frontiers | Frontiers in Communications and Networks

TYPE Review
PUBLISHED 26 July 2023
DOI 10.3389/frcmn.2023.1212743

OPEN ACCESS

EDITED BY
Mueen Uddin,
Universiti Brunei Darussalam, Brunei

REVIEWED BY
Nawaf Almolhis,
Jazan University, Saudi Arabia
Mehran Mozaffari Kermani,
University of South Florida, United States

*CORRESPONDENCE
Farkhund Iqbal,
farkhund.iqbal@zu.ac.ue

RECEIVED 26 April 2023
ACCEPTED 14 July 2023
PUBLISHED 26 July 2023

CITATION
Iqbal F, Jaffri A, Khalid Z, MacDermott A, Ali QE and Hung PCK (2023), Forensic investigation of small-scale digital devices: a futuristic view.
Front. Comms. Net 4:1212743.
doi: 10.3389/frcmn.2023.1212743

Forensic investigation of small-scale digital devices: a futuristic view

Farkhund Iqbal[1]*, Aasia Jaffri[2], Zainab Khalid[3], Aine MacDermott[4], Qazi Ejaz Ali[5] and Patrick C. K. Hung[6]

[1]College of Technological Innovation, Zayed University, Dubai, United Arab Emirates, [2]Air University, Islamabad, Pakistan, [3]School of Electrical Engineering and Computer Science (SEECS), National University of Science and Technology (NUST), Islamabad, Pakistan, [4]Liverpool John Moores University, Liverpool, United Kingdom, [5]Department of Computer Science, University of Peshawar, Peshawar, Pakistan, [6]Ontario Tech University, Oshawa, ON, Canada

Small-scale digital devices like smartphones, smart toys, drones, gaming consoles, tablets, and other personal data assistants have now become ingrained constituents in our daily lives. These devices store massive amounts of data related to individual traits of users, their routine operations, medical histories, and financial information. At the same time, with continuously evolving technology, the diversity in operating systems, client storage localities, remote/cloud storages and backups, and encryption practices renders the forensic analysis task multi-faceted. This makes forensic investigators having to deal with an array of novel challenges. This study reviews the forensic frameworks and procedures used in investigating small-scale digital devices. While highlighting the challenges faced by digital forensics, we explore how cutting-edge technologies like Blockchain, Artificial Intelligence, Machine Learning, and Data Science may play a role in remedying concerns. The review aims to accumulate state-of-the-art and identify a futuristic approach for investigating SSDDs.

KEYWORDS

digital forensics, investigation, smartphone, drone, gaming console, IoT forensics

1 Introduction

With technological advancements resulting in a more compact hand-held device with respect to size yet offering more storage on the hard drive and memory, the Internet of Things (IoT) realm condenses to comprise a subset of Small-Scale Digital Devices (SSDDs) that are *nearly* fit-in-your-pocket. Personal Data Assistants (PDAs) such as smartphones, tablets, and smart wearables, along with smart toys, gaming consoles, digital cameras, and drones are some of the more common SSDDs (Figure 1). There are applications of IoT devices and SSDDs in everyday life including wearable technology, fitness, smart homes, health care, smart cities, agriculture, industrial automation, etc. that emphasize their impact. Nearly every member of society uses a variety of IoT/SSDDs in today's digital world. Worryingly, with these devices, practically anything can be connected to the Internet or another "thing"– which highlights the fact that in many instances, we are creating our problems with a wider attack surface and underlying security issues (MacDermott, 2019a). The accessibility of technology makes it easier for cybercriminals to utilize IoTs and SSDDs to covertly commit criminal activity. The *Mirai* malware targeted vulnerable IoT devices, such as those with default passwords and unsafe protocols turning them

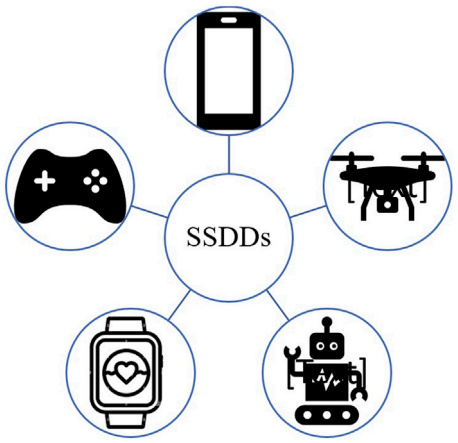

FIGURE 1
Small-scale digital devices.

into *a network of infected devices* (also known as a botnet) that was used to flood targeted services with traffic, making them unavailable to normal users (Buxton, 2022). SSDDs such as smartphones, for example, store a lot of user data including calls, texts, images, and address books that may be subject to similar criminal activities (Nelson et al. 2014). Users' personal information is constantly at risk of threats and security lapses in the digital environment.

The usage of cyberspace for conducting criminal activity has introduced *Digital Forensic (DF) investigation* as a mandatory part of conventional investigations. For SSDD Forensics (SSDDF), past events are reconstructed to extract potential evidence from the device. This process encompasses various forensic analysis categories, i.e., (1) the type of Operating System (OS), (2) memory, (3) network, (4) browser, and (5) any paired device's investigation. Each branch of forensic analysis facilitates investigators to identify criminal activity performed in cyberspace in a holistic manner, which helps piece together information (artifacts) to establish the *full picture* (Maria Jones and Godfrey Winster, 2018).

Useful artifacts concerning memory, OS, geo-location network activity, call logs, pictures, and videos can be extracted from IoT devices and SSDDs. In addition, browser history may store potential evidence. Memory artifacts, from slack and unallocated spaces, which preserve crucial information about running processes, are also the primary source of forensic artifacts. Digital devices are connected to the Internet by various means of communication, i.e., the wired network, Wi-Fi, Bluetooth Zigbee, ports, etc., and artifacts of forensic interest may be extracted from them.

The forensic processes in question pose challenges of various degrees. For example, finding the appropriate tool for forensic investigation is one of the major challenges because of diverse SSDDs. Such multifaceted issues stem from several variables such as different OSs, device models, and implemented security mechanisms that are constantly changing and evolving. In addition, jurisdictional issues present a unique barrier to forensic testing; only applicable laws are admissible in court. The entailing discussion elaborates on various other challenges in SSDD forensics and the use of cutting-edge technologies that may be utilized to annihilate them.

2 Small-scale digital devices

2.1 Smartphones

The smartphone is the most prevalent SSDD. With the world population currently amounting to 8 billion, approximately 6.84 billion smartphones exist, as of 2023 (Howarth, 2023). In addition, these smartphones connect to other IoT devices, which amounts to approximately 10.47 billion IoT connections in total. Smartphones store data inclusive of call logs, call records, SMS, MMS, chats, GPS information, voice recordings, calendars, address books, Web pages, browsing history, videos, music files, and financial data as well.

Some of the most dominant OSs in the smartphone marketplace include Android, iOS, Samsung, Windows, etc. Constant updates of OSs have resulted in a collection of versions that need individual study and research for apt forensic practices.

The prevalence also results in the most malicious attacks which emphasize the need for digital smartphone forensics as a top priority. It has been observed that criminals hide their footprints through data deletion or data hiding practices, generally known as *anti-forensic techniques*. Therefore, a forensic examiner must know the extraction, retrieval, analysis, interpretation, and presentation of both apparent and hidden artifacts.

2.2 Wearable technology

A rising technology trend is wearable technology, such as fitness bands with amazing functionalities. Users wear a variety of well-known fitness bands every day to monitor their activities such as sleeping, walking, and running, among others. Employers have recently started using them to monitor workers' productivity, resource utilization, etc.

These devices are developed with multiple applications and communication interfaces. Their OSs are diverse, including but not limited to WatchOS, Wear OS, Fitbit OS, Band, Pebble OS, Tizen, and Garmin (Loomis & Edward et al. 2019). Because such smart wearable devices are capable of being connected to smartphones, they are important evidence repositories from a forensics perspective as well. In addition, they are synchronized with the Internet and the cloud, making them the ideal source of evidence because they provide a wealth of personal information, biometrics, and other user data.

2.3 Gaming consoles

Recently, gaming consoles have also been connected to online offenses such as gambling, theft, fraud, kidnapping, and software violations. Therefore, it is essential to be able to thoroughly evaluate such devices while minimizing the risk of data corruption.

The eighth-generation Xbox One console was released in 2013. Microsoft introduced the Xbox One, which runs on a version of

Windows specifically made for it. The OS for Xbox One games, and any associated applications are separate. The OS is stored on the internal hard drive and has a backup in the internal console storage, so it may be restored in the event of corruption, or a factory reset. The Xbox One includes a central processing unit and 8 GB of DDR3 RAM, of which 3 GB is set aside for the OS and the remaining space is used by games and applications (Khanji et al. 2016).

The Sony-made PlayStation 4 (PS4) is an 8th-generation video game console with a lot of Internet features. The PS4 does accept FAT and exFAT formatted USB storage devices, but its internal hard drive utilizes a proprietary system structure. Using USB-attached devices, the PS4 enables users to view images, watch videos, and play music. Full hard drive encryption is a major challenge with the forensic analysis of PS4. Nintendo makes the Nintendo 3DS, a handheld, portable gaming system. In addition to the integrated NAND chip, the 3DS can save data on an external memory card.

2.4 Drones

Drones are widely used in the market for a range of applications, mostly to decrease manual labor and increase process efficiency in both commercial and non-commercial applications. Drone applications are special and can be used practically everywhere to conduct reconnaissance, gather data or resources, and deploy resources, with a variety of payloads. Major players in the consumer market including 3D Robotics, Parrot, and DJI are constantly updating their Unmanned Aerial Vehicles (UAV) product lines with new features, better performance and energy efficiency, smaller size, lighter weight, and greater usability. Drone forensics, anti-drone technologies, and more restrictions are required because of the rise in occurrences and unlawful use of drones.

2.5 Smart toys

Smart or internet-connected toys now come in a variety of sizes and designs with Wi-Fi, Bluetooth, microphones, cameras, and GPS tracking capabilities. They also contain microprocessors, microcontrollers, non-volatile memories, input-output devices, and storage devices (Hosani et al. 2020). For executing digital forensic tasks, such as the recovery of deleted records in the hard drive, memory, etc., conventional investigation skills with the proper understanding of the most recent methodology and instruments are very important. Smart Connected Toys (SCTs) make it more challenging to examine digital evidence and locate the evidence's difficult-to-remove digital footprint. In a normal SCT crime case, there is no way to charge suspects if the investigator is unable to present strong evidence against the culprit (Yankson et al. 2020). To establish the facts essential to prove a person's guilt or innocence in a court of law, it is important to be able to extract evidence. By the use of Bluetooth, Wi-Fi, the cloud, and mobile apps, connected toys link events, and data. They frequently have cameras and microphones for gathering audio and video information. Future iterations of smart toys might have Artificial Intelligence (AI)-enhanced facial recognition technologies. With those links, information is gathered, saved, and shared that feeds the toys; yet there are numerous security concerns, reports stating that up to 98% of IoT traffic is not encrypted.

3 SSDD forensics

The primary research problem for forensic investigators is rooted in the scale of the devices of forensic interest, relevance, and hazy/edgeless network boundaries (Perumal et al., 2015). The authorization, planning, and securing of a warrant should be the first step in almost every digital forensic investigation model. The proposed model's base device identification would refer to machine-to-machine (M2M) communication or device-to-device communication. Any of these M2M communication channels, including Z-Wave, 4G, 3G, LTE, Wi-Fi, Ethernet, and Power Line Communication (PLC), could be used. Investigators must exercise caution during the triage examination because fragile data are crucial to IoT and SSDD forensics. Routers, gateways, cloud platforms, and fog platforms are the most prevalent devices or platforms that need to be supported.

Another gap, in addition to physical inaccessibility, is the collection of evidence from cloud storage and data centers. Since the data may be stored in different locations/nations, the issue of multiple jurisdictions must also be taken into consideration (Zulkipli et al. 2017). Also, to enable the correlation of incidents across various log sources, it is crucial to guarantee that prospective forensic data sources are time-stamped. All of the devices' time must be synchronized and securely managed. The use of cryptographic time stamping and NTP synchronization may ensure timestamps while also protecting the timestamps.

With various data formats, protocols, and physical interfaces involved; the evidence extraction procedure may be more difficult than conventional computing (Miorandi et al., 2012). Sometimes the evidence is partially kept on the cloud services or other devices connected to the same network. To obtain or extract data, the investigator must consider looking at the greater dimension or several alternatives to data storage.

Digital evidence is extremely fragile and is easily altered, removed, or tampered with. There is a danger of gadgets remotely shutting down or evidence being overwritten. As an option to deal with this issue, the majority of devices save their data in the cloud. In comparison to traditional computing, the problems with evidence volatility in the IoT environment are far more complicated. On the IoT, data may be stored locally, where its lifespan is constrained before it is compressed or rewritten.

The amount of data acquired depends on the acquisition method employed (logical vs. physical); it is more difficult to get data from a smartphone (or any other SSDD) than from a typical hard disk (Al Hosani et al. 2020). To ensure that SSDDs are not connected remotely and to avoid device tracking and remote data wiping, it is required to carry the SSDDs in *Faraday bags* when they are on. From the time of the seizure, until it is presented as evidence in court, it is required to prevent digital evidence from being tampered with.

The logical acquisition provides context information such as date-timestamps and location within the target device's file system

and gets a copy of entities such as files and directories that reside in the logical storage means (Casey, 2011). It primarily relates to data that has not been destroyed/deleted and is done by accessing the device's file system (Hoog, 2011). The likelihood of acquiring deleted data is decreased, as unallocated spaces cannot be accessed using this method.

Physical acquisition methods access lower locations. Acquiring physical storage calls for immediate access to the flash memory of the gadget. Using this technique, the forensic examiner can access all of the data on the device in the form of a *bit-by-bit copy,* even deleted files and unallocated space.

The *Joint Test Action Group (JTAG)* extraction technique retrieves data from physical components such as the processor, flash memory, or other devices (Breeuwsma, 2006). The JTAG-compliant component provides memory addresses, and the JTAG testing unit accepts responsibility for storage and rendition. For extracting and analyzing binary pictures using JTAG, proper training is necessary.

In the *chip-off technique*, the flash memory chip must be physically removed to collect data at the binary level. Examiners can produce a binary image of the removed chip; the same as hard disc imaging.

Micro read is used even when data has been rewritten on magnetic media; this technique uses an electron microscope to examine logic gates. However, because of its high cost, it is normally exclusively employed in situations requiring national security. The data can be synchronized across several devices and criminals might remotely delete or alter the data. data preservation in forensics is difficult and poses a challenge as well (Al Hosani et al. 2020).

Access to system locations that were secured by default by each OS manufacturer is made possible through low-level modifications. Various OSs have differences in the privileges users receive after applying a low-level modification. Low-level modifications can go by many different names like jailbreak (iOS), root access (Android, Windows Mobile), or capability hacked (Symbian) depending on the OS they are using. Following the seizure of a specific device from the chosen area and the extraction of necessary data, the process resumes with standard steps for conducting digital forensic analysis, such as chain of custody, lab analysis, results, reporting, and archive and storage. These steps must be in line with the current state-of-the-art/standard methodologies and frameworks for conducting digital forensics.

3.1 Frameworks, methodologies and techniques in SSDD forensics

Kebande et al. (2020) proposed an IoT framework based on ISO/IEC 27043. IoT System Architecture is defined by ISO/IEC 27043 as "*the endpoints, network, software, and data that make up an organization's information system*". It is crucial to recognize the data cycle inside an organization to include the data components in the IoT system design for ready procedures. To process and save valuable DF data, it is advised that it be sent to an IoT gateway or an external DF database since IoT devices store less data, due to limited memory.

Various approaches for conducting an IoT forensic investigation were presented by Zulkipli et al. (2017) who suggested complying with the inherent IoT characteristics. These approaches emphasize the pre-investigation stage and use the real-time (live) investigation to make sure that data and potential evidence are gathered and preserved throughout the investigation. The availability of more affordable devices has sparked a new discussion about the diversity of OSs and applications.

Al-Sharrah et al. (2018) developed a framework for conducting smartwatch forensics based on the physical backup, and wireless communication stages of examination. They applied the suggested framework to analyze an Apple watch. It was discovered that the watch retains a great deal of personal data, including contact information, text message content, calendar information, emails, photographs, and wallet data, which may include payment card information, access codes, and event tickets, if any. Smartwatches are designed to be worn on the wrist, which means that they are constantly in motion. This can result in sensor data that is noisy or inaccurate, making it harder to interpret.

A study by Dermott et al. (2019b) analyzed three fitness trackers: a Generic low-cost HETP fitness tracker, a Fitbit Charge HR, and Garmin Forerunner 110. Potential evidence could be viewed on the screen of the Garmin Forerunner 110 device without a password or pin. You can examine the user profile, device settings, and any actions saved to the device by merely browsing through the device choices. The information on the Fitbit and HETP devices was minimal, and the step, floor, and other counters reset to zero each night at 0:00 on both of the devices. Even when the files of interest were located, viewing them in FTK Toolkit or Autopsy was difficult due to the data's file types. Viewing and analyzing the gathered evidence required the use of both the GoldenCheetah and the FitSDK packages. These software programs helped evaluate the data validity and correctness of prospective evidence. A combination of tools can be used to interpret or extract artifacts of interest.

Hutchinson et al. (2022) performed a forensic analysis of the controlling applications for three well-known fitness bands and smartwatches (Amazon Halo, Garmin Connect, and Mobvoi) to give forensic investigators a road map of forensically relevant data that are stored within these applications and draw attention to any privacy concerns that the stored data within these applications may present to the applications' users. They obtained a complete forensic picture of a rooted A50 smartphone using a Cellebrite UFED 4PC, giving a copy of the device bit-by-bit. AXIOM can be used to analyze artifacts in a variety of ways, the *File system View* or an *Artifacts View*. While the analysis phase entails searching through all recovered artifacts from the selected apps under investigation to establish what data are recoverable and their locations in the Android file system, the examination phase merely entails filtering any apps and date ranges. The user's profile information, daily, weekly, and monthly activity and health statistics, and even the outcomes of the user's tone analysis sessions were all included in the vast artifacts from the Amazon Halo app. The fact that the voice recordings utilized for the tone analysis could not be recovered, even though those used for enrollment (the construction of voice profiles) could, is significant. The Connect and Mobvoi apps' user profiles and health-related information were both restored. Regarding GPS information, even while the Connect app does save the user's precise GPS coordinates when on a walk, there is still a way to determine the

user's approximate location by using the app's weather notifications. The location of a Mobvoi app user can be discovered from the app's retrieved phone number. In a forensic inquiry, where all other conventional methods of determining the user's geo-location are ineffective, such artifacts would be essential (Hutchinson et al. 2022).

Alabdulsalam et al. (2018) conducted a forensic investigation of a smartwatch in which the forensic artifacts were retrieved through logical and physical extractions. A concealed diagnostic port is present on the Apple Watch Series 2. As a result, an Apple iPhone and an Apple Watch were synchronized, and Cellebrite UFED was utilized to carry out a logical acquisition that recovered pertinent information from the iPhone. A manual acquisition was also carried out by swiping the Apple Watch to examine and capture the data displayed on the screen. The artifacts of interest included GPS information, heart rate information, timestamps, MAC addresses, information about linked devices, text and email messages, phone logs, and contacts. The logical data collection approach entails obtaining user data with the aid of specialized tools and retrieving active data by connecting the wearables to a forensic workstation via interfaces like cable or wireless connections. In the case of wearable technology, the Software Development Kit (SDK) must be installed because it offers manufacturer-level access to the device's hardware and software, which is necessary for forensic investigation. To collect physical data, it is necessary to create a bit-by-bit clone of all the data stored on the wearable device, including any hidden or deleted files. Physical data collection involves either removing cards from the mobile device or copying the entire file system to extract data, regardless of whether it is unallocated or allocated to a file system.

A technique proposed by Pessolano et al. (2019) to extract and decode the data from the 3DS's NAND memory chip was used by Nintendo as part of a forensic analysis investigation. Important information can be accessed here, including plaintext user credentials, deleted photos, contacts and friends' information, internet history, and serial numbers.

A study was conducted by Khanji et al. (2016) in which Xbox One and PS 4 gaming consoles' hard drives were taken out to obtain a hard disk image. To avoid any alteration with the original hard drive during the acquisition procedure, an ATA serial was utilized in conjunction with a Tableau SATA bridge, which serves as *a write blocker*. The FTK Imager was successfully used to physically acquire and validate both images (in raw format). Images were then taken before and after resetting both video game systems to their factory default settings. The analysis phase was carried out by using three forensic tools, FTK Imager, X-ways, and Autopsy. X-ways easily traced user accounts and games played but were unable to explore file system and disk images. It was observed that using Autopsy instead of X-Ways was more effective because it enabled keyword searches to be done over the entire disk image. In addition to the identification of usernames and gameplay, it also explores file systems for disk images. AccessData despite not providing any parsing tools for the study of either disk, FTK 5.5 detected the file-system partitions of each video game console. FTK discovered that the PS4 image contained unallocated space in addition to 15 partitions. Internally, the Microsoft Xbox One's system architecture is comparable to that of Windows-based computers. Due to this, it is easier to analyze than the PS4 using modern forensic techniques. We may also reveal artifacts from unallocated space as well. The evidence on both game console images can only be partially parsed and carved with the use of forensic equipment. As a result, a *live analysis* might be the most useful technique for the forensic examination of current gaming consoles. Utilizing this strategy requires careful thought to minimize evidence contamination and modification (Al Hosani et al. 2020). As long as the adjustments are minor, well-documented, and repeatable, the evidence is still considered admissible in a court of law. The PlayStation 4's hard drive cannot be identified by forensic tools, and as a result, no relevant data could be recovered. However, it was discovered that with current forensic techniques, Xbox One was a little bit easier to probe.

Zhang & Gao et al. (2019) analyzed the Xbox One; a brand-new game console's hard drive was taken out and forensically imaged using a *write-blocker*. Because it was known that Xbox One could be used in an online setting, network traffic analysis was done. It was revealed in partition and file analysis that the Xbox One runs on a unique OS. Additionally, the files in each disk appear to be encrypted and challenging to decrypt. In a study, a physical examination of the hard disk to find the important file timestamp information, and a logical study via the graphical user interface was used in this research of the Xbox One. A write-protected Xbox One could be logically analyzed by a digital forensics expert using the proposed analysis recommendations. They may also obtain the valuable NTFS file timestamp from the Xbox One hard disk. The original evidence source is protected from information alteration, maintaining the integrity of the evidence. However, the time of the incident and the date of the investigation has a direct impact on the amount of data that may be recovered (Al-Haj et al. 2019). Connection capabilities of SmartGlass on a smartphone app and tablets with gaming consoles can be explored for retrieval of forensic artifacts.

A Nintendo Switch game system was examined forensically by Berg & Lagerholm et al., 2020. It can hold useful information about how the console is used both at home and elsewhere because it is both a portable and stationary device. Data extraction techniques included recording network traffic, utilizing an exploit to access storage memory, and removing the contents of the SD card.

The process of gathering drone data for the first phase starts with the seizure, imaging, or collecting of digital evidence to record questionable media, network activity, and logs. The intended digital evidence consists of ownership information, flight data, and EXIF information found in recorded media files saved on the drone. A forensic image of the original media evidence is made and verified when digital media are gathered. The French business Parrot SA produces the remote-controlled quadcopter known as the Parrot AR. Drone 2.0. Typically, the drone's wireless router, which includes a wireless 802.11 chipset, is used to create the connection. Smartphones and tablets running the IOS (Freelight application) or Android (AR.Freelight) OSs can be used to control the Parrot AR. This complicates the forensic procedure because the coupled devices must be examined for the examination of the data retrieved. The Parrot AR and the smartphone pair with each other automatically after communication has been established between the two devices**.** Establishing Flight Path Data, accessing the media files taken by the device, identifying the controller's ID, and establishing ownership, during the forensic investigation phase, it is required to look at the Wi-Fi connection details between the drone

TABLE 1 Forensic frameworks comparison.

Research paper	Framework	Comparative analysis		
		Holistic	Comprehensive artifacts extraction	Standardized
Holistic digital forensic readiness framework for IoT-enabled organizations (Kebande et al., 2020)	An IoT framework based on ISO/IEC 27043; the authors adopt a holistic approach to cover the challenge of heterogeneity of various types of forensic artifacts extractable from an array of sources in an organizational structure; also performing a qualitative analysis of their framework.	✓	✓	✓
Watch your smartwatch (Al-Sharrah et al., 2018)	A framework for conducting smartwatch forensics based on the physical backup, and wireless communication stages of examination.	✓	✓	✗
Forensic analysis of the nintendo 3ds nand (Pessolano et al. 2019)	A technique to extract and decode the data from the 3DS's NAND memory chip.	✗	✓	✗
IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things (Zulkipli et al. 2017)	Various approaches comply with the inherent IoT characteristics, emphasizing the pre-investigation stage and using live investigation to make sure data and potential evidence are gathered and preserved throughout the investigation.	✗	✗	✗

and controller, the geo-location data from the drone, the storage, the camera, and all other drone-related places where data is handled. The set of forensic instruments chosen for the inquiry must be used for this analysis. By adding a GPS tracker to all of these devices, the use of drones may be tracked. The investigators could retrieve flight information and inspect usage. Law enforcement officials and digital forensic analysts investigating drone usage face a variety of challenges as these devices continue to show the potential for use in nefarious activities.

In the process of obtaining evidence from smart toys, the investigator extracts the data and makes a copy of the original data for storage. To ensure the integrity of the evidence at this stage of the investigation, the investigator verifies that both the original copy and duplicate copy have been hashed and that the value is the same. Pro Discover forensic tool can be used for logical data acquisition by connecting the device directly with the network in the absence of the physical interface to connect SCT, but unfortunately due to restriction, other approaches were applied, i.e., memory chip reading having SCT firmware. The logical acquisition method could not view deleted files or unallocated space. Live memory analysis involves capturing and analyzing the contents of a device's memory while it is still running. This technique can be used to capture encryption keys or to analyze the data stored in the memory. The Investigator uses several forensic analytical methods and techniques on the extracted electronically stored information to determine feature analysis. Both the SCT features and the copy of the extracted and stored information are subject to forensic investigation and procedures by the investigator. Privacy and security ought to be built into every system. A connected smart toy is a component of a vast, intricate matrix since the IoT is not a stand-alone system. System design should be a process that considers security and privacy from all angles, from the user-facing front end through the data lifecycle via the system's back end. The SCT OS functions and the high-level information obtained are still the subjects of forensic analysis and processing procedures being used by the Investigator. The examination produces data from SCT OS functions, high-level information obtained, storage file type & data analysis, and SCT feature analysis, and stores all the information at the "OS and functionality, file, type, data classification" stage of the framework. Artifacts that were obtained user information, email address, location, and media files (image, video, music, other audio files). Signal strength can be used by a malicious opponent to identify the potential residence where the SSDD is located.

Table 1 details a comparative analysis of the forensic frameworks discussed.

3.2 Popular tools in SSDD forensics

Artifact retrieval from devices is possible with forensics toolkits. These forensic toolkits are mostly used to collect data from devices and to provide detailed reports on the acquired data. While the majority of tools were designed and developed for smartphones, most function with other SSDDs efficiently as well. However, it is pertinent to highlight the need for more specialized tools and utilities for each SSDD. Table 2 details the most prevalent forensic tools.

4 Challenges in SSDD forensics

The pace of technological advancements in SSDDs is so rapid that forensic investigators must constantly update their knowledge and techniques to keep up with new devices, OSs, and data storage technologies.

Perpetrators of crimes are becoming more sophisticated in their attempts to thwart digital forensics. This includes the use of *anti-forensic techniques to hide or destroy evidence*, such as wiping the device or using encryption to make the data unreadable. Man-in-the-middle (MITM) and other attacks pose a significant challenge in forensic inquiries of SSDD and IoT devices. These attacks can bypass encryption, alter data, and hide the attacker's presence on the network. As such, it is essential to take steps to prevent MITM

TABLE 2 Prevalent forensic tools.

Tools	Details
XRY Forensic Examiner's Kit[a]	A mobile forensics tool that supports over 32,000 device profiles and over 4,200 app profiles. It can extract data from physical and logical acquisitions and supports advanced analysis of deleted data.
Oxygen Forensic Detective[b]	A popular mobile forensic tool that supports over 28,000 mobile devices and over 500 apps. It can extract data from various sources, including device backups, cloud storage, and SIM cards.
Cellebrite's Universal Forensic Extraction Device (UFED)[c]	A popular tool used by law enforcement agencies and digital forensics investigators. It supports a wide range of devices and OSs and can perform both physical and logical acquisitions.
Elcomsoft Phone Breaked[d]	Used for the extraction of data from device storage, cloud backup, and password-protected devices.
Magnet AXIOM[e]	Used for mobile devices and can extract data from devices and cloud storage, and has advanced features for analyzing chat messages and social media data.

[a]https://www.msab.com/product/xry-extract/.
[b]https://oxygenforensics.com/en/.
[c]https://www.cellebrite.com/en/products/ufed-ultimate/.
[d]https://www.elcomsoft.com/eppb.html.
[e]https://www.magnetforensics.com/products/magnet-axiom/.

attacks, such as using strong encryption, ensuring data integrity, and implementing robust network security measures.

General Data Protection Regulation (GDPR) is another challenging part of forensic investigations where restrictions are made in the extraction of data due to user privacy laws. Data that is necessary for the forensic investigation is collected only. Collecting unnecessary data can be considered a violation of GDPR. Compliance with GDPR is essential when conducting IoT forensics. The best approach is to ensure that all GDPR requirements are met and that personal data is collected, processed, and protected in compliance with the regulations.

SSDDs often have *limited storage capacity*, which means that data can be easily overwritten or fragmented, both in memory and secondary storage (file system). As a result, forensic investigators may need to resort to live forensics, use specialized tools and techniques to recover data and reassemble it into a meaningful format.

SSDDs are often protected by *encryption* and passwords that can prevent forensic investigators from accessing their data. This is particularly challenging when encryption or password protection is implemented at the hardware level. In cases where encryption is particularly complex, investigators must possess the required knowledge and skills to access the encrypted data and/or work with cryptography experts to assist with the decryption process. Cryptography experts can provide insights into the encryption method used and advise on the appropriate tools and techniques to use.

With the increasing use of *cloud storage and remote backup services*, SSDDs often do not store all their data on the device itself. This can make it difficult for forensic investigators to access all the relevant data and metadata.

Digital forensics investigators must be careful to respect the privacy of the device owner and comply with legal requirements, such as obtaining the necessary warrants and following proper chain of custody procedures.

4.1 Device-specific challenges and future prospects in SSDDF

It is challenging for the forensic examiner to stay up to date on forensic procedures that are compatible with the diversity of smartphones that are available instantly in the market. Another challenge is that one tool might not support all devices and OSs, and multiple tools may be needed to access all data on one device. Also, the growth in introducing new smartphones and accessories per day is higher than the development and release of new forensic acquisition tools. In addition, one of the critical issues relates to type 2 smartphone hypervisors which are being developed and will make forensic investigations much more difficult (Tamma and Ahamad, 2018). A standardized forensic procedure may be developed that can be used across different smartphone devices, OSs, and proprietary software. This can help to ensure consistency in approach, making it easier to manage the challenges associated with device diversity and OS differences. Industry tools may be used as designed to work with different devices, software, and OSs. Machine learning approaches can be used to conduct smartphone forensics processes easier with the help of pattern recognition, abnormal behavior detection, and deep learning algorithms.

With a market share of approximately 75% in wearable technology, Android is the most popular OS in comparison to Apple Watch which is pricey and runs iOS. An iPhone is always required to be paired with an Apple Content from the linked iPhone is continuously backed up to the Apple Watch. The iTunes backup contains the Apple Watch data that has been synchronized (Dorai et al. 2020). Because of Apple's security policy, sensitive data, such as data from health apps, does not appear in the iOS backup. Apple wearables implement restricted passcode attempts; if many unsuccessful attempts are found, the gadget instantly enters factory-reset mode and deletes all previous user data.

The challenge of interpretability is higher in smartwatches as they may interact with other devices such as smartphones or cloud services and make it difficult for forensics examiners to trace the origin of information or flow of the data. Augmented Reality (AR) technology has the potential to improve the usability and clarity of data visualization for fitness band users. This might make it simpler for forensic investigators to identify patterns and trends in the data. AI could help identify anomalies and patterns gathered from fitness bands' evidence. Future fitness bands might have remote access to the information the device collects. This could make it possible for

forensic investigators to get a suspect's fitness band data even if they do not have physical access to it. Maintaining the integrity of the evidence is the most difficult aspect of forensic investigation. This can be done using blockchain technology, where each data block is tamper-free. Biometric authentication features, like fingerprint or facial recognition, could be added to fitness bands in the future. This might simplify connecting a particular individual to the fitness band's data collection.

Drones may hit objects or crash into them, inflicting harm to their internal parts. This can make it challenging to study the drone's flying characteristics or to extract data from the internal storage of the drone. Some drones encrypt data to keep it safe, which might make it challenging for forensic analysts to obtain the data. Evaluating the drone's flight patterns or pinpointing its location at a specific moment due to encryption is often difficult. Drones may have a little amount of data storage, which might make gathering all of the necessary data challenging. It may also be a problem in identifying the drone's operator or ascertaining the drone's flight route as a result. It could be difficult to identify the operator's location if the drone is controlled via an encrypted connection. Without the individual's knowledge or consent, drones may be used to take pictures and videos of people. As a result, forensic analysts must be careful to manage any data they obtain in a way that respects the privacy of the people who are involved. In some cases where a device does record flight data, practitioners must consider the possibility that this information could be stored on either the controller or the UAV, emphasizing the importance of a comprehensive inspection of both. A standard must be developed for the forensic analysis of drones, in connection with manufacturers, law enforcement agencies, and privacy advocates. This will assist forensic examiners to provide guidelines and procedures for conducting a forensically sound investigation. There is an urgent need for specific training to study drone variants manufacture to manufacture and development of tools to address the tailored techniques, for the execution of the state-of-the-art forensic process. Regulations governing the use of drones can help address privacy concerns and provide guidelines for how forensic analyses should be conducted. Emerging technologies, such as AI and Machine Learning (ML), may offer new tools for analyzing drone-related incidents. These technologies can help automate certain aspects of forensic analysis and improve the accuracy of results.

Most of the time, smart toy manufacturer websites lack a clear privacy policy and are careless about protecting the personal information they acquire from children. Default passwords and lack of access controls along with limited memory increased the attack surface and enhance the forensic difficulties. A defense-in-depth strategy for security works well with the IoT concept. Furthermore, just because something is a toy does not justify putting security last. Smart toys present unique forensic challenges, including data collection, encryption, remote access, firmware updates, lack of standards, and ethical concerns (Infosec Resources, 2021). Digital forensic professionals must stay up-to-date with emerging technologies and be prepared to handle the challenges that arise from smart toys. It is crucial to ensure that privacy and data protection laws are respected while also considering the needs of criminal investigations. Network traffic analysis involves capturing and analyzing the data that is transmitted between the smart toy and other devices on the network. This technique can be used to identify the types of data being transmitted and determine who is accessing the smart toy. The use of AI and ML can help detect anomalies and identify potential security threats in smart connected toys. AI and ML can help identify patterns of behavior that may indicate a security breach and provide alerts to help prevent further damage. Smart-connected toys should undergo regular security audits to identify potential vulnerabilities and ensure that security measures are up to date. This can include penetration testing and code reviews to identify any security flaws that may be present. One way to counter the forensic challenges of smart connected toys is to implement strong encryption. Encryption can help protect sensitive data by converting it into code that is unreadable without a decryption key. By encrypting data both in transit and at rest, smart connected toys can help safeguard personal information.

4.2 The role of cutting-edge technologies in alleviating challenges

SSDDF presents a constantly evolving set of challenges that require digital forensic investigators to be well-trained, flexible, and adaptive to new technologies and techniques. It is important to have a comprehensive *incident response plan* in place to detect and respond to any potential attacks.

Additionally, AI enable forensic investigators to extract digital evidence related to a wide variety of computer crimes, including malware, spyware, hacking, data theft, identity theft, etc. by integrating algorithms with computational methods (Al-Fahdi et al. 2016). AI may prove beneficial in many ways when it comes to digital forensics (Franke & Srihari, 2008):

- Tracing evidence in a more targeted and detailed manner
- Identification of critical artifacts and also perform further objective analysis
- Assessing forensic investigation methods' quality, effectiveness, and standardization
- Search and identification of important trends from large volumes of data, and their visualization
- Assisting in the correlation of results revealing trends and patterns previously unknown.

The vast amounts of data collected from digital devices are frequently too complex for people to analyze, hence **ML** technologies must be used for thorough analysis (Rath et al. 2023). By using frameworks, statistical tools, techniques, and models for the study and recognition of patterns in input data, ML refers to the use of algorithms that can recognize, learn, analyze, and adapt. These methods frequently produce excellent results that are on par with human intelligence. In particular, ML may aid in:

- Search and seizure: The deployment of autonomous robots necessitates the employment of ML to carry out some fundamental human-like activities, such as object detection and other computer vision functions, navigation in uncharted territory, etc.
- Evidence retrieval and analysis: Data recovery, gunshot wound identification, facial recognition, suspect identification, and evidence detection from crime scene photos are all tasks that can be accomplished using machine learning (ML) throughout the evidence retrieval and analysis process.

- Documentation: By assisting law enforcement officials in creating reports from data pieces, ML tools and approaches can aid in the reporting process. Additionally, it can be utilized for text-to-speech functions (using a method called natural language processing).
- Link analysis: Link analysis can make use of a variety of deep learning techniques, which may need to be modified to handle various data sources including textual strings, time-series data, photos, audio files, etc.
- Fraud detection: Because they can be used to look into financial transactions and analyze data points related to them, ML algorithms can be very helpful in detecting fraud.

Similarly, blockchain-based frameworks, from the primary review by Akinbi et al. (2022), provide a proof-of-concept use of blockchain in preserving the provenance, integrity, and secure chain of custody of evidentiary SSDD forensic data. Overall, the solutions put forth in each framework do not alter the current forensic investigation procedure but rather make use of the benefits of blockchain technology to guarantee the integrity, security, and immutability of the evidence gathered and stored during the investigation process. However, considerations like privacy, performance, computational cost, energy consumption, practical implementation, and overall effectiveness influence the choice of blockchain technology and platform.

According to Al-Khateeb et al. (2019), systems based on blockchains could bring about an automatic implementation where all activities are logged as part of a growing list of records (blocks). Along with a timestamp, each block includes a cryptographic hash of the one before it. Systems will therefore be forensically capable by design. The steps of identification and preservation both focus on the media that will be recorded. Regardless of whether it is network traffic, volatile memory, physical storage, or other types of electronic data, the medium in this situation may include an artifact of interest.

The introduction of blockchain aids the forensics process in various ways (Al-Khateeb et al. 2019):

- Data availability: Records can be duplicated and kept in multiple locations, and when necessary, their integrity can always be independently validated using the blockchain.
- Continuous fraud detection and forensic readiness: The blockchain enables systems to be forensically ready, automates procedures, and reduces the danger of deletion by having many copies of the blockchain spread over different remote sites.
- Efficiency: The investigators will not need to spend much time maintaining the integrity of the data.
- Reliability: Because records have already been hashed as part of a reliable automated procedure that creates a chain of blocks, the inquiry will not be at risk due to incorrect hash calculations. Hashes are typically calculated multiple times when the crime scene is examined.

5 Conclusion

This review paper examined significant research to assess the best methods applied in SSDD forensic investigations. Devices inclusive of smartphones, smart wearables, gaming consoles, smart connected toys, and drones are covered. Each device presents unique challenges for forensic investigators. It is observed that SSDD and IoT forensics are somewhat challenging due to their specific characteristics, including heterogeneity, scalability, diversified ranges of devices, limited storage, and cloud services. NIST SP 800-86 guidelines[6] are widely used for performing forensic analysis of digital devices with slight differences due to device and OS diversity. To create automated tools that can be useful in obtaining forensic soundness in digital investigations, it is necessary to use emerging technologies like Machine Learning, Deep Learning, Artificial Intelligence, Blockchain, and Augmented Reality. It would be interesting to extend the scope and review forensics' state-of-the-art of large-scale digital devices that include broader IoT and cover the practices followed and challenges encountered in those cases.

Author contributions

FI Main exploration, research, and data collection AJ and ZK. Literature review and state-of-the-art AM. Idea and problem statement QA and PH Proofreading, structure, and formatting. All authors contributed to the article and approved the submitted version.

Acknowledgments

This research study is supported by Research Incentive Funds (R21096 and R21111) and Provost Fellowship Research Award (R20093), Zayed University, United Arab Emirates.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Akinbi, A., MacDermott, Á., and Ismael, A. M. (2022). A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. *Forensic Sci. Int. Digital Investigation* 42-43, 301470. doi:10.1016/j.fsidi.2022.301470

Alabdulsalam, S., Schaefer, K., Kechadi, T., and Le-Khac, N.-A. (2018). "Internet of things forensics – challenges and a case study," in *Advances in Digital Forensics XIV*, 35–48. doi:10.1007/978-3-319-99277-8_3

Al Fahdi, M., Clarke, N. L., Li, F., and Furnell, S. M. (2016). A suspect-oriented intelligent and automated computer forensic analysis. *Digit. Investig.* 18, 65–76. doi:10.1016/j.diin.2016.08.001

Al-Haj, A. (2019). Forensics analysis of Xbox one game console. Available at: https://arxiv.org/ftp/arxiv/papers/1904/1904.00734.pdf ([online].

Al-Khateeb, H., Epiphaniou, G., and Daly, H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. *Blockchain Clin. Trial*, 149–168. [online]. doi:10.1007/978-3-030-11289-9_7

Al-Sharrah, M., Salman, A., and Ahmad, I. (2018). "Watch your smartwatch,", Kuwait, Kuwait, 11-13 March 2018 (IEEE), 1–5.

Breeuwsma, I. M. F. (2006). Forensic imaging of embedded systems using JTAG (boundary-scan). *Digit. Investig.* 3, 32–42. [online]. doi:10.1016/j.diin.2006.01.003

Buxton, O. (2022). What is the mirai botnet? Available at: https://www.avast.com/c-mirai ([online].

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Google Books, Academic Press. [online]. Available at: https://books.google.com.pk/books?hl=en&lr=&id=lUnMz_WDJ8AC&oi=fnd&pg=PP1&dq=casey+2011&ots=aLw9JcGQT9&sig=FRqZKwrR9dCNN3StcBTW1ioEoaw&redir_esc=y#v=onepage&q=casey%202011&f=false (Accessed July 20, 2023).

Dorai, G., Houshmand, S., and Aggarwal, S. (2020). *Data extraction and forensic analysis for smartphone paired wearables and IoT devices*. Hawai: University of Hawai.

Franke, K., and Srihari, S. N. (2008). Computational forensics: An overview. *Comput. Forensics*, 1–10. doi:10.1007/978-3-540-85303-9_1

Hoog, A. (2011). Android forensics: Investigation, analysis and mobile security for google android. Google Books. Elsevier. [online]. Available at: https://books.google.com.pk/books?hl=en&lr=&id=i-yWIVd4z7MC&oi=fnd&pg=PP1&dq=hoog+2011&ots=L_A76GzBSm&sig=7ujaxOM1bLq0-sY57yA8VX5T3CU&redir_esc=y#v=onepage&q=hoog%202011&f=false (Accessed July 20, 2023).

Hosani, H. A., Yousef, M., Shouq, S. A., and Iqbal, F. (2020). "State of the art in digital forensics for small scale digital devices," in 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, April 7-9 2020.

Howarth, J. (2023). How many people own smartphones? 80+ smartphone stats [online] exploding topics. Available at: https://explodingtopics.com/blog/smartphone-stats.

Hutchinson, S, Mirza, M. M., West, N., Karabiyik, U., Rogers, M. K., Mukherjee, T., et al. (2022). Investigating wearable fitness applications: Data privacy and digital forensics analysis on android. *Appl. Sci.* 12 (19), 9747. doi:10.3390/app12199747

Infosec Resources (2021). Smart toys and their cybersecurity risks: Are our toys becoming a sci-fi nightmare? [updated 2021]. Available at: https://resources.infosecinstitute.com/topic/smart-toys-and-their-cybersecurity-risks-are-our-toys-becoming-a-sci-fi-nightmare/ ([online].

Kebande, V. R., PhathutshedzoMudauVenter, P. R. A. I. H. S., Kwang Raymond Choo, K., and Choo, K. K. R. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Sci. Int. Rep.* 2, 100117. doi:10.1016/j.fsir.2020.100117

Khanji, S., Jabir, R., Iqbal, F., and Marrington, A. (2016). "Forensic analysis of Xbox one and playstation 4 gaming consoles," in 2016 IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, UAE, December 4-7, 2016 (IEEE), 1–6.

Loomis, M. E. (2019). *Wearable device forensics*. Tulsa: The University of Tulsa.

MacDermott, A., Stephen, L., Iqbal, F., Idowu, I., and Shah, B. (2019b). "Forensic analysis of wearable devices: Fitbit, Garmin and HETP watches," in 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, 24 to 26 June 2019 (IEEE), 1–6.

MacDermott, Á., Kendrick, P., Idowu, I., Ashall, M., and Shi, Q. (2019a). "Securing things in the healthcare internet of things," in 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17-21 June 2019 (IEEE), 1–6.

Maria Jones, G., and Godfrey Winster, S. (2018). Forensics analysis on smart phones using mobile forensics tools. *Int. J. Comput. Intell. Res.* 13 (8), 1859–1869.

Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* 10 (7), 1497–1516. doi:10.1016/j.adhoc.2012.02.016

Nelson, B., Phillips, A., and Steuart, C. (2014). *Guide to computer forensics and investigations*. Massachusetts, United States: Cengage Learning.

Nik Zulkipli, N. H., Alenezi, A., Wills, B., and Gary, B. (2017). "IoT forensic: Bridging the challenges in digital forensic and the internet of things," in Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, London, United Kingdom, December 20-22, 2017. [online].

Perumal, T., Sulaiman, M. N., and Leong, C. Y. (2015). "Internet of Things (IoT) enabled water monitoring system," in 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE). doi:10.1109/gcce.2015.7398710

Pessolano, G., Read, H. O. L., Sutherland, I., and Xynos, K. (2019). Forensic analysis of the nintendo 3ds nand. *Digit. Investig.* 29, S61–S70. doi:10.1016/j.diin.2019.04.015

Rath, S., Das, T., Astaburuaga, I., and Sengupta, S. (2023). Less is more: Deep learning framework for digital forensics in resource-constrained environments. *IEEE Xplore*. [online]. doi:10.1109/ISDFS58141.2023.10131803

Tamma, L. N. D., and Ahamad, S. S. (2018). A novel chaotic hash-based attribute-based encryption and decryption on cloud computing. *Int. J. Electron. Secur. Digit. Forensics.* 10 (1), 1. doi:10.1504/ijesdf.2018.089203

Yankson, B., Iqbal, F., and Hung, P. C. K. (2020). "4P based forensics investigation framework for smart connected toys," in Proceedings of the 15th International Conference on Availability, Reliability and Security, Ireland, August 25 - 28, 2020.

Zhang, Y., and Gao, F. (2019). Forensic analysis of Xbox one. *IOP Conf. Ser. Earth Environ. Sci.* 252, 042097. doi:10.1088/1755-1315/252/4/042097