Catch Me if You Can: Analysis of Digital Devices and Artifacts Used in Murder Cases

John Jankura[1], Hannah Catallo-Stooks[1], Ibrahim Baggili[2(✉)], and Golden Richard[2]

[1] University of New Haven, West Haven, CT 06516, USA
[2] Louisiana State University, Baton Rouge, LA 70803, USA
ibaggili@lsu.edu

Abstract. The rapidly advancing field of digital forensics has become a crucial component in murder trials. We present an analysis of murder investigations that utilize digital evidence within the United States. One hundred six (n = 106) murder cases were examined with an emphasis on associated digital devices and artifacts that played an important evidentiary role. While other works attempt to identify relevant evidence in different types of criminal investigations, few, if any, attempt to do so using real-world cases with multiple digital devices and artifacts. Our results for devices showed favorable trends towards cell phones, where 66.98% of the examined cases employed a cell phone's contents as digital evidence. An analysis of the digital artifacts identified location services (39.62%), photo/video/audio (33.96%), and SMS/iMessage (25.47%) as high-use evidence when conducting an investigation. Guilty verdicts made up 64.15% of the examined cases and 98.11% of the evidence was deemed inculpatory, or evidence that proves guilt. This work seeks to provide a refined outlook as to how digital evidence is used when conducting a criminal investigation to ameliorate the efficiency of the digital forensics process.

Keywords: digital evidence · digital artifacts · digital forensics · murder · investigation · case analysis

1 Introduction

The advancement of digital devices has made modern life more productive, entertaining, and connected. While devices aim to integrate these features, the digital evidence they produce aids in the criminal investigative process. The employment of digital forensics to assist in solving crimes has created a need for examiners that can reliably investigate digital devices and artifacts. The 2015 murder of Connie Dabate [8] was an example of the need for reliably examiners. Connie's death was originally thought to be a home invasion, however, after investigators

S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 570, pp. 19–32, 2024.
https://doi.org/10.1007/978-3-031-56580-9_2

examined data extracted from her smartwatch, they were able to find inconsistencies in her husband's story, who has since been convicted of killing Connie. The use of digital forensics continues to sustain efforts in investigations. Artifacts such as text messages, location services, browser history, and health data found on digital devices yields valuable information that can help piece together a murder investigation.

The continued growth of applying digital forensics in criminal cases makes it of the utmost importance to collect and analyze digital evidence related to these cases. This growth in digital forensics can, in part, be attributed to the increased use of digital devices. Pew Research Center found in a 2021 survey [4], that 97% of American adults own a cell phone, and 85% of Americans adults own a smartphone. The use of digital devices has continued to grow exponentially and with it, the digital evidence they provide.

The increased popularity of digital forensics as evidence is personified through the sheer volume of digital forensic examinations. The collaboration between the Federal Bureau of Investigation (FBI) and other federal, state, and local law enforcement agencies known as the Regional Computer Forensics Laboratory (RCFL) provides "forensic services and expertise to support law enforcement agencies in collecting and examining digital evidence" [1]. As outlined in the RCFL's 2020 fiscal year report, they assisted 649 different federal, state, and local law enforcement agencies on 7,576 service requests, with the New England division of RCFL (NERCFL) doubling the number of examinations from 2019 to 2020 [3].

By exploring trends related to digital evidence used in murder cases, a new understanding of the role that the evidence plays in helping piece together a case can be ascertained. From this, a projected path for the future of digital forensics can be assessed. The implications of this research will allow for investigators to adapt and more quickly identify areas that could be of high importance to them.

The immense amount of digital evidence that is used in criminal investigations calls for an analysis of how it is used to build, supplement, and close criminal cases. The contributions from our work are as follows:

- We provide the primary account for the exploratory analysis of digital evidence in real murder cases.
- We explore digital forensic trends that occur within real-world investigations. This will help provide an answer to the question of how digital devices and artifacts are being used in criminal investigations. A more refined outlook of how digital forensic investigations are conducted, how to improve them, and an educated prediction of future trends within the field can be determined.
- We provide a new data set of (n = 106) resources about murder cases in the United States (U.S.) that employ digital evidence.

The remainder of this paper is organized into several sections. Section 2 describes background information and related work. We then share the limitations in Sect. 3, followed by our research methodology in Sect. 4. The results and analysis are then presented in Sect. 5, followed by the conclusion in Sect. 6.

2 Background and Related Work

Understanding the challenges presented by digital evidence in a murder investigation can help improve upon previously utilized methods. This can boost the overall efficiency and accuracy of investigations. We analyzed literature to understand both tangential work and the challenges faced in Digital Forensics (DF).

2.1 Related Work

Little work exists related to digital evidence in murder cases. A 2014 survey of mobile digital evidence related to different case types was investigated [26]. The data for the survey was collected from investigators and examined nineteen types of evidence and seven different case types. It was concluded that Short Message Service (SMS) messages were the most relevant digital evidence used in all seven types of cases. Other types of relevant digital evidence included Multimedia Message Service (MMS), phonebook and contacts, and audio calls. This survey aimed to help save investigators time and effort in understanding what type of evidence was most relevant in an investigation. While this work contributed to understanding the relevance of digital evidence to a particular case for mobile forensics, it did not address other types of devices. Additionally, this prior work presented the perceived relevance of digital evidence from its respondents and was not based on DF being used in real cases [26].

2.2 Previous Works with Digital Evidence

We examined related work associated with sources of digital evidence, mainly location data, smart watches, health and fitness applications, social media, vehicles, smart home devices and CCTV.

Location. Previous research noted that traditional Global Positioning System (GPS) devices are no longer of significant relevance to digital examiners, and are being supplanted by smartphones and applications such as Google Maps, Apple Maps, Waze, among others [25]. The results outlined critical artifacts that can be employed in criminal investigations, including navigation data, addresses, and latitude/longitude points that could be forensically recovered.

While applications containing geographic information are relevant, instances of location services based on cell phone tower triangulation are increasingly of interest to investigators. While its popularity increases, questions surrounding constitutional rights related to the Fourth Amendment, which protects citizens from unlawful searches and seizures are often raised. An article in the Saint Louis University Public Law Review examined the admissibility of cellular records in court [28]. A question brought up by investigations is, does a defendant have a reasonable expectation of privacy when a cell phone tower is pinged for a phone call or other matters? While opponents of pulling the cell tower records argue

that there is no "voluntary transfer of location information", proponents of it state that there is no Fourth Amendment violation, as explained in United States v. Benford, because "historical cell site data is similar to pen registrations and banking records in that the caller voluntarily used the equipment and, therefore, ran the risk that the call records would be given to police" [22]. Currently, most district courts find there to be no violation of a defendant's constitutional rights when cellular data records are examined in criminal investigations.

Smart Watches. In 2019, an analysis of a Samsung Gear 3 Frontier smart watch showed that wearable technology can provide relevant digital evidence to an investigation [12]. In the analysis, the smart watch was used for three hours and the findings displayed artifacts such as user activity, connection to a phone, notifications, and saved images that were on the watch. A similar 2015 study [9] performed a digital analysis of a Samsung Gear 2 Neo watch and the LG G watch. Messages, health and fitness data, e-mails, contacts, events, and notifications were all able to be extracted from the watches as well. These works illustrate how smart watches can be analyzed for digital evidence.

Health and Fitness Applications. Health and fitness applications are another intriguing place where digital evidence can be found. A 2019 study examined thirteen health and fitness applications from the Google Play store. Personal information such as name, birthday, sex, height, weight, email, and location were extracted from Android mobile devices that had these applications [19].

Social Media. Social media often provides valuable information to DF examiners, as discussed in a 2012 study of social media artifacts found on mobile devices [6]. It was determined that social network applications such as Twitter, Facebook, and MySpace left valuable information on iPhones and Android phones for investigators to uncover. Other work regarding Snapchat on Android devices yielded evidence in the textual form of "event logs, sent snaps, 100% friends, 100% user, 58% chat messages, and 6% delivered video with detailed information about artifact such as sender, receiver, time, and status" [7]. DF work has also been extended to other social platforms [5], alt-tech social platforms [29] and immersive virtual social environments [13]. Being able to recover information about activities on social media is yet another valuable resource for investigators.

Vehicles. In a case study [27] of vehicle forensics, evidence such as frequent routes, saved locations, data from linked phones, such as call history, contact directory, SMS, and pictures were able to be extracted. With the advancement of technology in cars, they can now be equipped with cellular connections, WiFi, Near Field Communication (NFC), and Bluetooth. From these connections, more data is able to be extracted. Many modern vehicles come with an infotainment

system which can gather and store data from a connected cell phone. While this case study only analyzed one manufacturer of cars, similar technologies are used by many other car companies, which leads one to expect that similar conclusions can be drawn for other vehicle types.

Smart Home Devices. In 2021, a forensic analysis [20] of an Amazon Echo yielded information that could prove useful for criminal investigators. After conducting a forensic examination on the Echo device, it was concluded that cloud forensics produced the most relevant data. The only issue was that the data was only easily obtained if the user credentials were known. This presents a major challenge to investigators to conduct a lawful search. This can be a recurring issue for smart devices that store data in a cloud.

In 2015, following the murder of a man in Arkansas, law enforcement believed that an Amazon Echo contained an incriminating conversation that happened during the time of the murder. Amazon initially refused to provide the information that was being asked of them by police, but cooperated after the defendant gave them permission. What they found was that the Amazon Echo utilizes a "wake word", which is often either "Amazon" or "Alexa", that turns them on and records what the user is saying [15]. At the time of the murder no wake word had been uttered, so there was no data of value recorded on the Amazon Echo. A study [14] of the Google Home Mini, which has similar capabilities as an Amazon Echo, found that investigators were able to find artifacts such as "whether anyone manually calibrated the thermostat, whether the user was present at home during a certain time, whether the user spoke to the Google Home Mini device to make any adjustments to the thermostat, and whether the camera was intentionally turned off at a certain time". While the death in Arkansas proved to be a dead end, the potential for evidence to be stored on a smart home-type device remains realistic.

CCTV. Closed-circuit television (CCTV) became a popular way to record and prevent crimes during the early 1970's. There has been a thorough analysis and procedures documented to deal with CCTV video evidence with the first edition of *Best practices for the retrieval of video evidence from digital CCTV systems* [2] being published in 2006. This is an 80 page documentation walk through of all the steps law enforcement need to take to correctly retrieve video data. CCTV is still heavily relied on today as seen in the Boston Marathon bombing manhunt in 2013. The FBI and local police used the CCTV from businesses around the marathon to retrace the steps of the bombers, and with the help of other pictures and videos taken by the public, they were able to identify the suspects.

2.3 Challenges of Digital Forensics in Investigations

To best frame our research for enhancing future investigations, understanding the challenges posed in the field is crucial. One such challenge is the vast amount of

data encountered during investigations. This has created a backlog of cases that can delay a pivotal piece of evidence in an investigation. Sometimes devices are not examined until months or even years from when they are received, which can cause a significant delay [24]. Therefore, efficiency is of paramount importance in DF [21].

DF training and education can improve investigative efficiency but is yet another challenge due to a lack of standards for best practices and a non-unified DF curricula [21,23]. One way to improve education is to learn from artifacts encountered in past investigations [10,17,18], and this requires realistic DF datasets [16]. However, previous research outlined challenges in DF datasets stating that only 36.7% of DF datasets employ real-world data [17].

Our work helps in overcoming the aforementioned challenges and provides a dataset derived from real-world cases. This allows for a realistic perspective into what examiners can expect when investigating a murder. The dataset and its analysis assists in future DF investigations and may help expedite the process.

3 Limitations

While this work was conducted to the best of our ability, we recognize the following as potential limitations:

- **Non-Technical Reporting:** With the main source of data collection being from local news reports and legal documents, much of the technically rich explanations had been lost in the description of the cases.
- **Human Analysis:** The data was collected by humans, which leads towards an intrinsic possibility of error. The Delphi Method was performed by examining each case in order to come to a consensus on what was reported.
- **Ongoing Cases:** While a majority of the cases examined had been closed (70.75%), there were still ongoing cases in either the criminal or appellate proceedings. These cases often provide the most up to date examples of digital evidence being used in court. It is noted that the digital evidence was not in question in these, and cases in which the digital evidence was in question were disregarded in our analysis.
- **Unreported Data:** There remains a possibility that not all of the digital evidence that was used in a trial was mentioned in our sources. To limit this as much as possible, each case was examined from multiple sources to extract as much information as possible.

4 Methodology

The following methodology was employed to conduct this research:

1. Using keyword searches, Google was utilized to find news articles that pertained to murder cases that contained digital evidence. This made up for 88.68% of the examined cases.

2. Keyword searches in legal databases such as WestLaw and CaseText made up 11.32% of the cases that were analyzed for this research.
3. The date, location, devices, artifacts, verdict, defendant and victim age and gender, anti-forensic techniques, and inculpatory/exculpatory evidence uses were collected in an Excel spreadsheet.
4. Data was reviewed by researchers to agree on which category each device and artifact belonged which finalized the data set.
5. Using Excel formulas, percentages for each category were derived from the data.
6. The data was analyzed for trends, anomalies, and patterns.

4.1 Search Terms

The cases were found by using a combination of multiple search terms. To maintain consistency in searching for the devices and artifacts, searches were conducted using a device/artifact appended to "murder". An example of a search would include "cell phone murder", "smart watch murder", and "social media murder". Other searches were used in an attempt to find more cases by using more generic terms such as "digital forensic murder".

4.2 Case Requirements

Only murder cases were selected during this study. This is due to availability due to wide-spread reporting. Murder cases that did not contain digital evidence were not considered for this study, as the focus was to examine how digital evidence is being used in murder investigations. To maintain consistency, the cases being examined only occurred in the United States. This was in an effort to work within an area that has mostly the same laws and regulations as it relates to digital evidence.

4.3 Collected Information

In order to best analyze trends related to digital evidence in murder investigations, several categories of each case were recorded. Basic information of the case, such as the date of the murder, the location, the investigating department or agency, the defendant, and the outcome of the case were recorded. Demographics of the victim and the defendant were also recorded, such as age and gender.

In terms of digital evidence, the device(s) and the artifact(s) that were used in the cases were recorded. In several instances, a single case yielded several devices (22.64%) and/or artifacts (47.17%). Each case was permitted to have multiple instances of devices and artifacts recorded, as this would help provide insight as to the full scope of investigations. Specifications about the digital evidence were also noted, such as if the use of anti-forensics was utilized and if the evidence was inculpatory or exculpatory.

4.4 Digital Device Categories

In the process of data collection, the digital devices were sorted into categories. These categories served as data points that would allow for analyzing trends. In total, ten categories were derived from the data that was collected.

- Cars
- CCTVs
- Cell Phones
- Computers/Laptops
- GPS Devices
- Smart Doorbells
- Smart Speakers
- Smart Watches
- Smart Water Heaters
- Video Game Consoles

4.5 Digital Artifact Categories

The types of evidence that can be found on a particular device vary. These variations make way for trends to be discovered between digital artifacts and other variables. In total, the digital artifacts were placed into thirteen categories that allow for analysis of trends related to this work.

- Biometric Data
- Call Logs
- Car Statistics
- Device Activity
- Email
- Internet History
- IP Tracing
- Location Services
- Messenger Apps
- Photo/Video/Audio
- Social Media
- SMS/iMessage
- Water Temperature

5 Results

Through conducting this exploratory research into digital devices and artifacts that were used in (n = 106) murder investigations within the U.S., trends were uncovered. In the following sections we explore the importance of these trends.

5.1 Devices

As referenced in Table 1, the most commonly utilized device in the examined murder investigations were cell phones (66.98%). Cell phones occur 3.74 times more frequently than computers and laptops (17.92%) in the cases that were examined. Other instances of devices include CCTV (12.26%), Cars (8.49%), Smart Doorbells (7.55%), and Smart Watches (5.66%). Smart speakers, gaming consoles, and smart water heaters each had one instance (0.94%).

Table 1. Devices Used In Murder Investigations

Device	#	%
Cell Phone	71	66.98
Computer/Laptop	19	17.92
CCTV	13	12.26
Car	9	8.49
Smart Doorbell	8	7.55
Smart Watch	6	5.66
GPS Device	3	2.83
Smart Speaker	1	0.94
Video Game Console	1	0.94
Smart Water Heater	1	0.94

5.2 Artifacts

As referenced in Table 2, the most commonly utilized artifact in the examined murder investigations was location services (39.62%). Location services occur 1.17 times more frequently than photographs, videos, and audio (33.96%) in the cases that were examined. Other instances of artifacts include SMS/iMessages (25.47%), social media (16.98%), internet history (15.09%), call logs (5.66%), email (5.66%), car statistics (4.72%), biometric data (4.72%), device activity (4.72%), IP tracing (2.83%), and messenger applications (1.89%). There was a single instance (0.94%) where water temperature was collected as an artifact.

Table 2. Artifacts Used In Murder Investigations

Artifact	#	%
Location Services	42	39.62
Photo/Video/Audio	36	33.96
SMS/iMessage	27	25.47
Social Media	18	16.98
Internet History	16	15.09
Call Logs	6	5.66
Email	6	5.66
Car Statistics	5	4.72
Biometric Data	5	4.72
Device Activity	5	4.72
IP Tracing	3	2.83
Messenger Applications	2	1.89
Water Temperature	1	0.94

5.3 Verdicts

As referenced in Table 3 the outcome of the examined cases was that a majority ended in a guilty verdict for the defendant (64.15%). Case that are still ongoing accounted for (29.25%) and defendants were found innocent in only two instances (1.89%). Other outcomes included death before the trial (2.83%), a dropped case (0.94%), and not guilty by reason of insanity (0.94%).

Table 3. Verdicts of Examined Cases

Verdict	#	%
Guilty	68	64.15
Ongoing	31	29.25
Death Before Trial	3	2.83
Innocent	2	1.89
Dropped	1	0.94
Insanity	1	0.94

5.4 Type of Evidence

The conducted research found that the evidence in 104 of the 106 cases was inculpatory evidence, meaning that it was evidence which was incriminating of the defendant. Contrarily, only 2 of cases were found to have exculpatory evidence, which is evidence which aids in proving the innocence of a defendant.

5.5 Anti-forensics

Anti-forensic techniques used by defendants were noted in 7.55% of the examined cases. One instance of anti-forensics coming into play is with former U.S. Air Force Staff Sergeant Steven Carrillo [11]. Carrillo was a member of an extremist militia group known as the "Grizzly Scouts", which is associated with the extremist "Boogaloo" group. In 2020, during protests against police brutality, Carrillo, with other members of the Grizzly Scouts, performed a drive-by shooting in front of a federal courthouse which killed Federal Protective Service Officer David Patrick Underwood. The members of the group deleted previous conversations they had with one another on the messaging application Whatsapp. In addition to this, Dropbox files between the Grizzly Scouts were deleted.

5.6 Trends Within a Five Year Period

Device Trends. An analysis depicted in Table 4 demonstrates potential trends within DF as it relates to devices used. Two time periods, five years in length, were examined for growth or decay in the percentage of cases that contain the particular device. The cases that occurred in time period of 2012–2017 (n = 47)

had cell phones as the most frequently used device (65.96%). From 2018–2022 (n = 59) cell phone usage remained as the number one device used (67.80%). The difference in the two years shows growth of 1.84% in the number of cases that it was used in. Significant growth was seen in smart doorbells. In 2012–2017, smart doorbells were used in 2.13% of cases. In the next five years (2018–2022), it increased by 9.74% and was found to be included in 11.86% of murder cases.

Table 4. Devices Used in Murder Investigations Over Time

Device	2012–2017 (%)	2018–2022 (%)	+/− (%)
Cell Phone	65.96	67.80	1.84
Computer/Laptop	27.66	10.17	−17.49
CCTV	8.51	15.25	6.74
Car	6.38	10.17	3.79
Smart Doorbell	2.13	11.86	9.74
Smart Watch	4.26	6.78	2.52
GPS Device	1.89	0.94	−0.95
Smart Speaker	0.94	0.00	−0.94
Video Game Console	0.00	0.94	0.94
Smart Water Heater	0.94	0.00	−0.94

Artifact Trends. Table 5 examines trends of artifacts in real-world DF investigations. Similarly to Table 4, Table 5 examines two time periods of five years in length. The same time frame is used, 2012–2017 and 2018–2022. Location services and photo/video/audio artifacts had the same frequency in examined cases from 2012–2017 (29.79%). Location services increased by 17.67% for a total of appearing in 47.46% of examined cases. The photo/video/audio artifact category also increased by 7.50%. Both call logs and email decreased by 8.94% after both appearing in 10.64% of cases and then both dropping to 1.69%.

Table 5. Artifacts Used In Murder Investigations Over Time

Artifact	2012–2017 (%)	2018–2022 (%)	+/− (%)
Location Services	29.79	47.46	17.67
Photo/Video/Audio	29.79	37.29	7.50
SMS/iMessage	27.66	23.73	−3.93
Social Media	17.02	16.95	−0.07
Internet History	19.15	11.86	−7.28
Call Logs	10.64	1.69	−8.94
Email	10.64	1.69	−8.94
Car Statistics	4.26	5.08	0.83
Biometric Data	2.13	6.78	4.65
Device Activity	6.38	3.39	−2.99
IP Tracing	2.13	3.39	1.26
Messenger Applications	2.13	1.69	−0.43
Water Temperature	2.13	0.00	−2.13

6 Conclusions and Future Work

As digital devices continue to improve and become more available, the data that these devices produce will further assist in criminal investigations. Continuing to update methods, research, and education surrounding DF topics will help ensure that this ever-changing field remains filled with professionals who are confident in their abilities to efficiently and accurately extract and analyze digital evidence.

With cell phones being used in 68.63% of the cases that were examined, a call for action is required. This is a significantly high number and it is recommended that more resources are made available to best prepare investigators for mobile related forensics. Due to the portability and large ownership population of cell phones, evidence from location services is particularly of interest. Location services were found in 39.62% of the examined cases and 85.71% of location services were found in cell phones. Correlating the two together makes for a particularly strong piece of evidence that investigators should pursue.

Future work should explore repeating this study on five-year basis to explore how the data changes overtime. It would be also interesting to explore how the data changes from one country to another - outlining the needs for certain geographic locations to focus on specific artifact and device types.

According to our analysis of trends over the past ten years, it remains paramount that investigators are able to adapt to changing technologies around them. While cell phones are a large portion of digital evidence, being flexible enough to understand how to examine a smart doorbell or a Nintendo Switch can be just as critical to another case. A creative mind is a requirement in forensic work and the more fluid investigators are in their abilities, the more effective they will be as investigators.

References

1. About RCFL. https://www.rcfl.gov/about
2. Best practices for the retrieval of video evidence from digital CCTV systems. [electronic resource]. Technical Support Working Group (2006). https://www.hsdl.org/?view&did=747950
3. RCFL 2020 annual report (2020). https://www.rcfl.gov/file-repository/fy20-annual-report.pdf/view
4. Mobile fact sheet (2021). https://www.pewresearch.org/internet/fact-sheet/mobile/
5. Al Mutawa, N., Al Awadhi, I., Baggili, I., Marrington, A.: Forensic artifacts of Facebook's instant messaging service. In: 2011 International Conference for Internet Technology and Secured Transactions, pp. 771–776. IEEE (2011)
6. Al Mutawa, N., Baggili, I., Marrington, A.: Forensic analysis of social networking applications on mobile devices. Digit. Invest. **9**, S24–S33 (2012). https://doi.org/10.1016/j.diin.2012.05.007, https://www.sciencedirect.com/science/article/pii/S1742287612000321. The Proceedings of the Twelfth Annual DFRWS Conference
7. Alyahya, T., Kausar, F.: Snapchat analysis to discover digital forensic artifacts on android smartphone. Procedia Comput. Sci. **109**, 1035–1040 (2017). https://doi.org/10.1016/j.procs.2017.05.421, https://www.sciencedirect.com/science/article/pii/S1877050917311006. 8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology, SEIT 2017, 16–19 May 2017, Madeira, Portugal
8. Associated Press: 'fitbit' murder trial closing arguments heard in rockville court (2022). https://www.fox61.com/article/news/crime/dabate-fitbit-murder-trial-heads-to-closing-arguments/520-38434662-d531-41c0-a0c5-f28b7a23bb33
9. Baggili, I., Oduro, J., Anthony, K., Breitinger, F., McGee, G.: Watch what you wear: preliminary forensic analysis of smart watches. In: 2015 10th International Conference on Availability, Reliability and Security, pp. 303–311 (2015). https://doi.org/10.1109/ARES.2015.39
10. Balon, T., Herlopian, K., Baggili, I., Grajeda-Mendez, C.: Forensic artifact finder (ForensicAF): an approach & tool for leveraging crowd-sourced curated forensic artifacts. In: The 16th International Conference on Availability, Reliability and Security, pp. 1–10 (2021)
11. Bay City News: 'boogaloo' group members accused of deleting digital evidence related to law enforcement murders (2021). https://www.sfexaminer.com/news/boogaloo-group-members-accused-of-deleting-digital-evidence-related-to-law-enforcement-murders/
12. Becirovic, S., Mrdovic, S.: Manual IoT forensics of a Samsung gear S3 frontier smartwatch. In: 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–5 (2019). https://doi.org/10.23919/SOFTCOM.2019.8903845
13. Casey, P., Lindsay-Decusati, R., Baggili, I., Breitinger, F.: Inception: virtual space in memory space in real space-memory forensics of immersive virtual reality with the HTC vive. Digit. Investig. **29**, S13–S21 (2019)
14. Dorai, G., Houshmand, S., Baggili, I.: I know what you did last summer: your smart home internet of things and your iPhone forensically ratting you out. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018. Association for Computing Machinery, New York (2018). https://doi.org/10.1145/3230833.3232814

15. Dwyer, C.: Arkansas prosecutors drop murder case that hinged on evidence from amazon echo (2017). https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo
16. Garfinkel, S., Farrell, P., Roussev, V., Dinolt, G.: Bringing science to digital forensics with standardized forensic corpora. Digit. Invest. **6**, S2–S11 (2009)
17. Grajeda, C., Breitinger, F., Baggili, I.: Availability of datasets for digital forensics - and what is missing. Digit. Invest. **22**, S94–S105 (2017). https://doi.org/10.1016/j.diin.2017.06.004, https://www.sciencedirect.com/science/article/pii/S1742287617301913
18. Harichandran, V.S., Walnycky, D., Baggili, I., Breitinger, F.: CuFA: a more formal definition for digital forensic artifacts. Digit. Invest. **18**, S125–S137 (2016)
19. Hassenfeldt, C., Baig, S., Baggili, I., Zhang, X.: Map my murder: a digital forensic study of mobile health and fitness applications. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3339252.3340515
20. Kapoor, A., Raza Qureshi, S.: Forensic analysis of digital evidence extracted from amazon echo. In: 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI), pp. 1–7 (2020). https://doi.org/10.1109/ICATMRI51801.2020.9398391
21. Luciano, L., Baggili, I., Topor, M., Casey, P., Breitinger, F.: Digital forensics in the next five years. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018. Association for Computing Machinery, New York (2018). https://doi.org/10.1145/3230833.3232813
22. Kennelly, M.F.: United states v. benford (2020). https://casetext.com/case/united-states-v-benford-19
23. McCullough, S., Abudu, S., Onwubuariri, E., Baggili, I.: Another brick in the wall: an exploratory analysis of digital forensics programs in the united states. Forensic Sci. Int.: Digit. Invest. **37**, 301187 (2021)
24. Montasari, R., Hill, R.: Next-generation digital forensics: challenges and future paradigms. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), pp. 205–212 (2019). https://doi.org/10.1109/ICGS3.2019.8688020
25. Moore, J., Baggili, I., Breitinger, F.: Find me if you can: mobile GPS mapping applications forensic analysis & SNAVP the open source, modular, extensible parser. J. Digit. Forensics Secur. Law **12**, 15 (2017). https://doi.org/10.15394/jdfsl.2017.1414
26. Saleem, S., Baggili, I., Popov, O.: Quantifying relevance of mobile digital evidence as they relate to case types: a survey and a guide for best practices. J. Digit. Forensics Secur. Law **9** (2014). https://doi.org/10.15394/jdfsl.2014.1186
27. Steiner, D., Lei, C., Hayes, D., Le-Khac, N.A.: Vehicle communication within networks - investigation and analysis approach: a case study. In: Proceedings of the Conference on Digital Forensics, Security & Law, pp. 1–16 (2019)
28. Wells, A.: Ping the admissibility of cellular records to track criminal defendants. Saint Louis Univ. Public Law Rev. **33**(2) (2014)
29. Yarramreddy, A., Gromkowski, P., Baggili, I.: Forensic analysis of immersive virtual reality social applications: a primary account. In: 2018 IEEE Security and Privacy Workshops (SPW), pp. 186–196. IEEE (2018)