DS=1%DC=D%G=Y%M=28C2DD
OS:%TM=59EDD441%P=i686-pc-windows-windows)SEQ(SP=0%GCD=17%ISR=3F%TI=I%CI=I%
OS:II=RI%SS=S%TS=U)SEQ(SP=0%GCD=17%ISR=3F%TI=RD%CI=I%II=RI%TS=U)SEQ(CI=I%II
OS:=RI)ECN(R=N)T1(R=Y%DF=N%T=FF%S=O%A=S+%F=AS%RD=0%Q=)T1(R=N)T2(R=N)T3(R=N)
OS:T4(R=Y%DF=N%T=FF%W=88%S=A%A=S%F=AR%O=%RD=0%Q=)T5(R=Y%DF=N%T=FF%W=88%S=A%
OS:A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=FF%W=88%S=A%A=S%F=AR%O=%RD=0%Q=)T7(R=
OS:Y%DF=N%T=FF%W=88%S=A%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=FF%IPL=38%UN=0%R
OS:IPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=FF%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   7.27 ms 192.168.10.1

NSE: Script Post-scanning.
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 381.01 seconds
```

**Figure 7: Nmap Scan Results**

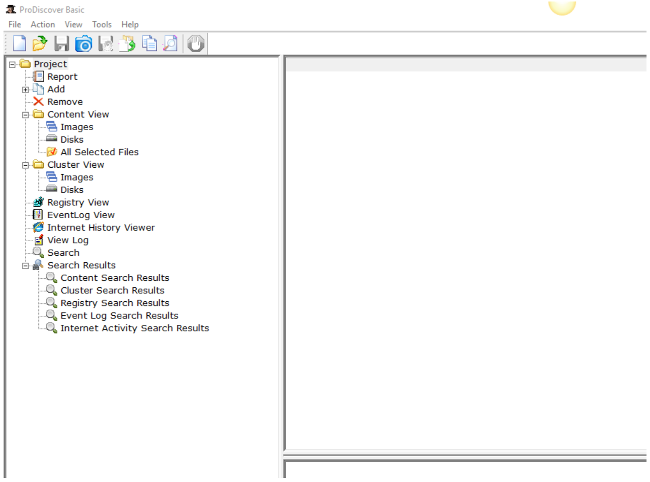


**Figure 8: ProDiscover Attempt for Remote Acquisition with No Result**

## 6 DISCUSSION & CONCLUSION

Digital forensic framework can aid investigators to determine perpetrators of crimes resulting from use of SCT or when SCT is a victim of a crime. This work demonstrated the exploration and current security and privacy issues which can result in privacy violation or child safety concerns needing digital forensic analysis of the SCT to resolve a crime. This work presented recent studies on SCT forensics, demonstrating factors that prevent traditional digital forensics to be used for SCTs with strength and weakness that affect ESI extraction with currently available forensic tool, and methods. We identified the gap in availability of digital forensic framework and related framework and presented an abstract 4P digital forensic framework which focus on on using non-conventional means which allow Investigators to successfully "Plan," "Preserve" "Process" and"Present" (4P) as a systematic means to conduct digital forensic analysis on an SCT in a situation where SCT is complicit in a criminal investigation or a subject of crime. Based on the 4P based forensics investigation framework, we are able to conduct SCT forensics of Hello Barbie case study although there are currently no easy to use forensic tools to allow extraction of data from Mattel's Hello Barbie. When we scanned, for example, Hello Barbie, the Wi-Fi results showed an open SSID, as demonstrated in Figure 9. The availability of such SSID can be a risk to safety, considering it will be an indication that someone is using Hello Barbie SCT. For example, an adversary with bad intent can be scanning around in the neighborhood to identify possible areas where children reside. As illustrated in Figure 8, the SSID clearly shows "Hello Barbie." Although such an example may be extreme and hard to locate the home in densely populated areas, in very rural areas where houses are sparse, an ill intent adversary (pedophile ) can use signal strength to determine the possible home the SSID is located. We demonstrated in this work and presented a forensic framework that allows the Investigator to conducted analysis on SCT. We demonstrated the various privacy and security plaguing the SCT industry and the possible safety risk SCT poses to our children as a result of a lack of serious consideration technical controls surrounding the collection, processing, and storage of children's information and possible exposure to crime which will require digital forensic investigation. This work demonstrates that although there are currently no unique tools designed for conducting a digital forensic investigation of SCT, we can develop a framework to serve as a guide to conduct forensic digital acquisition and analysis of ESI extracted from an SCT. Based on this work, we made it clear that on the premise of a privacy violation or crime committed while using SCT during possible criminal proceedings is essential. As a result of this, the ability to conduct a forensic investigation on Smart Connected Toys will become an increasingly vital area as more of these devices make their way into the homes of many people. Through our case study result, we have demonstrated how such investigation and analysis can take place in a situation where a SCT is involved or part of the digital crime investigation. This 4P based forensics investigation framework can be adapted and implemented in the investigation for other small scale devices during criminal or policy violation investigation. The abstract 4P based forensics investigation framework, as depicted in Figure 5, makes the digital investigation of SCT explicit and allows for reasoning surrounding decisions where the Investigator has to apply current forensic investigation best practices and other acquired knowledge through the investigator respect experience and context regarding jurisdiction law, best evidence practice, etc. The future work look

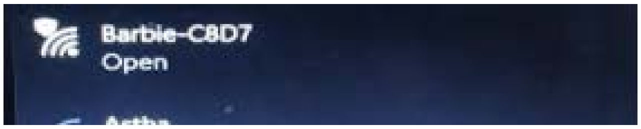


**Figure 9: Hello Barbie SSID**

to explore and apply 4P based forensics investigation framework to companion robot and other small scale connected devices. Further we intend to expand this work by conducting a research study to access the acceptance real world forensic investigators views on using of our proposed our abstract framework as compared to traditional forensic approaches. We seek to further our work in the area of SCT mobile connected application testing API, and understanding digital information process from SCT to the cloud.

## 7 ACKNOWLEDGMENTS

Not Applicable

## REFERENCES

[1] Marketwatch.com, “Connected Toys Market 2018-2026 with data by product types, applications, and regional analysis", MarketWatch, 2019. [Online]. Available:https://www.marketwatch.com/press-release/connected-toys-market-2018-2026-with-data-by-product-types-applications-and-regional-analysis-2019-01-31. [Accessed: 18- Jun- 2019].

[2] N. Bill, “Guide to Computer Forensics and Investigations.” 5th Edition. Published by Thomson Course Technology, 2016.

[3] M. Martinez, “FBI: New Barbie ’Video Girl’ doll could be used for child porn.” 2010. [Online]. Available:http://newsroom.blogs.cnn.com/2010/12/06/fbi-new-barbie-video-girl-doll-could-be-used-for-child-porn-2/ [ Accessed : 31-Jul. -2019]

[4] P. C. K. Hung, “Children Privacy Protection Engine for Smart Anthropomorphic Toys Proposal.” 2015.

[5] S. Chakraborty, K. R. Raghavan, M. P. Johnson, and M. B. Srivastava, “A Framework for Context-Aware Privacy of Sensor Data on Mobile Systems,” the Fourteenth Workshop on Mobile Computing Systems and Applications , pp. 6. 2013.

[6] H. Haifa, M.Yousef, S. Shaima & F. Iqbal, “ State of the Art in Digital Forensics for Small Scale Digital Devices”. 11th International Conference on Information and Communication Systems (ICICS), 2020

[7] G. Tsakalidis, and K. Vergidis “A Systematic Approach Toward Description and Classification of Cybercrime Incidents,” IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2017.

[8] FBI and NW3C, “2014 Internet Crime Report”. 2015. [Online]. Available:https://pdf.ic3.gov/2014_IC3Report.pdf [Accessed on July 21, 2017].

[9] Council of Europe, “Convention on Cybercrime.” Nov. 23, 2001. [Online]. Available: http://www.coe.int/ el/web/conventions/full-list/-/. [Accessed: Jul. 21, 2017].

[10] “Internet Crime Complaint Center (IC3) | Search.” [Online]. Available:https://www.ic3.gov/search.aspx?q="personal choice outfitters"&p=4. [Accessed: 22-May-2020].

[11] P. C. K. Hung, “Children Privacy Protection Engine for Smart Anthropomorphic Toys Proposal.” 2015.

[12] J. McLaughlin, "New Court Filing Reveals Apple Faces 12 Other Requests to Break Into Locked iPhones". The Intercept. February 23, 2016.

[13] PricewaterhouseCoopers, “The Global State of Information Security_ Survey 2015—Managing Cyber Risks in an Interconnected World”. Sep. 30, 2014. [Online]. Available: http://www.pwccn.com/webmedia/doc/635527689739110925_rcs_info_security_2015.pdf. [Accessed: Jul. 21, 2017].

[14] F. Howard, "Exploring the Blackhole exploit kit: 2.3.4 Payload". March 29, 2012. [Online]. Available:https://nakedsecurity.sophos.com/exploringthe-blackhole-exploitkit14/. [Accessed: 31-Jul-2019].

[15] D. L. Shinder and M. Cross, Scene of the Cybercrime. Burlington, MA, USA: Syngress, 2008.

[16] P. C. K. Hung, M. Fantinato, and L. Rafferty, “A Study of Privacy Requirements for Smart Toys,” The 20th Pacific Asia Conference on Information Systems (PACIS 2016), Chiayi, Taiwan, June 27 - July 1, 2016.

[17] D. Forbrukerra, “Investigation of privacy and security issues with smart toys,” Available:https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical- analysis-of-the-dolls-bouvet.pdf, Nov.2016.

[18] V. Verdoodt and E. Lievens, “Toying with children’s emotions, the new game in town? The legality of advergames in the EU.” Computer Law & Security Review vol. 32, no. 4, 599-614. 2016.

[19] B. Yankson, F. Iqbal, and P. C. K. Hung, “Privacy Preservation Framework for Smart Connected Toys.” Computing in Smart Toys, pp. 149-164. 2017

[20] L. G. de Carvalho and M. M. Eler, “Security Tests for Smart Toys.” ICEIS (2). pp.111. 2018.

[21] B. Yankson, “PDCA Based Privacy Preservation Framework.” International Journal of Information Security, Springer

[22] Rapid7. HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities.https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor- Exposures-and-Vulnerabilities.pdf, Sept. 2015.

[23] E. Taylor and K. Michael, “Smart Toys that are the Stuff of Nightmares.” IEEE Technology and Society Magazine, 35(1). pp.8–10. 2016.

[24] Inc. Somerset Recon, “Hello Barbie Initial Security Analysis,” Jan. 2016.

[25] T. Denning, C. Matuszek, K. Koscher, J. R. Smith, and T. Kohno, “A spotlight on security and privacy risks with future household robots: attacks and lessons.” The ACM international conference on Ubiquitous computing pp.105–114. 2009.

[26] M. Dhanhani, B. AlRasebi, A.Nuaimi, and F. Iqbal, “Forensics of “Hello Barbie” Smart Toy,” Student Paper, Zayed University College of Technological Innovation

[27] Barbiemedia.com, “Mattel Focuses on Dad with New Campaign.” Jan 23, 2017. [Online]. Available:http://www.barbiemedia.com/news/detail/150.html. /. [Accessed: 31-Jul-2019].

[28] B. Yankson, F. Iqbal, S. Aleem, B. Shah, P. C. K. Hung and A. P. de Albuquerque, "A Privacy-Preserving Context Ontology (PPCO) for Smart Connected Toys," 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), Copenhagen, Denmark, 2019, pp. 1-6, doi: 10.1109/CMI48017.2019.8962141.

[29] B. Yankson, F. Iqbal, Z. Lu, X. Wang, and P.C.K Hung, P. “Modelling Privacy Preservation in Smart Connected Toys by Petri-Nets,” Proceedings of the 52nd Hawaii International Conference on System Sciences, pp. 1696-1705, January 8 – 12, 2019.

[30] A. Hilts, C. Parsons, and J. Knockel, “Every step you fake: A comparative analysis of fitness tracker privacy and security,” 2016.