doi:10.20944/preprints201812.0313.v1

Wearables as Digital Evidence

FITBIT EVIDENCE CASE STUDY

Princess Sumaya University for Technology (PSUT)
King Abdullah I Faculty of Graduate Studies and Scientific Research
tar20168014@std.psut.edu.jo

Tariq Khairallah

1. Abstract

Digital Evidence is considered as an important type of evidence in many legal cases. Many legislations have dedicated laws to the collection, handling and admissibility of digital evidence. New technologies and new devices are rapidly being developed, which creates new sources of digital evidence. This presents a challenge to law enforcement agencies and digital investigators to stay up to date with the rapid development in the digital field. This paper discusses a relatively new source of digital evidence which is the evidence extracted from Wearable devices. A Fitbit fitness tracker is one of the most common wearable devices used by many people today. This paper presents a case study whereby data extracted from a Fitbit was used as a digital evidence. The admissibility and the challenges of using Wearables as digital evidence is also discussed.

Keywords: Forensics, digital forensics, wearable,law

2. Introduction

Technology has infiltrated every aspect of our lives. Computers, mobile phones, wearable devices and smart TVs are becoming essential devices for most people. This widespread of technology has opened new doors to criminals through which they can commit their crimes. New forms of crimes have evolved in what is known as Computer crime or Cybercrime. This includes crimes like hacking, information theft, cyber extortion, credit card fraud, and illegal distribution of pornographic material [1]. In all of these crimes, as well as in traditional crimes, pieces of evidence can be found within digital devices. For example, a person’s mobile phone can contain messages and pictures that might contain evidence regarding their intent, their location at the time of the crime, and their relationship with the victim or other suspects [2].

Since digital evidence is critical in all types of crime, not just computer crime, a new field of forensic science has evolved concerning the collection and analysis of digital evidence. Digital forensics is defined as the “scientific knowledge and methods applied to the identification, collection, preservation, examination, and analysis of digital evidence in a manner acceptable for application in legal matters”[3]. The National Institute of Justice defines Digital evidence as the "information and data of value to an investigation that is stored on, received or transmitted by an electronic device"[4].

From the above definitions, it can be concluded that proper identification and handling of digital evidence is of critical importance to its admissibility in court. Hence, Law enforcement agencies are incorporating the collection and analysis of digital evidence into their investigation processes. However, Law enforcement agencies are being challenged by the need to train their staff to stay up to date due to the rapidly evolving nature of new technologies in the digital field [2].

There are several characteristics pertaining to the nature of digital evidence that distinguishes it from typical evidence. Digital evidence can be time sensitive, latent (hidden), and can be easily altered, damaged or destroyed [4]. In addition, digital evidence crosses jurisdictional boundaries, which presents even greater challenges for digital investigators and law enforcement officials. A forensic analyst must make sure that the procedures used are fully compliant with all applicable laws and regulations in that particular jurisdiction [5].

In this paper, different sources of digital evidence are discussed, with the focus being on Wearable devices as digital evidence. A case study related to this particular digital evidence is presented. The rest of this paper is organized as follows: the process of digital forensic investigation is presented in section 2. An overview of the different sources of digital evidence is presented in section 3. A focus on Wearables as a source for digital evidence is presented in section 4. A discussion of the admissibility of wearables as digital evidence is presented in section 5. A case study whereby a digital evidence is extracted from a wearable device is presented in on page 8. A discussion of the challenges on using Wearables as digital evidence is presented in section 7, and a conclusion is presented in section 8.

3. Process of Digital Forensic Investigation

Digital Forensic Investigation may be needed in many different situations, such as evidence collection for legal proceedings, and internal corporate investigation of Security Policy violations [6]. The techniques and tools used by forensic investigators may vary depending on the type of incident and the type of investigated digital evidence, hence a defined procedure is required to govern the process of digital investigation and comply with industry standards and appropriate laws [3]. There are various proposed models for the Digital Investigation Process. The basic four phases of digital investigation were outlined by the National Institute of Standards and Technology's special publication 800-86 "Guide to Integrating Forensic Techniques into Incident Response" [6]. The four phases are Collection, Examination, Analysis, and Reporting as outlined in Figure 1 Phases of Digital Investigation Process.

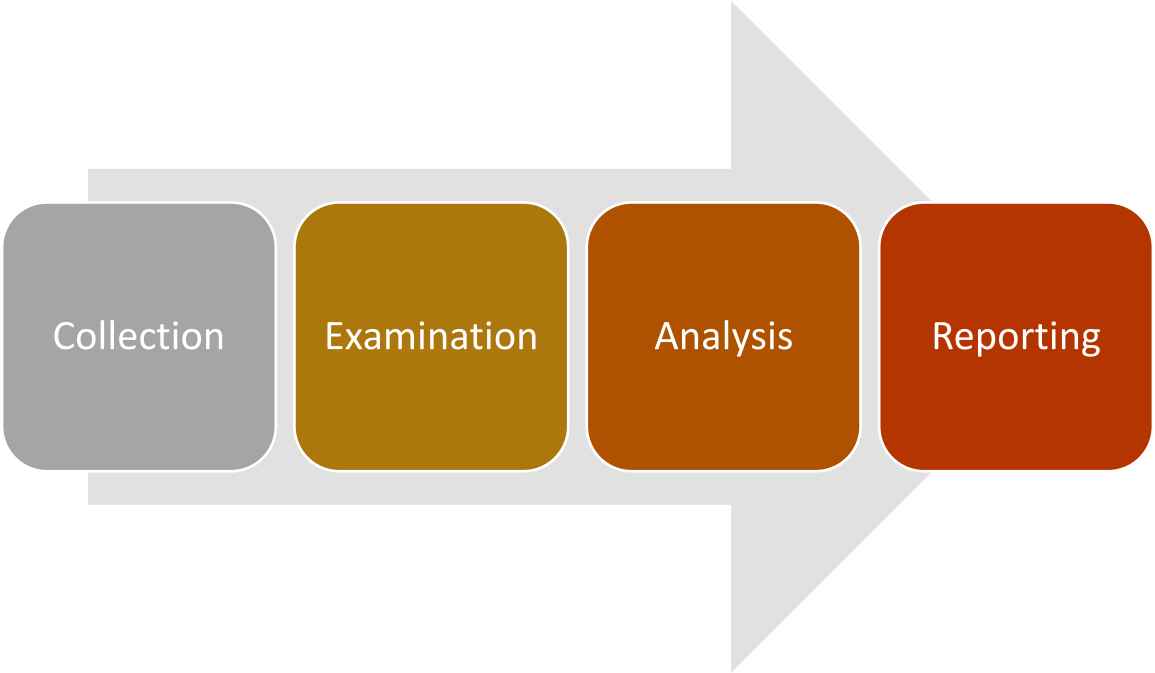

Figure 1 Phases of Digital Investigation Process.

Generally, a digital forensic investigation starts with the identification of the incident and the identification of the sources of digital evidence. Then a search warrant is issued by the delegated Law enforcement agency to collect and analyze the digital evidence. The forensic investigator must be aware that the use of improper methodology or unlawful search and seizure can negatively affect the admissibility of the evidence [3]. Once the search warrant is obtained, the forensic investigator will prepare the tools and the techniques needed for the rest of the process. The four phases of the process are then followed as described below:

The Collection phase refers to the collection of digital evidence from the various sources related to the incident being investigated. When collecting the evidence, it is critical that no changes are made to the original data. For example, when collecting evidence form a computer hard disk, a forensic copy of the data stored on the hard disk is taken in order to perform the analysis on that copy. A special device called a write blocker is used during the copying process to prevent any changes to the data on the hard disk [7].

The collection phase is of utmost importance as the rest of the phases depend on the current collection of evidence. Two critical factors in this stage are the Authenticity of the evidence data collected, and the Preservation of the digital evidence. Authenticity of digital evidence refers to the proof that the evidence has not been altered and that it comes from a certain source. In Federal Courts, authenticity is governed by Rule 901(a), which requires that to establish that an item is authentic, a proponent must produce admissible evidence “sufficient to support a finding that the item is what the proponent claims it is.” [8]

The preservation of digital evidence refers to following general best practices and guidelines when handling the evidence. The most important guidelines are as follows [7]:

- Ensure that all digital evidences collected are properly documented, labeled, marked, photographed, video recorded or sketched, and inventoried.
- Ensure that special care is taken with the digital evidences material during transportation to avoid physical damage, vibration and the effects of magnetic fields, electrical static and large variation of temperature and humidity.
- Ensure that the digital evidence is stored in a secure, climate-controlled environment or a location that is not subject to extreme temperature or humidity. Ensure that the digital evidence is not exposed to magnetic fields, moisture, dust, vibration, or any other elements that may damage or destroy it.

The Examination phase involves assessing and extracting the relevant pieces of information from the collected data. For example, an acquired hard drive may contain hundreds of thousands of data files. The examination phase involves identifying the data files that contain information of interest, including information concealed through file compression and access control. There are various tools and techniques that an investigator can use to reduce the amount of data that has to be searched through. These tools help in finding relevant documents and files by searching for a person, or email address. Some tools help in determining the type of contents of each file (text, image, audio, video) which can help when a certain type of content is being searched for [6].

The Analysis phase refers to analyzing the data resulting from examination phase to reach appropriate conclusions based on the evidence found or determine that no conclusion can yet be drawn. The analysis should include identifying people, places, items, and events, and determining how these elements are related so that a conclusion can be reached. The technical knowledge and experience of the analyst plays a major role in performing an effective analysis. The analysis should be conducted using legally justifiable methods and techniques [6][9].

The Reporting phase refers to the process of preparing and presenting the information resulting from the analysis phase. This done by presenting the evidence and the investigator’s conclusion to the person or group requesting the DF investigation [7].

4. Sources of Digital Evidence

Various types of digital devices that can be a source of digital evidence. The most familiar devices being computers and cell phones. However, what most people do not recognize is that any piece of technology that processes information can be a valuable source of digital evidence. For example, flash drives, PDAs, wearable devices, digital recorders, smart home appliances printers and network devices are all valuable sources of digital evidence. A digital evidence can be classified into two categories [5]:

- ***Computer-generated evidence***: which is an output of computer instructions without manual intervention. This will include output of programs, log files, receipts and reports.
- ***Computer-stored evidence***: which is based on human generated contents. This will include Emails, word documents, spreadsheets and text messages.

Regardless of the source and category of the digital evidence, it is critical that on-site forensic investigators are able to recognize and properly seize potential digital evidence from the various potential sources [10] .

5. Wearables as digital evidence

Wearable devices, also known as "Wearables" are the next generation of portable technology that has become an integral part of everyday life for so many people. The International Data Corporation has reported that the total volume of smart "Wearables" will reach 25.7 million units in 2015 [11]. Wearables are "devices worn, applied, or ingested that are designed to measure or capture health-related data in digital format without intervention by the subject and their associated apps" [12]. Examples include Biometric watches, ingestible sensors and smart contact lenses. The data stored on these devices can be an important source of intelligence.

One of the most popular wearables on the market are the Fitbit fitness trackers "Fitbit". A Fitbit is designed to measure the wearer's activity levels by collecting data using sensors that monitors the user's location, vital signs, sleep patterns, and physical activity [13]. A Fitbit is capable of creating detailed descriptions of the user's everyday activities and habits. The data gathered by the Fitbit is synced to the user's account on the Cloud for the purpose of monitoring their exercise progress, sleep quality, and medical statistics. This data can also be synced to a mobile application for easy access by the user to their activity history.

There are several technologies behind the Fitbit tracker that enable it to achieve its purpose [14], these are:

- Global Positioning System (GPS), which is used to determine the device's location.
- Wireless Networking (WIFI), which tracks the device's movement when it connects to the internet.
- Near Field Communication (NFC) which enables devices in close proximity to establish a connection to each other.
- Bluetooth, which is used by many Wearable devices to connect to a mobile phone, a tablet or a computer.

- Gyros and Accelerometers, which are sensors that are used to detect the orientation, tilt, and motion of the device.
- Heart Rate Monitor, which are sensors, embedded in the Wearable device to monitor the heart rate.

These sophisticated technologies enable the Fitbit to track steps, distance, calories burned, active minutes, stairs climbed, sleep habits, stationary time, continuous heart rate, breathing patterns, location, pace, elevation, and routes, among other calculable figures [15]. The Fitbit is designed as a wristband, which is worn by the user throughout the day. The Fitbit synchronizes automatically to a smartphone via Bluetooth. The Fitbit will gather data as long as the user is wearing the device and using it properly.

With the enormous amount of data gathered and saved by the Fitbit trackers, they have become a significant source of digital evidence in legal cases. Wearable device evidence has already been involved in a variety of court cases, including the following:

- In 2014, a Canadian law firm used the Fitbit data to show the effects an accident had on their client. The client's Fitbit data showed that her activity level had significantly decreased since the accident as a result of her injuries [16].
- In 2014, Police in Pennsylvania, US, proved that a woman was lying about being assaulted using data from her Fitbit. The woman claimed that she asleep when an intruder broke into her home and attacked her. However, her Fitbit data showed that she was awake and walking around during the time of the alleged attack. She was later changed with filing a false report [17].

6. Admissibility of Wearables as Digital Evidence

The value of digital evidence retrieved from Wearable devices has been recognized in several courts [18]. Under the US Federal Rules of Evidence, admitting data collected from portable devices and computers as evidence does not require much more than the admission of standard evidence [19]. There are legal requirements in most jurisdictions for the admissibility of digital evidence in legal proceedings. These requirements apply to all sources of digital evidence including evidence extracted from Wearable devices [20]. These requirements are:

- ***Legal Authorization***: Search warrants and legal authorization must be obtained prior to the search and seizure of electronic devices and digital evidence. The goal is to protect human rights, and the privacy of data.
- ***Digital Evidence Relevance***: For the evidence to be admissible, it must be relevant to the incident being investigated.
- ***Digital Evidence Authenticity***: For the evidence to be admissible, it must be proven without any doubt that the evidence comes from the claimed source.
- ***Digital Evidence Integrity***: For the evidence to be admissible, it must be complete and unaltered. Courts require a "Chain of Custody" document for each evidence, to guarantee its integrity during its entire lifecycle.
- ***Digital Evidence Reliability***: For the evidence to be admissible, there must be nothing that casts doubt about how the evidence was collected and subsequently handled [21].

7. Case Study

The most controversial criminal case where Fitbit data was used as digital evidence is a murder case in Connecticut in December 2015. In this case, police found the victim - Connie Dabate -dead from two gunshot wounds in the basement of her house. Her husband – Richard Dabate - was found tied to a folding chair on the kitchen floor with several cuts on his body [22].

Richard told the police his version of the events leading to the murder of his wife; however, data from her Fitbit and other digital devices contradict his story. A year after the incident and with the help of several digital evidence, Richard was charged with the murder of his wife [23].

In his story, the defendant claims that while he was driving to work on the morning of Dec 23, he received an alert on his cellphone indicating that the home alarm at his house has been activated. He claims that he sent an email to his boss from his cellphone indicating that he will be late for work. He drove back home and claims to have arrived at approximately 9 am [24].

The defendant claims that once he arrived at his house, he encountered a masked intruder. He claims that while he was struggling with the intruder, he heard his wife coming back home from the gym and arriving at the garage door. The defendant claims that the intruder was able to chain him to a chair in the kitchen and ran after his wife. The intruder followed Connie Dabate to the basement and shot her, and then escaped from the house. The defendant, although tied up to a chair, claims that he then managed to activate the panic button from the home's alarm system [24].

After initial investigation, the police found the husband's story a little suspicious. There was little sign of struggle in the house and no signs of forced entry. The dogs were not able to pick up the scent of an intruder, and there was no blood evidence to support the defendant's story. So, the police issued search warrants for the following electronic records [25]:

- Cellphone records for the defendant and his wife.
- Computer records from the defendant's laptop.
- Facebook records for the defendant and his wife.
- Text messages.
- Fitbit records for the wife.

After investigating the data from the aforementioned electronic records, the police found text messages showing that the defendant was involved with another woman and was discussing getting a divorce from his wife. Police were also able to construct a timeline of the events, which contradicted, with the defendant's version of the story. Following is an illustration of the timeline of events [23], [24]:

- At 8:30 am, the defendant claims to have left the house to go to work.
- At 8:46 am, the Wife's Fitbit records show idle time after activity, which is presumably the time she left the house.
- At 8:53 am, surveillance Cameras from the gym's parking lot show the wife arriving at the gym.
- Between 8:30 and 9:00 am, the defendant claims to have received an alert on his cellphone from the home alarm system. The defendant claims that he sent an email to his boss from his cellphone and drove back to his house.

- At 9:00 am, the defendant claims to have arrived back at his house and was faced by the intruder. A little after, the wife arrived and was chased by the intruder to the basement, and then shot dead.
- At 9:04 am, records from the defendant's laptop show that an email was sent from the defendant's laptop not cellphone. Geolocation data shows that the email was sent from the defendant's home, not while being on the road as he claims.
- At 9:18 am, Google search records from the defendant's laptop showing that he searched his wife's exercise schedule at the gym.
- At 9:18 am, surveillance cameras show the wife leaving the gym. Cellphone records show that she made a call that lasted almost 4 minutes.
- At 9:23 am, wife's Fitbit data show activity after being idle between 9:18 and 9:23 which is the time she was presumably driving home.
- At 9:23 am, data from the home alarm system showing the garage door was opened.
- At 9:40 to 9:46 am, Facebook data showing that the wife posted two videos on Facebook. The IP address for this transaction was traced to the house.
- At 10:05 am, wife's Fitbit record show last movement. Between the time she came home and when it stopped, she moved a distance of 1,217 feet inside the house.
- At 10:11 am, home alarm panic button was activated, which is approximately an hour after the defendant claims to have activated it.
- At 10.16 am, a call to the police was placed from the home alarm system company.
- At 10:20 am, the defendant called 911.

As seen from the above timeline, many sources of electronic devices and records provide digital evidence that tell another version of the story of how the events took place at the time of the incident. Correlation between the evidence gathered from several digital sources helped the police in knowing the facts of the incident. The most crucial evidence is the data retrieved from the victim's Fitbit, which shows that her last movement was at 10:05 am, which is an hour after the time her husband claimed that the intruder shot her. In addition, Fitbit records show that the victim moved a distance of 1,217 feet inside the house, which is 10 times the distance from her car to their basement.

doi:10.20944/preprints201812.0313.v1

8. Challenges on using Wearables Digital Evidence

Although digital evidence extracted from Wearable devices has been used in several legal cases as discussed above[16], [17] and [22]; there are some challenges with Wearable evidence that might be used to refute the validity and reliability of the evidence. In our opinion, these challenges can be categorized into Legal challenges, operational challenges, and misuse challenges as follows:

1. Legal challenges:

- Digital data evidence gathering is new and crime scene police may not be knowledgeable in how to collect, secure, transport or store digital data to ensure data is not compromised or lost.
- Not every law enforcement agency has laboratories or certified forensic investigators to examine and interpret data from Wearable devices.

2. Operational Challenges:

- The time-stamp within the Fitbit can be set to an inaccurate time, hence the time of the events will not be accurate, and correlation with other digital evidence will not be possible.
- Fitbit depend on GPS for data transmission and tracking. GPS requires a direct path to the satellite it is using for proper data transmission. If the GPS signal is being blocked for some reason - the user is underground, weather conditions – then the data collected will not be accurate.
- Many models of Wearable devices are available on the market, each with its own set of features and capabilities. Not all devices provide the same functionality and interpretation of movement. For example, some models will not distinguish arm movement from actual steps, and hence their data records will not be reliable.

3. Misuse Challenges

- More than one person may wear a Fitbit.

- The data records from the Fitbit are accurate as long as the user is wearing the device and using it properly. For example, wearing the device on the ankle will produce inconsistent data

9. Conclusion

Digital forensic investigation has developed enormously during the recent years. The advent of new devices that store data has been challenging to forensic investigators and law enforcement agencies. New forensic analysis tools and techniques were and still being developed in order to be able to process and analyze data from these devices. Computers and mobile devices are the most common sources of digital evidence; however, it has been proven from many legal cases that there are various other sources of valuable digital evidence.

Wearable devices store endless amounts of data about the user’s location, activity levels, sleep patterns, and moving habits; thereby creating a detailed narrative of the user’s everyday life. Evidence extracted from Wearable devices has not yet been used on a wide scale due to arguments regarding the reliability and accuracy of these devices. However, these devices are being improved continuously, their accuracy and reliability and thereby admissibility is improving specially when they are synced to other devices like mobile phones and computers which are already used as admissible evidence in court.

Provided that the evidence meets the requirements of admissibility, Wearable devices should be considered as one of the sources of digital evidence that can be helpful in many legal cases.

References

[1] INTERPOL, "The changing nature of cybercrime." [Online]. Available: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

[2] NIJ, "Digital Evidence and Forensics." [Online]. Available: https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx. [Accessed: 20-Aug-2003].

[3] J. T. Ami-Narh and P. A. H. Williams, "Digital forensics and the legal system: A dilemma of our times," *6th Aust. Digit. Forensics Conf.*, pp. 30–40, 2008.

[4] N. C. J. U.S. Department of Justice, "Electronic Crime Scene Investigation: A Guide for First Responders," *NIJ Res. Rep.*, no. NCJ 187736, p. 96, 2001.

[5] S. Sivanathan, "Digital Evidence Management Framework For Computer Forensics." [Online]. Available: http://www.forensicfocus.com/Content/pid=98/.

[6] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," 2006.

[7] H. Guo, B. Jin, and D. Huang, "Research and review on computer forensics," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.*, vol. 56, pp. 224–233, 2011.

[8] H. O. N. P. W. Grimm, for Authenticating Digital Evidence. 2016.

[9] C. Harrell, "Overall DF Investigation Process." [Online]. Available: http://journeyintoir.blogspot.com/2010/10/overall-df-investigation-process.html.

[10] National Forensic Science Technology Center, "A Simplified Guide To Digital Evidence," 2009.

[11] T. Priestley, "Goodbye Apple Watch, Hello Again G-Shock." [Online]. Available: https://www.forbes.com/sites/theopriestley/2015/06/27/goodbye-apple-watch-hello-again-g-shock/#31b86f13f3c7.

[12] T. Schoenwaelder and V. President, "ROLE OF WEARABLE DEVICES FOR REAL-WORLD DATA COLLECTION : ENGAGEMENT OR TODAY ' S," 2017.

[13] K. Crawford, “When Fitbit Is the Expert Witness.” [Online]. Available: https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/.

[14] W. Kruse, “Your Employee May Be Wearing Their Alibi - Or Your Evidence Vice President for Digital Forensics,” p. 8, 2015.

[15] “Fitbit Charge 2.” [Online]. Available: https://www.fitbit.com/charge2.

[16] Sarah Griffiths, “Fitbit data is now being used in COURT.” [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-2838025/Fitbit-data-used-COURT-Wearable-technology-set-revolutionise-personal-injury-claims.html.

[17] Kate Pickels, “Police claim woman lied about being raped.” [Online]. Available: http://www.dailymail.co.uk/news/article-3134701/Police-claim-woman-lied-raped-Fitbit-fitness-watch-showed-not-dragged-bed.html.

[18] S. Gibbs, “Court sets legal precedent with evidence from Fitbit health tracker.” [Online]. Available: https://www.theguardian.com/technology/2014/nov/18/court-accepts-data-fitbit-health-tracker.

[19] K. E. Vinez, “The Admissibility of Data Collected from Wearable Devices,” *Stetson J. Advocacy Law*, vol. 1, pp. 1–23, 2017.

[20] A. Antwi-boasiako and H. Venter, “A Model For Digital Evidence Admissibility Assessment,” *Adv. Digit. Forensics XIII*, vol. 511, pp. 23–38, 2017.

[21] O. Leroux, “Legal Admissibility of Electronic Evidence,” *Int. Rev. Law, Comput. Technol.*, vol. 18, no. 2, pp. 193–220, 2007.

[22] J. N. Goldman, “The Fitbit Murder and Our New Digital Witnesses.” [Online]. Available: http://goldmandefense.com/fitbit-murder-new-digital-witnesses/.

[23] D. Altimari, “A Marriage Marked By Secrets, A Murder Case Months In The Making.” [Online]. Available: http://www.courant.com/news/connecticut/hc-ellington-murder-fit-bit-20170422-story.html.

[24] N. Black, “Fitbit data, other digital evidence used by prosection in murder case.” [Online]. Available: http://www.legalnews.com/washtenaw/1443244.

[25] S. C. State of Connecticut, “Police Investigation Report.”